Dr.WEB®
с 1992 года

DWCERT-070-5

Защита от спама и фишинга

Dr.WEB®
с 1992 года

План курса

Дополнительная информация

Просветительский проект	Нерекомендуемые сайты
«Антивирусная правДА!»	Рубрики «Чисто почта» и «На удочке», а также другие выпуски с хэштегами #спам и #фишинг
Тесты ВебIQметра	Facebook. Вход со двора Вокруг света, или Опасная география Всего лишь один из верных способов мгновенно получить троянца Жизнь в эпоху спама Игра слов, или Время рыбалки Именем закона, или Последняя ошибка хакера Как потерять свободу, или Основы ботоведения Кошки-мышки, или Время рыбалки – 2 Песочные часы еще идут, или На что мы тратим жизнь Почтальон Печкин меняет профессию Психологическая удочка, или Ваши действия СМС-спам – это больше, чем просто СМС
Полезные советы	Фишинг. Советы по безопасности
Видео	Настройка Родительского контроля
Часто задаваемые вопросы	Антиспам Dr.Web

Вступление

Представить себе современную жизнь без использования электронной почты, регистрации на многочисленных ресурсах, подтверждения различных соглашений на страницах Интернета, конечно, можно. Но без возможностей современного цифрового мира жить станет существенно труднее. Поэтому мы общаемся, покупаем товары и услуги, отправляем и получаем документы, подписываемся на рассылки, заводим страницы в социальных сетях и рассказываем там о себе...

К сожалению, не все сайты, на которых мы оставляем свою информацию, являются добропорядочными. Далеко не все они в достаточной мере защищены от хакеров – большинство сайтов так или иначе уязвимы. А результатом уязвимости станет утечка ваших контактных данных.

Если компьютер или устройство заразит троянец, первым делом он просканирует его в поисках списка контактов. После чего рано или поздно у вас в почтовом ящике появится некое письмо, открытие которого может привести к потере ваших денег или денег ваших знакомых и родственников.

Существенную часть почтового трафика составляет спам — массово разосланные сообщения, обычно с рекламным содержанием, которые вы не выражали желания получать.

Спам не так безобиден, как кажется. Несмотря на то, что о нем знают все, кто так или иначе пользуется средствами электронных коммуникаций, количество пострадавших от действий мошенников, использующих спам, не сокращается. Заражение локальной сети компании вследствие того, что было открыто некое вложение или сотрудник перешел по ссылке из спам-письма, – достаточно частый случай. Такой метод заражения используется как в целевых атаках на конкретные компании, так и в случае использования банковских троянцев, направленных на кражу средств из систем ДБО.

К сожалению, невозможно ни запретить сотрудникам открывать подозрительные письма и/или автоматически на них отвечать, ни гарантировать отсутствие уязвимостей в системе безопасности компании. По оценке экспертов, наиболее эффективными мерами противодействия является обучение сотрудников и особенно – тренинги для них.

Участники рынка спам-рассылок

Спамерство – это теневой бизнес, а значит, спамеры занимаются незаконной деятельностью.

На рынке спам-рассылок есть несколько участников.

1. **Заказчик спамерских услуг.** Это может быть как легальный, так и теневой бизнес. Кем бы ни был заказчик, он – участник незаконного бизнеса и главная движущая сила этого рынка (а вовсе не спамер), поскольку порождает спрос на услуги спамеров, на который находится и предложение.
2. **Спамер,** он же распространитель рассылок, передает информацию по сети Интернет и берет за это вознаграждение от Заказчика. Деятельность по передаче информации по сети Интернет регулируется в России путем выдачи лицензии на «Услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации». Без такой лицензии для спамера наступает следующая ответственность:

- Кодекс об административных правонарушениях, **статья 14.1.** Осуществление предпринимательской деятельности без государственной регистрации или без специального разрешения (лицензии) влечет наложение **административного штрафа в размере от пятисот до пятидесяти тысяч рублей**.
- Уголовный кодекс РФ, **статья 171.** Незаконное предпринимательство. Осуществление предпринимательской деятельности без регистрации или без лицензии в случаях, когда такая лицензия обязательна, если это деяние причинило крупный ущерб гражданам, организациям или государству либо сопряжено с извлечением дохода в крупном размере (1 500 000 руб.), – наказывается **штрафом в размере до трехсот тысяч рублей** или в размере заработной платы или иного дохода осужденного за период до двух лет, либо **обязательными работами на срок до четырехсот восьмидесяти часов, либо арестом на срок до шести месяцев**.

  Но вряд ли рекламодатели при обращении к спамерам просят показать лицензию на этот вид деятельности, поскольку в большинстве случаев знают, что заказывают незаконную услугу.

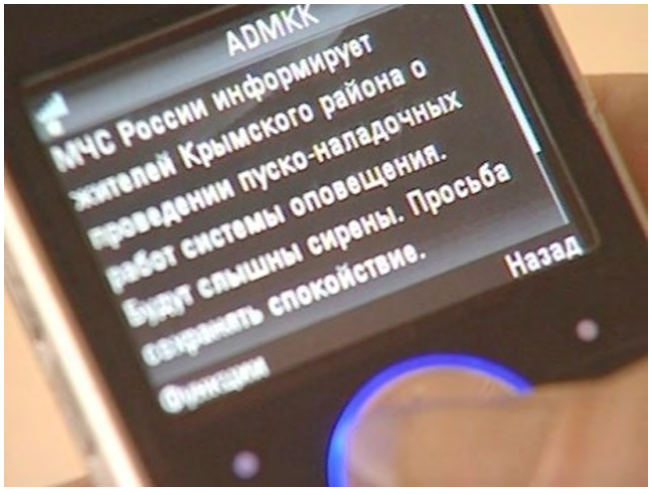
3. **Получатели спама**
   Получатели рассылок становятся невольными участниками этого рынка. Они теряют деньги уже потому, что платят за время доступа к Интернету или за трафик, а также за дисковое пространство, на котором находится почтовый ящик, и за время работников, вынужденных сортировать рабочую переписку и спам. Несут денежные потери и провайдеры услуг.
4. **Разработчики** специального программного обеспечения для рассылки спама и сбора адресов электронной почты пользователей (так называемые «харвестеры») и вирусописатели.

Транспорт для спама

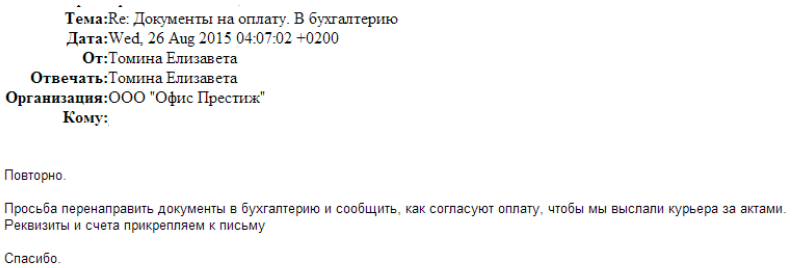
Любую информацию, в том числе незапрошенную — спам, — можно донести до целевой аудитории (в контексте этого курса — жертвам спама) огромным количеством способов. Для транспортировки нежелательных писем спамеры используют все современные возможности.

- **Почтовые сообщения**
  Это первозданный классический спам. Часто e-mail-рассылка производится для заражения компьютера получателя спама или с целью выманивания его данных для последующей их перепродажи или кражи денежных средств (фишинговые письма).
- **СМС**
  Такой вид спама получил название «смишинг» (англ. SMiShing — от SMS и fishing). Это технология интернет-мошенничества, разновидность фишинга. Преступники рассылают СМС-сообщения, содержащие ссылку на фишинговый сайт. Жертва сама заходит на него и вводит свои личные данные, тем самым передавая их злоумышленникам.

Не все подобные сообщения являются спамом. Например, не считаются спамом уведомления соответствующих органов о приближающихся стихийных бедствиях, массовой эвакуации или мобилизации граждан и т. п.



- **Телефон**
  Незапрошенные обзвоны (спам по телефону) назвали «вишингом» (англ. vishing – от voice (голос) и fishing). Это разновидность фишинга – технология интернет-мошенничества, использующая для кражи личных конфиденциальных данных несколько сценариев атаки.
- Обзвоны при помощи автонабирателей (war diallers) и возможностей интернет-телефонии (VoIP). Потенциальным жертвам звонят якобы от имени легальных организаций и просят ввести с телефонного устройства пароли, PIN-коды и другую личную информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы и в других противоправных действиях.
- Рассылка фишинговых писем с просьбой перезвонить по телефону и решить проблему (например, с неожиданной для вас блокировкой банковской карты). Позвонив на указанный номер, пользователь заслушивает сообщение автоответчика с инструкциями о необходимости ввести номер своего счета и PIN-код. Обзвоны компаний и частных лиц с целью заставить человека открыть зараженное вложение к ранее отправленному e-mail-сообщению или переслать его другому лицу (как правило, бухгалтеру или руководителю компании). Такие атаки, как правило – таргетированные.

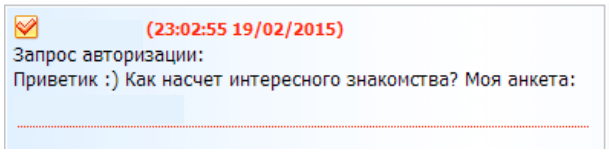

Тема: Re: Документы на оплату. В бухгалтерию
Дата: Wed, 26 Aug 2015 04:07:02 +0200
От: Томина Елизавета
Отвечать: Томина Елизавета
Организация: ООО "Офис Престиж"
Кому:

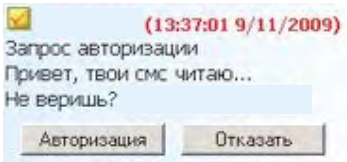
Повторно.

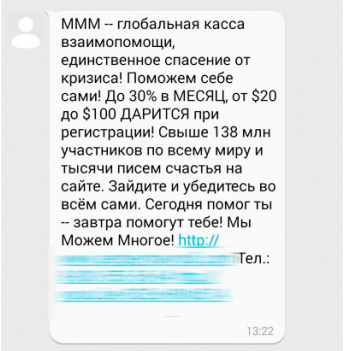
Просьба перенаправить документы в бухгалтерию и сообщить, как согласуют оплату, чтобы мы выслали курьера за актами.
Реквизиты и счета прикрепляем к письму

Спасибо.

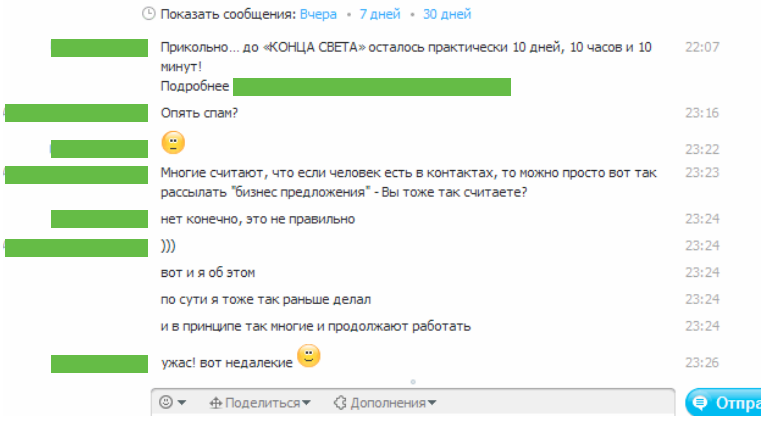
- **Системы мгновенного обмена сообщениями — мессенджеры** (например, ICQ). Этот вид спама называется SPIM (англ. Spam over IM или SPam + Instant Messenger);


(23:02:55 19/02/2015)
Запрос авторизации:
Приветик :) Как насчет интересного знакомства? Моя анкета:


(13:37:01 9/11/2009)
Запрос авторизации
Привет, твои смс читаю...
Не веришь?
Авторизация
Отказать



- **Программы для IP-телефонии (например, Skype).** Спам, поступающий через этот канал, называется SPIT (англ. Spam over IT, Spam over IP Telephony).



В обоих вышеуказанных случаях спам распространяется через рекламные сообщения от имени ваших друзей (в случае взлома их аккаунта) или через запросы от пока еще не известных вам людей, якобы мечтающих подружиться с вами.

- **Социальные сети и сайты знакомств.** Совершенно особую группу представляет френдоспам (англ. friend — друг). По этому каналу спам распространяется через приглашения в группы/сообщества, заявки на «дружбу», «стены»/«гостевые книги». Заинтересовавшийся приглашением человек присоединяется к рекламируемой группе или просто посещает страницу, указанную в спам-сообщении.
- **Спам на форумах, сайтах новостных агентств и других СМИ** или в комментариях — явление, пока не имеющее собственного названия. Спам распространяется под видом комментариев (постов) рекламного характера, часто с извинениями за якобы нечаянную рекламу.
- **Доски коммерческих и частных объявлений.** Спам-объявления, замаскированные под коммерческие, размещаются спамерами во всех доступных разделах того или иного сайта, чтобы увеличить релевантность сообщения в индексируемых поисковыми механизмами страницах. В одном объявлении могут быть десятки ссылок, ведущих на разные страницы.
- **Сайты и блоги** — интернет-ресурсы, созданные для распространения спама и маскирующиеся под блоги, окрестили сплогами (спам-блогами) (англ. splog от spam blog — спам-блог). По этому каналу спам распространяется в целях раскрутки товара или сайта. Сообщения на нем чаще всего генерируются путем RSS-каналов с других сайтов (т. е. тексты не аутентичные, а заимствованные, автоматически подгружаемые из источника сразу множеством ресурсов). Используется на таких площадках и френдоспам — когда пользователей (последователей блогера) автоматически вносят в список «друзей» без знакомства с их персональными страницами, как правило, с целью искусственного повышения рейтинга сплога путем получения «взаимной» дружбы либо для привлечения внимания к сетевой рекламе, размещенной в блоге спамера.

Внимание! *Данный перечень не означает, что иных видов спама не существует. Спамеры быстро осваивают любые становящиеся популярными средства электронной связи.*

Сколько времени мы теряем из-за спама?

Человеку требуется от 4 до 7 секунд на то, чтобы выявить рекламный характер письма и удалить спам-сообщение.

Таким образом, на удаление 100 спам-писем мы тратим от 6 до 11 минут в день.

Чтобы заново сконцентрироваться на работе, если внимание отвлечено на чистку ящика от спама, в среднем необходимо до 15 минут!

А теперь давайте посчитаем, сколько всего времени отнимает спам. Напоминаем: все это время человек не работает. Допустим, вы занимаетесь чисткой ящика три раза в день. В таком случае вы дарите спамерам почти час своей жизни!

Потери несет не только получатель спама – нежелательная почта приводит и к другим неприятным последствиям:

- Потери предприятия в заработной плате сотрудников, т. к. в момент чистки спама люди не работают – чем выше служебное положение сотрудников, тем больше теряет предприятие на оплате труда.
- Потери производительности труда сотрудников – это ведет к снижению эффективности работы предприятия.
- Потери в эффективности работы предприятия, что может привести к его закрытию (банкротству).

Использование антиспама позволяет сократить потери ценных минут на 95-98%!

Кто они – покупатели ваших персональных и аутентификационных данных, а также другой конфиденциальной информации?

Любые персональные или конфиденциальные данные – это товар, который на черном рынке стоит денег. Их можно продать, и на них есть спрос у нескольких категорий покупателей.

1. Спамеры

Что нужно спамерам и мошенникам, пользующимся их услугами? Ваши контактные данные. Для чего? С целью рассылки спама.

- **Ваш e-mail** – на него можно отправить спам-письмо, в том числе с вредоносной ссылкой. Даже если вы просто перейдете на какой-то сайт из спам-письма и увидите размещенную там рекламу, спамер уже на вас заработает – за вас ему заплатит рекламодатель. Вы потеряете как минимум время или же купитесь на рекламу недоброкачественного или бесполезного товара и заплатите за него рекламодателю. Так что без потерь от спамера вам не уйти.
- **Номер вашего мобильного телефона** – на него можно отправить СМС-рекламу, в которой тоже может быть вредоносная ссылка.
- **Адреса в вашей книге контактов** (e-mail, телефоны, логины к Skype, Viber, WhatsApp) – с этих адресов можно организовать массовую рассылку спама по всем контактам или разослать троянца.

2. Фишеры

А вот фишеров и других мошенников интересует совсем иная информация.

- Ваша фамилия и должность – поскольку персонализированный спам на вес золота. А еще, обладая этими данными, можно обойти секретаря или установить более доверительные отношения с адресатом незапрошенного письма – вы ведь не помните всех людей, с которыми когда-либо общались.
- Паспортные данные.
- Данные кредитных карт.
- Номер автомобиля и свидетельства о его регистрации.
- Данные о компании.
- Логины и пароли к онлайн-банкингу.

Работая в тесной связке со спамерами, фишеры сначала рассылают с их помощью фишинговые письма – преимущественно со ссылками якобы на сайты банков, платежных систем, интернет-магазинов и т. д. Если вы перейдете на такой сайт, фишер выудит у вас нужную ему информацию. Причем отдадите вы свои данные по собственной воле, введя их в предложенную форму, думая, что находитесь на настоящем сайте организации.

Более миллиона долларов (или 8 млн шведских крон) украли злоумышленники с помощью фишинговых писем, разосланных клиентам банка Nordea. Жертвы получили письма от имени администрации, в которых рекомендовалось установить специальную программу, якобы защищающую клиентов от спама и интернет-атак. В результате 250 человек установили необходимое злоумышленникам приложение и потеряли свои деньги.
Источник: http://www.windxp.com.ru/nws/article43.htm

3. Вишеры

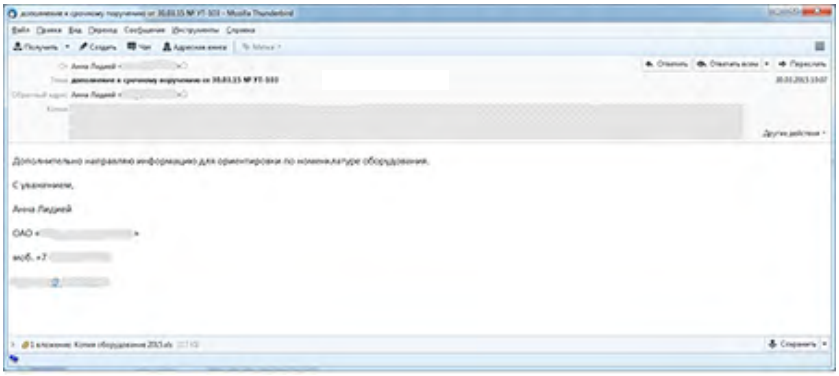
Подобно фишерам, эти мошенники собирают персональные данные (Ф.И.О. и должности людей, а также номера их телефонов), но используют их не для рассылки писем, а для организации обзвонов – зачастую с целью внедрения троянской программы.

Сценарий работы вишера
Мошенник*: Здравствуйте, я Иванов Сергей Юрьевич из налоговой инспекции, мы решили провести у вас выездную проверку 20 августа.*
Сотрудник*: Но у нас уже была проверка 3 месяца назад.*
М*: Это внеочередная. Продиктуйте адрес электронной почты, отправлю вам информацию, какие документы нужно подготовить и предоставить. Не вешайте трубку, сейчас отправлю вам письмо.*
М*: Пришло письмо?*
С*: Да.*
М*: Там ссылка в конце, жмите.*
С*: Нажала, ничего не происходит.*
М*: Наверное, у вас не установлена какая-то программа, перешлите письмо коллегам, пусть они попробуют открыть. Если будут вопросы, звоните, телефон на нашем сайте. Всего доброго.*
По мотивам http://www.yaplakal.com/forum7/topic1171600.html

4. Организаторы заказных атак, акций по дискредитации конкретных коммерческих компаний или политических акций

Им позарез нужны контакты владельцев ПК и мобильных устройств – клиентов или сотрудников соответствующих организаций. На основе этих данных организуются адресные рассылки. Большинство известных целевых или APT-атак начинались с заражения компьютера интересующего преступников человека путем рассылки специально сформированных сообщений.

В начале апреля 2015 года специалисты компании «Доктор Веб» зафиксировали целенаправленную почтовую рассылку по личным и служебным адресам сотрудников ряда российских оборонных предприятий, с помощью которой злоумышленники распространяли опасного троянца.

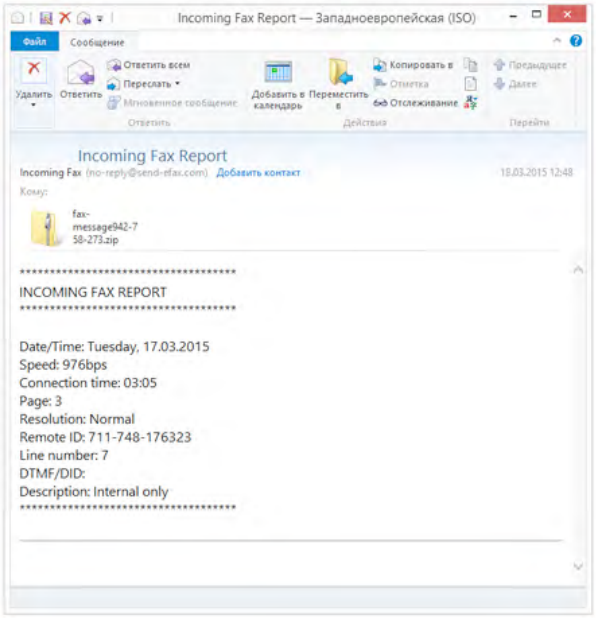


Вредоносная программа, получившая наименование **BackDoor.Hser.1**, *способна по команде передать на удаленный сервер список активных процессов на зараженном ПК, загрузить и запустить другое вредоносное приложение, а также открыть командную консоль и выполнить перенаправление ввода-вывода на принадлежащий киберпреступникам сервер, благодаря чему злоумышленники получают возможность дистанционного управления инфицированным компьютером.*
http://news.drweb.com/show/?c=5&i=9420&lng=ru

5. Вирусописатели

Спам – это не только рекламные e-mail-рассылки, но и мощный инструмент распространения вредоносных программ и ссылок на сайты, где пользователя ожидает заражение.

- Наиболее опасных на сегодняшний день троянцев-шифровальщиков злоумышленники распространяют в том числе и с использованием массовых почтовых рассылок. Так, в апреле 2015 года вирусописатели активно рассылали письма с заголовком «Incoming Fax Report» от имени службы по передаче факсов через Интернет. В приложении к письму под видом факсимильного сообщения содержался ZIP-архив, внутри которого располагался вредоносный SCR-файл, детектируемый антивирусным ПО Dr.Web как Trojan.DownLoader11.32458.



При попытке открытия вложения вредоносная программа **Trojan.DownLoader11.32458** распаковывает и запускает на атакуемом компьютере троянца-энкодера **Trojan.Encoder.514**, шифрующего хранящиеся на диске пользовательские файлы и требующего выкуп за их расшифровку.

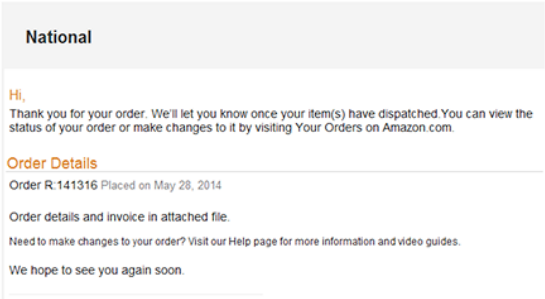
По статистике компании «Доктор Веб», расшифровка поврежденных троянцами-шифровальщиками файлов возможна только в 10% случаев.

Узнайте больше об опасности шифровальщиков и возможностях «Доктор Веб» по расшифровке на странице проекта «Трояницы-шифровальщики – угроза №1».

- 10 августа 2015 года злоумышленники организовали рассылку от имени Роскомнадзора с «требованием» осуществить блокировку обрабатываемых персональных данных ввиду нарушения требований Федерального закона № 152-ФЗ «О персональных данных». При этом никаких конкретных данных о нарушении обработки не приводилось, но в письме упоминалось «Постановление Роскомнадзора № 319 от 10.08.2015 г.», а в само письмо был вложен архив в формате RAR, который предлагалось открыть с использованием пароля roscomnadzor. Открытие файла могло повлечь повреждение информационной системы.

Источник: http://25.rkn.gov.ru/news/news83753.htm

- Троянец-загрузчик **BackDoor.Tishop.122**, который сами вирусописатели называют Smoke Loader, распространялся в том числе путем массовых почтовых рассылок. Назначение данного троянца заключается в загрузке на инфицированный компьютер и запуске других вредоносных приложений. В 2014 году злоумышленники часто рассылали **BackDoor.Tishop.122** под видом писем от различных популярных интернет-ресурсов. Так, в июне он массово распространялся от имени интернет-портала Amazon с информацией о поступившем заказе.


National

Hi,
Thank you for your order. We'll let you know once your item(s) have dispatched.You can view the status of your order or make changes to it by visiting Your Orders on Amazon.com.

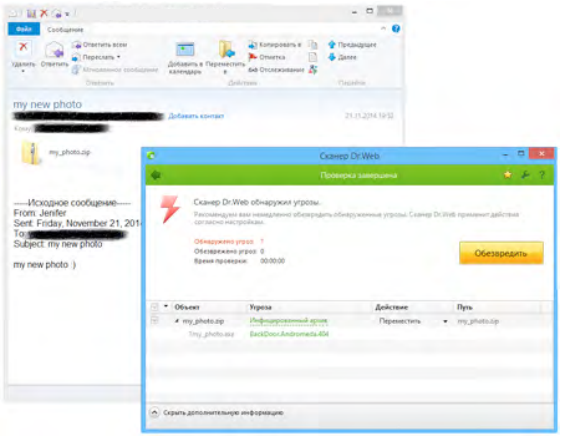
Order Details
Order R:141316 Placed on May 28, 2014

Order details and invoice in attached file.

Need to make changes to your order? Visit our Help page for more information and video guides.

We hope to see you again soon.

- Бэкдор **BackDoor.Andromeda.404** способен по команде злоумышленников загружать на инфицированный компьютер другие опасные приложения. В ноябре 2014 киберпреступники активно рассылали этого троянца по электронной почте, в частности, в сообщениях с темой «my new photo», при этом сама вредоносная программа скрывалась в приложенном к письму архиве my_photo.zip.



Вирусописатели распространяют вредоносные программы, используя похищенные из вашего компьютера персональные данные,— например, имена и почтовые адреса ваших знакомых. Они формируют персонифицированные письма от лица реально существующих людей, обращаясь к адресату по имени. Жертва такого обмана сама открывает вредоносное вложение к письму, потому что получено оно якобы от знакомого ей человека.

*По оценкам экспертов, заражению вирусом **VBS.LoveLetter**, известным также как **I love you**, подверглось от 30 до 80% компьютерных сетей в разных странах мира. **VBS.LoveLetter** распространялся, используя данные адресных книг. Количество зараженных компьютеров на третий день расследования оценивалось в 3 миллиона. В итоге убытки от эпидемии в США оценили в 10 миллиардов долларов.*

Похищенные у вас доступы к различным сервисам — например, пароли и логины к банковским счетам, PIN-коды — вирусописатели используют для атак с целью хищения денежных средств.

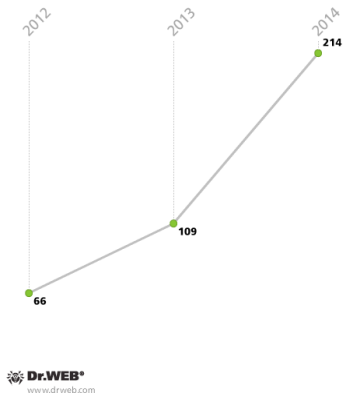
- Для распространения т.н. троянцев-банкеров среди жителей Южной Кореи в апреле 2015 года злоумышленники применяли рассылку нежелательных СМС со ссылкой на загрузку вредоносного приложения. Специалисты компании «Доктор Веб» зафиксировали более 80 подобных спам-кампаний. Киберпреступники использовали в качестве темы нежелательных сообщений приглашения на свадьбу, уведомления от судебных, налоговых и других правовых органов. http://news.drweb.com/show/?c=5&i=9422&lng=ru

6. Шпионы (спецслужбы, конкуренты)

Следящие за вами люди благодаря похищенным у вас аутентификационным данным или путем внедрения на ваш компьютер или смартфон троянца-шпиона могут читать вашу переписку, вести записи ваших разговоров, загружать на удаленный сервер ваши фотографии. Они также покупают или похищают персональные данные тех, с кем вы общаетесь, в том числе для того, чтобы найти ваши уязвимые места.

Есть троянцы-шпионы и для мобильных устройств. Например, **Android.Spy.130.origin** передает злоумышленникам сведения об СМС-переписке, совершенных звонках, текущих GPS-координатах, а также способен незаметно выполнить звонок на заданный номер, превращая зараженный смартфон или планшет в прослушивающее устройство.

График роста количества записей троянцев семейства Android.Spy в вирусной базе Dr.Web



7. Шантажисты

Они выкупают данные, украденные с зараженных троянцами компьютеров, чтобы шантажировать вас или ваших знакомых с целью получения выкупа или выполнения вами определенных действий.

- Сотрудники отдела «К» ГУВД по Иркутской области пресекли незаконную деятельность неработающего 26-летнего молодого человека, который при помощи вредоносной программы получал доступ к конфиденциальным базам организаций и вымогал у них деньги за нераспространение информации конкурентам.
  Источник: http://www.baikal-daily.ru/news/20/8485/?sphrase_id=2222430
- Добычей хакеров стали откровенные снимки, которые телеведущая Ксения Бородина делала на свой телефон, и ее личная переписка в социальных сетях и чатах. С Бородиной потребовали миллион рублей.
  Источник: http://moscvichka.ru/moscvichka/2014/07/02/hakeri-vimogali-million-rublej-u-ksenii-borodinoj-za-ee-snimki-v-golom-vide-11095.html
- Хакеры взламывали электронную почту и других телезвед. За рубежом интимными фотографиями шантажировали Скарлетт Йохансон и Кристину Агилеру. Обидчик последней получил 10 лет тюрьмы.
  Источник: http://www.mk.ru/culture/2012/12/18/788660-haker-ukravshiy-intimnyie-foto-skarlett-yohansson-poluchil-10-let-tyurmyi.html

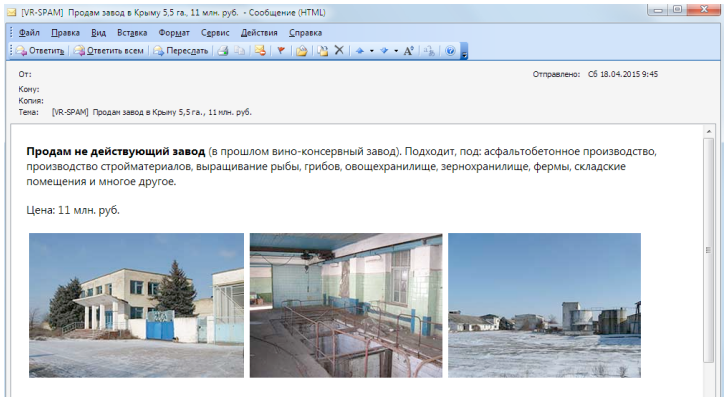
Как спам работает на рекламодателей

Целью любого спам-письма является **побуждение его получателя к действию** – к покупке рекламируемого товара, переходу на вредоносный сайт или открытию вредоносного вложения и заражения компьютера. Все зависит от **заказчика** рассылки и преследуемых им **целей**.

К сожалению, многие предприниматели относятся к спаму как к доступному инструменту для рекламы своих товаров или услуг. Как правило, заказчики спама активно отрицают его использование. Это свидетельствует о том, что компании, прибегающие к спам-рекламе, хорошо осведомлены о негативном отношении пользователей к этому явлению, равно как и о незаконности этого «бизнеса». Поскольку спам используют, как правило, маленькие компании, их не беспокоит вопрос репутации и создания положительного имиджа.

Цели рекламодателей, прибегающих к услугам спамеров

- Продвижение вполне законных товаров и услуг при желании сэкономить на рекламе.


[VR-SPAM] Продам завод в Крыму 5,5 га., 11 млн. руб. - Сообщение (HTML)

Файл Правка Вид Вставка Формат Сервис Действия Справка

Ответить | Ответить всем | Переслать

От:
Отправлено: Сб 18.04.2015 9:45
Кому:
Копия:
Тема: [VR-SPAM] Продам завод в Крыму 5,5 га., 11 млн. руб.

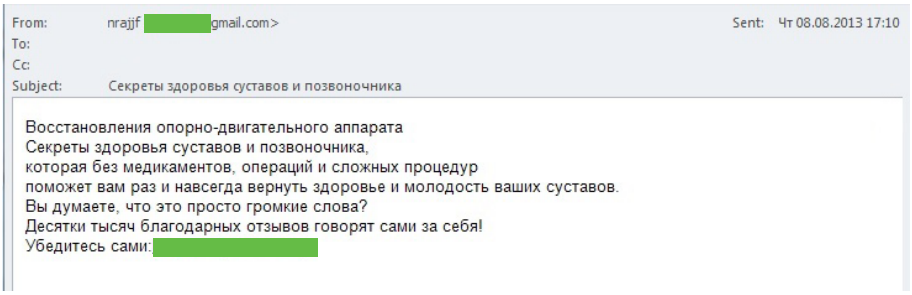
Продам не действующий завод (в прошлом вино-консервный завод). Подходит, под: асфальтобетонное производство, производство стройматериалов, выращивание рыбы, грибов, овощехранилище, зернохранилище, фермы, складские помещения и многое другое.

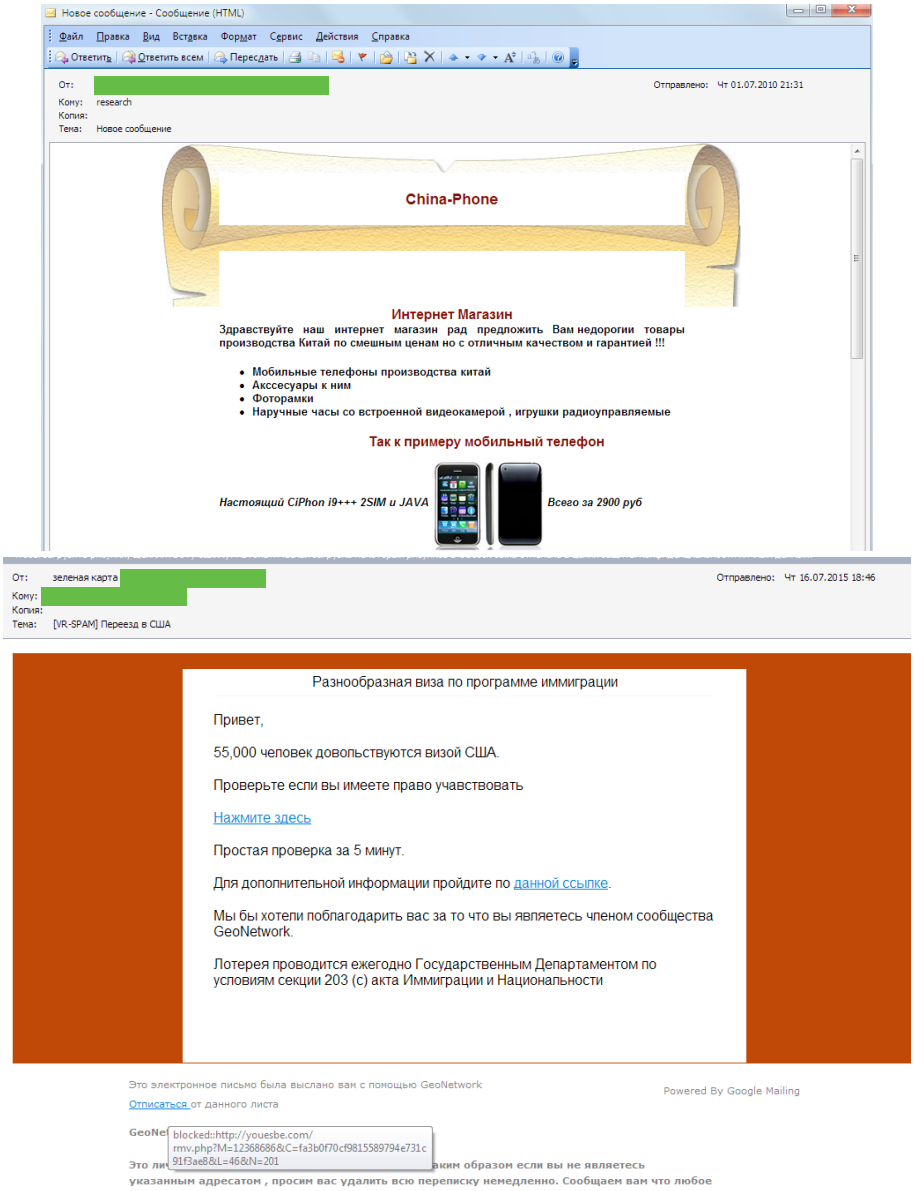
Цена: 11 млн. руб.

Это единственный «безобидный» вид спама, не угрожающий пользователям, но и он является незаконным.

