НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Угроза целевых атак на коммерческие и государственные компании в Российской Федерации

ALRT-20210803.1 | 3 августа 2021 г.

Уровень угрозы: КРИТИЧЕСИКЙ

TLP: AMBER

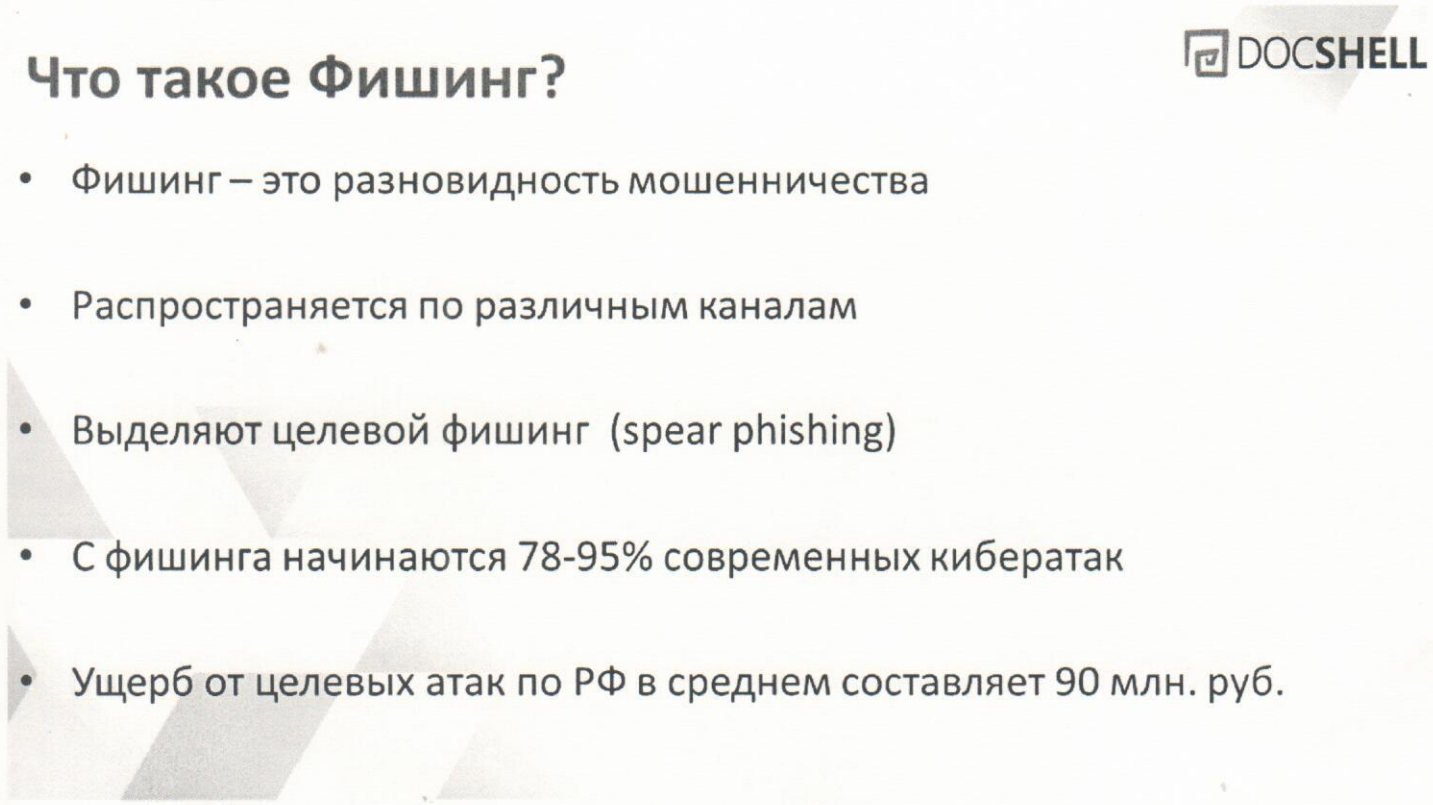
Цели	Коммерческие и государственные компании
Актуальность угрозы	Актуально по настоящее время
Описание	Специалистами Экспертного центра безопасности компании Positive Technologies (PT Expert Security Center, PT ESC) были выявлены новые атаки группировки APT31. Данная группировка, также известная как Hurricane Panda (CrowdStrike) и Zirconium (Microsoft), осуществляет свою деятельность примерно с 2016 года. Ключевыми интересами группировки является кибершпионаж и сбор конфиденциальных данных, представляющих стратегическую важность. Для внедрения ВПО в информационно-телекоммуникационную сеть (ИТС) организаций злоумышленники используют фишинговые рассылки. С января по июль 2021 года было зафиксировано более десятка таких рассылок. По имеющимся сведениям, интересы данной группировки в настоящее время нацелены на российские компании. В ходе исследования образцов ВПО специалисты PT ESC обнаружили ссылку на фишинговое доменное имя inst.rsnet-devel[.]com, имитирующее сайт федеральных органов государственной власти. По мнению экспертов Positive Technologies, такое доменное имя предназначено для введения в заблуждение госслужащих и сотрудников компаний, которые работают с госструктурами. Подробный отчет об исследовании данной вредоносной компании приведен по ссылке, представленной в соответствующем разделе бюллетеня.

Рекомендации по нейтрализации угрозы	В целях локализации данной угрозы рекомендуем: 1. Применить решающие правила, представленные в файле «apt31.rules», для выявления признаков компрометации элементов ИТС. 2. Проверить на ресурсах ИТС и в сетевом трафике наличие индикаторов компрометации, представленных в файле «IOC.csv». 3. Провести мероприятия, нацеленные на повышения бдительности и осведомленности сотрудников Вашей компании в части противодействия фишинговым атакам и иным методам социальной инженерии. В случае выявления признаков компрометации ИТС Вашей компании просим сообщить об этом в НКЦКИ.
Ссылки	https://www.ptsecurity.com/ru-ru/research/analytics/apt31-new-attacks/

Обучение ИБ. Фишинг и другие угрозы ИБ для пользователей. Часть 1. Введение

Инструктаж для пользователей по угрозам, связанным с Фишингом, вирусами и другими актуальными угрозами

Что такое фишинг?



! Фишинг (phishing) – это разновидность мошенничества, целью которого является получение паролей, банковских данных, конфиденциальной информации или заражения АРМ и серверов.

Как правило, злоумышленники массово рассылают электронные письма содержащие вредоносные вложения или ссылки на поддельные сайты новостных агенств, социальных сетей, банков или государственных органов. Возможны варианты массовых мошеннических рассылок СМС или автоматических голосовых вызовов.

Отдельно выделяют **целевой фишинг (spear phishing)**, когда рассылка готовится под определенную организацию или отрасль.

С фишинга начинаются большинство современных кибератак. Вас - пользователей корпоративных информационных систем, злоумышленники хотят обмануть, заставить запустить какой-то вредоносный файл или перейти на поддельный сайт. Поэтому несмотря на применяемые в организации меры защиты, не смотря на труд специалистов по защите информации в определенных ситуациях именно от пользователей, от их действий зависит – будет ли атака успешной и произойдет ли заражение.

К каким последствиям может привести успешная кибератака начавшаяся с Фишинга

Чем всё может закончится

DOCSHELL

Похищение важной информации

Для того чтобы понимать важность проблемы, давайте рассмотрим к каким последствиям может привести атака, в которой пользователь попался на Фишинг со стороны мошенников.