> ***Пункт 1 статьи 18 Федерального закона № 38-ФЗ «О рекламе» гласит:***
> *1. Распространение рекламы по сетям электросвязи, в том числе посредством использования телефонной, факсимильной, подвижной радиотелефонной связи, допускается* ***только при условии предварительного согласия абонента или адресата на получение рекламы****. При этом реклама признается распространенной без предварительного согласия абонента или адресата, если рекламораспространитель не докажет, что такое согласие было получено. Рекламораспространитель обязан немедленно прекратить распространение рекламы в адрес лица, обратившегося к нему с таким требованием.*
> *Наказанием за нарушение запрета на распространение рекламных сообщений без наличия предварительного согласия получателей является штраф, предусмотренный п. 1 ст. 14.3 Кодекса Российской Федерации об административных правонарушениях:*
> *«1. Нарушение рекламодателем, рекламопроизводителем или рекламораспространителем законодательства о рекламе, за исключением случаев, предусмотренных частями 2 – 6 настоящей статьи, частью 4 статьи 14.3.1, статьями 14.37, 14.38, 19.31 настоящего Кодекса, –*
> *влечет наложение* ***административного штрафа на граждан в размере от двух тысяч до двух тысяч пятисот рублей; на должностных лиц – от четырех тысяч до двадцати тысяч рублей; на юридических лиц – от ста тысяч до пятисот тысяч рублей****».*

- **Продвижение сомнительных, бесполезных или незаконных товаров и услуг, которые невозможно рекламировать легальными способами.** Сюда относятся порнография, подделки (например, швейцарских часов, именуемые также «репликами»), лекарственные средства, запрещенные к распространению, сомнительные БАДы, бесполезные методики и тренинги и т. д. Никто не гарантирует, что подобная реклама не является мошеннической, не говоря уже об отсутствии гарантии качества этих товаров и услуг.





Статья 171 Уголовного кодекса РФ «Незаконное предпринимательство» гласит:

1. Осуществление предпринимательской деятельности без регистрации или без лицензии в случаях, когда такая лицензия обязательна, если это деяние причинило крупный ущерб гражданам, организациям или государству либо сопряжено с извлечением дохода в крупном размере, – наказывается ***штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо арестом на срок до шести месяцев****.*

Если в спаме рекламируется порнография и/или проституция, такие действия подпадают под статьи 241, 242 и 242.1 Уголовного кодекса РФ:

Статья 241. Организация занятия проституцией
1. Деяния, направленные на организацию занятия проституцией другими лицами, а равно содержание притонов для занятия проституцией или систематическое предоставление помещений для занятия проституцией –
наказываются ***штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.***

Статья 242. Незаконные изготовление и оборот порнографических материалов или предметов
1. Незаконные изготовление и (или) перемещение через Государственную границу Российской Федерации в целях распространения, публичной демонстрации или рекламирования либо распространение, публичная демонстрация или рекламирование порнографических материалов или предметов –
наказываются ***штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.***

Статья 242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних
1. Изготовление, приобретение, хранение и (или) перемещение через Государственную границу Российской Федерации в целях распространения, публичной демонстрации или рекламирования либо распространение, публичная демонстрация или рекламирование материалов или предметов с порнографическими изображениями несовершеннолетних –
наказываются ***лишением свободы на срок от двух до восьми лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пятнадцати лет либо без такового.***

Если спам-сообщение преследует цель получения от пользователя денег путем обмана или злоупотребления доверием – к примеру, содержит рекламу поддельных товаров или услуг, выдающихся за оригинальные («айфоны» за 3000 рублей, платное предоставление информации о генеалогическом дереве и т. д.), то в зависимости от содержания письма и способа его распространения такие действия могут подпадать под статьи 159 и 159.6 Уголовного кодекса РФ.

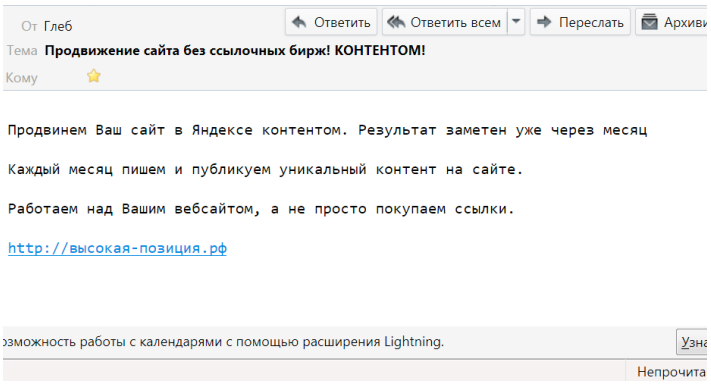
Статья 159. Мошенничество

1. Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, – наказываются ***штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет.***

Статья 159.6. Мошенничество в сфере компьютерной информации

1. Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, – наказываются ***штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.***

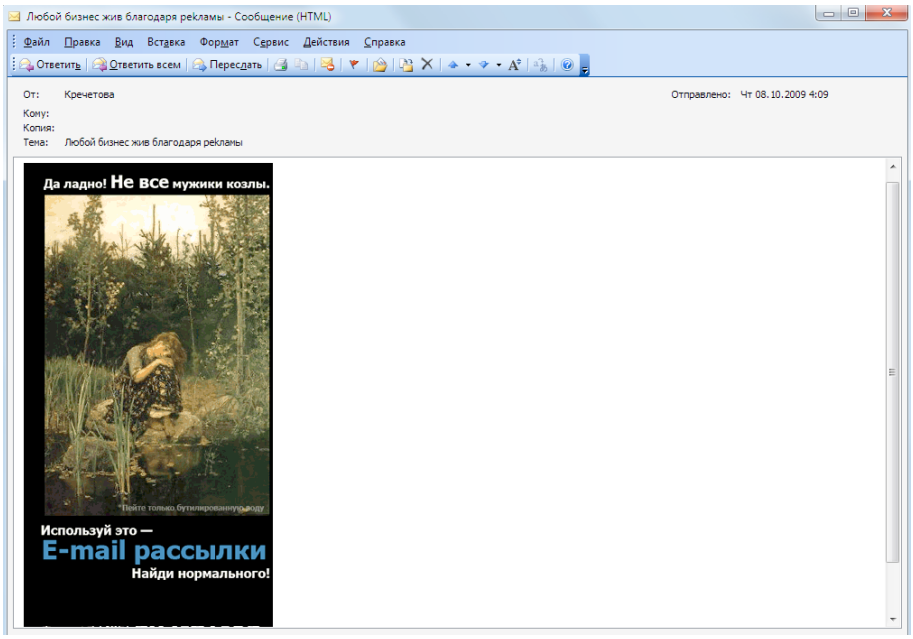
- **«Раскрутка» сайта или партнерской программы**



От этого вида деятельности спамеры и их клиенты-рекламодатели получают выгоду сразу по двум направлениям:

1. Каждый сайт, на который ведет ссылка из такого спам-письма, содержит рекламу. Цель спамера — заставить вас увидеть эту рекламу, то есть зайти на сайт. А каждое посещение сайта по спамерской ссылке, в свою очередь, оплачивается рекламодателем.
2. Количество заходов на продвигаемый спамерами сайт влияет на индексы его цитируемости в поисковиках (в частности, в Google PR или ТИц Яндекса) и перемещает ссылку на него на более высокие строчки результатов выдачи поискового запроса.

- **Реклама спамерских услуг**
  Спамеры тоже ищут клиентов и рекламируют свою деятельность при помощи... спама! Стоит ли говорить, что и такая деятельность является незаконной.



Как спам работает на мошенников

Спам – это не только рассылка безобидной рекламы. Он используется преступниками для массового тиражирования мошеннической информации или ссылок, ведущих на мошеннические сайты. Для распространения незаконной информации мошенники используют незаконные средства – «распространение рекламы по сетям электросвязи без предварительного согласия абонента или адресата на получение рекламы» (ст. 18 ФЗ «О рекламе») – т. е. спам.

1. Использование спама для рассылки мошеннической информации

«Нигерийские письма» (они же Nigerian letter и 419 scam)
Это название давно уже стало нарицательным и обозначает письма, «посвященные» тем или иным драматическим событиям. Большинство писем подобного содержания приходило из Нигерии и других стран Африки, но на сегодняшний день события в иных точках мира (например, бегство украинского президента Януковича) также приводят к появлению «нигерийских писем».

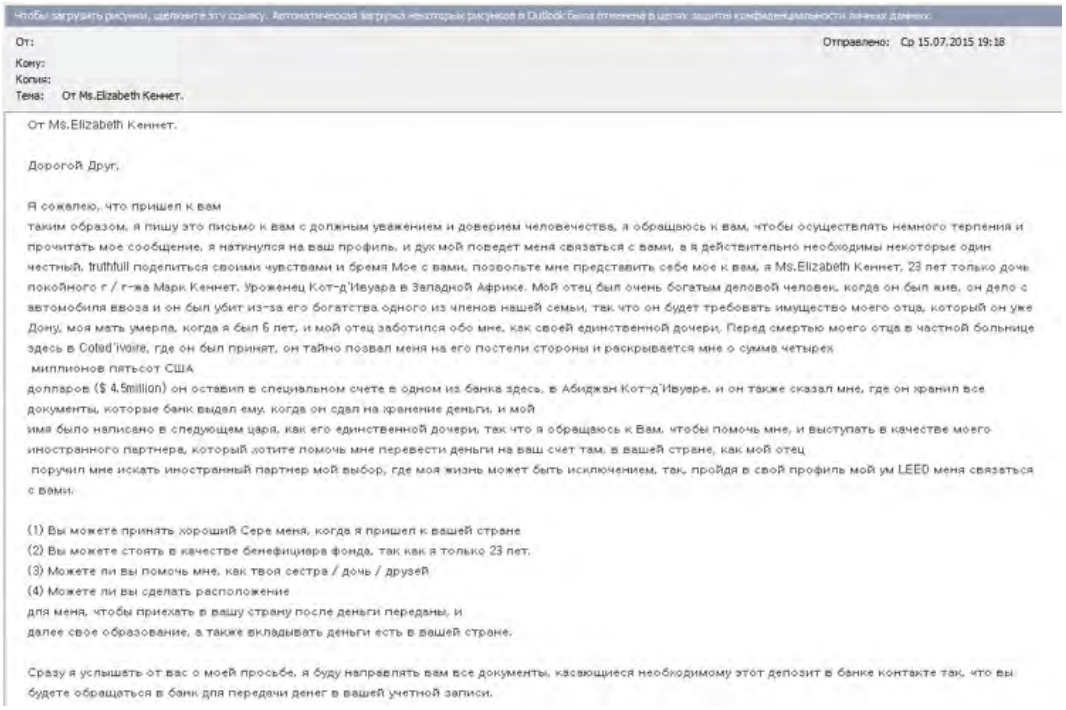
5 декабря 2012 года многие информационные агентства сообщили об авиакатастрофе в Нигерии. Разбился вертолет, на борту которого находился губернатор нигерийского штата Кадуна **Патрик Якова** (Patrick Yakowa). Все, кто был на борту, погибли. И вот как это печальное событие было использовано злоумышленниками.

От: «Death of Kaduna State Governor Nigeria, wife pleads for help.»
Тема: Re: Death of Kaduna State Governor Nigeria, wife pleads for help.
Dear Sir/Ma,
My name is Mrs Amina Elizabeth Yakowa, wife and widow of the late Governor of Kaduna State in Nigeria. My husband died in an helicopter plane crash last saturday the 15th December 2012 where he attended an important official matter. News of this is all over the whole world and so please do not see my message as oneof those internet dirty business.
Following his death, the Federal Government of Nigeria has asked me to present my bill for the sum of $15Million dollars that is due to me and my family as enshrined in the constitution of Nigeria. What i want from you is to claim the said funds for me and invest judiciously for me and my children. I shall legitimately apply for the funds and have them approved by the same Governement who asked me to forward my bill for the claim of my husband gratuity. You shall be entitled to 15% of the whole sum for your assistance in working with us.
Details of his death can be seen at the site below.
http://www.thisdaylive.com/articles/yakowa-azazi-die-in-helicopter-crash/133710/
http://www.aljazeera.com/news/africa/2012/12/20121215225147473906.html
Please respond back to me so that i could give you more details as i am giving only one week to claim the funds from the Nigerian affiliate in Denmark Bank.
Yours Faithfully,
Lizzy Yakowa
Widow of Kaduna State Governor.
http://nigerian-letters.blogspot.ru/2013/01/kaduna-yakowa.html

Типичное письмо такого типа написано с грамматическими ошибками и содержит грустную историю какого-нибудь наследника (принца, адвоката, владельца банка или бывшего госчиновника из какой-нибудь страны) с упоминанием крупной денежной суммы, которую он в силу бедности или иных проблем не может получить самостоятельно. Адресату предлагается посодействовать в решении этого вопроса, выслав некоторое количество денег – например, чтобы открыть счет на имя получателя письма (оплатить услуги адвокатов или налог на наследство). В качестве вознаграждения авторы рассылки предлагают процент от суммы в несколько миллионов долларов.

Потенциальную жертву просят прислать личные данные – имя, фамилию, адрес проживания и т. п. А при дальнейшем общении – копии документов (паспорта или водительского удостоверения). Получив эти данные, мошенники могут использовать их, например, для снятия средств с банковского счета жертвы.

Преступники используют жадность получателей таких писем. Зачастую перевод денег является поводом для продолжения общения мошенников с жертвой (у них это называется «животноведение»), в ходе которого адресата вынуждают переводить все новые и новые суммы. Обещанной в начале переписки суммы тот, разумеется, никогда не увидит.



Чтобы загрузить рисунки, щелкните эту ссылку. Автоматическая загрузка некоторых рисунков в Outlook была отменена в целях защиты конфиденциальности личных данных.

От:
Отправлено: Ср 15.07.2015 19:18
Кому:
Копия:
Тема: От Ms.Elizabeth Кеннет.

От Ms.Elizabeth Кеннет.

Дорогой Друг,

Я сожалею, что пришел к вам
таким образом, я пишу это письмо к вам с должным уважением и доверием человечества, я обращаюсь к вам, чтобы осуществлять немного терпения и прочитать мое сообщение, я наткнулся на ваш профиль, и дух мой поведет меня связаться с вами, а я действительно необходимы некоторые один честный, truthfull поделиться своими чувствами и бремя Мое с вами, позвольте мне представить себе мое к вам, я Ms.Elizabeth Кеннет, 23 лет только дочь покойного г / г-жа Марк Кеннет. Уроженец Кот-д'Ивуара в Западной Африке. Мой отец был очень богатым деловой человек, когда он был жив, он дело с автомобиля ввоза и он был убит из-за его богатства одного из членов нашей семьи, так что он будет требовать имущество моего отца, который он уже Дону, моя мать умерла, когда я был 6 лет, и мой отец заботился обо мне, как своей единственной дочери. Перед смертью моего отца в частной больнице здесь в Coted'Ivoire, где он был принят, он тайно позвал меня на его постели стороны и раскрывается мне о сумма четырех
миллионов пятьсот США
долларов ($ 4.5million) он оставил в специальном счете в одном из банка здесь, в Абиджан Кот-д'Ивуаре, и он также сказал мне, где он хранил все документы, которые банк выдал ему, когда он сдал на хранение деньги, и мой
имя было написано в следующем царя, как его единственной дочери, так что я обращаюсь к Вам, чтобы помочь мне, и выступать в качестве моего иностранного партнера, который хотите помочь мне перевести деньги на ваш счет там, в вашей стране, как мой отец
поручил мне искать иностранный партнер мой выбор, где моя жизнь может быть исключением, так, пройдя в свой профиль мой ум LEED меня связаться с вами.

(1) Вы можете принять хороший Сере меня, когда я пришел к вашей стране
(2) Вы можете стоять в качестве бенефициара фонда, так как я только 23 лет.
(3) Можете ли вы помочь мне, как твоя сестра / дочь / друзей
(4) Можете ли вы сделать расположение
для меня, чтобы приехать в вашу страну после деньги переданы, и
далее свое образование, а также вкладывать деньги есть в вашей стране.

Сразу я услышать от вас о моей просьбе, я буду направлять вам все документы, касающиеся необходимому этот депозит в банке контакте так, что вы будете обращаться в банк для передачи денег в вашей учетной записи.

Чтобы вынудить жертву совершить те или иные действия, мошенники могут предлагать огромные суммы, которые, якобы, достанутся ей совершенно задаром.

От:
Кому:
Тема: Hello

Дорогой друг!
Это письмо может быть сюрпризом для вас, потому что вы не дали мне разрешение на это и ни ты меня знаешь, но, прежде чем я расскажу о себе я хочу вас, пожалуйста, простите меня за отправку этого письма без вашего разрешения. Я пишу это письмо в уверенности полагать, что, если на то будет воля Божия для вас, чтобы помочь мне и моей семье, Всемогущий Бог благословит и вознаградит вас обильно. Мне нужен честный и достойный доверия человек, как вы доверить это огромный проект к передаче.

Меня зовут г-н Джонсон Кваме, руководитель филиала финансового учреждения. Я получил ваш контакт через надежный источник называется базой данных через Гану торговой палаты. Я женился Ганский с 3 детьми. Я пишу для получения вашей помощи в передаче США $ 7,500,000.00 долларов. Этот фонд является сверх того, что моя отрасли, в которой я, как менеджер сделал прибыль в прошлом году (т.е. 2012 финансового года).
Я уже представил ежегодный доклад за этот год моей головной офис в Аккре-Гане как Я наблюдал с большим интересом, поскольку они никогда не узнаем этого избытка. Я с тех пор, поместил эту сумму US $ 7,500,000.00 долларов на Escrow кодированный счет без бенефициаром (Anonymous), чтобы избежать следов.

Как офицер банка, я не могу быть непосредственно подключены к этому таким образом деньги я побудило просить за вашу помощь, чтобы получить эти деньги на ваш банковский счет от моего имени. Я согласен, что 45% этих денег будет для вас в качестве иностранного партнера, в отношении предоставления счета в иностранном, а 55% будет для меня. Я должен подчеркнуть, что не существует практически никакого риска в этом. Это собирается быть банком-К-Банка. Все что мне нужно от вас, чтобы выступать в качестве оригинального вкладчиков этого фонда так, что фонд может быть передан на ваш счет.

Если вы примете это предложение, я по достоинству оценят ваш своевременное реагирование на меня. Вот почему и единственная причина, почему я связался с вами, я готов вместе с компаньонами инвестиций с вами благодаря вашим богатый опыт, Поэтому, пожалуйста, если вы заинтересованы, чтобы помочь на этом предприятии просьба связаться со мной назад для краткого обсуждения о том, как продолжить.
С уважением,
Г-н Джонсон Кваме.
http://nigerian-letters.blogspot.ru

Типичным признаком «нигерийского письма» является то, что

- оно адресовано не конкретному человеку – в обращении отсутствует имя адресата, а поле «Кому» не заполнено или там не указан адрес получателя;
- оно содержит нечистоплотное предложение — перевод или обналичивание чьих-то уже украденных средств;
- максимально неопределенны детали предложения, что провоцирует получателя на диалог о подробностях сделки;
- называются огромные цифры вознаграждения за услуги.

В Интернете достаточно часто публикуются образцы переписки с мошенниками, которые сами оказываются обманутыми. Кроме того, многие отвечают на «нигерийские письма» просто из любопытства – узнать, что будет дальше.

Но не надо недооценивать преступников – на той стороне действуют профессионалы.

- Адрес, с которого пришел ответ на письмо (независимо от его содержания), спамеры сразу же включат в базу как «живой» и могут продать «коллегам» – на него сразу начнет приходить гораздо больше спама.
- В письмах могут содержаться опасные троянцы, в том числе пока не определяемые антивирусом, или фишинговые ссылки, предназначенные для похищения ваших персональных данных.
- В случае успеха фишинговой атаки злоумышленники с легкостью могут получить доступ к вашим банковским счетам. Особенно если вы делаете покупки через Интернет или используете онлайн-банкинг с того же компьютера, с которого ведете переписку.

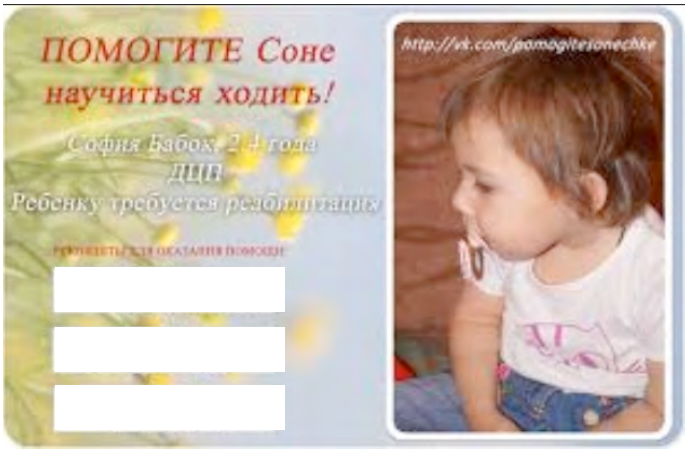
2. Использование спама для распространения ссылок на мошеннические сайты

В этом случае спам содержит ссылки на заранее созданные мошеннические сайты.

К числу мошеннических сайтов могут относиться сайты по сбору средств детям и инвалидам, жертвам катастроф и другим обездоленным, сайты партнерских программ, онлайн-казино, сайты, рекламирующие финансовые пирамиды и сомнительные способы быстрого обогащения (кликерные и бонусные способы «заработка», «волшебные кошельки» и т. д.), сайты по распространению чудодейственных «лекарственных средств» и других бесполезных или вредных товаров и услуг.

Спам о сборах пожертвований (детям, инвалидам, животным и т. д.)

Спам с призывами пожертвовать деньги, например на лечение ребенка, может сопровождаться ссылкой на мошеннический сайт, на котором размещены фотографии больного, копии его медицинских справок, чаще всего настоящие.



Мошенники могут использовать фотографии даже здоровых детей или заимствовать изображения действительно больных с сайтов благотворительных фондов, добавляя при этом на страницы свои номера электронных счетов, например Яндекс.Кошелька или Qiwi.

Вероятность того, что собранные таким образом пожертвования дойдут до самого больного, – мала. Даже если нуждающийся действительно существует, не факт, что собранные деньги будут потрачены по назначению. Бывает даже, что родители собирают средства якобы для больных детей, но тратят их на себя.

«За 14 лет Русфонда мы десятки раз сталкивались с мошенниками: они перепечатывали из «Ъ» истории наших детей, подставляя свои банковские счета. В начале 2000-х не проходило месяца, чтобы в интернете не объявлялся очередной «русфонд». Воришки тогда могли урвать разве что сущие копейки. Жулики-2010 понаглей: только что в одной из социальных сетей появилась группа «Российский фонд помощи» с сайтом в системе uCoz. Новость в том, что фальшак публикует свидетельство Минюста РФ о регистрации НКО с этим названием. Если кто не знает, «Ъ» с 2000 года трижды и безуспешно пытался зарегистрировать нашу программу «Российский фонд помощи» в качестве НКО». http://www.kommersant.ru/daily/?date=20101126

В данном случае расчет мошенников – **на эмоциональный порыв и лень**. Большинство людей поленится идти в банк и переведет деньги через Интернет, не выходя из дома. А если кто-то захочет удостовериться в том, что пациент существует, то найдет полную информацию о нем на сайте подлинного фонда. Создастся впечатление, что добрые люди распространяют сведения, чтобы помочь ребенку.

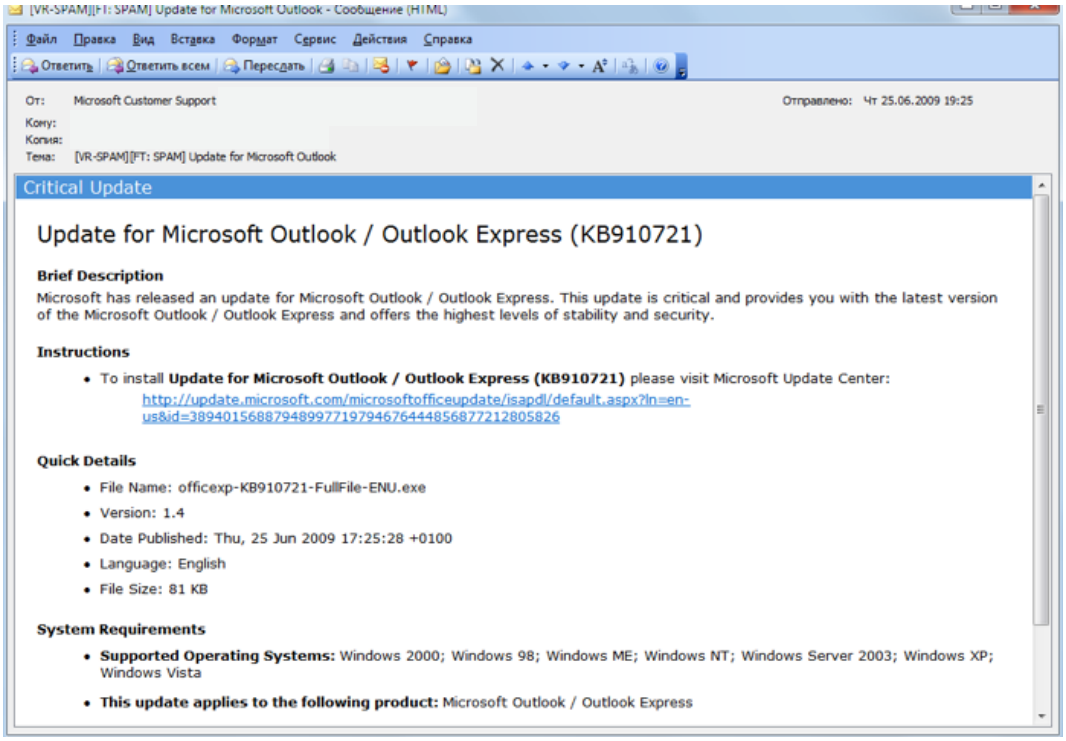
История про 20 овчарок, которых якобы должны были усыпить в связи с расформированием отдела охраны, ходила по Интернету **2,5 года!** Мошенники из многих городов успели распространить этот пост с разными телефонами, чтобы нажиться на людях, желающих помочь. До сих пор добрые, но невнимательные люди делают перепосты с надеждой помочь несуществующим животным.

Зачастую спам о помощи сопровождается призывам распространить это сообщение среди знакомых.

Такой прием называется вирусным маркетингом. Эмоциональное сообщение работает как вирус, вызывая желание им поделиться, – даже если сам ты не стал участвовать в сборе средств. Сеть «зараженных вирусом» может расти в геометрической прогрессии, если каждый будет пересылать сообщение всем своим знакомым. При этом настает момент, когда первоначальный источник «вируса» найти уже невозможно, в то время как доверие к информации растет, так как жертвы получают ее от своих друзей. Вирусное сообщение охватывает огромную аудиторию, достаточную, чтобы получить значительное количество «откликов» – звонков по указанному в объявлении номеру (в реальности платному) или переводов на указанный счет. Даже если на ваш звонок никто не ответит, с вашего счета будут списаны средства.

Одним из видов вирусного спама являются «письма счастья». Те, кто организует такие рассылки, отправляют первые несколько писем с предупреждением о какой-либо опасности: например, что не следует добавлять себе в контакты какое-то определенное лицо, иначе ваш компьютер подвергнется вирусной атаке. Не доверять этим письмам, казалось бы, нет причины: они приходят к нам от знакомых людей. И мы спокойно рассылаем их копии дальше по своим спискам адресов, наивно полагая, что делаем доброе дело.

Такие письма могут быть и безобидными («перешлите письмо 10 получателям и будете счастливы»), а могут использоваться для распространения вредных слухов и мифов. Вот пример подобного спама от имени известной компании:



Такие схемы хорошо работают во время резонансных мировых событий, когда люди в едином порыве рвутся помочь, забывая о безопасности. Будь то землетрясение в Японии или события на Украине – для мошенников людская беда лишь повод для наживы.

1. Помогать нуждающимся нужно. Но при этом надо взять за правило не лениться и тщательно перепроверять любую информацию, которая касается перечисления пожертвований, — до того, как принять решение о переводе средств.

2. Поищите в Интернете название фонда или имя и фамилию ребенка, на лечение которого планируете пожертвовать деньги. Вполне возможно, что имя и фотография уже используется длительное время различными мошенниками.
3. **Жертвуйте средства благотворительным организациям.** На сайте легально работающего фонда обязательно будут размещены:

- общая информация о фонде (если речь идет о медицинском фонде, то должен быть список диагнозов, с которыми он работает – крайне редко встречаются фонды, которые помогают по всем группам заболеваний);
- копии уставных документов организации;
- финансовые отчеты;
- отчеты по детям, которые уже получили помощь;
- годовой отчет.

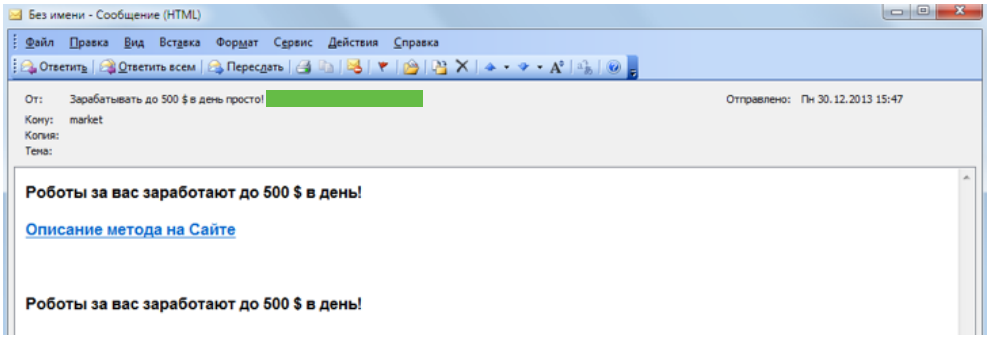
«Лохотроны»

К числу так называемых «лохотронов» относятся незаконные онлайн-лотереи, онлайн-казино, различного рода методики — от «честного» ухода от налогов, способов легкого заработка и до чудодейственных лекарств — во всех этих случаях мошиенники гарантированно поживятся за ваш счет.

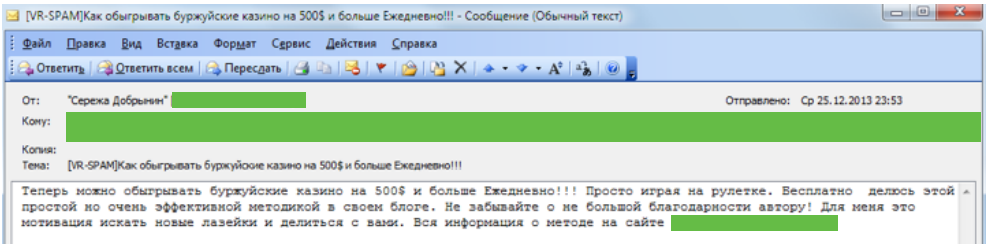
Киберпреступники, специализиоующиеся на «лохотронах», эксплуатируют **жадность, нежелание трудиться, жажду легкой наживы, склонность к авантюризму** и другие человеческие пороки.

Спам-сообщение «лохотронщиков» составлено так, чтобы заинтриговать и заставить вас перейти на сайт мошенников — раскрутка жертв на деньги происходит там. В письме могут упоминаться выигрыши денежных сумм,

предлагаться подозрительно дешевый кредит или ипотека, рассказываться о доступе к секрету небывалого успеха или легкого заработка,

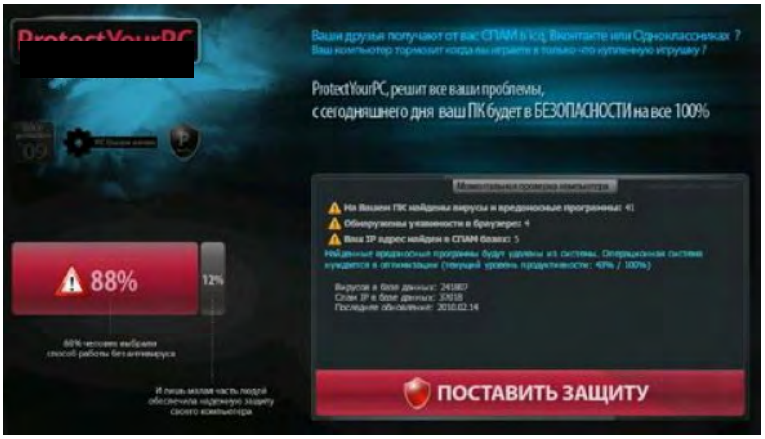


методики обмана онлайн-казино, за доступ к которым, конечно же, надо заплатить, и т. д.



Часто «лохотронщики» пытаются воспользоваться стремлением людей к безопасности. Многим наверняка знаком выскакивающий «сканер», сообщающий, что:

- на вашем ПК найдено столько-то вирусов и вредоносных программ;
- обнаружено столько-то уязвимостей в браузере;
- ваш IP-адрес найден в стольких-то спам-базах.



http://www.ho24me.com/node/146
Чтобы получить доступ к услугам сайта, необходимо отправить 3 (три!) СМС-сообщения на указанный сервисный номер (и при этом автоматически принять условия пользовательского соглашения) и ввести полученный код доступа в соответствующее поле формы. Стоимость СМС составляет до 300 рублей.

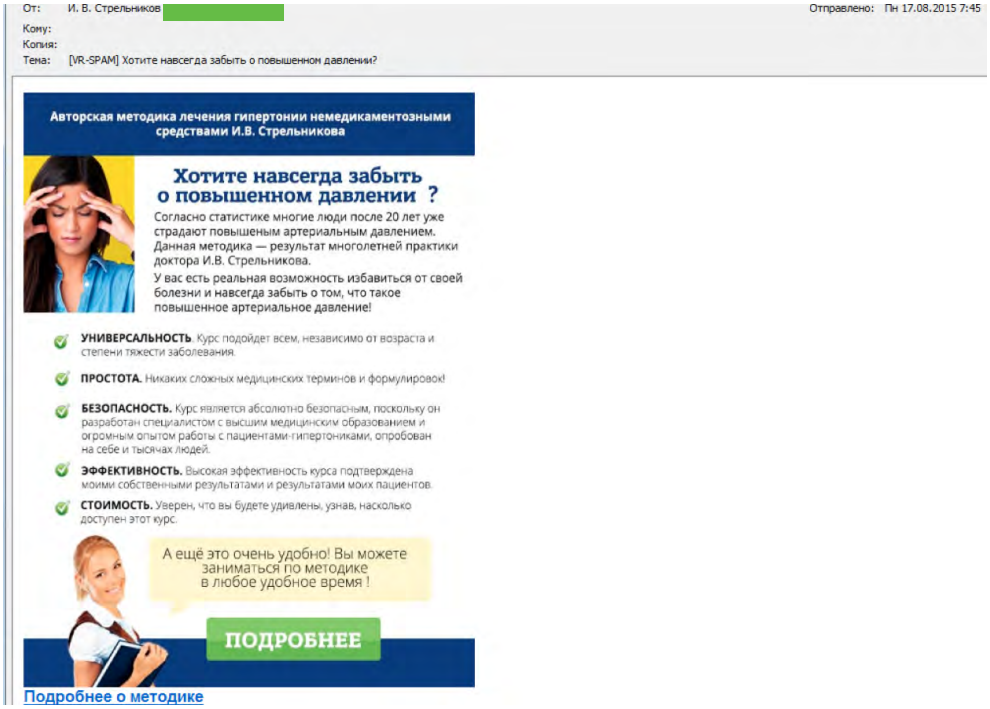
«СМС-лохотроны»
Для извлечения выгоды в таких схемах задействованы СМС-сообщения. С типичным примером такого мобильного спама знакомы многие:

«Мама, у меня неприятности, на мой сотовый не звони. Срочно положи 1000 рублей на этот номер. Позже все объясню».

А вот как «СМС-лохотрон» работает в почтовом спаме:

«Чудодейственный» спам

Спам о чудесном/быстром/легком/беспроблемном и т. д. излечении от болезни или изучении чего-либо:

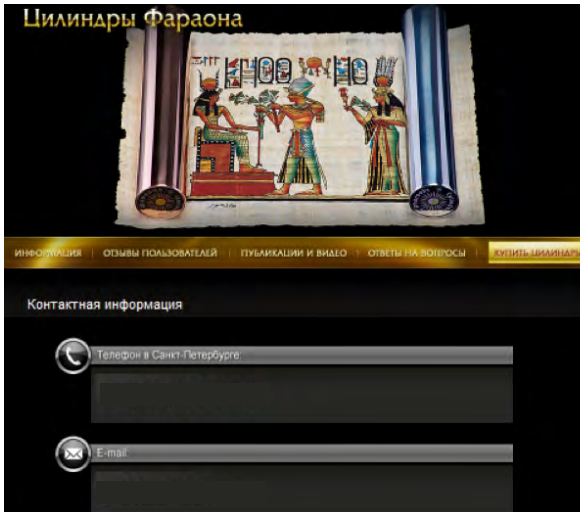


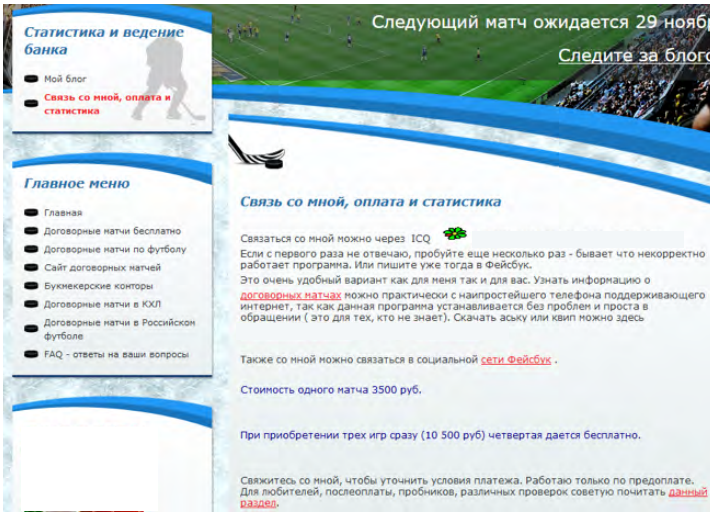
На самом деле нет такого профессора и нет такой методики. Но ведь надо не полениться это разузнать!

Признаки мошеннического сайта

Мошеннический сайт можно распознать, если внимательно отнестись к следующим моментам:

- На главной странице для связи даны только электронные адреса, без телефона, часто без физического адреса. Даже если телефон будет указан, на звонок по нему никто не ответит или всегда будет срабатывать автоответчик («мы вам обязательно перезвоним, ваш звонок важен для нас»). Иногда указывают телефоны реальных людей, ничего не подозревающих о том, что их номер задействован в мошеннической схеме. Это наиболее характерный признак мошеннических сайтов. Воспользовавшись сомнительным предложением, вы потом не сможете предъявить претензии или вернуть товар.





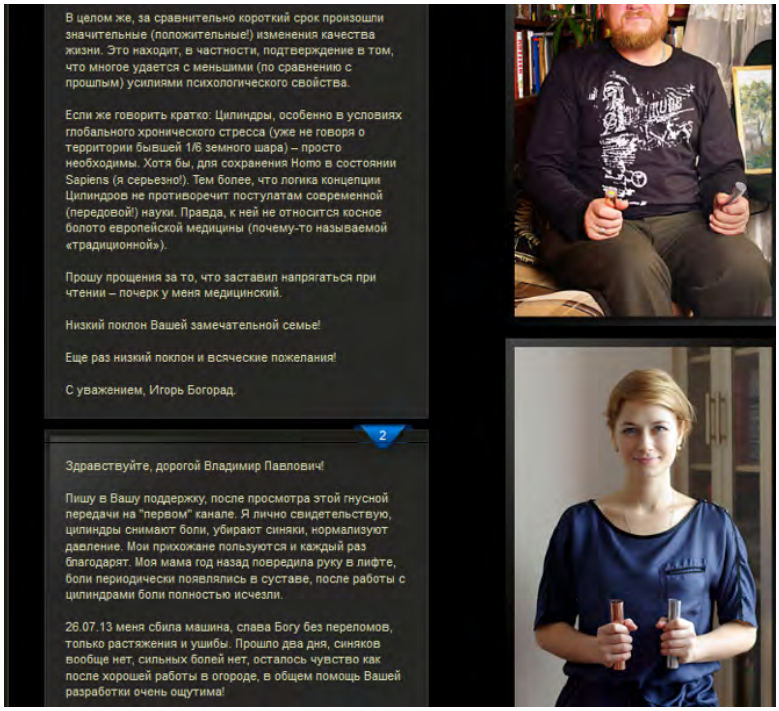
Сайты мошенников постоянно мигрируют – их время жизни невелико. Поэтому зачастую на месте знакомого вам сайта вы увидите это или подобное сообщение:

Forbidden

You don't have permission to access / on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

- На форумах мошеннических сайтов и в разделах отзывов размещаются исключительно положительные мнения. И очень часто (что нехарактерно для отзывов в сети) – написанные хорошим русским языком.



- Поддержка или вовсе не отвечает на ваши вопросы, или делает это спустя много дней и даже недель.

Мошенники не брезгуют и дополнительным заработком, поэтому также должны настораживать следующие особенности:

- обильная реклама сторонних товаров и услуг;
- перечни людей, якобы получающих благодаря этому сайту астрономические суммы;
- предложения по установке плагина якобы для распознавания мошеннических сайтов (на самом деле это гарантированно окажется троянец);
- помимо бесплатных сервисов сайт предлагает доступ к премиум-акканту и дополнительным услугам с оплатой через СМС;
- предложение написать положительные отзывы на форуме и получить за это вознаграждение (некоторые легальные компании тоже опускаются до такого, но это, скорее, исключение).

На таких сайтах категорически нельзя заполнять какие-либо формы и оставлять в них свои данные, а также подписываться на рассылки. *Даже если присутствует текст договора о конфиденциальности, соблюдать его никто здесь не станет.*

Но лучше на такие сайты вообще не заходить и не тратить время на попытки выявить признаки обмана. Для защиты от случайного попадания на мошеннические сайты в антивирусах предусмотрены специальные модули. Например, в Dr.Web Security Space (для Windows, macOS или Linux) это веб-антивирус SpIDer Gate.

С помощью этого модуля вы сводите к минимуму риск посещения:

- интернет-ресурсов, которые используются для распространения вредоносных или потенциально опасных программ, преимущественно троянцев;
- фишинговых сайтов;
- сайтов, на которых используются методы социальной инженерии для обмана посетителей.

Для предотвращения посещения потенциально опасных сайтов с мобильного устройства в Dr.Web Security Space для Android используется облачный фильтр Cloud Checker.

Специалисты «Доктор Веб» анализируют такие сайты и вносят их в базу нерекомендуемых к посещению.

При этом ни одна антивирусная компания, в том числе «Доктор Веб», не блокирует такие сайты — у нас нет для этого возможностей. Мы только предупреждаем о нежелательности их посещения.

Узнайте больше о потенциально опасных сайтах и способах защиты от их посещения с помощью Dr.Web на страницах информационного проекта «Нерекомендуемые сайты».

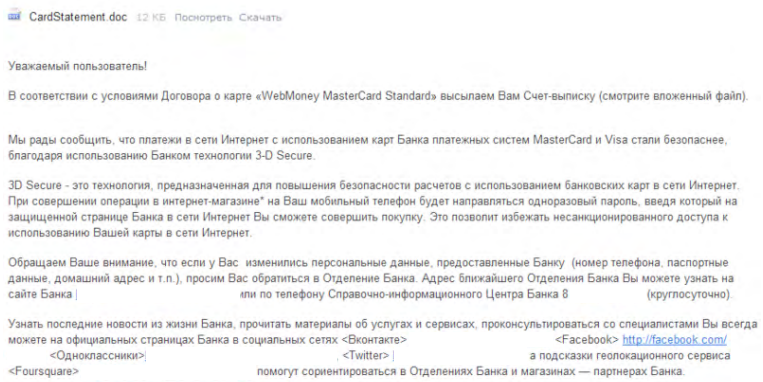
Куда жаловаться на мошенников?

- *О волнах «нигерийского спама» периодически предупреждает МВД России. Как правило, все ведущие СМИ публикуют эти сообщения.*
- *Борьбой с компьютерными аферами, как и с другими видами IT-преступлений, в России занимается Управление «К» МВД России. О факте мошенничества вы можете сообщить через «Общественную приемную МВД России в Интернете» (https://мвд.рф/request_main), выбрав необходимое подразделение.*
- *На международных интернет-аферистов вы можете пожаловаться через Internet Crime Complaint Center (www.ic3.gov/default.aspx).*
- *О мошенничестве в банковском секторе можно сообщать в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) Банка России.*

Как спам работает на фишеров

Фишер – злоумышленник, занимающийся обманом пользователей при помощи фишинга.

Фишер – (англ. phishing, от fishing – рыбная ловля, выуживание) – технология интернет-мошенничества, одна из разновидностей социальной инженерии. С помощью фишинга мошенники получают персональные, аутентификационные и прочие конфиденциальные данные своих жертв. Для этого пользователям рассылаются спам-сообщения, написанные от лица банков, интернет-магазинов или платежных систем, названия которых на слуху. В этих сообщениях предлагается перейти по ссылке на некий сайт, где требуется указать о себе те или иные данные.



CardStatement.doc 12 КБ Посмотреть Скачать

Уважаемый пользователь!

В соответствии с условиями Договора о карте «WebMoney MasterCard Standard» высылаем Вам Счет-выписку (смотрите вложенный файл).

Мы рады сообщить, что платежи в сети Интернет с использованием карт Банка платежных систем MasterCard и Visa стали безопаснее, благодаря использованию Банком технологии 3-D Secure.

3D Secure - это технология, предназначенная для повышения безопасности расчетов с использованием банковских карт в сети Интернет. При совершении операции в интернет-магазине* на Ваш мобильный телефон будет направляться одноразовый пароль, введя который на защищенной странице Банка в сети Интернет Вы сможете совершить покупку. Это позволит избежать несанкционированного доступа к использованию Вашей карты в сети Интернет.

Обращаем Ваше внимание, что если у Вас изменились персональные данные, предоставленные Банку (номер телефона, паспортные данные, домашний адрес и т.п.), просим Вас обратиться в Отделение Банка. Адрес ближайшего Отделения Банка Вы можете узнать на сайте Банка | или по телефону Справочно-информационного Центра Банка 8 (круглосуточно).

Узнать последние новости из жизни Банка, прочитать материалы об услугах и сервисах, проконсультироваться со специалистами Вы всегда можете на официальных страницах Банка в социальных сетях <Вконтакте> <Facebook> http://facebook.com/ <Одноклассники>| , <Twitter> | а подсказки геолокационного сервиса <Foursquare> помогут сориентироваться в Отделениях Банка и магазинах — партнерах Банка.

Фишинговые письма – зачастую их отправителем может быть указан реально существующий человек, а в теле письма могут быть данные, говорящие о том, что вы ему хорошо известны. Дело в том, что информацию о вас злоумышленники могут найти в открытом доступе – например, в соцсетях или на мошеннических форумах. Поскольку эти письма могут рассылаться с зараженных компьютеров ваших знакомых (или даже с вашего!), они не будут вызывать подозрения, т. к. в поле «Отправитель» окажется известный вам адрес из вашей же адресной книги.

Фишинговые ссылки – ссылки на сайт, очень похожий на легитимный ресурс, который на самом деле является подделкой злоумышленников. Также такие ссылки могут вести непосредственно на загрузку вредоносного файла. Чаще всего они содержатся в спам-письмах или могут появиться в сервисных окнах программ под видом:

- важного сообщения (например, от банка) с предложением срочной установки некоего сертификата безопасности, необходимого для дальнейшего получения финансовых услуг (примечательно, что часто жертвы такого рода фишинга даже не являются клиентами этого банка, но все равно из любопытства переходят на поддельную страницу);
- срочного обновления операционной системы/браузера/приложения/онлайн-игры, для загрузки которого жертве следует указать в соответствующей форме свой номер мобильного телефона и ввести пришедший в ответном СМС код. Таким образом, пользователь соглашается с условиями платной подписки, за которую со счета его мобильного телефона будет регулярно списываться определенная сумма;
- ОЧЕНЬ выгодной акции, которая проводится только сегодня и участвовать в которой надо немедленно, перейдя на некий сайт;
- сообщения о подарке или выигрыше (например, в онлайн-казино или лотерее), для получения которого надо ввести номер мобильного телефона или отправить платное СМС;
- предложения ответить на вопросы анкеты и получить подарок (при условии ввода номера банковской карты и пароля доступа к интернет-банку);
- сборника обоев для рабочего стола или другого бесплатного контента (тут возможны сотни вариантов), доступ к которому можно получить, нажав на кнопку в письме/приложении.

Новые сценарии атак появляются ежедневно!

Фишинговые сайты

Примеры фишинговых сайтов

Главная опасность фишинга заключается в том, что пользователи сами, по доброй воле раскрывают свои данные, вводя их на мошеннических сайтах.

Зачастую при клике по фишинговой ссылке пользователи не только переходят на поддельный сайт, но и загружают на свой компьютер вредоносную программу.

Пример такого рода фишинга с использованием бренда Dr.Web

https://news.drweb.ru/show/?i=9631&c=9&lng=ru&p=0

Dr.WEB®
с 1992 года

Уважаемый

Приглашаем вас стать участником Бета-Тестирования!
Мы разработали новую, улучшенную систему антивирусной проверки "Dr.Web CureIt 2", и просим вас помочь Нам с нахождением в ней: Багов, глюков и других неприятных вещей!

Как стать участником нашей программы бета-тестирования? Легко!
1. Выключите предустановленную антивирусную программу, Она может конфликтовать с нашей!
2. Скачайте установщик нашей программы: Dr.Web CureIt 2!
3. Запустите, введите свой почтовый адрес в форме входа.
4. Пользуйтесь, и при нахождении ошибок программы - пишите Нам через специальную форму обратной связи

С уважением,
администрация сайта компании «Доктор Веб»

«Доктор Веб» 2003—2015

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Антивирусная защита Dr.Web позволяет информационным системам клиентов эффективно противостоять любым, даже неизвестным угрозам.

«Доктор Веб» стал первой компанией, предложившей на российском рынке инновационную модель использования антивируса в качестве услуги, и по сей день продолжает оставаться безусловным лидером российского рынка интернет-сервисов безопасности для поставщиков ИТ-услуг. Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

Вы всегда можете отписаться от нашей рассылки по этой ссылке: Отменить подписку

Защити созданное

ООО«Доктор Веб»
Адрес: 125124, Россия, Москва, 3-я улица Ямского поля, вл.2, корп.12А
Телефон: +7 (495) 789-45-87 (многоканальный)
Факс: +7 (495) 789-45-97

Разновидностями фишинга являются вишинг и смишинг.

Цели фишеров

- Кража пароля доступа к банковскому счету и хищение денежных средств с помощью «банковских троянцев».
- Подписка пользователей на платные СМС-рассылки и различные контент-услуги.
- Инфицирование компьютера с целью включения его в бот-сеть (для кражи средств с банковского счета жертвы, постоянной слежки за действиями пользователя на компьютере, рассылки спама и т. д.).
- Кража аккаунтов в социальных сетях и рассылка спама от лица жертвы.
- Кража адресов электронной почты из книги контактов для рассылки спама.

Можно ли защититься от фишинга программными средствами?

- Программных средств, которые «вычисляют» преступные намерения владельцев фишинговых сайтов, не существует.
- Нет таких программ, которые помешали бы пользователю ввести пароль.

- Ни один антивирус не может гарантировать пользователям полную защиту от фишинга. Для предотвращения посещения потенциально опасных сайтов (в том числе фишинговых) предусмотрен веб-антивирус, который является одним из компонентов антивирусной программы. Однако фишинговые сайты появляются постоянно, и их не всегда удается оперативно добавить в базы антивируса. Поэтому какое-то время о новом фишинговом сайте антивирусная компания может не знать. Кроме того, пользователи нередко сами отключают модуль веб-антивируса или облако Dr.Web, тем самым добровольно повышая «фишинговые» риски.

Фишинг – это уголовно наказуемое преступление.

Статья 159. Мошенничество
1. Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, — наказываются ***штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет.***

Статья 159.6. Мошенничество в сфере компьютерной информации
1. Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, — наказываются ***штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.***

Фишинговая деятельность с применением троянских программ подпадает под действие ряда статей УК РФ.

Статья 272. Неправомерный доступ к компьютерной информации
1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, —
наказывается ***штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.***
2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, -
наказывается ***штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.***
3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, —
наказываются ***штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.***
4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они
повлекли тяжкие последствия или создали угрозу их наступления, —
наказываются ***лишением свободы на срок до семи лет.***
Примечания.
1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.
2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, —

наказываются ***ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.***

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, —

наказываются ***ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.***

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, —

наказываются ***лишением свободы на срок до семи лет.***

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

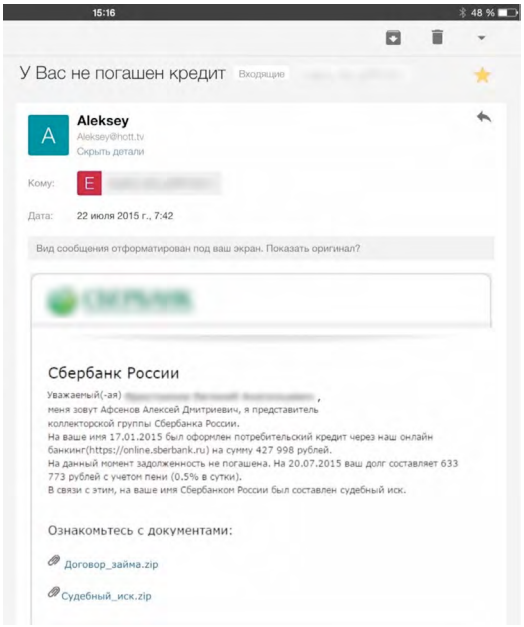
1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, — наказывается ***штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.***

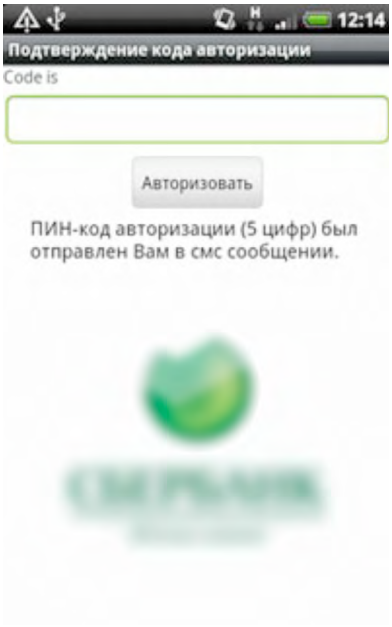
2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, — наказывается ***принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.***

Сценарии фишинговых атак

- **Выуживание аутентификационных данных**

  Чтобы получить эти данные, фишеры притворяются представителями известных компаний, банков или государственных органов. Они оформляют письмо так, чтобы у пользователя не возникло подозрений о том, что оно отправлено кем-то другим. Доверяя отправителю, пользователь совершает требуемое действие, будь то переход по ссылке, звонок по телефону или отправка СМС, запуск или открытие вложенного файла. Чаще всего злоумышленников интересуют данные для доступа в системы онлайн-банкинга. Поэтому фишинговые письма и интернет-ресурсы имитируют фирменный стиль банков – содержат логотипы, идентичные официальным, а также другие данные, взятые с настоящих веб-сайтов или из легальных рассылок соответствующей организации. Это усыпляет бдительность жертв фишеров.

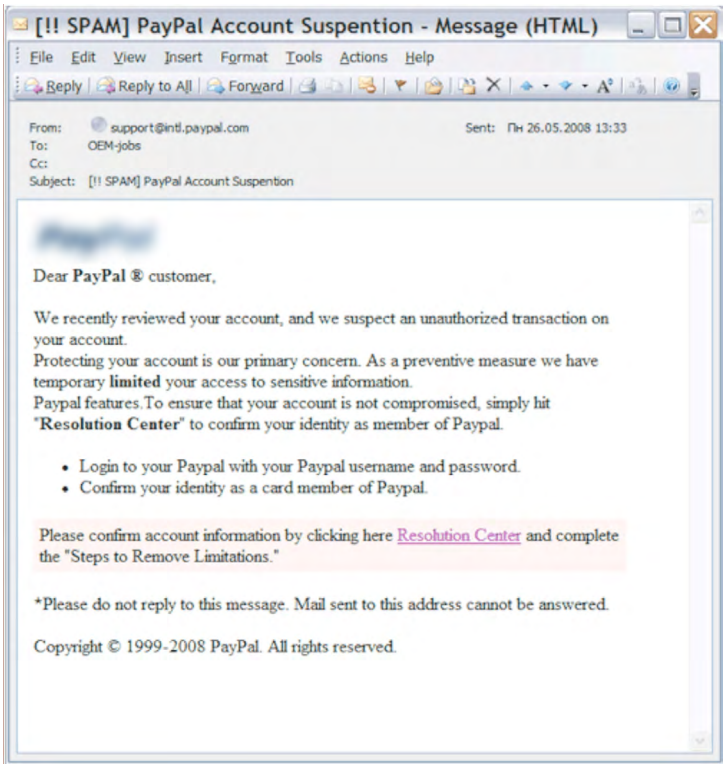




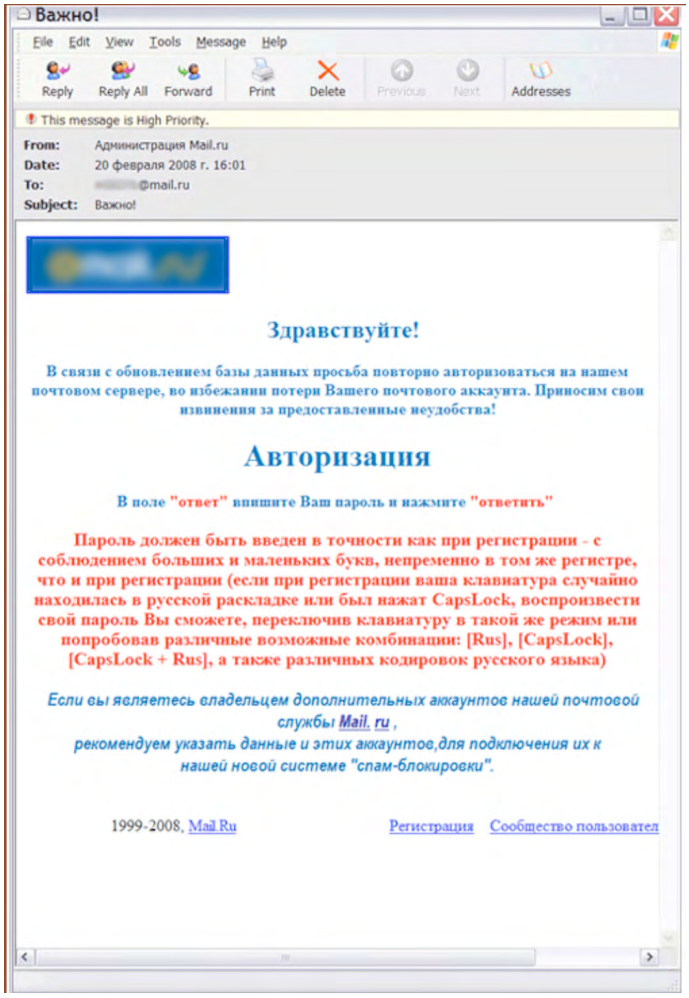
Перейдя по ссылке из фишингового письма, пользователь сталкивается с требованием ввести свои реквизиты доступа к системе интернет-банкинга. Эти данные запрашиваются, например, под предлогом необходимости срочной замены пароля. Нередко при нажатии на такую ссылку на ПК загружается вредоносная программа.

По такому сценарию были организованы атаки на пользователей систем Web-Money, «Яндекс.Деньги», Citibank и некоторых известных российских банков.

Чтобы у пользователя не возникло мыслей об обмане, злоумышленники прикрываются брендами, которые у всех на слуху, – например, Paypal, Amazon или AppStore.



Также фишеры широко используют рассылку запросов от имени администрации того или иного сервиса. В них под разными предлогами (как правило – под угрозой закрытия аккаунта) они требуют от жертвы прислать пароль от учетной записи на указанный адрес. Таким образом злоумышленники могут получить доступ к почтовым аккаунтам и рассылать спам или фишинговые письма от имени своих жертв.



Внимание! *Ни банки, ни другие официальные организации или их представители никогда не запрашивают у своих клиентов конфиденциальные данные (например, пароли, имена пользователей, номера социального страхования) по электронной почте. Они никогда не просят перейти по ссылке из письма и ввести эти данные на открывшейся странице. Для взаимодействия с клиентами предусмотрены другие процедуры, гарантирующие полную конфиденциальность.*

Фишинговые письма, отправленные от имени банка, могут не только вынудить пользователя перейти на поддельный или взломанный сайт, но и сообщить о необходимости совершить звонок по определенному номеру – например, для решения проблем с банковским счетом. Этот вид мошенничества называется вишингом (голосовым фишингом).

- **Выуживание телефонных номеров**
  Для этой цели создавать фишинговый сайт злоумышленникам необязательно — достаточно письма с просьбой отправить СМС на короткий номер. Обоснованием необходимости этого может служить, например, подтверждение личности или активация почтового ящика. Отправка такого сообщения, как правило, обходится дороже, чем предусмотрено тарифом сотового оператора. Но жертва, скорее всего, узнает об этом слишком поздно: упоминание о стоимости СМС в фишинговых письмах либо отсутствует, либо набрано мелким шрифтом в конце письма.

> ***Внимание!*** *Отправка таких сообщений может привести не только к разовому списанию денег с мобильного счета, но и к подписке на дорогостоящий СМС-сервис мошенников. В этом случае деньги будут незаметно списываться вплоть до обнуления счета.*

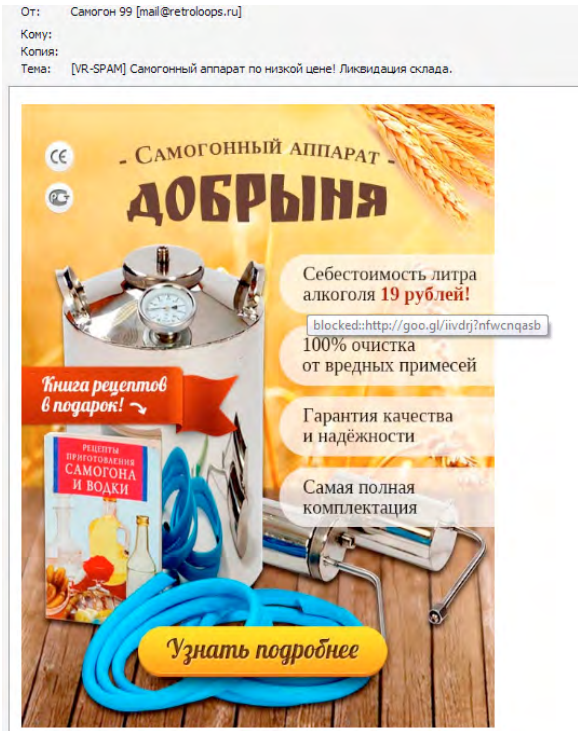
Технологии на службе фишеров

- **Поддельные ссылки**
  Для большей достоверности фишеры уделяют внимание не только оформлению письма в стиле соответствующей компании, но и ссылке, по которой жертва должна перейти. Такая ссылка может полностью или частично содержать реальное название той или иной компании, но в процессе перехода происходит перенаправление на мошеннический ресурс, для чего используются возможности JavaScript. Они позволяют видоизменять ссылку так, что она не будет соответствовать адресу сайта, на который в итоге попадает пользователь.Фишеры могут замаскировать ссылку при помощи картинки с поддельным URL. Если письмо распространяется в виде картинки, мошенники размещают на ней любой необходимый адрес, в то время как при клике по любой части изображения, не обязательно по ссылке, жертва перейдет на совершенно другой сайт.

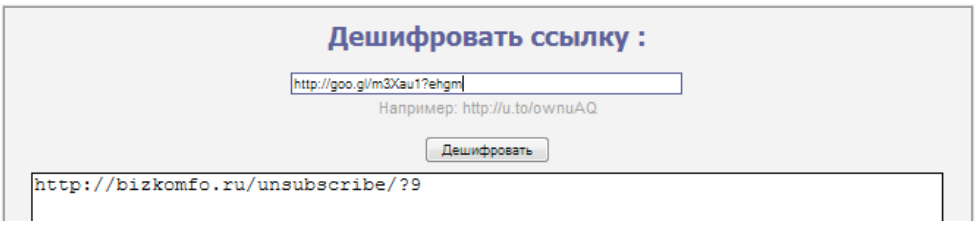
Еще один вариант обмана рассчитан на невнимательность жертвы: в легитимный адрес могут быть внесены незначительные изменения, которые не бросаются в глаза. Например, вместо www.microsoft.com ссылка может выглядеть так:
www.micosoft.com
www.mircosoft.com
www.verify-microsoft.com

- **Межсайтовый скриптинг**
  Вместо того чтобы подделать тот или иной легитимный сайт, злоумышленники могут перехватить контроль над ним путем взлома. В этом случае ни малейшая деталь не насторожит жертву, вводящую свои данные на этом сайте. Конфиденциальная информация просто попадет в руки злоумышленников. Этот вид мошенничества (известный как межсайтовый скриптинг) наиболее опасен, потому что обнаружить такой обман без специальных навыков практически невозможно.
- **«Сокращатели» ссылок**
  Зачастую ссылки бывают настолько длинными, что запомнить их невозможно, да и выглядят они некрасиво. Поэтому появились платные и бесплатные сервисы сокращения ссылок (URL shorteners), позволяющие любой адрес уместить всего в несколько символов. Конечно же, такие сервисы оказались настоящей находкой для фишеров, а вирусописатели стали с их помощью маскировать ссылки на загрузку вредоносных программ. Так, например, ссылка http://ru.wikipedia.org/wiki/Правда ведет на статью Википедии о... лжи!

Вот что можно увидеть, наведя курсор на картинку:



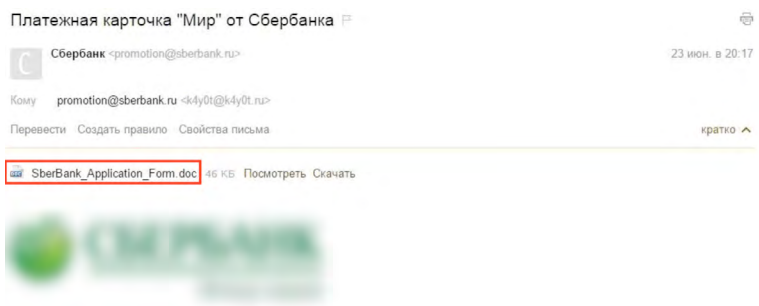
Увидеть, куда на самом деле ведет такой URL, можно при помощи сервисов дешифровки коротких ссылок:



Обратите внимание: в данном случае домен не соответствует тому, с которого якобы было отправлено письмо. Переходить по такой ссылке категорически не рекомендуется.

Вирусописатели и фишеры

- Нередко фишинговые письма приходят с вложениями, которые могут содержать вредоносные файлы или требовать для своего открытия авторизации на определенных ресурсах, в ходе которой мошенники получат ваши персональные данные.



- Для выуживания информации используются в том числе и троянские программы. Чтобы доставить троянца на компьютер жертвы, злоумышленники применяют следующие методы.

1. Заражение при посещении инфицированных сайтов

Пользователю не нужно ничего предпринимать, чтобы «получить троянца»: заражение происходит автоматически при посещении сайта.

Многие веб-ресурсы, независимо от содержимого, могут быть инфицированы вирусами или вредоносными скриптами. Файлы с расширением .js или .vbs — скрипты на языке JavaScript или Visual Basic — обычно используются на веб-страницах, к примеру, для регистрации пользователей или для авторизованного входа на сайт. Но эти же скрипты могут содержать и вредоносный код для кражи информации.

Ресурсы, наиболее часто являющиеся источниками вредоносного ПО (начиная с самых «заразных»)

- Сайты, посвященные технологиям и телекоммуникациям.
- Бизнес-сайты: бизнес-СМИ, порталы деловых новостей, бухгалтерские сайты и форумы, интернет-курсы/лекции, сервисы для повышения эффективности бизнеса.
- Сайты с контентом для взрослых.

Почему происходят заражения?

Большинство пользователей:

- выходит в Интернет с компьютера, на котором установлено ПО с уязвимостями;
- работает в Windows с правами администратора;
- использует простые пароли, взлом которых не составляет труда;
- не производит обновления безопасности всего программного обеспечения, установленного на ПК.

2. Использование уязвимостей в установленном ПО

Уязвимостями программного обеспечения называют ошибки в нем, используя которые можно проникнуть в систему и вмешаться в ее работу. Теоретически абсолютно любую ошибку в программе можно использовать для причинения вреда системе в целом.

ПО без уязвимостей не существует. Уязвимы любые ОС, включая macOS и Linux, а также системы дистанционного банковского обслуживания, через которые пользователи производят онлайн-платежи. Но особенно много уязвимостей в операционных системах Windows и Android.

Разработчики программного обеспечения прилагают усилия для закрытия уязвимостей, особенно критических, но вирусописатели часто узнают о «дырах» в ПО раньше, чем разработчики (это так называемые «уязвимости нулевого дня» — 0day exploits, о которых пока известно только вирусописателю или для исправления которых производитель ПО пока еще не выпустил «заплатки»). Подавляющее большинство современных «эффективных» троянцев проникает в системы именно через уязвимости, в том числе через уязвимости нулевого дня.

Внимание, опасность!

Современные троянцы в большинстве случаев незаметны для пользователей. Жертва не подозревает об угрозе вплоть до момента срабатывания вредоносной программы, а зачастую вообще не догадывается о том, что в компьютере обосновалось нечто постороннее. Таким образом, пользователь может и не знать о том, что его персональные данные уже похищены, а деньги с банковского счета обналичены злоумышленниками.

Почему пользователи так часто клюют на наживки фишеров?

- Некоторые не проявляют должной бдительности, полностью полагаясь на антивирус.
- Многие вообще не верят в существование интернет-угроз, считая их вымыслом антивирусных компаний.
- Иногда фишеры используют в своих письмах нейролингвистическое программирование (НЛП), против чего некоторые жертвы устоять не могут.
- Фишеры заманивают пользователей в психологические ловушки, используя приемы социальной инженерии, против чего бессильно любое программное средство защиты.

Подделка сайтов легальных организаций и использование элементов чужого бренда – это преступления.

- К лицам, ответственным за подделку сайтов с последующим хищением данных, применяются уже упомянутые статьи 159 и 159.6 УК РФ.
- Противоправное использование чужого бренда подпадает под действие ст. 180 УК РФ.

Статья 180. Незаконное использование средств индивидуализации товаров (работ, услуг)

1. Незаконное использование чужого товарного знака, знака обслуживания, наименования места происхождения товара или сходных с ними обозначений для однородных товаров, если это деяние совершено неоднократно или причинило крупный ущерб, —
наказываются ***штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на срок до двух лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев.***

2. Незаконное использование предупредительной маркировки в отношении не зарегистрированного в Российской Федерации товарного знака или наименования места происхождения товара, если это деяние совершено неоднократно или причинило крупный ущерб, —
наказываются ***штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года.***

Что делать, если вы подозреваете, что стали жертвой фишинга

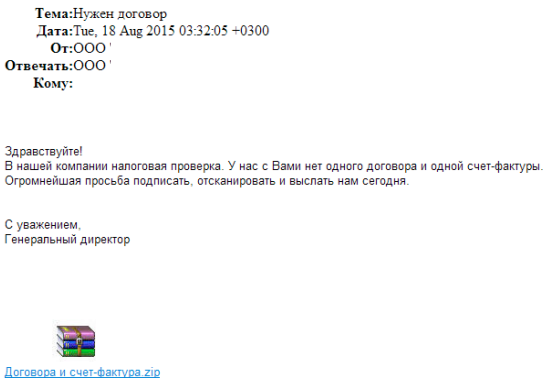
Если у вас возникло подозрение, что вы указали свои личные или финансовые данные, ответив на фишинговое письмо или перейдя на мошеннический сайт по ссылке, для минимизации возможного ущерба немедленно выполните следующие действия.

- Если на момент перехода по подозрительной ссылке или открытии файла у вас не был установлен антивирус Dr.Web, проверьте свой компьютер или устройство лечащей утилитой Dr.Web CureIt!
- Если вы ввели пароль или иные данные на поддельной странице, обязательно смените их. Задайте новые пароли или PIN-коды во всех своих онлайн-аккаунтах, измените контрольные вопросы и ответы на них. Данное действие лучше выполнить с иного компьютера или после антивирусной проверки.
- Если вы предполагаете, что к мошенникам попали данные вашей кредитной карты — свяжитесь с банком для ее немедленной блокировки.
- Если вам стало известно о том, что злоумышленники получили доступ к вашему счету, сообщите об этом в банк и заблокируйте счет до выяснения ситуации.
- Если кто-то открыл новый счет от вашего имени — сообщите об этом в банк и потребуйте закрыть его, а также незамедлительно смените пароль доступа к онлайн-банкингу.
- Не реже раза в неделю просматривайте историю операций по карте и счетам, обращая внимание на странные транзакции или изменение настроек, которые вы не производили, а также на запросы, которые вы не инициировали. Обязательно подключите услугу СМС-информирования о каждой операции по карте или счету — в большинстве случаев это бесплатно.
- В случае отправки СМС на мошеннический номер потребуйте возврат средств у своего мобильного оператора или у компании, обслуживающей этот номер.

Как спам работает на вирусописателей

Вирусописатели активно используют спам для рассылки вредоносных программ, а вредоносные программы – для рассылки спама. Для достижения обеих целей преступникам требуется заразить как можно больше компьютеров.

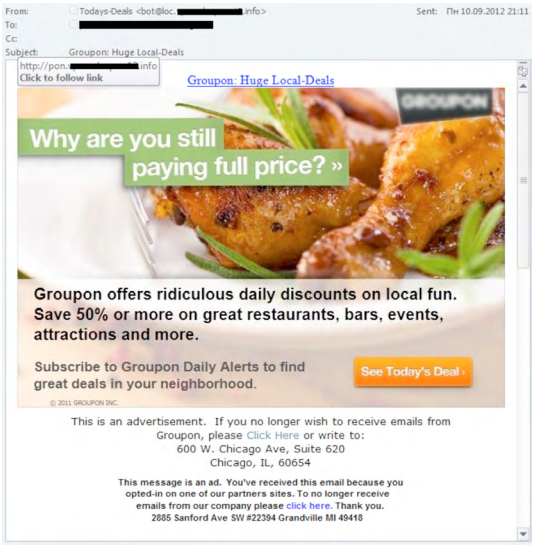
1. **Спам используется для транспортировки вредоносных программ и/или ссылок на их загрузку**
   Письма спамеров содержат либо вредоносное ПО (в виде вложений), либо ссылки, при переходе по которым ваш компьютер или мобильное устройство подвергнется заражению. Вредоносные файлы, вложенные в сообщение, могут быть заархивированы, так как достаточно часто антивирусная проверка архивов отключается ради быстродействия компьютера.



   В приведенном примере письмо, разосланное по реальным адресам сотрудников определенной компании, содержало заархивированного троянца-шифровальщика **Trojan.Encoder.567**.

   Чтобы обойти антивирусную проверку вложений в почтовые сообщения, вирусописатели также используют вложения, которые сами по себе не представляют опасности, но содержат ссылки на загрузку вредоносного ПО. Для защиты от этого способа заражения необходимо использовать фильтрацию по спискам заведомо вредоносных интернет-ресурсов – Офисный контроль.

   В данном примере рассылки с элементами бренда Groupon ссылки через несколько переадресаций ведут на вредоносный ресурс с эксплойтами.



Все без исключения современные антивирусы могут какое-то время не определять новейшие образцы троянцев, рассылаемые вирусописателями в спам-письмах. Почему это происходит?

Современные вредоносные программы разрабатываются не просто вирусописателями-профессионалами — это хорошо организованный криминальный бизнес, вовлекающий в свою преступную деятельность высококвалифицированных системных и прикладных разработчиков ПО.

Структурные элементы некоторых преступных сообществ

В ряде случаев роли злоумышленников внутри преступных сообществ могут быть распределены следующим образом:

1. **Организаторы** — лица, которые организуют процесс создания и использования вредоносного ПО и руководят им. Результаты этой деятельности они могут использовать сами либо продавать их другим преступникам или их объединениям.
2. **Участники**

- Разработчики вредоносного ПО
- Тестировщики созданного ПО
- Исследователи уязвимостей в операционных системах и прикладном ПО в преступных целях
- «Специалисты» по использованию вирусных упаковщиков и шифрованию
- Распространители вредоносного ПО, специалисты по социальной инженерии
- Системные администраторы, обеспечивающие распределенную безопасную работу внутри преступного сообщества и управление бот-сетями

Перед выпуском вредоносной программы в «живую природу» криминальные группировки тестируют их на **необнаружение** всеми актуальными антивирусными решениями, что позволяет злоумышленникам внедрять вирусы и троянцев в систему в обход антивирусной защиты. Именно поэтому до поступления образцов вредоносных программ в антивирусную лабораторию многие из них не обнаруживаются антивирусом.

Также все чаще криминальные группировки создают так называемые **таргетированные (целенаправленные) угрозы** — вредоносные программы, разработанные для заражения компьютеров или мобильных устройств конкретных групп пользователей (например, клиентов определенного банка). Как правило, это качественно написанные вредоносные программы, рассчитанные на долговременное присутствие на компьютерах жертв. Они не оказывают существенного влияния на работу инфицированных машин и в момент заражения не распознаются средствами защиты, что позволяет им оставаться необнаруженными в течение длительного времени. Некоторые из них даже борются с «конкурентами» и удаляют иные вредоносные программы. Есть даже троянцы, закрывающие уязвимости на компьютере!

Еще одна причина, по которой антивирус может не увидеть троянца в спаме, — уязвимости нулевого дня (так называемые 0day exploits — «дыры», о которых пока известно только вирусописателю или для закрытия которых производитель ПО пока еще не выпустил «заплатки»).

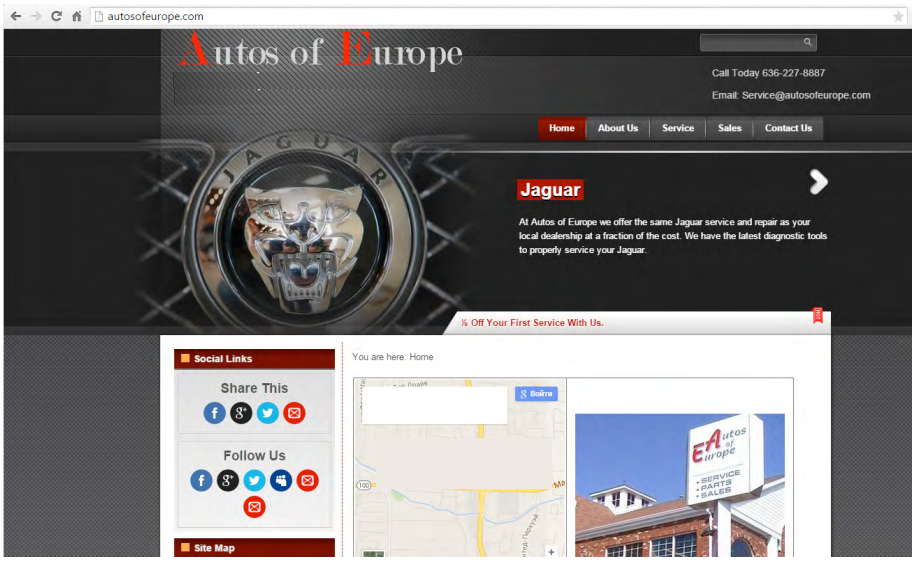
Также троянца может **запустить сам пользователь**, например, отключив самозащиту антивируса, когда злоумышленник, используя вишинг, рекомендует это сделать в ходе общения со своей жертвой (якобы самозащита антивируса мешает установке «нужной» программы или открытию файла).

Задачей антивируса является обнаружение и уничтожение вредоносных файлов, но ликвидировать он может только **известные** вирусной базе угрозы или те из них, которые могут быть обнаружены эвристическими механизмами. До получения обновлений антивирус не может ни обнаружить, ни уничтожить **новую неизвестную** угрозу. Вот почему так важно не отключать его автоматические обновления – антивирус должен обновляться как можно чаще.

Современный антивирус далеко не беспомощен перед лицом **неизвестных** угроз. Также антивирус не перестал быть **единственным** эффективным средством защиты от всех типов вредоносных программ — как **известных**, так и **неизвестных** вирусной базе. В высокотехнологичных антивирусных продуктах, в том числе Dr.Web, для обнаружения и обезвреживания **неизвестного вредоносного ПО** применяется множество эффективных **несигнатурных технологий**, сочетание которых позволяет обнаруживать такие угрозы до внесения записей о них в вирусную базу.

2. Использование вредоносных программ для рассылки спама

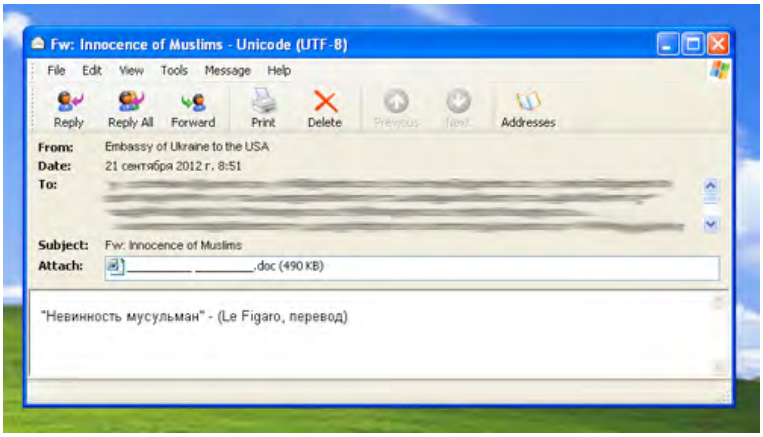
В начале июня 2015 года вирусные аналитики компании «Доктор Веб» выявили новую троянскую программу Trojan.Proxy.27552. Основное предназначение троянца — рассылка почтового спама со ссылками на веб-страницы, расположенные на взломанных сайтах.



Источник: http://news.drweb.com/show/?c=5&i=9474&lng=ru

Для рассылки спама используются так называемые «спам-боты» — зараженные троянцами компьютеры обычных пользователей, управляемые мошенниками удаленно. В спам-бот компьютер превращает вредоносная программа, помещенная на него злоумышленниками или, что случается не менее часто, самими пользователями.

Бэкдор **BackDoor.BlackEnergy** *рассылался вместе с письмами, в теме которых было указано название скандального фильма «Невинность мусульман». При этом направлены эти письма были в украинские госструктуры. Ботнет, создававшийся* **BackDoor.BlackEnergy**, *использовался для осуществления массовых спам-рассылок — в пик активности на его долю приходилось до 18 миллиардов сообщений в день, организация DDoS-атак и других противоправных действий.*



Источник: http://news.drweb.ru/show/?c=5&i=2807&lng=ru

Рассылки спама через спам-боты наиболее эффективны по ряду причин. В частности, против них практически бесполезны фильтры по IP-адресам, так как они не только принадлежат обычным пользователям, но и достаточно быстро восполняются в базе спамеров.

После инсталляции троянца спам-бот связывается с одним из принадлежащих спамерам серверов в Интернете и передает отчет об установке. Адреса этих серверов обычно заданы в теле спам-бота. В ответ спам-бот получает конфигурацию, в которой указано, с каких серверов он должен запрашивать данные для рассылки спама. Далее спам-бот связывается с указанным сервером и получает список e-mail-адресов для рассылки, шаблоны для формирования писем и прочие настройки. После выполнения рассылки спам-бот отсылает отчет, в котором обычно содержится статистика и список адресов, по которым не удалось отправить почту с указанием ошибок.

Кроме рассылки спама, спам-бот может решать ряд сопутствующих задач, в частности пополнять базы данных спамеров почтовыми адресами, найденными на компьютерах жертв.

Бэкдоры семейства **BackDoor.BlackEnergy**, *предназначенные для создания вышеупомянутых ботнетов, представляют собой модульных троянцев, действующих при помощи отдельно загружаемых плагинов, поэтому они могут не только рассылать спам. Согласно инструкциям, получаемым с управляющего сервера бот-сети,* **BackDoor.BlackEnergy.18** *может выполнить загрузку модулей, предназначенных для:*

- *кражи паролей от популярных интернет-приложений (браузеры, почтовые клиенты и т. п.);*
- *взаимодействия с файловой системой и сбора информации о компьютере;*
- *создания скриншотов (в том числе для кражи паролей) и видеозаписей;*
- *получения своих обновлений;*
- *управления компьютером при помощи функции удаленного рабочего стола (в том числе для получения доступа к системе онлайн-банкинга).*

Помимо модулей для операционных систем семейства Windows, были обнаружены плагины, которые представляют собой исполняемые ELF-файлы, работающие в ОС Linux на базе процессоров Intel с 32-битной системной логикой и предназначенные для:

- *взаимодействия с файловой системой (например, получения списка имеющихся файлов и директорий);*
- *получения обновлений троянца;*
- *осуществления DDoS-атак.*

СМС-спам становится все более популярным методом распространения современных Android-угроз. Такие сообщения содержат ссылку на загрузку вредоносной программы.

Например, **Android.Wormle.1.origin** *может распространяться при помощи СМС-сообщений среди всех знакомых владельца зараженного устройства. На конец ноября 2014 года* **Android.Wormle.1.origin** *успел заразить более 15 000 мобильных Android-устройств жителей порядка30 стран.*

Источник: http://news.drweb.com/show/?c=5&i=7076&lng=ru

Спам – оружие в конкурентных войнах

В нежелательных письмах зачастую распространяется клеветническая информация. Целью заказчиков спам-рассылок может стать дискредитация неугодного конкурента, срыв сделки, снижение доверия к компании, провоцирование паники и оттока клиентов, подрыв финансовой устойчивости предприятия (в том числе путем снижения котировок на бирже из-за распространенных спамерами порочащих компанию слухов).

- **Использование спама для рассылок порочащей жертву информации**
  В качестве примера можно привести письмо с темой «ОАО С***, Аресты.», содержавшее
  недостоверные данные, целью которого было обрушить стоимость акций компании.
  Источники: http://habrahabr.ru/post/11793, http://www.specul.ru/events/009.html

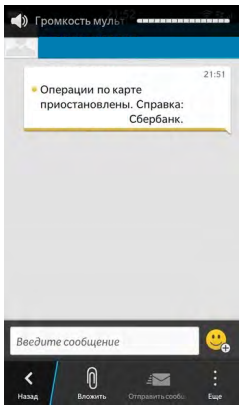
  Новости компании*
  03.06.2007
  Пресс центр компании С***:

  2 июля 2007 года были взяты под стражу генеральный директор ОАО «С***», а также председатель совета директоров по подозрению в уклонении от уплаты налогов, на часть имущества компании наложен арест. В связи с этим мы заявляем о временном завершении оборота акций нашей компании на биржевых площадках с 06.07.2007 вплоть до снятия ареста с активов предприятия. По заявлению представителя генеральной прокуратуры в Тюменской области Уголовное дело об уклонении от уплаты налогов было возбуждено ввиду нарушений, выявленных в ходе выездной проверки, завершившейся 22 июня 2007 года. Министерство по налогам и сборам сообщает о выявлении фактов уклонения от уплаты налогов с использованием офшоров в 2005 году. В результате МНС вручило требования на уплату налогов, пеней и штрафов на общую сумму 3,79 млрд рублей.

ОАО «С***» в свою очередь полностью отрицает свою вину и заявляет, что добросовестно уплачивало налоги в соответствии с законодательством Российской Федерации. Мы считаем данные действия провокацией со стороны властей. Юристы компании ведут работу по обжалованию решений об аресте активов компании. Правление ОАО «С***» сделает все возможное для того, чтобы не допустить срывов производственной и финансовой деятельности компании.
Пресс-центр компании С***.
® Все права принадлежат ОАО «С***».

** Орфография и пунктуация оригинала сохранены.*

- **Использование спама для распространения ложной информации от имени компании — жертвы атаки**
  В середине декабря 2014 года СМС-рассылка якобы от имени одного из крупнейших российских банков спровоцировала панику. Соцсети пестрили сообщениями о том, что «уже завтра банкоматы ***банка не будут выдавать наличку», по сарафанному радио передавали, что «знакомый знакомого сказал срочно снять все деньги», а по мобильникам велась СМС-рассылка:



Люди всю ночь стояли в очередях к банкоматам, чтобы снять деньги.
В результате атаки только за один день вкладчики забрали из банка несколько сотен миллиардов рублей.

Характерным признаком такого типа спама является тщательная проработка всех деталей распространяемой ложной информации — сообщение не должно оставить ни тени сомнения. Проведению атаки предшествовали мероприятия по размещению информации в Интернете, публикации в сетевых СМИ. В результате, даже перейдя по ссылкам или решив проверить некую информацию самостоятельно, вы только убедились бы в ее «достоверности». Особая опасность такого спама заключается в том, что его получатели, как правило, не верят официальным заявлениям и склонны считать их априори лживыми и скрывающими реальную ситуацию.

Распространение ложной информации в любом виде является преступлением. Лица, осуществляющие такое распространение, несут ответственность в соответствии с Уголовным кодексом РФ.

Статья 128.1. Клевета

1. Клевета, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию, – наказывается ***штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо обязательными работами на срок до ста шестидесяти часов.***

2. Клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, – наказывается ***штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до одного года либо обязательными работами на срок до двухсот сорока часов.***

3. Клевета, совершенная с использованием своего служебного положения, – наказываются ***штрафом в размере до двух миллионов рублей или в размере заработной платы или иного дохода осужденного за период до двух лет либо обязательными работами на срок до трехсот двадцати часов.***

4. Клевета о том, что лицо страдает заболеванием, представляющим опасность для окружающих, а равно клевета, соединенная с обвинением лица в совершении преступления сексуального характера, – наказываются ***штрафом в размере до трех миллионов рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо обязательными работами на срок до четырехсот часов.***

5. Клевета, соединенная с обвинением лица в совершении тяжкого или особо тяжкого преступления, – наказываются ***штрафом в размере до пяти миллионов рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо обязательными работами на срок до четырехсот восьмидесяти часов.***

Уголовная ответственность за это преступление начинается с 16 лет.

Статья 185.3. Манипулирование рынком

1. Манипулирование рынком, то есть умышленное распространение через средства массовой информации, в том числе электронные, информационно-телекоммуникационные сети (включая сеть «Интернет»), заведомо ложных сведений или совершение операций с финансовыми инструментами, иностранной валютой и (или) товарами либо иные умышленные действия, запрещенные законодательством Российской Федерации о противодействии неправомерному использованию инсайдерской информации и манипулированию рынком, если в результате таких незаконных действий цена, спрос, предложение или объем торгов финансовыми инструментами, иностранной валютой и (или) товарами отклонились от уровня или поддерживались на уровне, существенно отличающемся от того уровня, который сформировался бы без учета указанных выше незаконных действий, и такие действия причинили крупный ущерб гражданам, организациям или государству либо сопряжены с извлечением излишнего дохода или избежанием убытков в крупном размере, –
наказывается ***штрафом в размере от трехсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до четырех лет со штрафом в размере до пятидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех месяцев либо без такового с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.***

Статья 185.6. Неправомерное использование инсайдерской информации

1. Умышленное использование инсайдерской информации для осуществления операций с финансовыми инструментами, иностранной валютой и (или) товарами, к которым относится такая информация, за свой счет или за счет третьего лица, а равно умышленное использование инсайдерской информации путем дачи рекомендаций третьим лицам, обязывания или побуждения их иным образом к приобретению или продаже финансовых инструментов, иностранной валюты и (или) товаров, если такое использование причинило крупный ущерб гражданам, организациям или государству либо сопряжено с извлечением дохода или избежанием убытков в крупном размере, –
наказывается ***штрафом в размере от трехсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок от двух до четырех лет со штрафом в размере до пятидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех месяцев либо без такового с лишением права занимать определенные должности либо заниматься определенной деятельностью на срок до трех лет или без такового.***

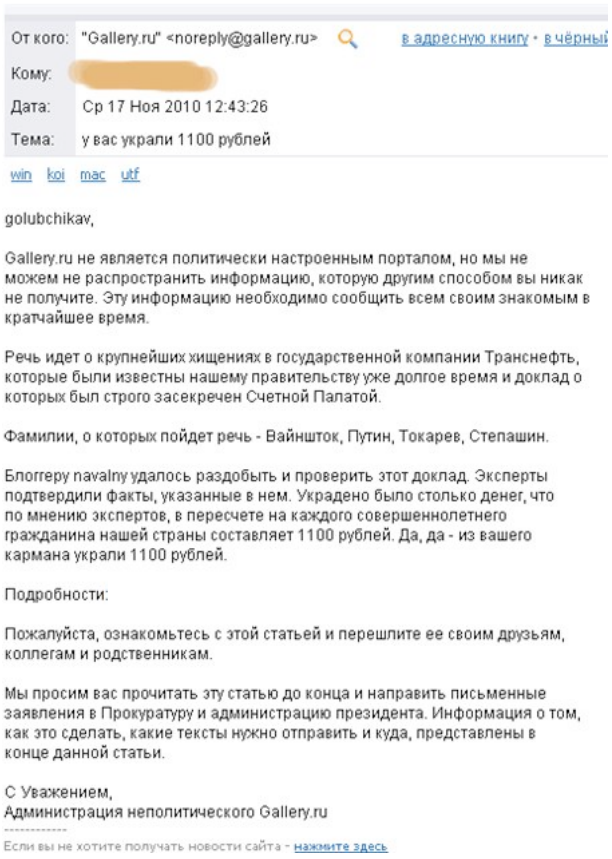
Как спам используется в политических целях

Политический спам
Так называют несанкционированные рассылки на темы, так или иначе связанные с политикой и общественной жизнью. Производятся они самыми разными людьми и предназначены для манипуляции общественным мнением и решения задач заказчиков. В большинстве случаев такие рассылки можно отнести к «черному пиару».

По своему внешнему виду политический спам сильно отличается от обычного. В текстах «политических» рассылок практически не используются характерные для спамеров приемы. С одной стороны, это говорит о том, что заказчики рассылок не считают эти письма спамом. С другой – затрудняет обнаружение таких рассылок с помощью антиспама. В отличие от обычных спам-писем с небольшим объемом текста, политические сообщения чаще всего существенно длиннее.

Какого рода рассылки производят «политические» спамеры?

- **Рассылки с целью давления** на людей или организации, например, с призывами подписать петицию в защиту/против какого-либо лица или компании. Данный вид рассылки может преследовать цель дискредитировать определенных политиков, поэтому такие письма могут содержать ложную информацию. Например, призывы «ко всем честным и неравнодушным людям» забросать заявлениями прокуратуру в поддержку якобы подавляемого государством информационного портала, распространяющего «только правду», и т. д.



От кого: "Gallery.ru" <noreply@gallery.ru> в адресную книгу · в чёрный

Кому: [redacted]

Дата: Ср 17 Ноя 2010 12:43:26

Тема: у вас украли 1100 рублей

win koi mac utf

golubchikav,

Gallery.ru не является политически настроенным порталом, но мы не можем не распространить информацию, которую другим способом вы никак не получите. Эту информацию необходимо сообщить всем своим знакомым в кратчайшее время.

Речь идет о крупнейших хищениях в государственной компании Транснефть, которые были известны нашему правительству уже долгое время и доклад о которых был строго засекречен Счетной Палатой.

Фамилии, о которых пойдет речь - Вайнштоk, Путин, Токарев, Степашин.

Блоггеру navalny удалось раздобыть и проверить этот доклад. Эксперты подтвердили факты, указанные в нем. Украдено было столько денег, что по мнению экспертов, в пересчете на каждого совершеннолетнего гражданина нашей страны составляет 1100 рублей. Да, да - из вашего кармана украли 1100 рублей.

Подробности:

Пожалуйста, ознакомьтесь с этой статьей и перешлите ее своим друзьям, коллегам и родственникам.

Мы просим вас прочитать эту статью до конца и направить письменные заявления в Прокуратуру и администрацию президента. Информация о том, как это сделать, какие тексты нужно отправить и куда, представлены в конце данной статьи.

С Уважением,
Администрация неполитического Gallery.ru

Если вы не хотите получать новости сайта - нажмите здесь

*Стараясь создать нужное общественное мнение, манипуляторы пытаются вызывать **резонансные скандалы**. Так, в Интернете была поднята мощная волна «праведного гнева» в ответ на внесение в реестр запрещенных к просмотру детям до 18 лет фильма «Ну, погоди!». Что же скрывалось за этим фактом на деле? Получивший ограничения «Ну, погоди!» не имеет отношения к советской мультипликации, будучи шведским фильмом категории «для взрослых».*

Рассылки от имени политических организаций и их деятелей

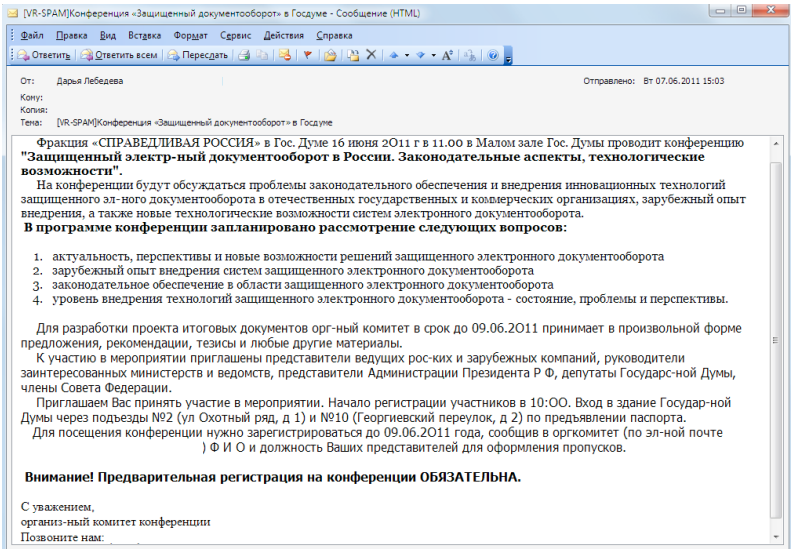
- Первый спам от имени российской политической партии зафиксирован 26 марта 2003 года, когда многие интернет-пользователи получили письмо якобы от «Единой России».
  «Генеральный совет и Центральный исполнительный комитет Партии настоятельно рекомендует организовать на базе Вашего предприятия (организации) первичную партийную ячейку и обеспечить вступление в нее новых членов (не менее 5% от списочного состава сотрудников)...»
  «Учитывая высокую государственную значимость обозначенной задачи, надеемся, что вы со всей ответственностью отнесетесь к ее выполнению и дальнейшей работе на благо нашего Отечества...» и т. д.

Помимо основного текста письмо содержало образец заявления для вступления в ряды «Единой России», а также список адресов и телефонов городских и окружных отделений партии [5].

Представители «Единой России» опровергли свою причастность к этой рассылке и заявили, что от их имени Рунет «заспамили» конкуренты – чтобы подорвать доверие интернет-общественности к «Единой России».

- 26 марта 2003 года, помимо рассылки от имени «Единой России», через электронную почту разослали ряд листовок от имени депутата из фракции «Яблоко». Обратным адресом значился действительный адрес С. Митрохина, а само письмо содержало «предложения о сотрудничестве» и ссылку на персональный сайт депутата.
  В течение 3 дней в адрес партии в массовом порядке поступали возмущенные звонки и письма интернет-пользователей, некоторые из которых получили до 400 одинаковых сообщений.

Рассылки активистов для продвижения их точки зрения


[VR-SPAM]Конференция «Защищенный документооборот» в Госдуме - Сообщение (HTML)

Файл Правка Вид Вставка Формат Сервис Действия Справка

Ответить | Ответить всем | Переслать

От: Дарья Лебедева
Отправлено: Вт 07.06.2011 15:03
Кому:
Копия:
Тема: [VR-SPAM]Конференция «Защищенный документооборот» в Госдуме

Фракция «СПРАВЕДЛИВАЯ РОССИЯ» в Гос. Думе 16 июня 2О11 г в 11.ОО в Малом зале Гос. Думы проводит конференцию **"Защищенный электр-ный документооборот в России. Законодательные аспекты, технологические возможности"**.

На конференции будут обсуждаться проблемы законодательного обеспечения и внедрения инновационных технологий защищенного эл-ного документооборота в отечественных государственных и коммерческих организациях, зарубежный опыт внедрения, а также новые технологические возможности систем электронного документооборота.

В программе конференции запланировано рассмотрение следующих вопросов:

1. актуальность, перспективы и новые возможности решений защищенного электронного документооборота
2. зарубежный опыт внедрения систем защищенного электронного документооборота
3. законодательное обеспечение в области защищенного электронного документооборота
4. уровень внедрения технологий защищенного электронного документооборота - состояние, проблемы и перспективы.

Для разработки проекта итоговых документов орг-ный комитет в срок до 09.06.2О11 принимает в произвольной форме предложения, рекомендации, тезисы и любые другие материалы.

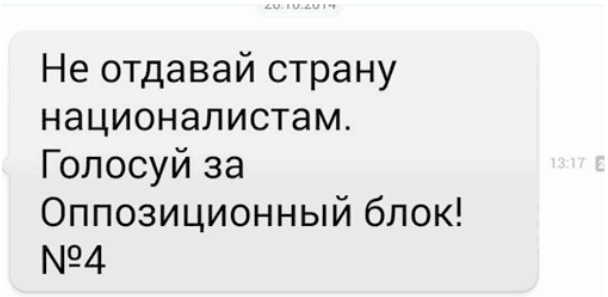
К участию в мероприятии приглашены представители ведущих рос-ких и зарубежных компаний, руководители заинтересованных министерств и ведомств, представители Администрации Президента Р Ф, депутаты Государс-ной Думы, члены Совета Федерации.

Приглашаем Вас принять участие в мероприятии. Начало регистрации участников в 10:ОО. Вход в здание Государ-ной Думы через подъезды №2 (ул Охотный ряд, д 1) и №10 (Георгиевский переулок, д 2) по предъявлении паспорта.

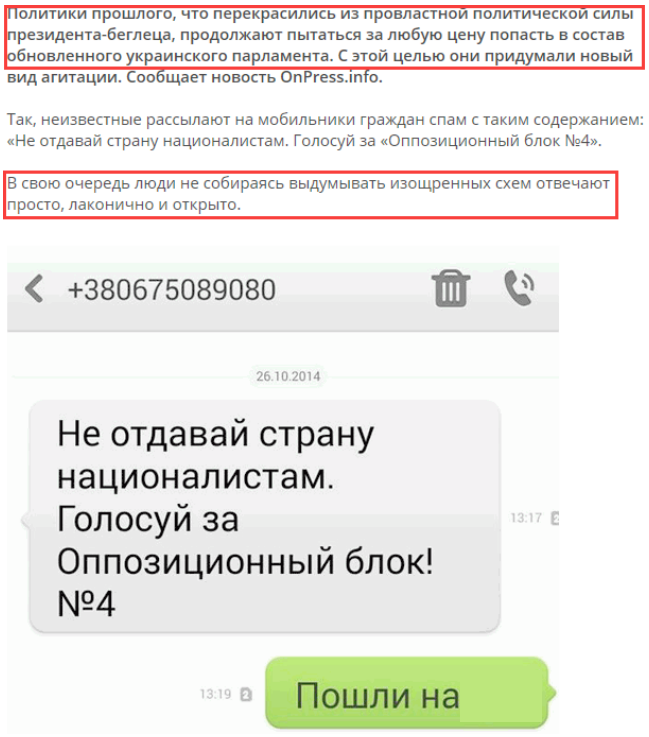
Для посещения конференции нужно зарегистрироваться до 09.06.2О11 года, сообщив в оргкомитет (по эл-ной почте) Ф И О и должность Ваших представителей для оформления пропусков.

Внимание! Предварительная регистрация на конференции ОБЯЗАТЕЛЬНА.

С уважением,
организ-ный комитет конференции
Позвоните нам:

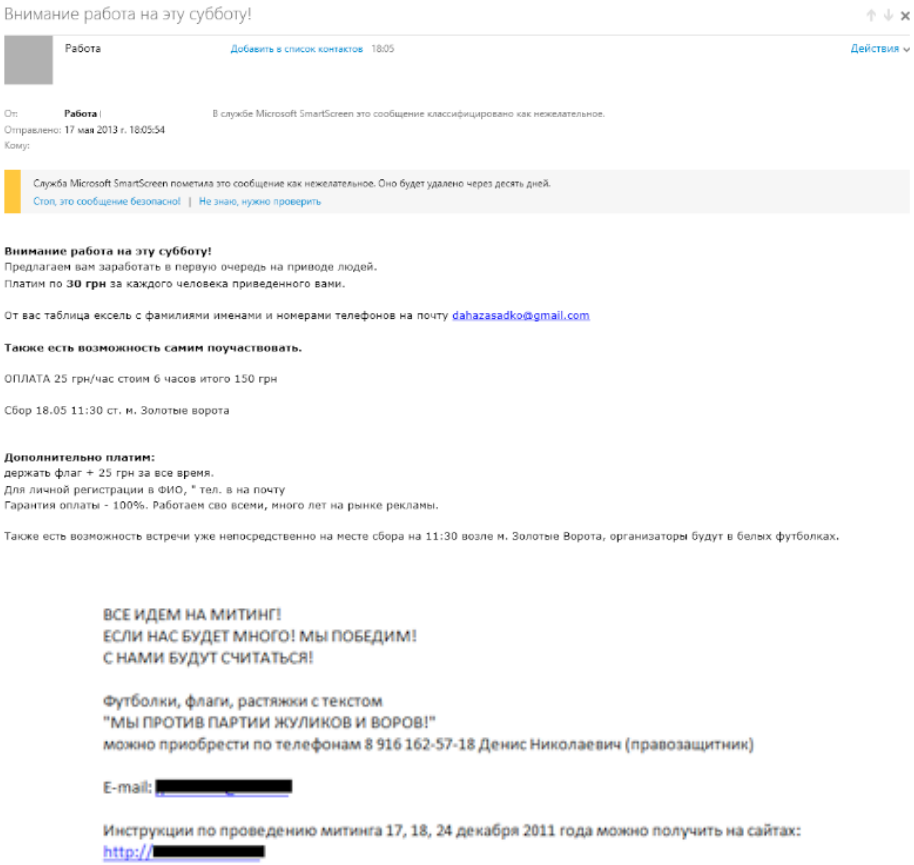


Кто отправил (и отправлял ли) данное сообщение – неизвестно, но вот как оно было использовано:



Рассылки с целью дискредитации (политика-конкурента, страны, правительства и т. д.). Иногда для ответа на спам-обвинения, дискредитирующие организацию или партию, также используются массовые рассылки! Так, например, поступила Интернет-партия Украины в феврале 2012 года. Но не исключено, что она сама и была инициатором первой волны спама...
Рассылки запрещенных организаций – у них нет легальных возможностей для рекламы, поэтому спам для них становится одной из незаконных возможностей напомнить о себе. По понятным причинам мы не приводим примеры таких писем.
Рассылка призывов к действиям – к сбору на (несанкционированный) митинг, неповиновению властям.

Данное сообщение вполне могло быть разослано активистами – или, наоборот, создано их противниками с целью дискредитации этих активистов.



Внимание работа на эту субботу!

Работа Добавить в список контактов 18:05 Действия

От: **Работа** | В службе Microsoft SmartScreen это сообщение классифицировано как нежелательное.
Отправлено: 17 мая 2013 г. 18:05:54
Кому:

Служба Microsoft SmartScreen пометила это сообщение как нежелательное. Оно будет удалено через десять дней.
Стоп, это сообщение безопасно! | Не знаю, нужно проверить

Внимание работа на эту субботу!
Предлагаем вам заработать в первую очередь на приводе людей.
Платим по **30 грн** за каждого человека приведенного вами.

От вас таблица ексель с фамилиями именами и номерами телефонов на почту dahazasadko@gmail.com

Также есть возможность самим поучаствовать.

ОПЛАТА 25 грн/час стоим 6 часов итого 150 грн

Сбор 18.05 11:30 ст. м. Золотые ворота

Дополнительно платим:
держать флаг + 25 грн за все время.
Для личной регистрации в ФИО, * тел. в на почту
Гарантия оплаты - 100%. Работаем сво всеми, много лет на рынке рекламы.

Также есть возможность встречи уже непосредственно на месте сбора на 11:30 возле м. Золотые Ворота, организаторы будут в белых футболках.

ВСЕ ИДЕМ НА МИТИНГ!
ЕСЛИ НАС БУДЕТ МНОГО! МЫ ПОБЕДИМ!
С НАМИ БУДУТ СЧИТАТЬСЯ!

Футболки, флаги, растяжки с текстом
"МЫ ПРОТИВ ПАРТИИ ЖУЛИКОВ И ВОРОВ!"
можно приобрести по телефонам 8 916 162-57-18 Денис Николаевич (правозащитник)

E-mail: [redacted]

Инструкции по проведению митинга 17, 18, 24 декабря 2011 года можно получить на сайтах:
http://[redacted]

Распространение призывов к свержению власти, подстрекательство к неповиновению властям, рассылка порочащей государственные структуры и госчиновников информации караются по закону в соответствии со статьей 280 УК РФ «Публичные призывы к осуществлению экстремистской деятельности».

2. Те же деяния (публичные призывы к осуществлению экстремистской деятельности), совершенные с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет», наказываются принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Внимание! *Если вы поделитесь ссылкой на чужую статью, содержащую клевету, на экстремистское онлайн-издание или книгу либо процитируете чье-то приглашение на несанкционированный митинг, например, на вашей странице «ВКонтакте», вас вполне может ожидать наказание — от штрафа в несколько тысяч рублей до лишения свободы. Это связано с тем, что пост на странице в социальной сети может увидеть неограниченное число лиц. Не имеет значения и то, где и каким образом вы распространили такую информацию, — важен факт вашего участия в ее распространении.*

На примере статьи 280 УК РФ «Публичные призывы к осуществлению экстремистской деятельности» можно продемонстрировать, что даже репост чужой статьи с призывами к экстремизму может считаться публичным призывом. Так, Верховный Суд Российской Федерации в Постановлении Пленума от 28.06.2011 № 11 дал следующее разъяснение:

«4. Под публичными призывами (статья 280 УК РФ) следует понимать **выраженные в любой форме (устной, письменной, с использованием технических средств, информационно-телекоммуникационных сетей общего пользования, включая сеть Интернет) обращения к другим лицам** с целью побудить их к осуществлению экстремистской деятельности».

Репост, т. е. цитирование чужого поста — это сообщение, автором которого являетесь вы. А если автор сообщения вы — значит, и «обращение к другим лицам с целью побудить их к осуществлению экстремистской деятельности» исходит от вас.

А если вашу страницу «ВКонтакте» или блог посещает более трех тысяч пользователей в сутки, то, по законам Российской Федерации, вы являетесь блогером и несете ответственность за то, что пишете сами, **а также за то, что пишут посетители на вашей странице или в блоге.**

Статья закона
Ст. 10.2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Статья 10.2 Особенности распространения блогером общедоступной информации

1. 1. Владелец сайта и (или) страницы сайта в сети «Интернет», на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети «Интернет» (далее — блогер), при размещении и использовании указанной информации, в том числе при размещении указанной информации на данных сайте или странице сайта иными пользователями сети «Интернет», обязан обеспечивать соблюдение законодательства Российской Федерации, в частности:

1) не допускать использование сайта или страницы сайта в сети «Интернет» в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань;

2) проверять достоверность размещаемой общедоступной информации до ее размещения и незамедлительно удалять размещенную недостоверную информацию;

3) не допускать распространение информации о частной жизни гражданина с нарушением гражданского законодательства;

4) соблюдать запреты и ограничения, предусмотренные законодательством Российской Федерации
о референдуме и законодательством Российской Федерации о выборах;

5) соблюдать требования законодательства Российской Федерации, регулирующие порядок распространения массовой информации;

6) соблюдать права и законные интересы граждан и организаций, в том числе честь, достоинство и деловую репутацию граждан, деловую репутацию организаций.

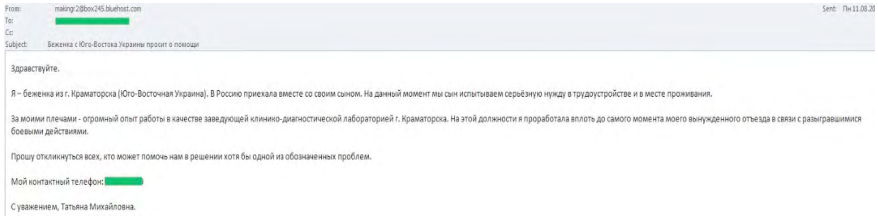
Уголовное законодательство Российской Федерации не разделяет ответственность за оригинальную (авторскую) публикацию и ее перепечатку другими лицами (не авторами оригинального текста) — так называемый репост (цитату) — как с собственным комментарием к распространенной информации, так и без. Отсутствие в репосте вашего отношения к транслируемой ВАМИ информации не освобождает ВАС от ответственности за ее распространение. Даже если вы удалите репост, но его присутствие будет зафиксировано органами правопорядка, вас могут привлечь к ответственности.

- **Спам-рассылки с целью привлечения внимания властей к той или иной проблеме.** Таким образом, соответствующая информация распространяется «вирусным» путем – ее подхватывают и начинают публиковать на своих страницах сами пользователи.

  - *В январе 2003 года США запустили в Интернете кампанию, в рамках которой тем, кто знает что-либо о производстве в Ираке оружия массового поражения, предлагалось пожаловаться по электронной почте «куда следует». Соответствующая «электронная листовка» была разослана по всем доступным иракским электронным адресам. Рассылка была организована государственной организацией США.*
  - *В октябре 2011 была произведена рассылка писем с обращением к премьер-министру РФ В. В. Путину от жителей Брянска – с просьбой наказать виновных в ДТП, в результате которого погибла маленькая девочка, а также рассылка от жителей Калужской области, сетующих на невыполнение местными депутатами обещаний по газификации одного из поселков.*

Спамеры и фишеры тоже оперативно реагируют на общественные события, но, разумеется, используют их в своих целях.

Например, бегство президента Украины и слухи о его богатстве мгновенно породили подвид нигерийского спама, а также рассылку писем с призывами о помощи пострадавшим или о сборе средств для ополченцев.


From: making-2@box245.bluehost.com Sent: Пн 11.08.20
To:
Cc:
Subject: Беженка с Юго-Востока Украины просит о помощи

Здравствуйте.

Я – беженка из г. Краматорска (Юго-Восточная Украина). В Россию приехала вместе со своим сыном. На данный момент мы сын испытываем серьёзную нужду в трудоустройстве и в месте проживания.

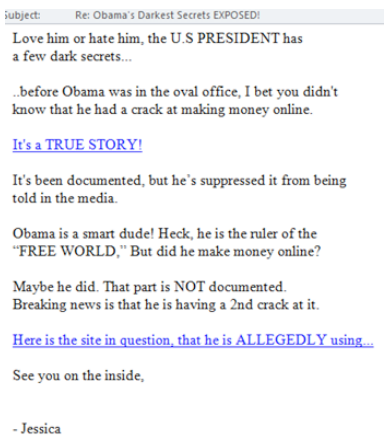
За моими плечами - огромный опыт работы в качестве заведующей клинико-диагностической лабораторией г. Краматорска. На этой должности я проработала вплоть до самого момента моего вынужденного отъезда в связи с разыгравшимися боевыми действиями.

Прошу откликнуться всех, кто может помочь нам в решении хотя бы одной из обозначенных проблем.

Мой контактный телефон:

С уважением, Татьяна Михайловна.

Используют мошенники и чрезмерное любопытство людей, желающих узнать какие-то «жареные факты» из жизни политиков.


Subject: Re: Obama's Darkest Secrets EXPOSED!

Love him or hate him, the U.S PRESIDENT has a few dark secrets...

..before Obama was in the oval office, I bet you didn't know that he had a crack at making money online.

It's a TRUE STORY!

It's been documented, but he's suppressed it from being told in the media.

Obama is a smart dude! Heck, he is the ruler of the "FREE WORLD," But did he make money online?

Maybe he did. That part is NOT documented.
Breaking news is that he is having a 2nd crack at it.

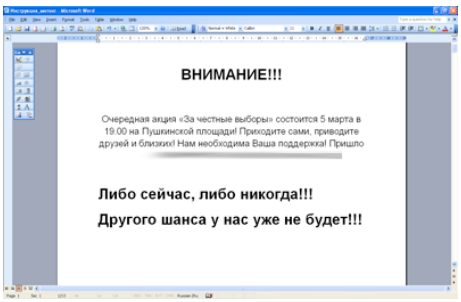
Here is the site in question, that he is ALLEGEDLY using...

See you on the inside,

- Jessica

Используют преступники политический спам и для заражения компьютеров или кражи данных у пользователей.

- *5 марта 2012 года специалисты «Доктор Веб» зафиксировали массовую почтовую рассылку с призывами принять участие в протестном митинге оппозиции на Пушкинской площади в Москве. Почтовые сообщения с темой «**Митинг Честные выборы**» или «**Все на митинг**» содержали короткий текст, например: «Внимательно изучи инструкцию что необходимо будет делать на этом митинге», «Митинг против Путина. Внимательно прочитай инструкцию» или «Очень важно чтобы ты изучил инструкции, на этом митинге все будут действовать по этому сценарию», а также вложенный документ Microsoft Word с именем **Инструкция_митинг.doc**.*



Данный документ включал в себя несколько макросов, которые в момент открытия файла в текстовом редакторе сохраняли на диск и запускали на исполнение троянскую программу **Trojan.KillFiles.9055**, *предназначенную для выведения из строя системы Windows.*
http://news.drweb.ru/show/?c=5&i=2272&lng=ru

Не исключено, что спамеры, исполняя заказ на распространение некой информации, могут иметь и свой интерес – заражение компьютеров.

- *Троянец Android.Arspam.1 встроен в легитимное приложение AlSalah, предназначенное для мусульман и реализующее функции компаса, который с помощью GPS-координат абонента определяет направление на Мекку и расстояние до нее. Стартовав на инфицированном устройстве, Android.Arspam.1 собирает перечень контактов, сохраненных в адресной книге мобильного устройства, и рассылает каждому из них одну из ссылок на интернет-форумы, посвященные политическим событиям на Ближнем Востоке.*

Интересно, что троянец содержится только в версии программы, распространяемой на арабоязычных форумах.
http://news.drweb.com/show/?c=5&i=2119&lng=ru

Как вас заставляют читать спам и переходить по ссылкам в нем. Психологические уловки спамеров и фишеров

Главная цель спамеров — вынудить жертву совершить запланированное ими действие. Злоумышленники пытаются вызвать получателя письма на диалог, заставить задуматься над прочитанным и одновременно притупить чувство осторожности. Для них важно, чтобы у вас не возникло желания выбросить письмо в корзину.

Главная опасность спама и фишинга заключается в том, что на удочку может попасться КАЖДЫЙ — и неопытный школьник, и убеленный сединой профессор.

При составлении спам-сообщений, преступники используют:
- технологии «социальной инженерии»;
- знание психологии, в том числе психологии толпы;
- разного рода манипуляции (зацепки) — лингвистические и визуальные;
- предсказуемые стандартные реакции человека на возбудители (информационные, психологические и т. д.), а именно – страх, сострадание, альтруизм, тревогу, готовность поддержать, доверчивость, глупость, радикальные выпады, жалость, чувство уязвимости, надежду на развитие ситуации по сценарию жертвы;
- моделирование ситуаций из жизни, которые по полученной статистике дали максимальный эффект нужных реакций со стороны жертв;
- незнание (когда жертва не разбирается в вопросе), в том числе бытовую неграмотность, отсутствие опыта в той или иной сфере;
- желание попробовать новое (достичь новых результатов, успеха);
- унижение как инструмент влияния – взывают к раскрепощенности, свободе и указывают на то, что «это пробуют сейчас все», опираясь на «отсталость» и «никчемность», поднимая на смех жертву и тем самым стимулируя ее стремление стать как все (т. е. лучше, чем сейчас).

Очень часто спамеры и фишеры используют те же методы, которые применяются для вербовки в секты и преступные сообщества, включая террористические и экстремистские организации:
- убеждают в том, что жизнь после покупки станет счастливей/легче/радостней;
- указывают на единственно верный «путь спасения»;
- призывают «стать свободным», не объясняя от чего и как именно;

- приглашают воссоединиться с теми, кто уже «излечился» или «озарен»;
- предлагают «стать частью людей, не знающих отныне проблем» (сомнений);
- обещают избавить от одиночества (а заодно и от излишних благ), манипулируя верой в Бога;
- соблазняют воспользоваться «многовековой мудростью»;
- призывают опереться на того, кто знает, что делает, и приведет к однозначно «спасительному результату»;
- сулят постоянную поддержку «собратьев»;
- советуют расстаться «с материальным» и со всем «гнетущим свободу духовную и телесную»;
- отрезают от семьи и близких, подменяя их своим «мессией, которому отныне надо довериться»;
- предлагают «обрести властвование над тем, что дано лишь избранным», по сути призывают (провоцируют) «стать избранным»;
- подстрекают защитить «избранных» — таких же, как и предполагаемая жертва;
- призывают освободиться, осознанно «став жертвой», а точнее – «героем», получив вечную славу в глазах потомков.

Чаще всего жертвами атак спамеров становятся:

- неуверенные в себе люди, зависимые от чужого (навязываемого) мнения, с пониженным уровнем психологической защиты и повышенной внушаемостью;
- люди с неустойчивыми взглядами, без фундаментальных жизненных ценностей и морально-этических принципов;
- находящиеся в сложных социально-экономических обстоятельствах, отчаянии или депрессии;
- находящиеся в стрессе или сильно уставшие физически;
- чрезмерно расслабившиеся — например, на отдыхе, когда из любопытства не лень ткнуть в заинтересовавшую картинку в спам-сообщении и купить предлагаемый товар, сделать ставку в онлайн-казино (чтобы испытать новые ощущения);
- страдающие от одиночества, испытывающие потребность в участии, сострадании, сочувствии;
- находящиеся в поиске любви или же не получающие тепла и нуждающиеся в нем (опираясь на мысль, что «такие, как я, пользуются этим продуктом/услугой»);
- ставящие вопреки всему на первое место друзей, пусть даже случайных (одержимость дружбой и тяга к ней);

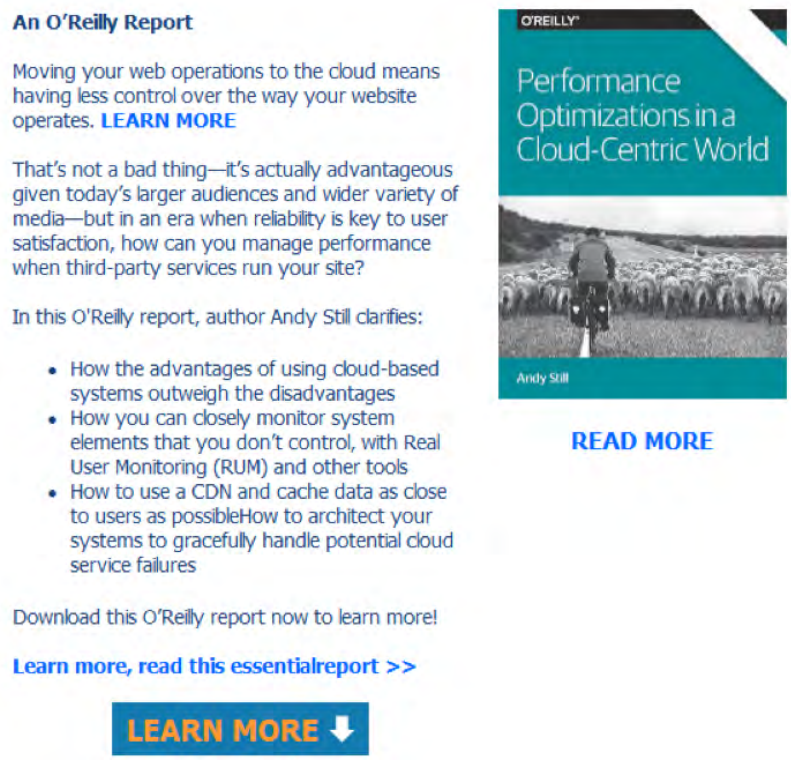
- испытывающие постоянную потребность в новых знаниях (при одновременном отрицании старых как «немодных», а не потому, что они перестали быть актуальными);
- стремящиеся угнаться за модой (популярным течением, явлением, методикой, лекарством и т. д.), быть «в тренде»;
- не желающие самостоятельно искать (вырабатывать) ответы на жизненные вопросы, стремящиеся жить по готовым (чужим) рецептам, по канонам стандартизированного потребления, не способные к критической оценке поступающей информации, а значит – к принятию самостоятельного решения.

Таким людям надо быть очень осторожными при любых интернет-контактах с незнакомцами, они – в зоне повышенного риска.

Сущность спамера

Кто именно действует на темной «спамерской» стороне? Как правило, это люди без общепринятых морально-этических принципов. Они прекрасно осознают, что занимаются незаконным бизнесом – совершают преступление. Они действуют осознанно, а значит – без здоровых эмоций, в большинстве случаев хладнокровно.

Спамер или фишер – это человек, относящийся к своим жертвам как к расходному материалу или, образно говоря, как к овцам в загоне.



Все овцы покорно должны следовать туда, куда их направляет хозяин. Так и жертвы, следуя по определенному пути (например, по ссылкам), приводят спамера к обогащению. Пока спамер управляет вашим сознанием – он ваш хозяин, который преследует лишь свои корыстные и порой крайне жестокие цели. И для него не важно, ребенок перед монитором или зрелый человек, инвалид или подросток, женщина или старик – любые жертвы годятся, если приносят доход злоумышленнику.

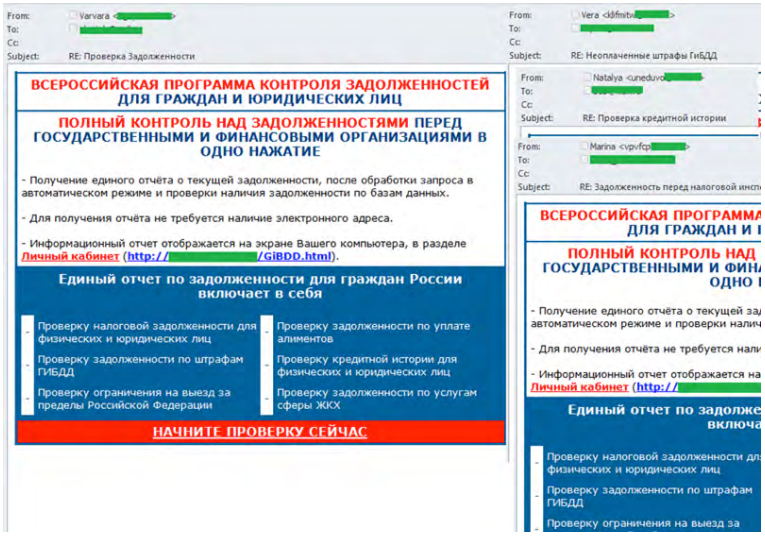
Спамер всегда обогащается за счет других.

Он считает себя самым умным и по этой причине, по его мнению, не должен быть бедным. Спамер применяет все новые способы манипуляции, используя свой «интеллект» в сочетании со слабостями других людей. Отношение спамеров к жертвам можно условно разделить на две категории – хладнокровное и особо жестокое. Хладнокровные спамеры «всего лишь» зарабатывают деньги и не стремятся специально навредить жертве. Особо жестокие готовы вывернуть вас наизнанку, оставить ни с чем и ни с кем. Чем хуже вам, тем лучше им.

После кражи персональных данных с сайта знакомств с целью измены Ashley Maddison и публикации шантажистами части информации об интимных подробностях ряда пользователей несколько человек покончили жизнь самоубийством.

Какие слабости используют спамеры

Страх – с помощью угроз или сведений, вызывающих тревогу. Например, они информируют о закрытии банковских счетов, вызове в суд или налоговую, уведомляют о штрафе. Такие письма особенно сильно пугают людей в сезон отпусков, когда из-за неуплаченного штрафа есть вероятность, что вас не выпустят из страны, и потому пропадут путевки и билеты. **Запугивание вызывает у жертвы потребность устранить причину дискомфорта**, исправить ситуацию, разобраться в том, что произошло (например, ввести свой телефонный номер, чтобы получить код разблокировки счета и устранить проблему).



Например, в этом письме содержались три ссылки, которые перенаправляли пользователя на один и тот же мошеннический сайт, где под предлогом проверки задолженности требовалось зарегистрироваться и ввести не только свои контактные данные и Ф.И.О., но и номер паспорта, ИНН, а также номер автомобиля и свидетельства о его регистрации. От юридических лиц требовали данные об организации. Таким образом, мошенники собирали информацию о гражданах РФ, которая в дальнейшем могла бы быть использована для различных махинаций.

Вот несколько тем, с помощью которых спамеры оказывают психологическое давление на получателя (для побуждения к действию):

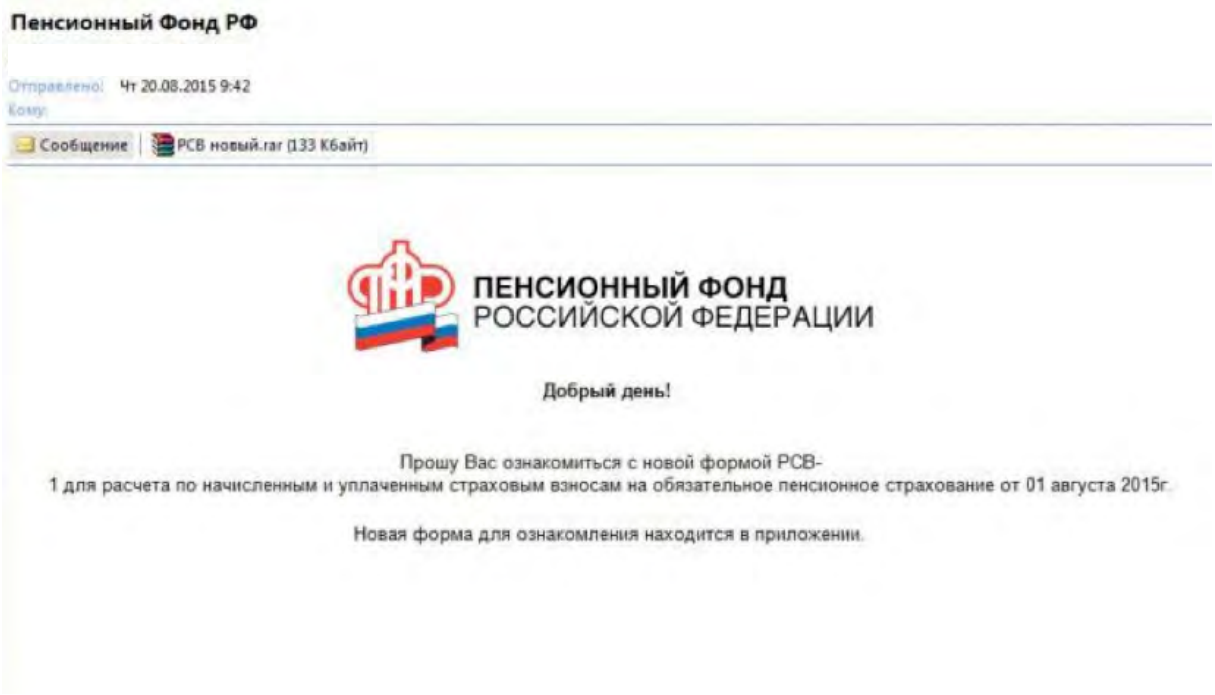
- если вы не ответите в течение ближайших 48 часов, ваша учетная запись будет заблокирована;
- ваш ящик будет заблокирован, если вы не отправите СМС-сообщение на указанный номер;
- ваш ящик будет удален, если вы не подтвердите свою активность с помощью отправки СМС-сообщения;
- ваш ящик замечен в рассылке спама, и для того, чтобы его не заблокировали, необходимо отправить СМС-сообщение;
- подтвердите свою учетную запись.

Как противостоять запугиваниям

- Перечитайте сообщение через час, а лучше на следующий день, когда первый испуг пройдет – что называется, «на трезвую голову». Оно покажется вам уже не таким пугающим, а значит, вы сможете реагировать на текст послания здраво, без эмоций.
- Помните, что легитимные организации никогда не запрашивают по электронной почте пароли, имена пользователей, номера социального страхования и любые другие личные сведения. Поэтому, если у вас требуют такие данные, просто не реагируйте на такое сообщение.
- Не паникуйте. Просто позвоните в компанию, от имени которой пришло тревожное сообщение (воспользовавшись ее **официальными** контактными данными), и выясните, что произошло. Скорее всего, поводов для беспокойства не окажется.
- Вы можете задать соответствующие вопросы администрации почтового сервиса или службе техподдержки проекта, о котором идет речь в спаме (но при этом не используйте ссылки из полученного сообщения).

Дисциплинированность, послушность (упор делается на воспитанность, убеждения, опыт жертвы) — потребность следовать полученной инструкции (например, немедленно заплатить штраф или установить предлагаемую программу).

В августовской рассылке 2015 года якобы от имени Пенсионного фонда РФ вложение содержало троянца. Если на компьютере не был установлен антивирус или же если он еще не знал этого троянца – заражение было неминуемо.

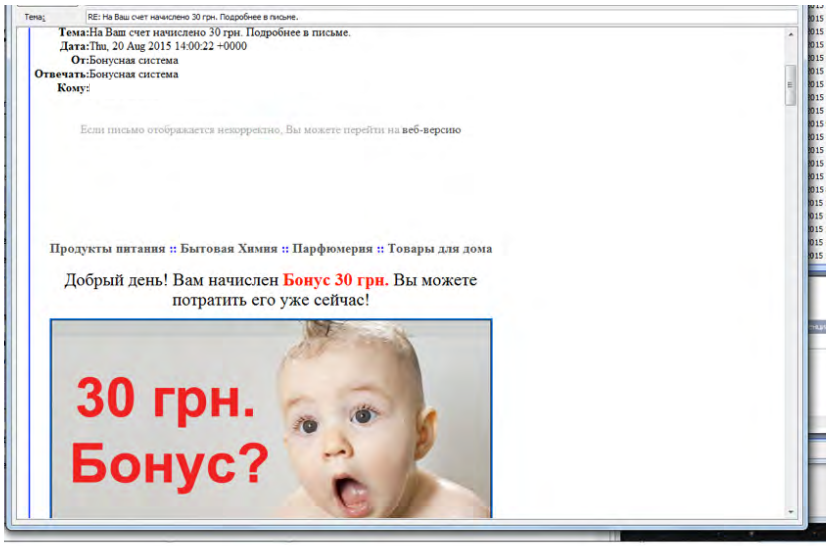


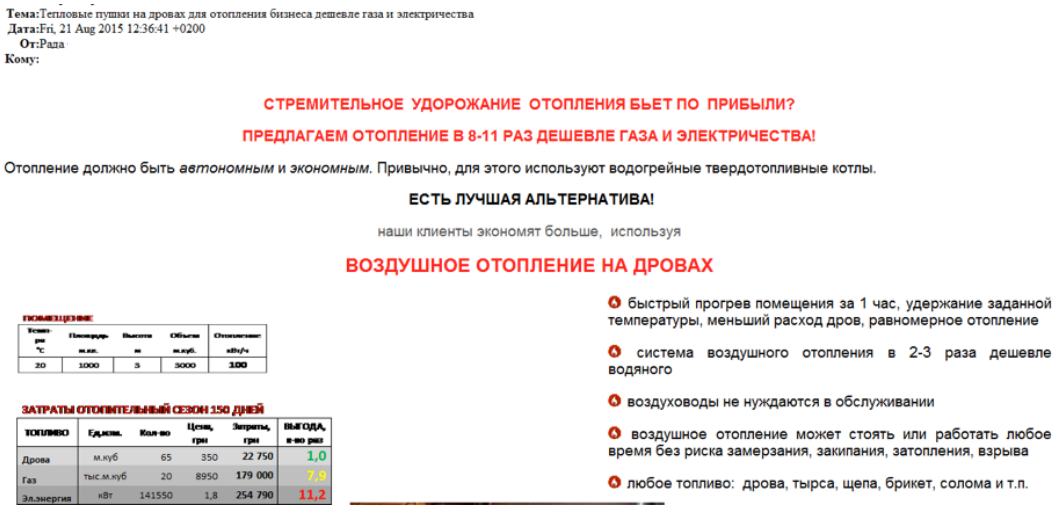
Источник: http://newsprom.ru/news/Proisshestvija/213829.html

Как противостоять

- Если полученное вами сообщение действительно каким-то образом связано с вашей работой или содержит информацию, которая вам может быть интересна (например, информация о пенсии или авиабилетах вполне может вызывать интерес), найдите альтернативный источник данных по этому вопросу: зайдите на официальный сайт Пенсионного фонда или авиакомпании.

Эмоциональный порыв – например, желание поучаствовать в выгодной акции или распродаже, обрести эмоциональную гармонию (основной мотив: «Я просто не могу это пропустить!»).

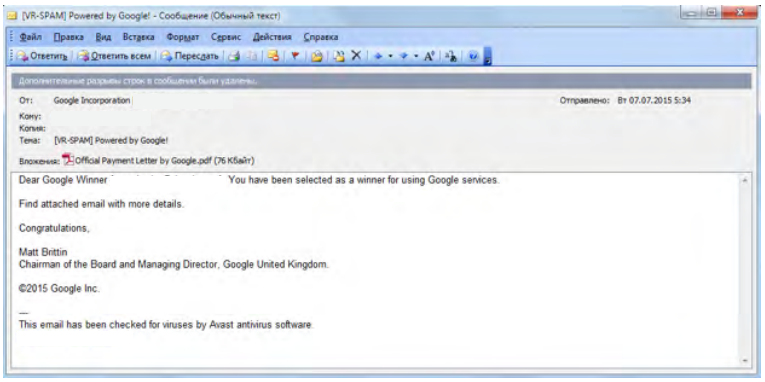




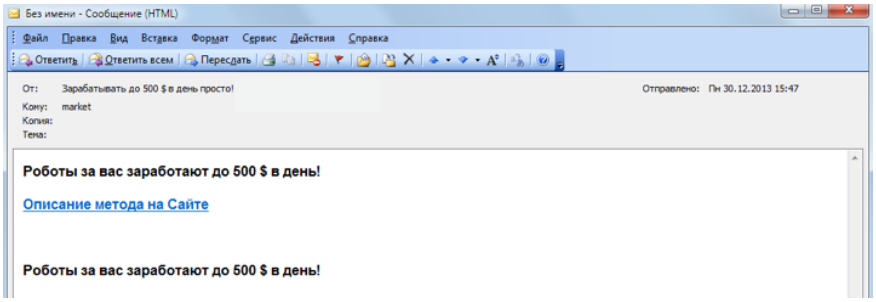
Как противостоять

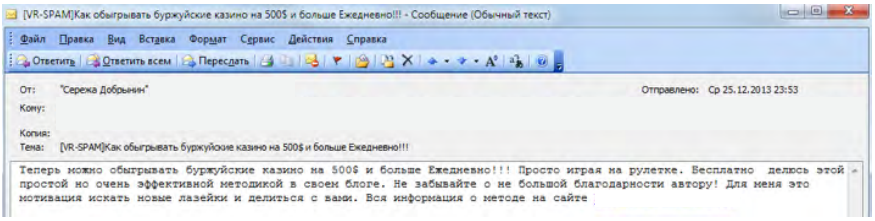
- Не обнадеживайте себя – для начала просто проверьте информацию по другим источникам.
- Старайтесь рассуждать здраво и отдавайте себе отчет в том, что на данный момент у вас нет проблем, но они могут появиться, если вы воспользуетесь полученным «предложением».

Потребность в везении, ощущении себя успешной личностью – стремление к большой денежной выгоде с минимальными усилиями или вовсе без них. Как вариант, в спам-сообщении может сообщаться о победе в каком-либо конкурсе, лотерее или об утверждении кандидатуры получателя на высокооплачиваемую должность. И требуется всего ничего – пройти по ссылке на сайт и ввести необходимые данные. Чтобы вынудить человека немедленно перейти на сайт для получения выигрыша, фишеры сообщают об ограниченном сроке действия предложения. Итогом для жертвы станет либо потеря денег, либо утечка логинов и паролей, которые окажутся в руках мошенников.



Зарабатывать миллионы и при этом почти ничего не делать – это, конечно, заманчво:

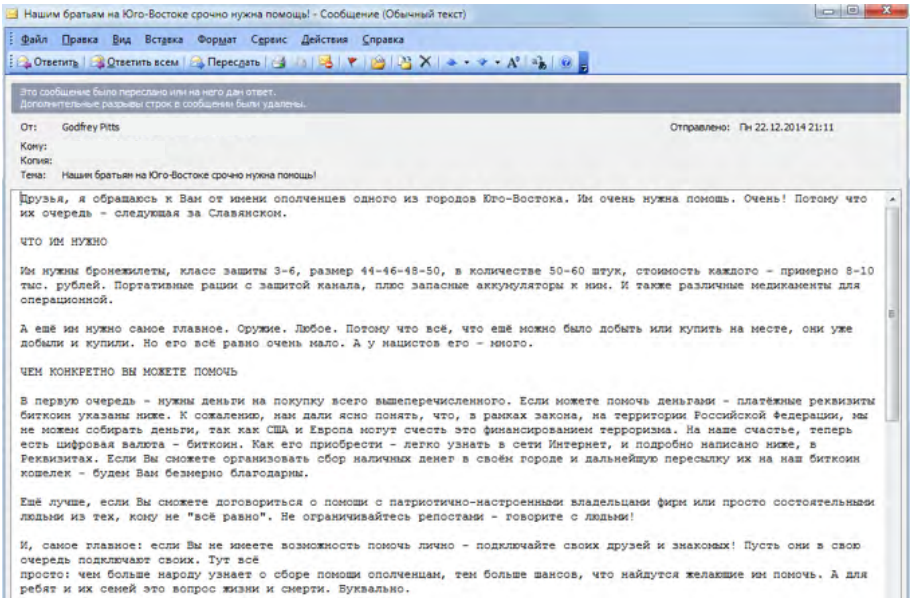




Как противостоять

- Помните о риске стать одной из многочисленных «овец» (спамеры делают миллионы именно на массовых рассылках) и о том, что «бесплатный сыр» может привести к отравлению, дорогому лечению, другим сопуствующим проблемам и даже к летальному исходу (Ashley Madisson, БАДы, наркотики).
- Настоящий работодатель не сможет выйти сразу на вас, поскольку не читает ваши мысли, а вот спамер, обладая всего лишь вашим электронным адресом, может получить неплохой куш и создать вам множество неприятностей вплоть до потери потенциальной возможности получить высокооплачиваемую должность или даже увольнения с нынешней работы (завалив ваш рабочий почтовый ящик своим спамом).

Сочувствие и сострадание также эксплуатируются мошенниками.

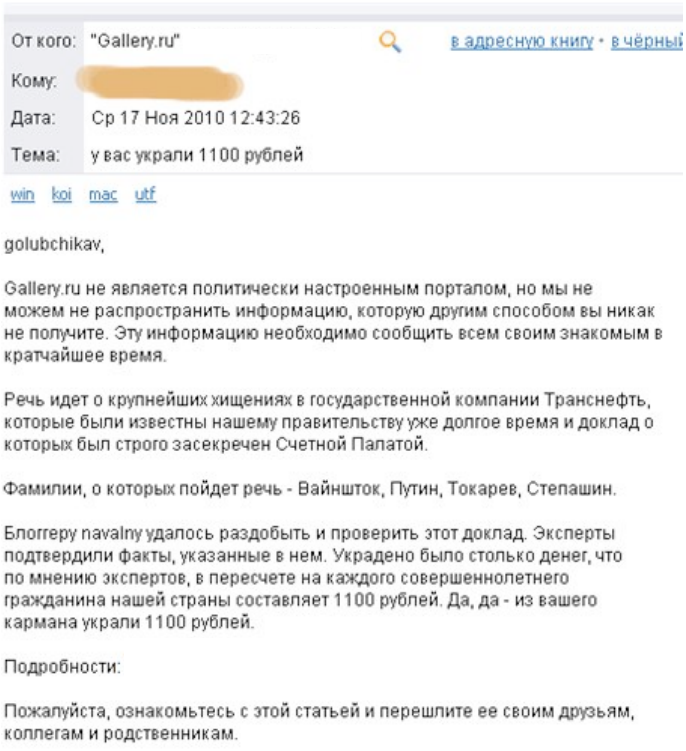


В таких случаях сообщение сопровождается просьбой разослать его всем, кому только можно. И обратите внимание: в приведенном выше письме никакой информации о волонтерах нет – присутствует только номер кошелька для перечисления денег.

Как противостоять

- Если и принимать подобные предложения, то только от официальных организаций, которые ручаются за достоверность информации (имеют проверенные юристами документы и т. п.) и держат в курсе о дальнейшем развитии ситуации (например, в случае помощи больным).
- Удостоверьтесь, что после перечисления ваших средств сумма, заявленная как необходимая, уменьшилась как минимум в соответствии с вашим взносом!
- Не верьте информации, не подкрепленной никакими доказательствами.
- Не реагируйте на слезы на фотографиях или видео, а также на необходимость перечислить деньги срочно – для вымогателей это обычный ход, преследующий цель вывести вас из стабильного эмоционального состояния и склонить к принятию убыточного решения.
- Мыслите рационально и логично – это поможет вам принять решение, которое не вступит в конфликт с вашим внутренним Я.

Задетые политические взгляды/религиозные убеждения – у жертвы это вызывает не только возмущение, но и потребность его выразить, перейдя на предлагаемую страницу.



От кого: "Gallery.ru" в адресную книгу • в чёрный

Кому: [redacted]

Дата: Ср 17 Ноя 2010 12:43:26

Тема: у вас украли 1100 рублей

win koi mac utf

golubchikav,

Gallery.ru не является политически настроенным порталом, но мы не можем не распространить информацию, которую другим способом вы никак не получите. Эту информацию необходимо сообщить всем своим знакомым в кратчайшее время.

Речь идет о крупнейших хищениях в государственной компании Транснефть, которые были известны нашему правительству уже долгое время и доклад о которых был строго засекречен Счетной Палатой.

Фамилии, о которых пойдет речь - Вайншток, Путин, Токарев, Степашин.

Блоггеру navalny удалось раздобыть и проверить этот доклад. Эксперты подтвердили факты, указанные в нем. Украдено было столько денег, что по мнению экспертов, в пересчете на каждого совершеннолетнего гражданина нашей страны составляет 1100 рублей. Да, да - из вашего кармана украли 1100 рублей.

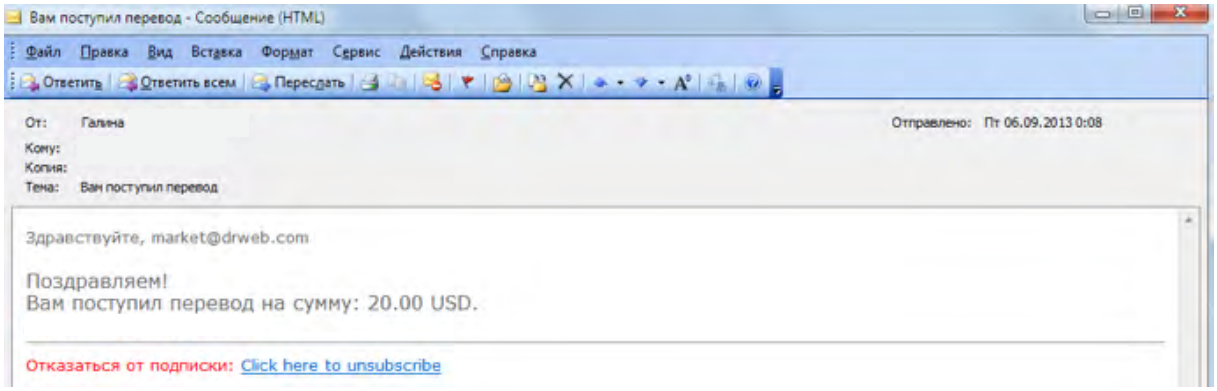
Подробности:

Пожалуйста, ознакомьтесь с этой статьей и перешлите ее своим друзьям, коллегам и родственникам.

Как противостоять

- Если вы принимаете на свой счет чужие дискуссии в отношении веры или политики и реагируете на них – это может говорить о психологических проблемах, в скрытых мотивах которых вам необходимо разобраться, хотя бы для того, чтобы не стать жертвой мошенников, – обратитесь к психологу.
- Оставайтесь эмоционально стабильны в вере и внутренних убеждениях, не ищите посредников и помощников в их выражении.
- Не стремитесь к высказыванию агрессивной или радикальной точки зрения о религии или политике: это вредит всем участникам дискуссии, а пользу может принести только мошенникам.
- Старайтесь принимать чужие убеждения как позицию, которая имеет право на существование и при этом не заслуживает бурных и тем более агрессивных эмоций с вашей стороны.
- Сдерживайте любые эмоции, так как спамеры намеренно пытаются играть на ваших чувствах, чтобы добиться своих целей.

Невнимательность, беспечность – склонность нажимать на все кнопки без разбора, следовать любым «советам», участвовать в любых акциях.

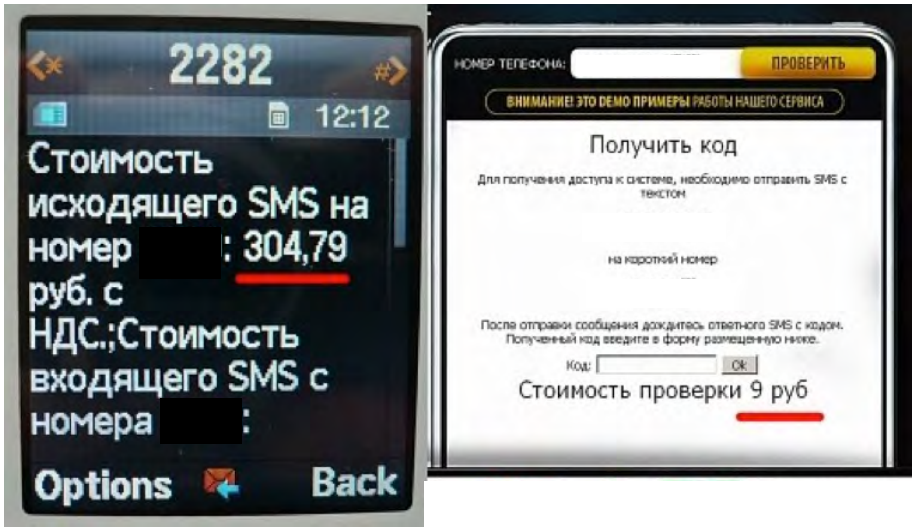


Как противостоять

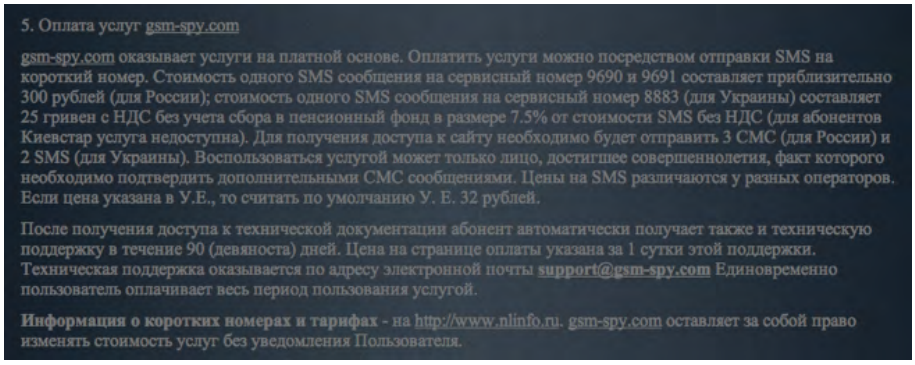
- Старайтесь больше внимания уделять своей безопасности – не реагируйте на «заманчивые предложения», отдавая себе отчет в том, что вас просто используют.
- Если вы получаете почту или сообщение от неизвестного адресата, исходите из того, что с вероятностью 50% это может быть спам, это позволит вам быть менее уязвимым.
- Иногда письма приходят по ошибке, либо же создается впечатление, что письмо попало к вам случайно, а на самом деле адресовано вашему коллеге. Прежде чем переслать такое письмо истинному адресату, убедитесь, что это не спам.

Любопытство – в этом случае уязвимы те, у кого есть потребность все время узнавать новое – их провоцируют разными способами: намекают, что о данном предложении все остальные уже давно в курсе, упирают на необычность либо же доступность предлагаемого товара или услуги, соблазняют возможностью узнать чужие секреты.

Не так давно мошенники рассылали спам-сообщения, в которых предлагалось воспользоваться средством для чтения чужих СМС или «уязвимостью», благодаря которой можно узнать пароль другого пользователя. Для этого предлагалось, например, выслать на определенный адрес логин будущей жертвы, а также свой пароль, либо установить некую программу. В результате – никаких секретов, а лишь заражение компьютера, хищение данных или денег.



http://www.mobile-review.com/articles/2009/mob-detector.shtml
Если прочесть пользовательское соглашение (в случае его наличия, конечно), мелкими буквами изложенное на сайте мошенников, то станет ясно, что все это – некая игра, и, естественно, никакой ответственности за результат никто не несет. И не стоит удивляться, что стоимость СМС-сообщения, которое требуется отправить для получения доступа к «игре», по факту оказывается намного выше заявленной...


5. Оплата услуг gsm-spy.com

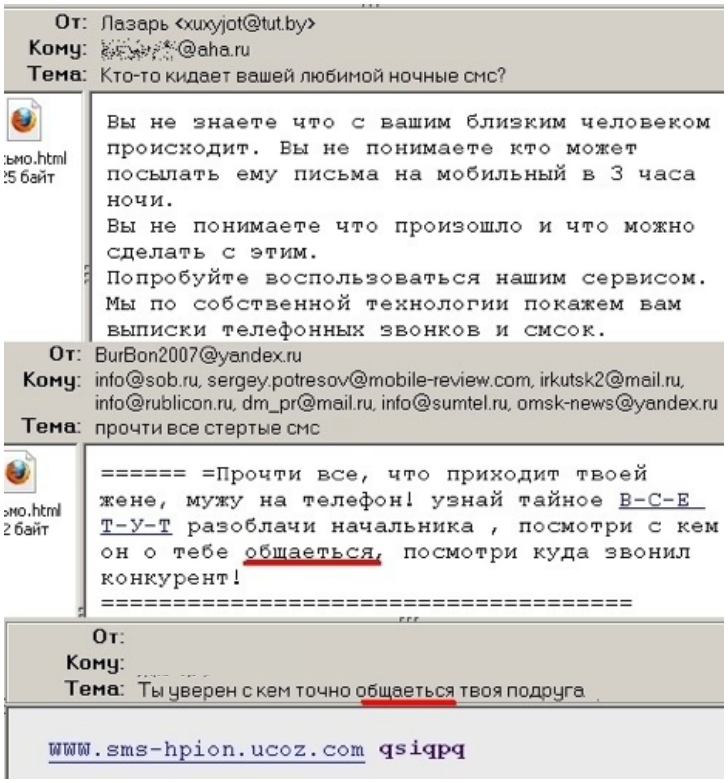
gsm-spy.com оказывает услуги на платной основе. Оплатить услуги можно посредством отправки SMS на короткий номер. Стоимость одного SMS сообщения на сервисный номер 9690 и 9691 составляет приблизительно 300 рублей (для России); стоимость одного SMS сообщения на сервисный номер 8883 (для Украины) составляет 25 гривен с НДС без учета сбора в пенсионный фонд в размере 7.5% от стоимости SMS без НДС (для абонентов Киевстар услуга недоступна). Для получения доступа к сайту необходимо будет отправить 3 СМС (для России) и 2 SMS (для Украины). Воспользоваться услугой может только лицо, достигшее совершеннолетия, факт которого необходимо подтвердить дополнительными СМС сообщениями. Цены на SMS различаются у разных операторов. Если цена указана в У.Е., то считать по умолчанию У. Е. 32 рублей.

После получения доступа к технической документации абонент автоматически получает также и техническую поддержку в течение 90 (девяноста) дней. Цена на странице оплаты указана за 1 сутки этой поддержки. Техническая поддержка оказывается по адресу электронной почты support@gsm-spy.com Единовременно пользователь оплачивает весь период пользования услугой.

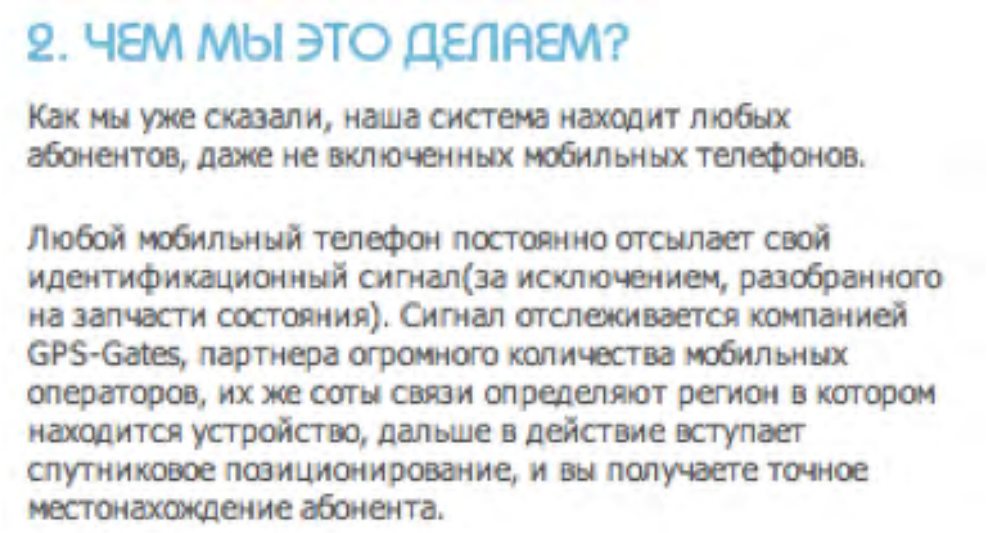
Информация о коротких номерах и тарифах - на http://www.nlinfo.ru. gsm-spy.com оставляет за собой право изменять стоимость услуг без уведомления Пользователя.

http://olyapka.ru/2009/12/sms-razvody

Аналогично действуют мошенники, предлагающие узнать содержимое чужой почты. Они предлагают свои «услуги» по взлому паролей к почтовым ящикам или сообщают о наличии некой уязвимости, позволяющий получить пароль от любого почтового аккаунта, выслав на указанный «системный» адрес (обычный ящик, владельцем которого является мошенник) свой пароль и ответ на секретный вопрос. Таким образом якобы можно обмануть систему и получить не свой пароль, а чужой. При этом, естественно, просят предоплату в виде платной СМС, и конечно, чужого пароля вам не видать, а вот ваш собственный – уплывет в Сеть.



http://www.mobile-review.com/articles/2009/mob-detector.shtml



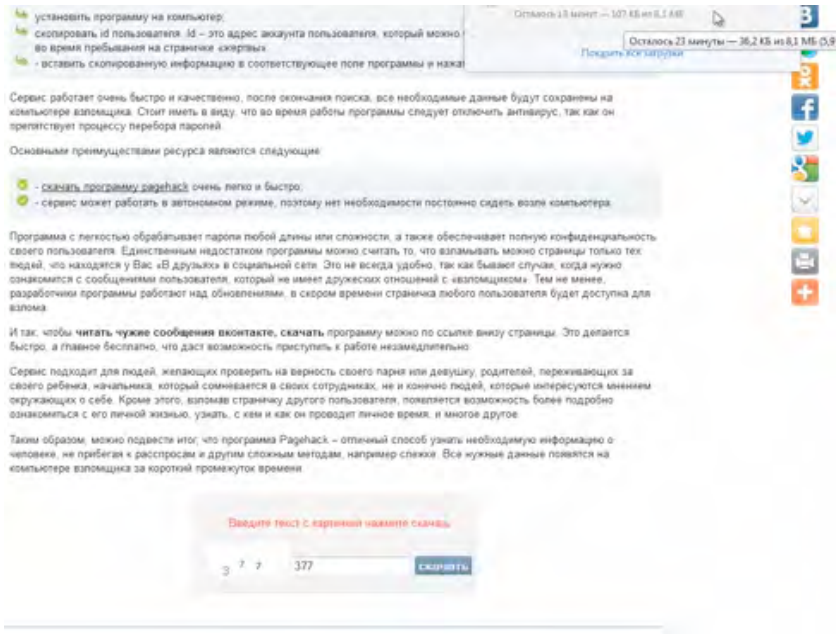
2. ЧЕМ МЫ ЭТО ДЕЛАЕМ?

Как мы уже сказали, наша система находит любых абонентов, даже не включенных мобильных телефонов.

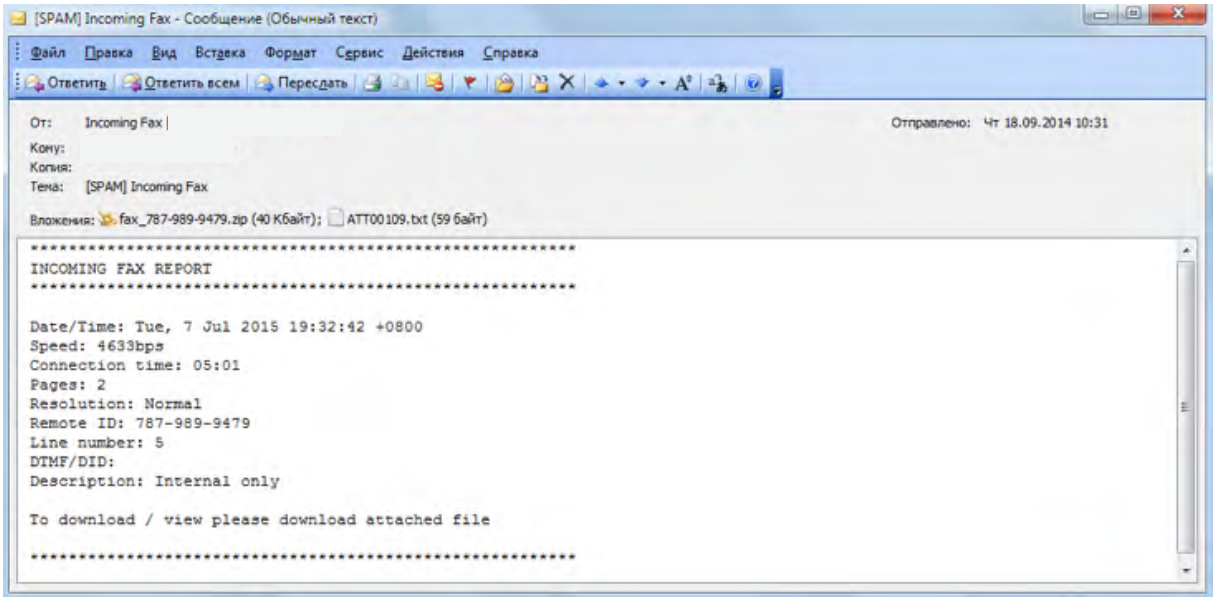
Любой мобильный телефон постоянно отсылает свой идентификационный сигнал(за исключением, разобранного на запчасти состояния). Сигнал отслеживается компанией GPS-Gates, партнера огромного количества мобильных операторов, их же соты связи определяют регион в котором находится устройство, дальше в действие вступает спутниковое позиционирование, и вы получаете точное местонахождение абонента.

http://olyapka.ru/2009/12/sms-razvody

Многих волнует, с кем переписывается «ВКонтакте» их вторая половинка (или ребенок), с какими «одноклассниками» общается. Спам-предложений взлома аккаунтов социальных сетей гораздо больше, чем всего остального, ведь многие даже не подозревают, что есть Интернет и вне «Фейсбука», «Твиттера» и прочих соцсетей! В дополнение к вышеописанным вариантам мошенники предлагают внести в файл host специальные адреса, которые якобы позволят управлять любым аккаунтом того или иного ресурса. В результате мошенники получат пароль доверчивого пользователя, когда он попытается авторизоваться уже не на настоящей странице, а на фишинговой копии социальной сети.


установить программу на компьютер;
скопировать id пользователя. Id – это адрес аккаунта пользователя, который можно
во время пребывания на страничке «жертвы»
- вставить скопированную информацию в соответствующее поле программы и нажа
Осталось 23 минуты — 36,2 КБ из 8,1 МБ (5,9
Сервис работает очень быстро и качественно, после окончания поиска, все необходимые данные будут сохранены на компьютере взломщика. Стоит иметь в виду, что во время работы программы следует отключить антивирус, так как он препятствует процессу перебора паролей.
Основными преимуществами ресурса являются следующие:
- скачать программу pagehack очень легко и быстро;
- сервис может работать в автономном режиме, поэтому нет необходимости постоянно сидеть возле компьютера.
Программа с легкостью обрабатывает пароли любой длины или сложности, а также обеспечивает полную конфиденциальность своего пользователя. Единственным недостатком программы можно считать то, что взламывать можно страницы только тех людей, что находятся у Вас «В друзьях» в социальной сети. Это не всегда удобно, так как бывают случаи, когда нужно ознакомится с сообщениями пользователя, который не имеет дружеских отношений с «взломщиком». Тем не менее, разработчики программы работают над обновлениями, в скором времени страничка любого пользователя будет доступна для взлома.
И так, чтобы **читать чужие сообщения вконтакте, скачать** программу можно по ссылке внизу страницы. Это делается быстро, а главное бесплатно, что даст возможность приступить к работе незамедлительно.
Сервис подходит для людей, желающих проверить на верность своего парня или девушку, родителей, переживающих за своего ребенка, начальника, который сомневается в своих сотрудниках, не и конечно людей, которые интересуются мнением окружающих о себе. Кроме этого, взломав страничку другого пользователя, появляется возможность более подробно ознакомиться с его личной жизнью, узнать, с кем и как он проводит личное время, и многое другое.
Таким образом, можно подвести итог, что программа Pagehack – отличный способ узнать необходимую информацию о человеке, не прибегая к расспросам и другим сложным методам, например слежке. Все нужные данные появятся на компьютере взломщика за короткий промежуток времени.
Введите текст с картинки нажмите скачать
377
скачать

Киберпреступники пользуются и тем, что всегда есть вероятность случайно получить «чужое» письмо, отправленное не на тот адрес (ведь человеку свойственно ошибаться). Здесь также сделан расчет на любопытство: что пишут вашему коллеге?



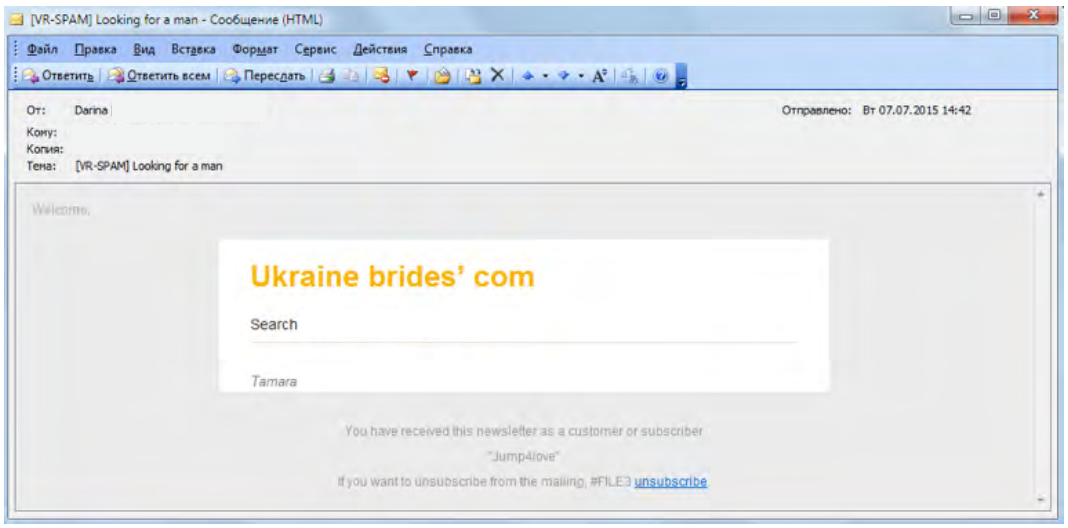
Нередко такие письма маскируются под личные и даже интимные послания:

«Привет, Вован!

Ну как, разобрался с женой?»

«Привет, дорогой! Помнишь еще меня? Вот мой сайт с ню».

Характерная особенность таких писем – наличие в них ссылки. Главная цель спамера – заставить вас по этой ссылке пройти. Известный прием – маскировка нужной ссылки под слова «Отписаться от данной рассылки».



Любопытной Варваре, как мы помним, на базаре нос оторвали, но в случае спамеров мы никогда не знаем, насколько крупным может быть ущерб от любопытства и связанных с ним необдуманных действий.

Как противостоять

- Любая информация в письме, адресованная не вам либо же труднодоступная по другим источникам, указывает на то, что это с 50% вероятностью спам.
- Если в письме есть частичное совпадение, например: имя получателя – ваше, но отправитель не знаком / имя не ваше, но отправитель знаком / имя не ваше, отправитель неизвестен, но тема до боли интересна – не рискуйте и не открывайте такое письмо.
- Помните, что интересующую вас информацию можно попробовать найти другими способами – например, при помощи поисковика, без необходимости открывать письма непонятно от кого.

Другие уловки

- **Правовые оговорки**
  Спам может содержать ссылки на соглашение о конфиденциальности, упоминания об ответственности и т. д. — но все это лишь уловки преступников. На людей, не разбирающихся в мошеннических технологиях, такие оговорки производят впечатление и вызывают доверие к мошенникам. Не поддавайтесь на такие фокусы!
- **Сообщения о проверке антивирусом**
  Они тоже рассчитаны на то, что вы поверите в добропорядочность отправителя, проникнетесь к нему доверием (через благодарность за заботу) и сделаете то, что он хочет, — ведь он якобы позаботился о том, чтобы письмо пришло к вам без вирусов, а значит, такой «честный» отправитель как минимум заслуживает внимательного прочтения его сообщения. Но спамеры не только не проверяют письма на вирусы — они часто рассылают вирусы или ссылки на вредоносные сайты. Не стройте иллюзий — безопасность вашего компьютера не является заботой спамера!

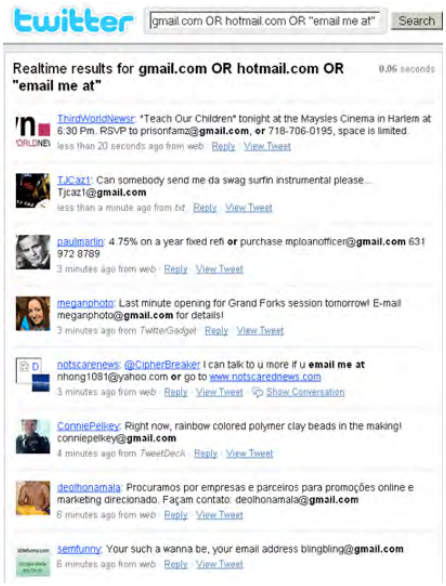
Как не попасть в список рассылки спамеров

Любые контакты являются ценным товаром и пользуются спросом на рынке интернет-мошенников: ведь адресная рассылка гораздо более эффективна, чем обезличенная. Кроме того, обладая данными получателя письма, злоумышленники могут организовать успешную фишинговую атаку.

Поскольку невозможно сохранить свой электронный адрес в тайне при переписке и регистрации на различных форумах и сервисах, избежать спама полностью можно, лишь отказавшись от использования e-mail, что неприемлемо. Поэтому необходимо сосредоточиться на том, чтобы уменьшить риск получения спама до минимума.

1. Рекомендуйте соблюдать правила безопасности своим знакомым: если они не устанавливают обновления безопасности и запускают или открывают все файлы без разбора, это приведет к возрастанию потока спама в ваш адрес. Вредоносные программы, проникшие на компьютер, сразу ищут, что можно украсть и продать: проверяют наличие адресных книг Outlook Express, сканируют почтовую базу в поисках адресов, а затем пересылают найденное своим владельцам.На сегодняшний день это для спамеров – основной способ раздобыть электронные адреса.
2. Сообщайте свой основной e-mail только знакомым адресатам. Пусть полностью обезопаситься с помощью такой «конспирации» не удастся (вредоносные программы активно охотятся за списками контактов), но все же риск существенно снижается.
3. Не оставляйте свой e-mail на страницах соцсетей и прочих интернет-ресурсах, в том числе на сайтах, посвященных поиску работу, да и на собственном сайте тоже.

   Для несанкционированного сбора электронных адресов разработаны специальные программы. Поэтому буквально сразу после того, как пользователь где-либо указывает свой адрес, к нему может прийти спам.



Часто можно встретить совет указывать e-mail без знака @, с заменой его на слово «собака» или at, а также с добавлением пробелов – считается, что программа в таком случае не сможет распознать адрес. Однако это не всегда помогает: зачастую программе достаточно выявить в адресе доменное имя (например, mail или yandex), после чего она автоматически подставляет все, что слева от него, в качестве потенциального имени клиента.

Более эффективно указание адреса в виде картинки или Java-скрипта, содержащего зашифрованный e-mail и выводящего его на экран только при нажатии на кнопку или иконку (HTML Protector (antssoft.fileburst.com/htmlprotector.zip), HTML Power (www.pullsoft.com/htmlpower.zip) или Encrypt HTML Pro (www.mtopsoft.com/download/enchp.zip)).

4. При регистрации на различных ресурсах обращайте внимание на поля о согласии продавать или передавать ваш адрес третьим лицам, а также получать рассылки. Отключите эти опции. Сделайте то же самое в свойствах ваших аккаунтов социальных сетей, форумов и на прочих сайтах.
5. Используйте отдельный адрес для регистрации на различных ресурсах и в соцсетях. Для работы с платежными системами и электронными кошельками также имеет смысл зарегистрировать отдельный e-mail.Можно воспользоваться специальными сервисами для создания одноразовых адресов – например, mailinator.com.
6. При регистрации адреса электронной почты указывайте по возможности длинное и сложное имя, содержащее не менее 7 символов. Популярные короткие имена отслеживаются спамерами и попадают в их базы. Используйте комбинации букв, цифр и других символов – чем сложнее логин, тем меньше риск получения спама
7. Периодически меняйте свой адрес, предварительно оповестив тех, для кого это актуально.

Спамеры разными способами стремятся проверить, получено ли их сообщение. На подобные уловки ни в коем случае нельзя реагировать – получив подтверждение, спамеры увеличат поток нежелательной почты на этот адрес.

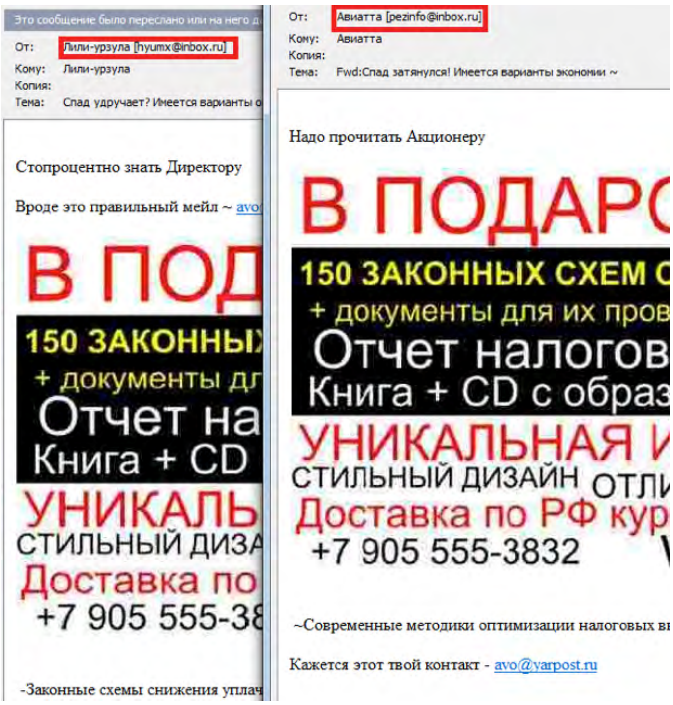
При этом спам может начать приходить из разных источников, если ваш адрес попадет к другим спамерам. Поэтому:

1. Никогда не отвечайте на подозрительные письма.
2. Не переходите ни по каким ссылкам из таких писем. Все ссылки открывайте, только набрав их вручную в адресной строке браузера, или пользуйтесь собственными закладками, особенно если речь идет о работе с банковскими счетами.
3. Если вы все же решите перейти по ссылке в письме или с интернет-страницы, наведите на нее курсор, чтобы увидеть конечный адрес. Если само сообщение не вызывает подозрений, но конечный адрес представляет собой бессмысленный набор символов, не переходите по этой ссылке.
4. Отключите автоматическую загрузку изображений во входящих письмах. Иногда для проверки активности почтового ящика спамеры используют невидимые однопиксельные gif-файлы.
5. Никогда не открывайте вложения, если сомневаетесь в том, что адресат вам известен, или если не уверены, что ожидали получить данное письмо.
6. Некоторые почтовые клиенты отправляют автоматические подтверждения о получении писем, что также является для спамеров сигналом о том, что адрес — действующий. Отключите отправку таких подтверждений.
7. В некоторых спам-письмах присутствует предложение об отмене подписки на рассылку, для чего предлагается отправить письмо по указанному адресу или перейти по предложенной ссылке. Этого не следует делать, поскольку ваш ответ также будет свидетельствовать об актуальности вашего почтового ящика для спамеров.

Как распознать спам и вредоносные ссылки в нем

Характерными признаками спама являются:

1. Массовость рассылки — множество одинаковых сообщений может регулярно приходить в почту. Как правило, спам рассылается с помощью специализированного ПО на сотни тысяч компьютеров одновременно.
2. Несоответствие темы письма его содержимому. Задача мошенников – «намозолить» вам глаза своими посланиями, поэтому зачастую приходит целая пачка писем с одинаковым (или почти одинаковым содержимым) и разными заголовками. А поскольку письма формируются автоматически, довольно часто заголовок не совпадет с содержимым.
3. Большое количество одинаковых сообщений от «разных» отправителей.



4. Обезличенность.
   Спам почти никогда не направлен на конкретного получателя, даже если в поле «Кому» вы видите именно свой адрес. Чаще всего приветствие и содержание письма обезличены – в обращении отсутствуют ваши имя/фамилия).

Утечки персональных данных (например, по причине заражения или взлома компьютеров и облачных сервисов) позволяют злоумышленникам совершать адресные персонализированные рассылки.

Так, летом 2015 года, после взлома сайта знакомств Ashley Madisson и похищения его базы данных прошло несколько волн массовых рассылок писем шантажистов с требованием немалого выкупа за неразглашение украденных данных (дело в том, что знакомства на сайте заводились с целью измены). Этот спам был персонализированным.

5. Повышенная эмоциональность темы письма и содержимого — психологическое давление на получателя спама.
6. Сокрытие адреса отправителя или указание несуществующего адреса.
7. Невозможность отписаться от получения спама.

Зачастую спамеры размещают в своих письмах ссылки, нажав на которые якобы можно отписаться от получения спама. На деле же при клике по такой ссылке в лучшем случае можно получить увеличение потока спама, а в худшем – загрузить вирус на свой ПК. Любое письмо спамеру, в том числе отказ от подписки, служит лишь подтверждением активности вашего адреса, после чего поток спама всегда возрастает.

Какие массовые рассылки не относятся к спаму

1. Почтовые рассылки, на получение которых пользователь согласился добровольно при регистрации на каком-либо ресурсе или мероприятии, либо же специально подписался через соответствующую форму. Одно из отличий большинства легальных рассылок от спама – наличие персонального обращения к получателю по имени/фамилии или по имени пользователя (логину), зарегистрированному вами на том или ином сервисе.
2. Почтовые рассылки от ваших партнеров и клиентов, сервисов, на которых вы зарегистрированы, оповещающие о проблемах, которые могут вас затронуть. Например, сообщения об утечке ваших персональных данных или о взломе некоего ресурса и рекомендации в связи с этим инцидентом.

Взлом легитимного ресурса, на котором вы зарегистрированы, может привести к массовой рассылке писем от его имени. В большинстве случаев это будет не спам, а распространение вирусов или фишинговая атака, причем в письмах будет имитироваться стиль взломанной компании. Возможен также и шантаж.

3. Сообщения государственных организаций, в том числе СМС-сообщения, например, о чрезвычайных ситуациях и армейских учениях для предотвращения паники среди населения, сообщения с целью сбора мнений о государственных услугах.

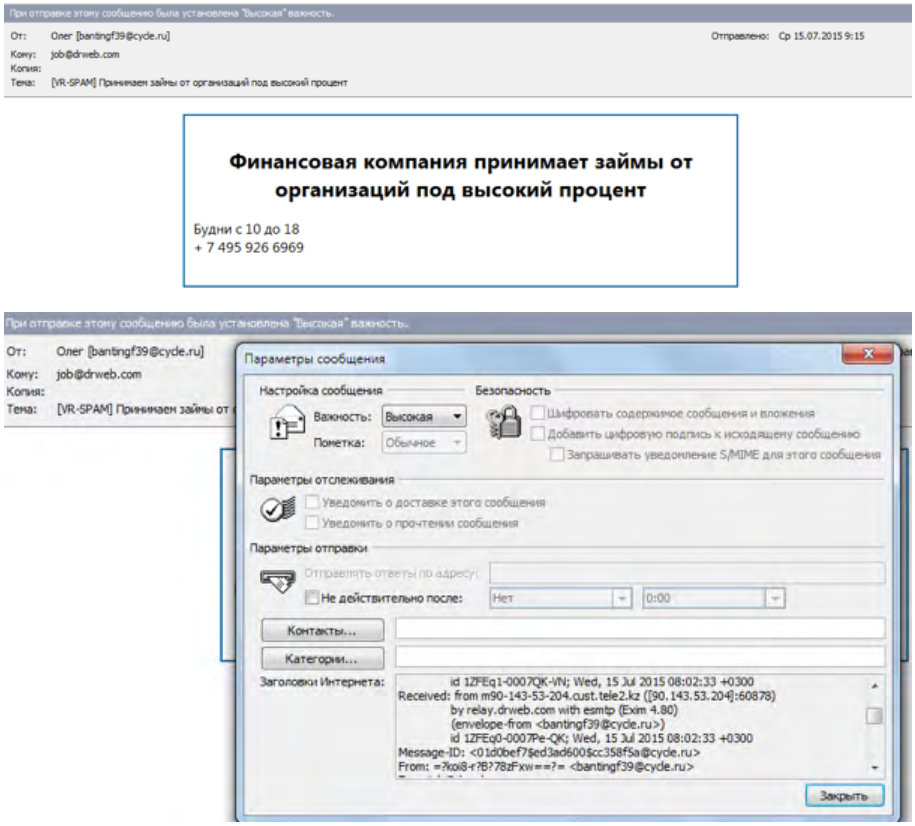
> *Не являются спамом сообщения Минкомсвязи России, рассылаемые с короткого номера 0919 — официального номера для оценки гражданами качества государственных услуг.*
> http://www.pcweek.ru/gover/news-company/detail.php?ID=176764

Как распознать спам

Проверьте поле «От» (информация об отправителе)

Как правило, вы получаете письма от известных вам людей. Если же отправитель вам незнаком, он поясняет в письме, откуда он получил ваш адрес, или же описывает причину обращения, которая должна быть каким-то образом связана с вашими делами (работой или хобби). В противном случае, скорее всего, это спам.

Достаточно часто адрес отправителя спама зарегистрирован на бесплатном домене. Зачастую в спам-письмах обратного адреса нет вообще.

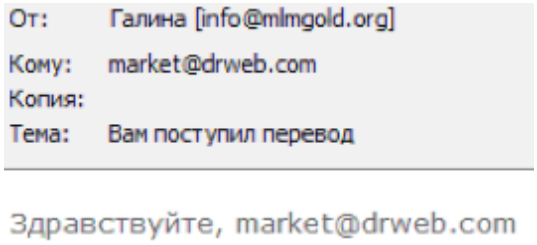


Данный пример демонстрирует, что «финансовая организация» не имеет обратного адреса, а если заглянуть в служебные заголовки, то видно, что первым сервером, принявшим сообщение от <bantingf39@cycle.ru> (судя по адресу компании – из зоны Ru), был m90-143-53-204.cust.tele2.kz – сервер из Казахстана.

Проверьте поле «Тема письма»
Спам-сообщения о покупке лекарств, посещении «бесплатных» семинаров или легкого получения кредитов, как правило, имеют заголовки типа «Уникальное предложение», «Невероятная сделка», «Специальный отчет» или «Ограниченное предложение».

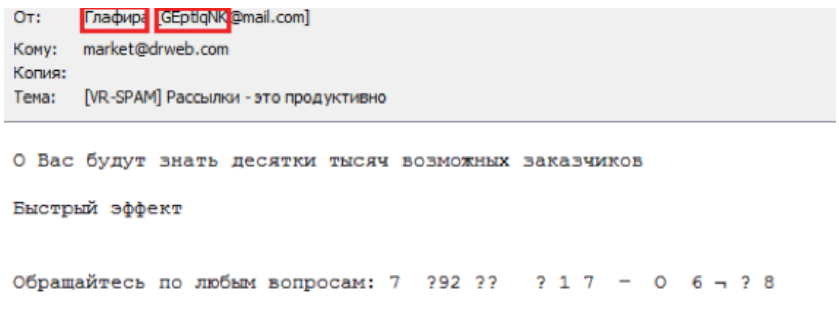
Фишинг-сообщения в большинстве имеют заголовки типа «Необходимо срочно ...» или «Проверка вашего аккаунта». Такие темы призваны воздействовать на ваши эмоции или побудить автоматическую реакцию на уведомление.

Проверьте поле «Кому»
Как правило, спамеры не знают нашего имени, им известен только адрес. Либо же вообще они отправляют письма на общий адрес рассылки (admin, info, market – адреса, которые имеются в большинстве компаний).



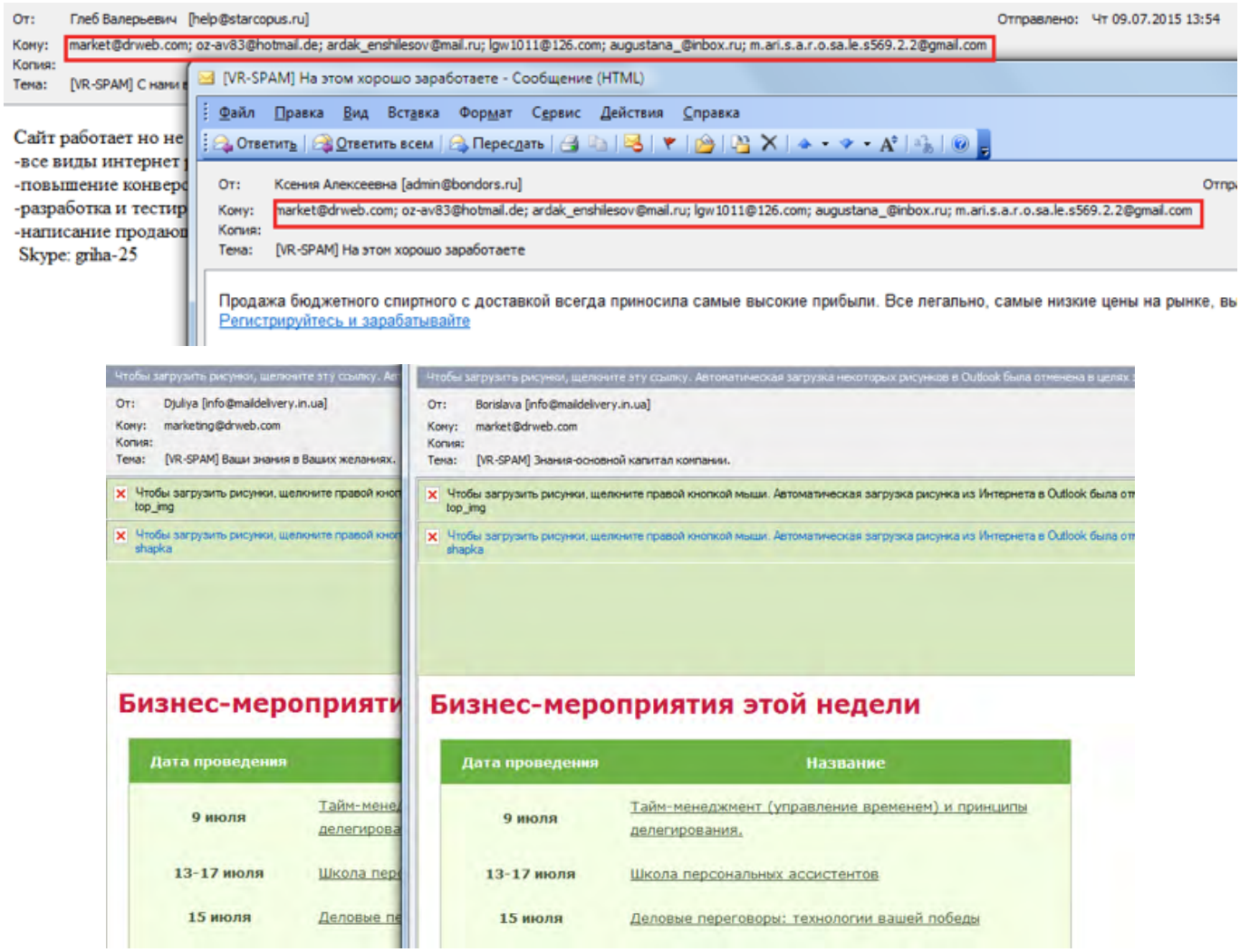
Всегда проверяйте адрес получателя. Отсутствие в этом поле вашего e-mail или наличие только неизвестных вам получателей должно настораживать.

Рекомендуется также обращать внимание на то, как выглядит сам адрес. Даже если в компании не принят общий для всех порядок формирования адресов, зачастую адреса отправителей спама (или их имена) выделяются своей экзотичностью.



Если в поле получателей указано множество адресов, совершенно вам неизвестных, — это верный признак спама.

Часто спамеры используют один и тот же набор адресов для самых разных рассылок.



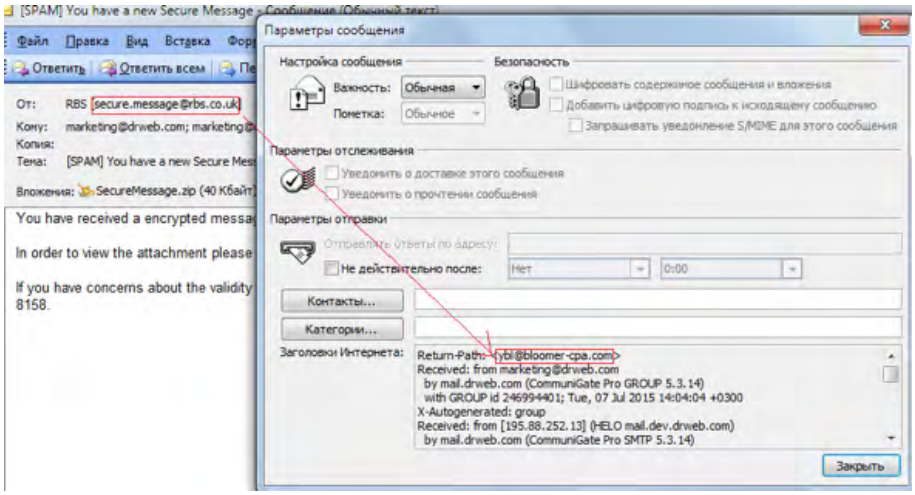
Проверьте поле «От кого»

Обычно спамеры не указывают обратный адрес или он спрятан глубоко в «теле» письма.

К сожалению, в спам-сообщениях поле «От» («From»), которое видит получатель письма, на самом деле не соответствует тому адресу, на который в действительности будет отправлено сообщение в случае ответа на него.

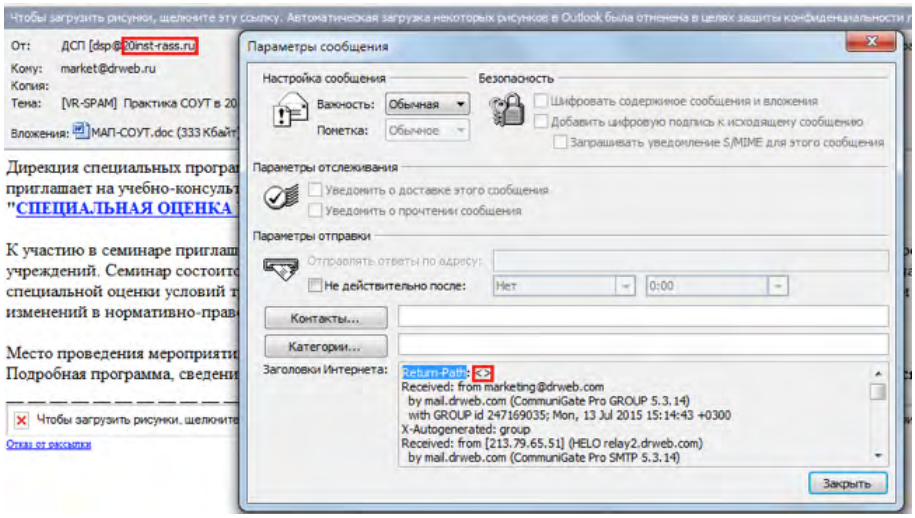
Наряду с информацией, видимой получателем письма, — полями «От», «Кому», «Тема» и т. д., — каждое письмо содержит служебную информацию, которая обычно не видна для пользователя, но необходима для успешной доставки письма.

Для установления истинного адреса отправителя необходимо проверить служебное поле «Return-Path». Это позволит выяснить, отсылает ли оно к почтовому ящику того же лица или организации, с которого было якобы отправлено предложение.



Более того, вполне возможно, что обратный адрес также окажется либо вымышленным, либо реально существующим, но не имеющим отношения к спамерам. Отправители могут прописать любой адрес и в поле «Return-Path», и в поле «От» («From»).

Отсутствие информации в поле «Return-Path» свидетельствует о желании отправителей письма скрыть информацию о себе. В этом случае сразу же удалите письмо – это спам.

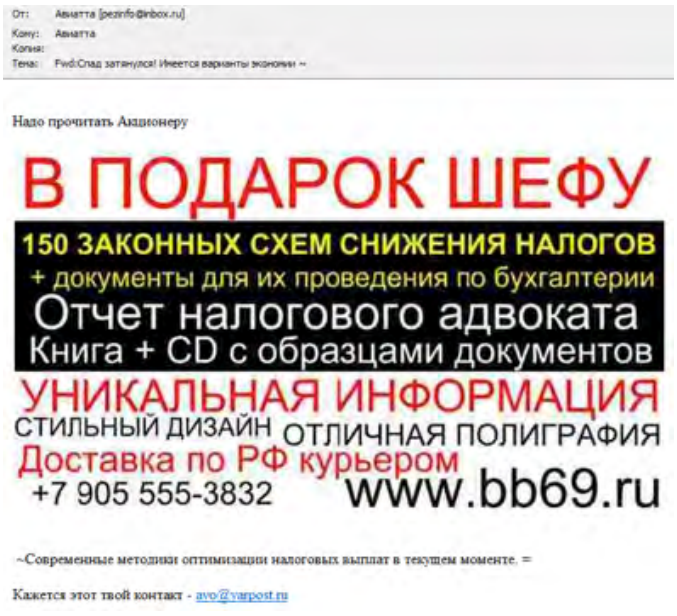


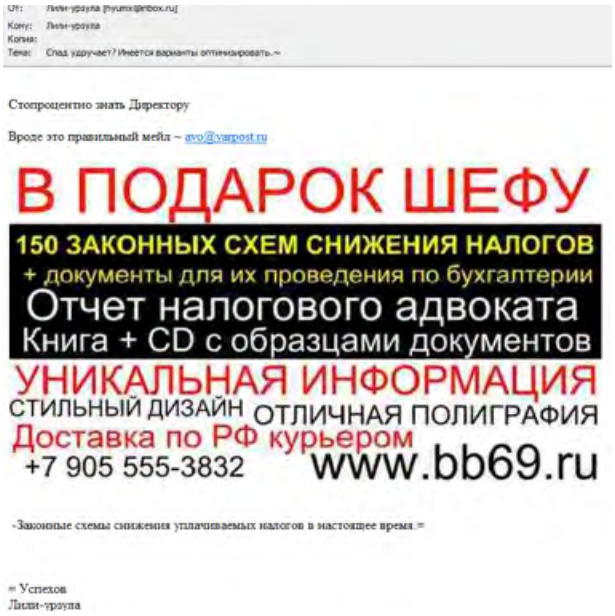
Проверьте время отправления письма

Если сообщение пришло к вам из далекого прошлого или будущего, скорее всего, это спам. Удалите это письмо немедленно.

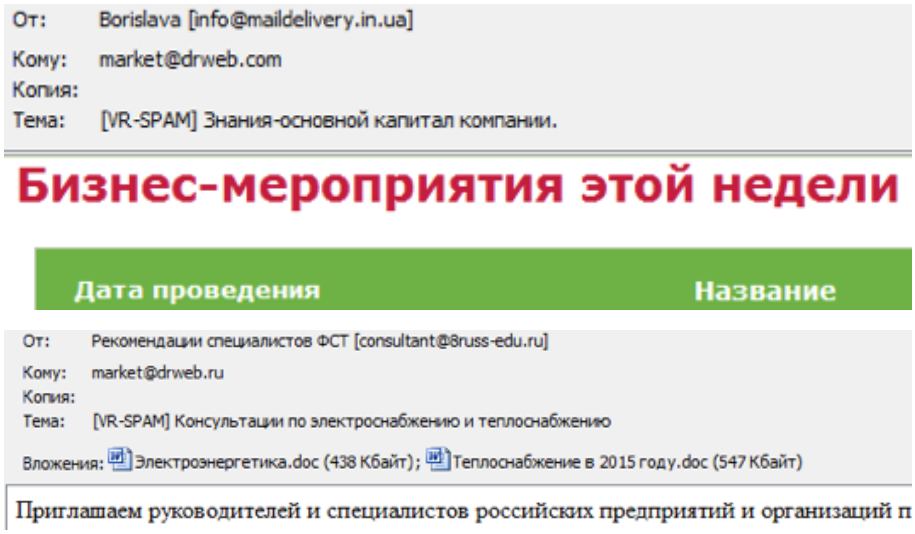
Обратите внимание на приветствие

Если письмо адресовано вам как «другу», «ценному клиенту» или «коллеге» (спам предназначается для массовой рассылки, поэтому текст такого послания обезличен) или если обращения нет вовсе — удалите это письмо немедленно. Пример одного и того же спам-сообщения с разными приветствиями и подписями:





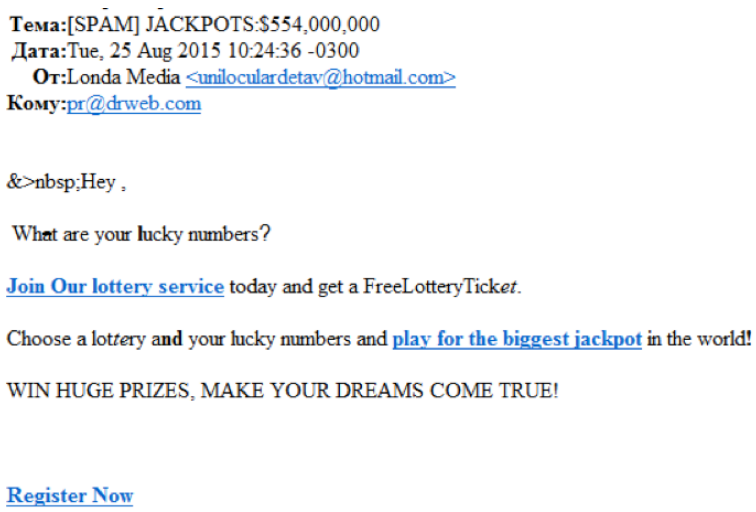
Чтобы скрыть незнание вашего имени/должности, спамеры зачастую вообще отказываются от приветствия:



Обратите внимание на общий вид текста

Чтобы заставить вас прочитать текст, злоумышленники применяют разные средства психологического давления. Некоторые приемы используют для затруднения обнаружение спама фильтрами:

- выделение отдельных слов заглавными буквами,



Тема:[SPAM] JACKPOTS:$554,000,000
Дата: Tue, 25 Aug 2015 10:24:36 -0300
От: Londa Media <uniloculardetav@hotmail.com>
Кому:pr@drweb.com

&>nbsp;Hey ,

What are your lucky numbers?

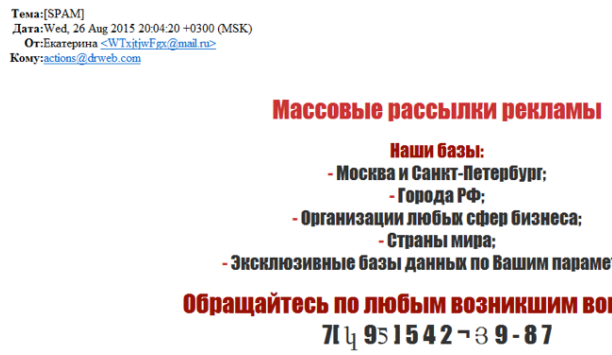
Join Our lottery service today and get a FreeLotteryTicket.

Choose a lottery and your lucky numbers and play for the biggest jackpot in the world!

WIN HUGE PRIZES, MAKE YOUR DREAMS COME TRUE!

Register Now

- написание слов с использованием разного регистра и шрифта,



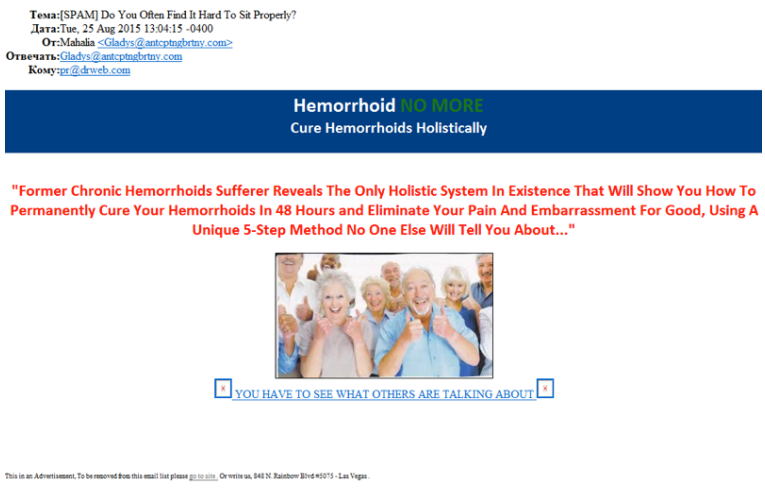
Тема:[SPAM]
Дата: Wed, 26 Aug 2015 20:04:20 +0300 (MSK)
От:Екатерина <WTxjtjwFgx@mail.ru>
Кому:actions@drweb.com

Массовые рассылки рекламы

Наши базы:
- Москва и Санкт-Петербург;
- Города РФ;
- Организации любых сфер бизнеса;
- Страны мира;
- Эксклюзивные базы данных по Вашим параметрам.

Обращайтесь по любым возникшим вопросам:
7[ч 95 1 5 4 2 ¬ з 9 - 8 7

- цветовое выделение отдельных частей текста,



Тема:[SPAM] Do You Often Find It Hard To Sit Properly?
Дата: Tue, 25 Aug 2015 13:04:15 -0400
От: Mahalia <Gladys@antcptngbrtny.com>
Отвечать: Gladys@antcptngbrtny.com
Кому:pr@drweb.com

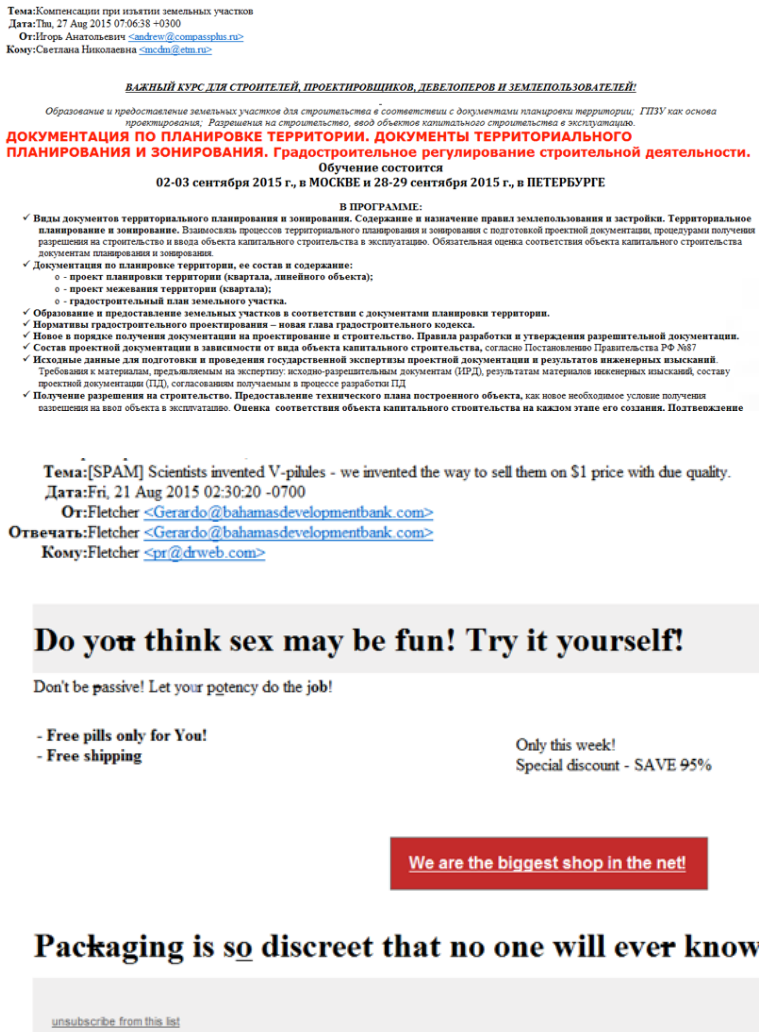
Hemorrhoid NO MORE
Cure Hemorrhoids Holistically

"Former Chronic Hemorrhoids Sufferer Reveals The Only Holistic System In Existence That Will Show You How To Permanently Cure Your Hemorrhoids In 48 Hours and Eliminate Your Pain And Embarrassment For Good, Using A Unique 5-Step Method No One Else Will Tell You About..."

YOU HAVE TO SEE WHAT OTHERS ARE TALKING ABOUT

This is an Advertisement. To be removed from this email list please go to site. Or write us, 840 N. Rainbow Blvd #5075 - Las Vegas .

- применение подчеркивания, полужирного шрифта или курсива к отдельным буквам в слове, а также использование разных шрифтов,



Тема:Компенсации при изъятии земельных участков
Дата: Thu, 27 Aug 2015 07:06:38 +0300
От:Игорь Анатольевич <andrew@compassplus.ru>
Кому:Светлана Николаевна <mcdm@etn.ru>

ВАЖНЫЙ КУРС ДЛЯ СТРОИТЕЛЕЙ, ПРОЕКТИРОВЩИКОВ, ДЕВЕЛОПЕРОВ И ЗЕМЛЕПОЛЬЗОВАТЕЛЕЙ!

Образование и предоставление земельных участков для строительства в соответствии с документами планировки территории; ГПЗУ как основа проектирования; Разрешения на строительство, ввод объектов капитального строительства в эксплуатацию.

ДОКУМЕНТАЦИЯ ПО ПЛАНИРОВКЕ ТЕРРИТОРИИ. ДОКУМЕНТЫ ТЕРРИТОРИАЛЬНОГО ПЛАНИРОВАНИЯ И ЗОНИРОВАНИЯ. Градостроительное регулирование строительной деятельности.

Обучение состоится
02-03 сентября 2015 г., в МОСКВЕ и 28-29 сентября 2015 г., в ПЕТЕРБУРГЕ

В ПРОГРАММЕ:

- ✓ **Виды документов территориального планирования и зонирования. Содержание и назначение правил землепользования и застройки. Территориальное планирование и зонирование.** Взаимосвязь процессов территориального планирования и зонирования с подготовкой проектной документации, процедурами получения разрешения на строительство и ввода объекта капитального строительства в эксплуатацию. Обязательная оценка соответствия объекта капитального строительства документам планирования и зонирования.
- ✓ **Документация по планировке территории, ее состав и содержание:**
  - o - **проект планировки территории (квартала, линейного объекта);**
  - o - **проект межевания территории (квартала);**
  - o - **градостроительный план земельного участка.**
- ✓ **Образование и предоставление земельных участков в соответствии с документами планировки территории.**
- ✓ **Нормативы градостроительного проектирования – новая глава градостроительного кодекса.**
- ✓ **Новое в порядке получения документации на проектирование и строительство. Правила разработки и утверждения разрешительной документации.**
- ✓ **Состав проектной документации в зависимости от вида объекта капитального строительства,** согласно Постановлению Правительства РФ №87
- ✓ **Исходные данные для подготовки и проведения государственной экспертизы проектной документации и результатов инженерных изысканий.** Требования к материалам, предъявляемым на экспертизу: исходно-разрешительным документам (ИРД), результатам материалов инженерных изысканий, составу проектной документации (ПД), согласованиям получаемым в процессе разработки ПД
- ✓ **Получение разрешения на строительство. Предоставление технического плана построенного объекта,** как новое необходимое условие получения разрешения на ввод объекта в эксплуатацию. **Оценка соответствия объекта капитального строительства на каждом этапе его создания. Подтверждение**

Тема:[SPAM] Scientists invented V-pilules - we invented the way to sell them on $1 price with due quality.
Дата: Fri, 21 Aug 2015 02:30:20 -0700
От: Fletcher <Gerardo@bahamasdevelopmentbank.com>
Отвечать: Fletcher <Gerardo@bahamasdevelopmentbank.com>
Кому: Fletcher <pr@drweb.com>

Do you think sex may be fun! Try it yourself!

Don't be passive! Let your potency do the job!

- **Free pills only for You!**
- **Free shipping**

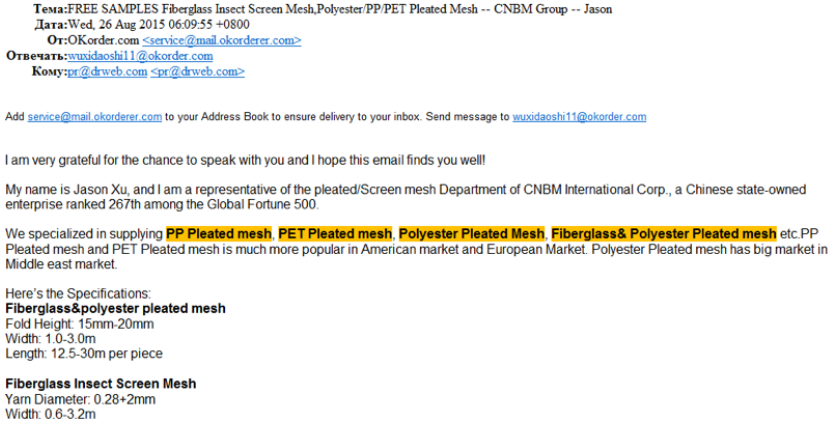
Only this week!
Special discount - SAVE 95%

We are the biggest shop in the net!

Packaging is so discreet that no one will ever know

unsubscribe from this list

- выделение ключевых слов маркером,



Тема:FREE SAMPLES Fiberglass Insect Screen Mesh,Polyester/PP/PET Pleated Mesh -- CNBM Group -- Jason
Дата: Wed, 26 Aug 2015 06:09:55 +0800
От:OKorder.com <service@mail.okorderer.com>
Отвечать:wuxidaoshi11@okorder.com
Кому:pr@drweb.com <pr@drweb.com>

Add service@mail.okorderer.com to your Address Book to ensure delivery to your inbox. Send message to wuxidaoshi11@okorder.com

I am very grateful for the chance to speak with you and I hope this email finds you well!

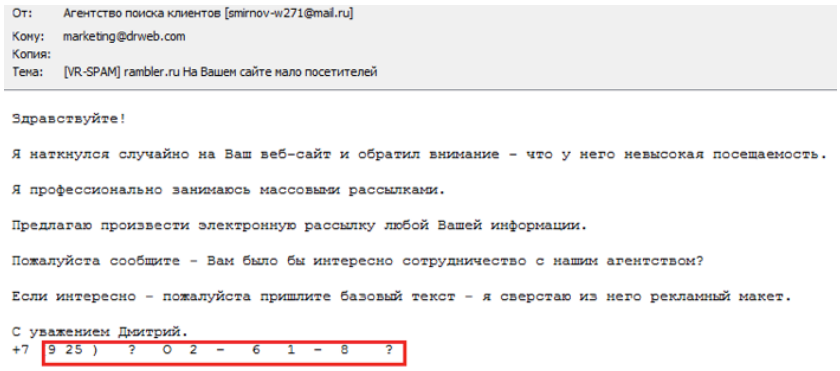
My name is Jason Xu, and I am a representative of the pleated/Screen mesh Department of CNBM International Corp., a Chinese state-owned enterprise ranked 267th among the Global Fortune 500.

We specialized in supplying **PP Pleated mesh**, **PET Pleated mesh**, **Polyester Pleated Mesh**, **Fiberglass& Polyester Pleated mesh** etc.PP Pleated mesh and PET Pleated mesh is much more popular in American market and European Market. Polyester Pleated mesh has big market in Middle east market.

Here's the Specifications:
Fiberglass&polyester pleated mesh
Fold Height: 15mm-20mm
Width: 1.0-3.0m
Length: 12.5-30m per piece

Fiberglass Insect Screen Mesh
Yarn Diameter: 0.28+2mm
Width: 0.6-3.2m

- использование пробелов внутри одного слова, а также в номерах телефонов и e-mail-адресах,



От: Агентство поиска клиентов [smirnov-w271@mail.ru]
Кому: marketing@drweb.com
Копия:
Тема: [VR-SPAM] rambler.ru На Вашем сайте мало посетителей

Здравствуйте!

Я наткнулся случайно на Ваш веб-сайт и обратил внимание - что у него невысокая посещаемость.

Я профессионально занимаюсь массовыми рассылками.

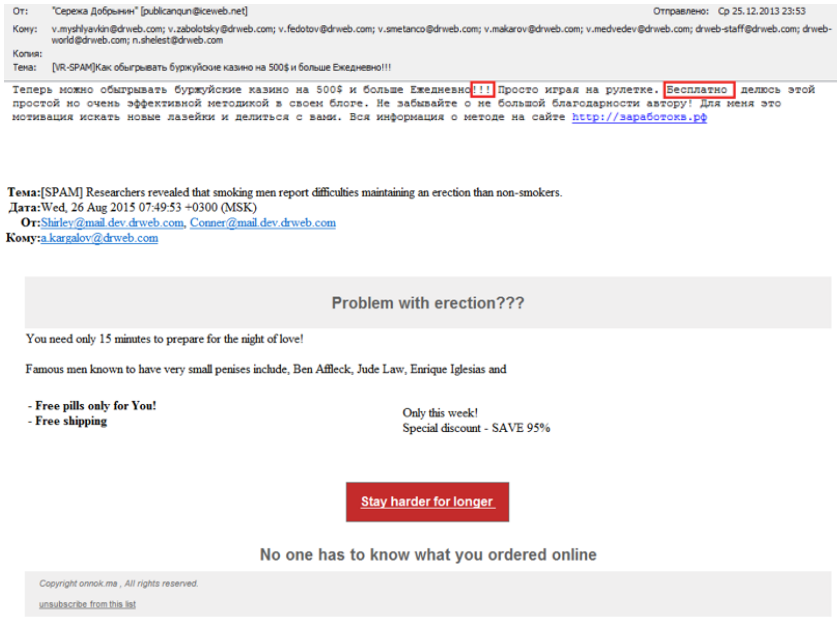
Предлагаю произвести электронную рассылку любой Вашей информации.

Пожалуйста сообщите - Вам было бы интересно сотрудничество с нашим агентством?

Если интересно - пожалуйста пришлите базовый текст - я сверстаю из него рекламный макет.

С уважением Дмитрий.
+7 (9 25) ? O 2 - 6 1 - 8 ?

- использование вместо букв похожих по начертанию цифр, латинских букв вместо русских и т. п,
- наличие в тексте множества восклицательных знаков для создания впечатления повышенной эмоциональности послания, иногда тревоги, что притягивает внимание, вызывает потребность дочитать текст до конца (и посочувствовать),



От: "Сережа Добрынин" [publicanqun@iceweb.net] Отправлено: Ср 25.12.2013 23:53
Кому: v.myshlyavkin@drweb.com; v.zabolotsky@drweb.com; v.fedotov@drweb.com; v.smetanco@drweb.com; v.makarov@drweb.com; v.medvedev@drweb.com; drweb-staff@drweb.com; drweb-world@drweb.com; n.shelest@drweb.com
Копия:
Тема: [VR-SPAM]Как обыгрывать буржуйские казино на 500$ и больше Ежедневно!!!

Теперь можно обыгрывать буржуйские казино на 500$ и больше Ежедневно!!! Просто играя на рулетке. Бесплатно делюсь этой простой но очень эффективной методикой в своем блоге. Не забывайте о не большой благодарности автору! Для меня это мотивация искать новые лазейки и делиться с вами. Вся информация о методе на сайте http://заработокв.рф

Тема:[SPAM] Researchers revealed that smoking men report difficulties maintaining an erection than non-smokers.
Дата: Wed, 26 Aug 2015 07:49:53 +0300 (MSK)
От: Shirley@mail.dev.drweb.com, Conner@mail.dev.drweb.com
Кому:a.kargalov@drweb.com

Problem with erection???

You need only 15 minutes to prepare for the night of love!

Famous men known to have very small penises include, Ben Affleck, Jude Law, Enrique Iglesias and

- **Free pills only for You!**
- **Free shipping**

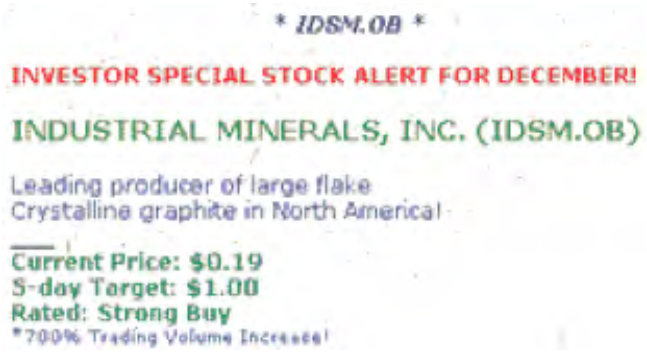
Only this week!
Special discount - SAVE 95%

Stay harder for longer

No one has to know what you ordered online

Copyright onnok.ma , All rights reserved.
unsubscribe from this list

- в случае графического спама (когда текст помещен на картинку) на изображение могут быть нанесены графические «шумы» в виде точек и линий, что также затрудняет распознавание спам-фильтрами.



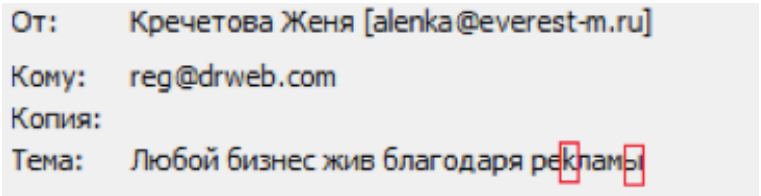
http://compress.ru/article.aspx?id=17269

Также применяются индивидуальные смещения каждой буквы текста, случайные изменения размера, типа и цвета шрифта, в изображении могут присутствовать сложные «шумы», рамки, разноцветные многоугольники.

http://compress.ru/article.aspx?id=17269

Ознакомьтесь с содержанием
(не соглашаясь отрыть заблокированные почтовым клиентом части писем, например графику).

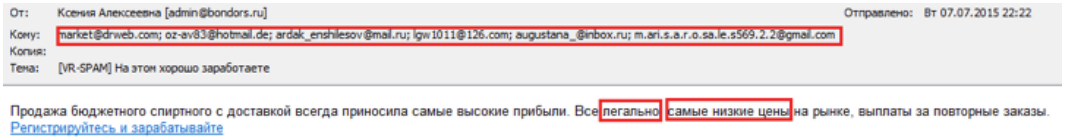
- применение свободного стиля изложения — часто предложения грамматически построены неправильно, что вызывает недоумение, потребность остановить чтение, чтобы понять, какую идею хотел донести автор. Используются непривычные сочетания слов, режущие глаз,



- наличие утверждения, что это не спам, а деловое предложение / крик о помощи и т. д.

Наталья Далакова поделилась группа в Хронике Я-Дитина України.
23 апреля ·

Это не спам!!!!
ПРОШУ О ПОМОЩИ!!!!!!!!
Нашему сыночку Кыслий Назару 9 месяцев
В 8 месяцев нам поставили диагноз: двухстороняя сенсоневральная глухота 4 степени
Наш малыш не слышит окружающий мир, а как следствие не может говорить. Мы преобрели слуховой аппарат, что бы ребенок мог слышать хотя бы какие-то звуки и учился выговаривать слова. Для того что бы он полноценно слышал и мог нормально говорить нам требуется кохлеарная имплантация, которая стоит на данный момент 943 470 грн, на сегодня собрали 128 000 грн. Даную операцию желательно провести до 1 года. Операцию делаю в Киеве в институте им. Коломийченка.
Прошу всех у кого есть желание и возможность помочь моему мальчику услышать наш мир!!!!!!
номер карты приват банка 4149 4378 3762 9276
Далакова Наталия Павловнател
067-208-77-51
Ссылка на группу https://www.facebook.com/groups/453731698116872/

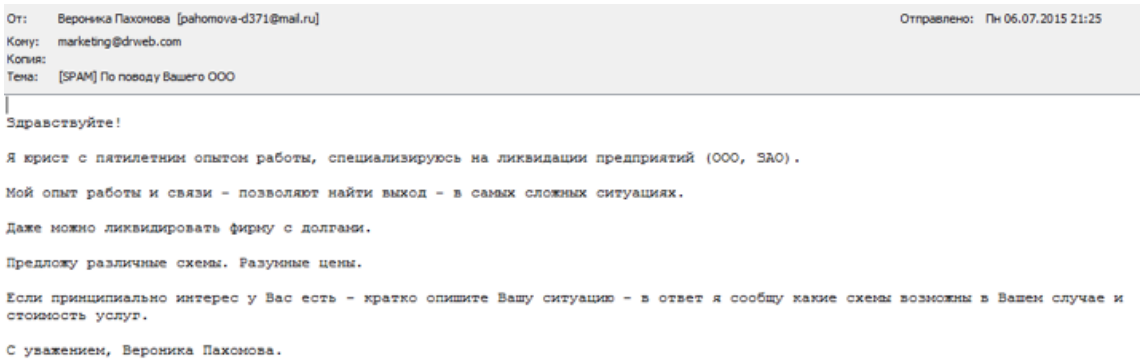


От: Ксения Алексеевна [admin@bondors.ru] Отправлено: Вт 07.07.2015 22:22
Кому: market@drweb.com; oz-av83@hotmail.de; ardak_enshilesov@mail.ru; lgw1011@126.com; augustana_@inbox.ru; m.ari.s.a.r.o.sa.le.s569.2.2@gmail.com
Копия:
Тема: [VR-SPAM] На этом хорошо заработаете

Продажа бюджетного спиртного с доставкой всегда приносила самые высокие прибыли. Все легально, самые низкие цены на рынке, выплаты за повторные заказы.
Регистрируйтесь и зарабатывайте

- спам часто содержит вначале фразы типа «НЕ УДАЛЯЙТЕ ЭТО ПИСЬМО» или «ЧИТАЙТЕ ВНИМАТЕЛЬНО ВЛОЖЕНИЕ».

Спамеры прекрасно понимают, что современный человек испытывает переизбыток информации и нехватку времени. Поэтому часто текст составляется без подробностей, предельно лаконично. Ведь главная цель — вынудить вас действовать на эмоциональном уровне, в том числе узнать больше информации о предложении на сайте, на который предлагается перейти.



От: Вероника Пахомова [pahomova-d371@mail.ru] Отправлено: Пн 06.07.2015 21:25
Кому: marketing@drweb.com
Копия:
Тема: [SPAM] По поводу Вашего ООО

Здравствуйте!

Я юрист с пятилетним опытом работы, специализируюсь на ликвидации предприятий (ООО, ЗАО).

Мой опыт работы и связи - позволяют найти выход - в самых сложных ситуациях.

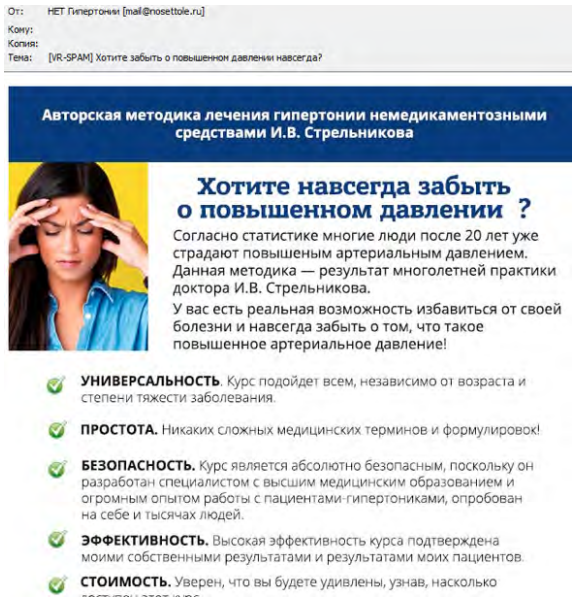
Даже можно ликвидировать фирму с долгами.

Предложу различные схемы. Разумные цены.

Если принципиально интерес у Вас есть - кратко опишите Вашу ситуацию - в ответ я сообщу какие схемы возможны в Вашем случае и стоимость услуг.

С уважением, Вероника Пахомова.

И наоборот — если рекламируется какой-то незаконный или бесполезный товар (например, БАДы) или методика, текст чрезмерно насыщен якобы «преимуществами» предложения, но по сути ни о чем не говорит.


От: НЕТ Гипертонии [mail@nosettole.ru]
Кому:
Копия:
Тема: [VR-SPAM] Хотите забыть о повышенном давлении навсегда?

Авторская методика лечения гипертонии немедикаментозными средствами И.В. Стрельникова

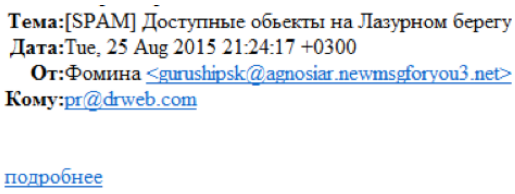
Хотите навсегда забыть о повышенном давлении ?

Согласно статистике многие люди после 20 лет уже страдают повышеным артериальным давлением. Данная методика — результат многолетней практики доктора И.В. Стрельникова.

У вас есть реальная возможность избавиться от своей болезни и навсегда забыть о том, что такое повышенное артериальное давление!

- **УНИВЕРСАЛЬНОСТЬ**. Курс подойдет всем, независимо от возраста и степени тяжести заболевания.
- **ПРОСТОТА.** Никаких сложных медицинских терминов и формулировок!
- **БЕЗОПАСНОСТЬ.** Курс является абсолютно безопасным, поскольку он разработан специалистом с высшим медицинским образованием и огромным опытом работы с пациентами-гипертониками, опробован на себе и тысячах людей.
- **ЭФФЕКТИВНОСТЬ.** Высокая эффективность курса подтверждена моими собственными результатами и результатами моих пациентов.
- **СТОИМОСТЬ.** Уверен, что вы будете удивлены, узнав, насколько

Спам-сообщение может состоять всего из одного слова-ссылки. Побудитель к действию в таком случае содержится в теме письма.


Тема:[SPAM] Доступные обьекты на Лазурном берегу
Дата: Tue, 25 Aug 2015 21:24:17 +0300
От:Фомина <gurushipsk@agnosiar.newmsgforyou3.net>
Кому:pr@drweb.com

подробнее

Все чаще тело спам-письма представляет собой одно изображение. Данный метод возник в связи с широким распространением антиспамов на основе анализа текстового содержимого письма. Текст графического спама отображен на картинке (как правило, в формате GIF или JPEG). При этом все изображение является ссылкой. Визуальный раздражитель привлекает внимание сильнее, чем текст. Особенно если на такой картинке – полураздетые девушки.

Изображение может быть анимированной GIF-картинкой с эффектом 25-го кадра. Оно состоит из несколько кадров — основного и еще 1-2 кадров, которые отображаются недолго и кроме графических «шумов» содержат установочные фразы, например, «BUY!». Мерцающая картинка привлекает внимание и усложняет работу анализаторов антиспам-системы. И очень раздражает!

http://compress.ru/article.aspx?id=17269

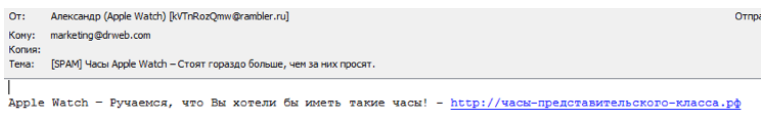
Установочные фразы — слова или их сочетания, настраивающие получателя на определенное отношение, эмоции или выполнение действий.

Пример анимированного спама с развернутыми под разным углом фрагментами изображения (картинка составлена из четырех отдельных кадров).

http://compress.ru/article.aspx?id=19069

Обратите внимание на подпись

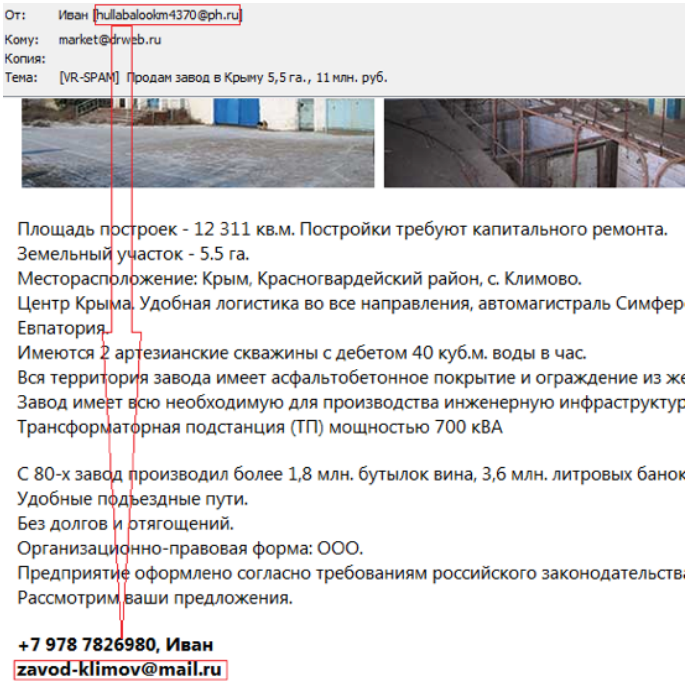
- Правилами хорошего тона в любой серьезной компании является указание в подписи контактов: адреса сайта, где можно найти подробную информацию, телефона/факса, e-mail. Отсутствие такой информации — тревожный сигнал, указывающий на низкое качество предлагаемой услуги или продукции, невозможность потребовать возврата или компенсации в случае возникновения проблем.


От: Александр (Apple Watch) [kVTnRozQmw@rambler.ru]
Кому: marketing@drweb.com
Копия:
Тема: [SPAM] Часы Apple Watch – Стоят гораздо больше, чем за них просят.

Apple Watch – Ручаемся, что Вы хотели бы иметь такие часы! – http://часы-представительского-класса.рф

В данном спам-сообщении подпись вообще отсутствует. Уважайте себя и не реагируйте на такие сообщения.

Адрес или имя отправителя могут не соответствовать контактам в подписи.

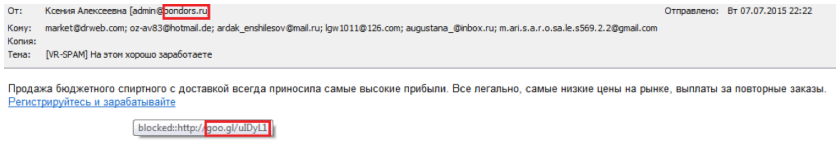


От: Иван [hullabalookm4370@ph.ru]
Кому: market@drweb.ru
Копия:
Тема: [VR-SPAM] Продам завод в Крыму 5,5 га., 11 млн. руб.

Площадь построек - 12 311 кв.м. Постройки требуют капитального ремонта.
Земельный участок - 5.5 га.
Месторасположение: Крым, Красногвардейский район, с. Климово.
Центр Крыма. Удобная логистика во все направления, автомагистраль Симфер
Евпатория.
Имеются 2 артезианские скважины с дебетом 40 куб.м. воды в час.
Вся территория завода имеет асфальтобетонное покрытие и ограждение из же
Завод имеет всю необходимую для производства инженерную инфраструктур
Трансформаторная подстанция (ТП) мощностью 700 кВА

С 80-х завод производил более 1,8 млн. бутылок вина, 3,6 млн. литровых банок
Удобные подъездные пути.
Без долгов и отягощений.
Организационно-правовая форма: ООО.
Предприятие оформлено согласно требованиям российского законодательства
Рассмотрим ваши предложения.

+7 978 7826980, Иван
zavod-klimov@mail.ru

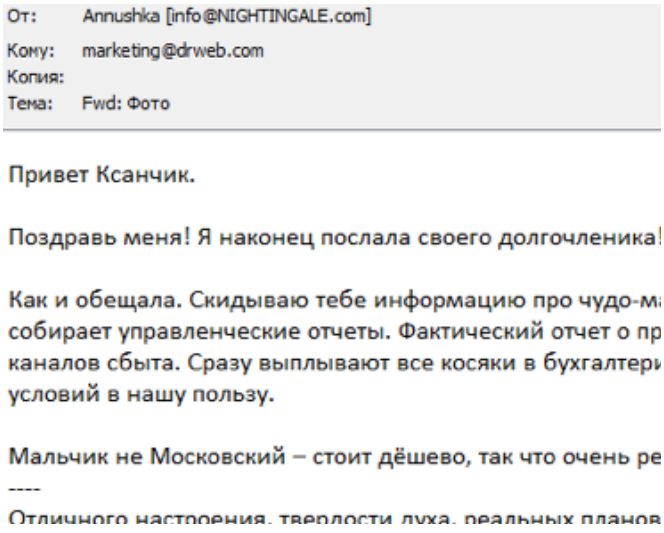


От: Ксения Алексеевна [admin@pondors.ru] Отправлено: Вт 07.07.2015 22:22
Кому: market@drweb.com; oz-av83@hotmail.de; ardak_enshilesov@mail.ru; lgw1011@126.com; augustana_@inbox.ru; m.ari.s.a.r.o.sa.le.s569.2.2@gmail.com
Копия:
Тема: [VR-SPAM] На этом хорошо заработаете

Продажа бюджетного спиртного с доставкой всегда приносила самые высокие прибыли. Все легально, самые низкие цены на рынке, выплаты за повторные заказы.
Регистрируйтесь и зарабатывайте

blocked::http://goo.gl/ulDyL1

Отправитель этого письма, судя по адресу, — администратор, что явно нехарактерно для продаж. Обычно все домены адресов легального письма принадлежат одной компании. Тут домен, по которому мы должны перейти, отличается от домена отправителя.



От: Annushka [info@NIGHTINGALE.com]
Кому: marketing@drweb.com
Копия:
Тема: Fwd: Фото

Привет Ксанчик.

Поздравь меня! Я наконец послала своего долгочленика!

Как и обещала. Скидываю тебе информацию про чудо-м
собирает управленческие отчеты. Фактический отчет о пр
каналов сбыта. Сразу выплывают все косяки в бухгалтери
условий в нашу пользу.

Мальчик не Московский – стоит дёшево, так что очень ре

Отличного настроения, твердости духа, реальных планов

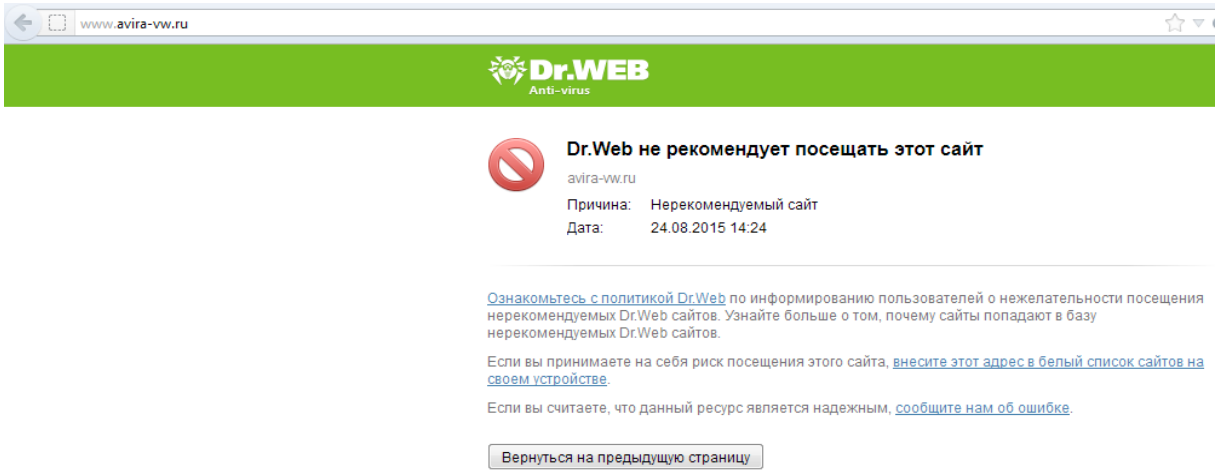
Письмо составлено от лица некой Аннушки, а подписано Дмитрием.

Будьте осторожны со ссылками в письме!

- Никогда не переходите по ссылкам в виде выделенных в тексте слов. Наведите на это слово курсор и проверьте, как выглядит ссылка.
- Никогда не переходите по ссылкам непосредственно из самого письма. Возможности современных почтовых клиентов (а именно, исполнения в письмах Java-скриптов) позволяют при нажатии ссылки перенаправить вас совсем на другой сайт, отличный от отображаемого в URL.
- Спам-письма могут не содержать ссылок, если в мошеннической схеме отъема денег задействован вишинг (в этом случае в письме будет указан только номер телефона) или смишинг (с номером мобильного, на который надо перевести деньги).
- Введите ссылку из сомнительного сообщения в браузер вручную — это позволит вам избежать подмены символов.

Современные антивирусы позволяют проверить репутацию сайта до перехода по ссылке на него.

- Если на вашем ПК используется Dr.Web Security Space, все ссылки проверяются веб-антивирусом SpIDerGate на принадлежность к уже известным вредоносным или потенциально опасным ресурсам. Убедитесь, что веб-антивирус не отключен.



- Если вы еще не используете Dr.Web, проверить ссылку можно при помощи Dr.Web LinkChecker – бесплатного расширения для браузеров, сканирующего интернет-страницы и файлы, скачиваемые из Интернета. В данном случае установка самого антивируса на компьютер или устройство не требуется — Dr.Web LinkChecker является облачным сервисом.

В подписи к спам-сообщению может присутствовать QR-код, который содержит ссылку. При считывании такой ссылки QR-сканером велик риск заражения мобильного устройства.

Length: 20-2000m

We could guarantee to reply your email within **2** working hours after your response and also free sample could be delivered if required.

Skype:jasonxujiajun

Tel: 0086-18112351020

Regards

Jason Xu

Sales Manager

Tel.: 86-510-85929121 Mon-Sun 8:30am to 5:30pm (China Time)
Fax: 86-510-85929115
Email:jasonxu@okorder.com

Source Using The OKorder.com App

Available on App Store

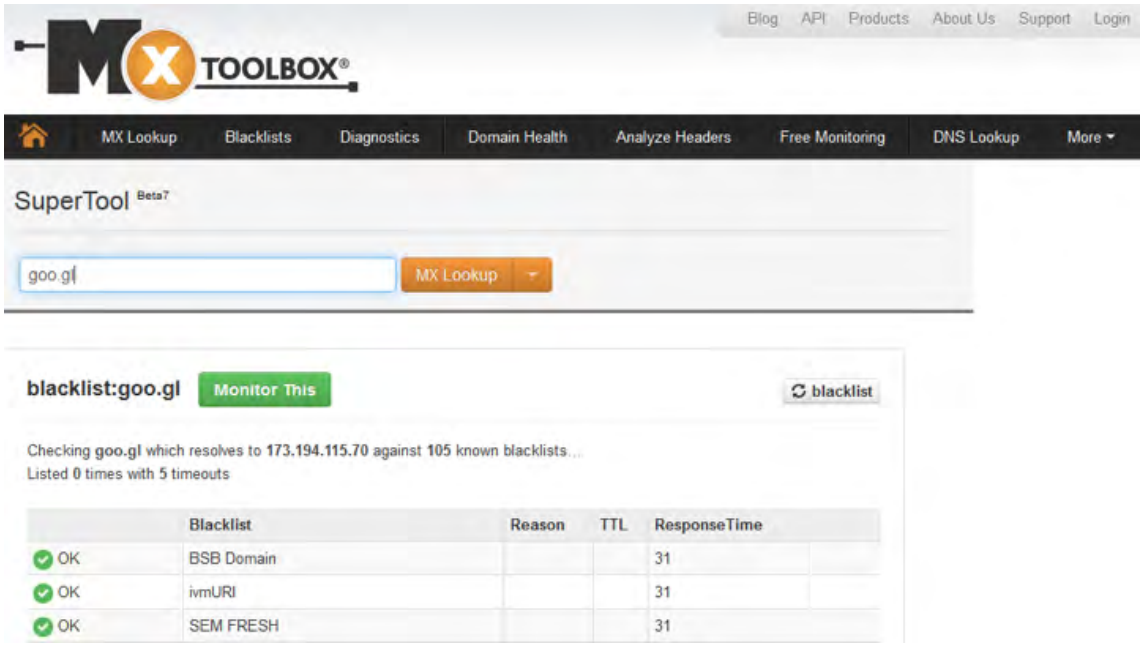
Available on Google Play

Should you refuse to receive this service, click unsubscribe at any time.

This email was sent from a notification-only address that cannot accept incoming email. PLEASE DO NOT REPLY to this message. If you have any questions or concerns, please Contact Us»

Проверьте домен спамеров

Проверить домен на наличие его в черных списках можно, например, с помощью сервиса mxtoolbox.com, просто введя команду “blacklist: domain_name.com”.

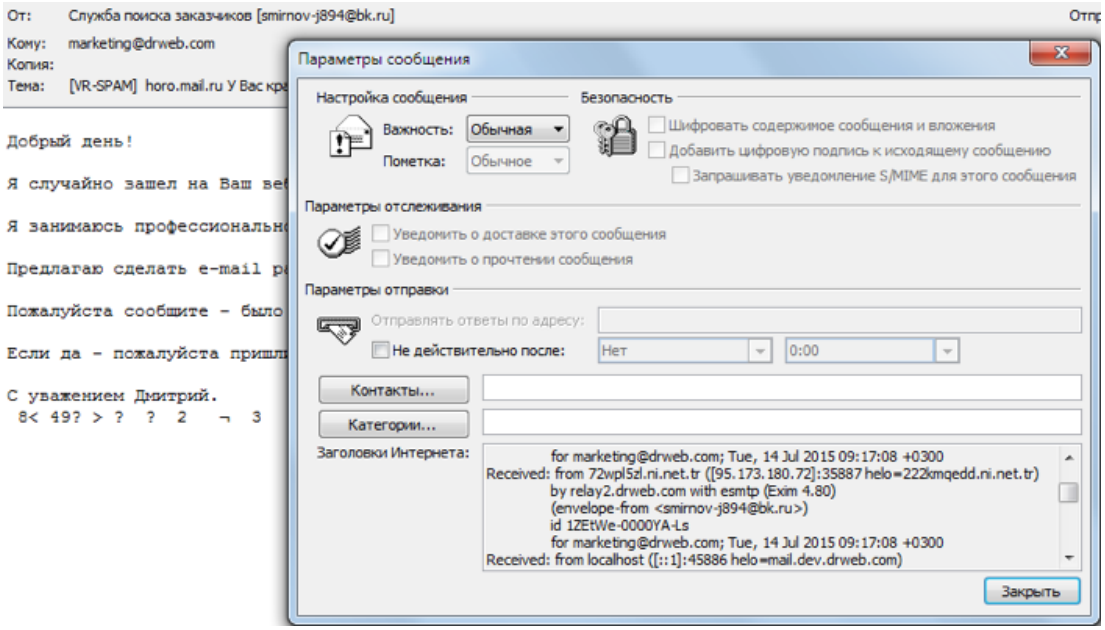


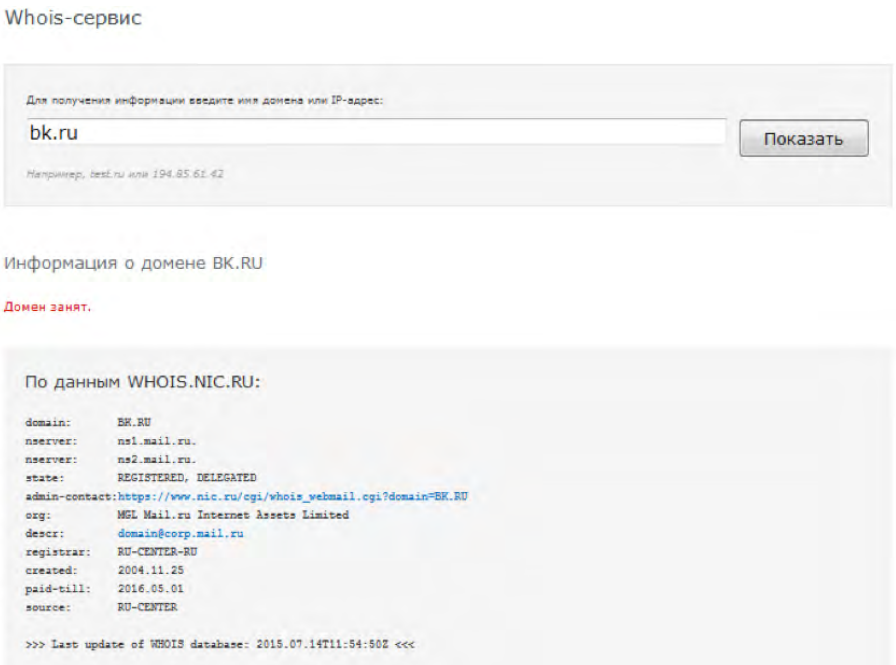
Как определить владельца домена, с которого рассылается спам?
К сожалению, при регистрации доменов можно указывать любые данные, а значит, найти владельца можно далеко не всегда.

Найти информацию о владельце домена проще всего при помощи сервисов Whois:

- https://www.nic.ru/whois
- https://www.reg.ru/whois
- http://www.webnames.ru/scripts/whois.pl

Например:





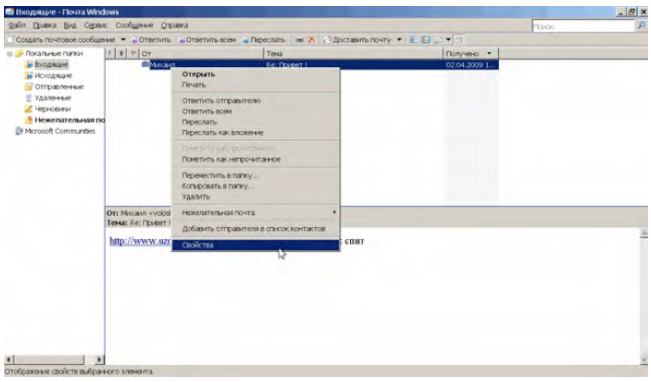
Здесь отображаются данные о владельце домена и его контакты. Если в поле «Администратор домена» (или Person) указано Private Person, это означает, что владелец по каким-то причинам хочет остаться неизвестным. В таком случае можно сделать следующее:

- Если известен email, то найти владельца можно через сервис http://2ip.ru/domain-list-by-email. Здесь можно узнать обо всех доменах, зарегистрированных на этот адрес. Возможно, в каких-то доменах опция Private Person будет отключена.
- Можно ознакомиться с историей домена с помощью следующих бесплатных сервисов (или их аналогов, в том числе платных (reg.ru)):
  http://who.is (доступна история с 2011-2012 годов);
  http://whoishistory.ru (работает в том числе и с доменами .рф, требуется авторизация);
  http://1stat.ru;
  http://whoistory.com (работает только с доменами .ru).

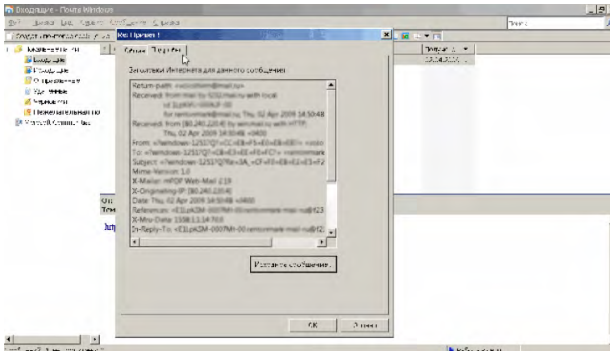
Как узнать служебную информацию полученного сообщения

Способ просмотра служебных заголовков зависит от почтового клиента:

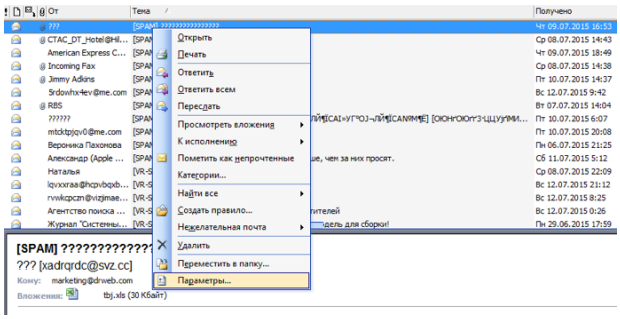
- Microsoft Outlook Express (Windows XP) или почта Windows (Windows Vista). Необходимо щелкнуть правой кнопкой мыши по письму в списке входящих и выбрать «Свойства» → «Подробности». Или нажать комбинацию клавиш Ctrl + F3.

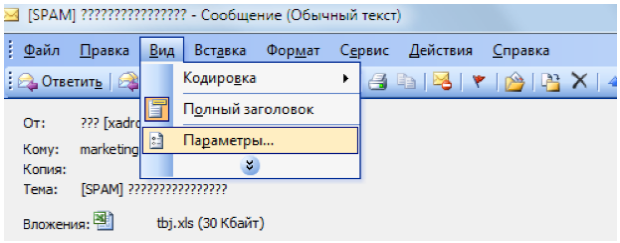


В открывшемся окне вы увидите заголовок письма для данного сообщения.

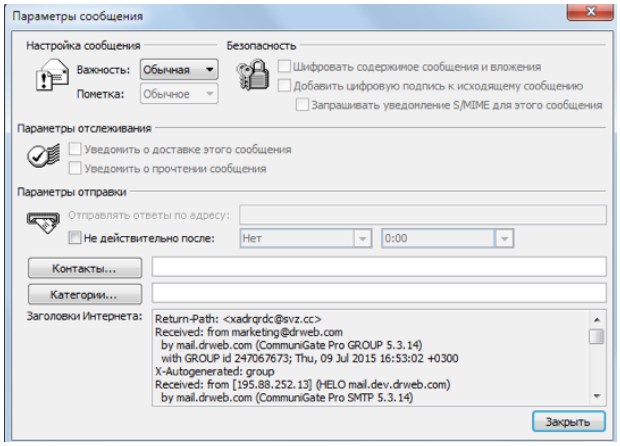


- Microsoft Outlook. Действия, которые нужно предпринять для получения необходимой информации, зависят от версии почтового клиента. Необходимо щелкнуть правой кнопкой мыши по письму в списке входящих и выбрать «Параметры».

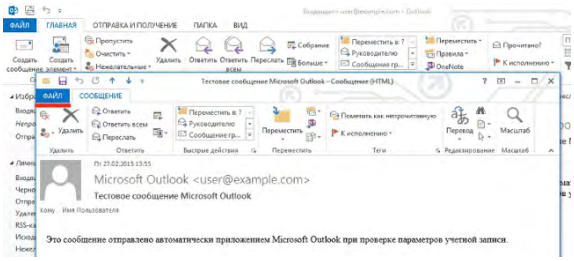


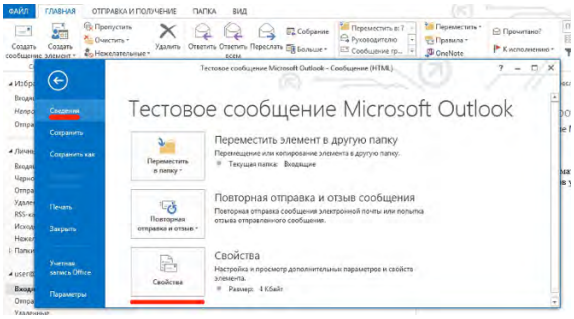


Далее следует открыть письмо в отдельном окне, в списке входящих дважды щелкнув по нему правой кнопкой мыши, затем нажать «Файл» → «Сведения» → «Свойства» или «Вид» → «Параметры». В открывшемся окне, в поле «Заголовки Интернета», вы увидите служебный заголовок.



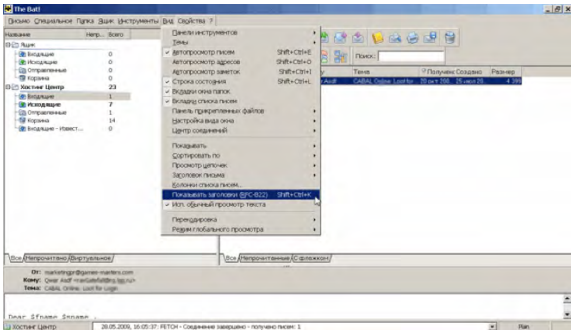
В Microsoft Outlook 2010 и 2013 необходимо открыть письмо двойным щелчком левой кнопки мыши, выбрать в меню «Файл» раздел «Сведения» и нажать на кнопку «Свойства».



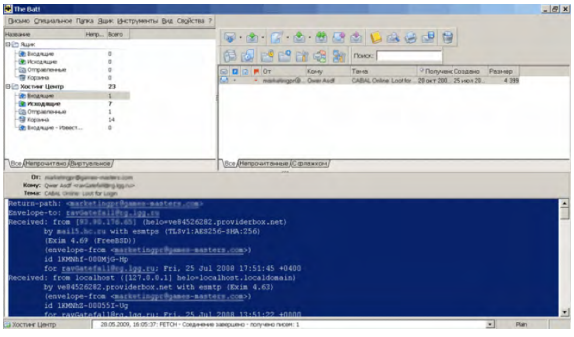


Служебные заголовки письма будут отображены в нижней части окна, в поле «Заголовки Интернета».

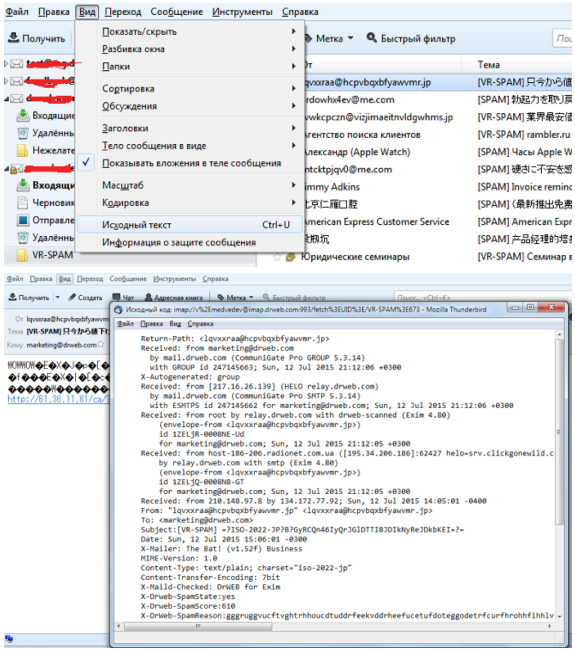
- The Bat! Необходимо в пункте меню «Вид» выбрать пункт «Показывать заголовки RFC (822)» или нажать комбинацию клавиш Shift + Ctr +K.



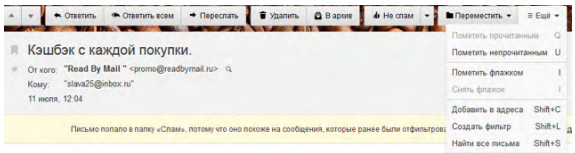
Заголовки отобразятся в нижнем окне просмотра:



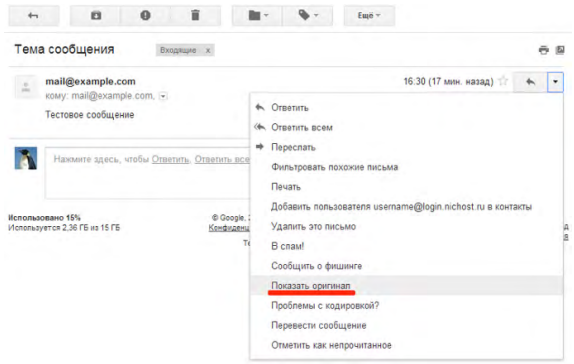
- Mozilla Thunderbird. Необходимо либо в пункте меню «Вид» (почтового клиента или открытого письма) выбрать «Исходный текст» сообщения или нажать Ctrl + U, либо в пункте меню «Вид» выбрать «Заголовки» → «Все».



- Mail.ru. Открыв письмо, нужно нажать «Еще» и в выпадающем списке выбрать «Служебные заголовки».



- Gmail.com. Необходимо открыть письмо, в правом верхнем углу нажать на кнопку со стрелкой вниз рядом с кнопкой «Ответить» и выбрать пункт меню «Показать оригинал».



В других почтовых клиентах или облачных сервисах почты методы получения служебной информации могут отличаться от приведенных выше.

Dr.WEB®
с 1992 года

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Компания имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Стратегической задачей компании, на которую нацелены усилия всех сотрудников, является создание лучших средств антивирусной защиты, отвечающих всем современным требованиям к этому классу программ, а также разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз.

Обучение
Кабинет заочника Dr.Web (требуется регистрация)
Курсы для инженеров | Курсы для пользователей | Брошюры

Просвещение
«Антивирусная правДА!» | ВебIQметр | Брошюры

Контакты
Центральный офис ООО «Доктор Веб»
125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а

Телефоны

Схема проезда

Контакты для прессы

Офисы за пределами России

антивирус.рф | www.drweb.ru | www.free.drweb.ru | www.av-desk.ru | www.drweb-curent.com

Присоединяйтесь к нам в социальных сетях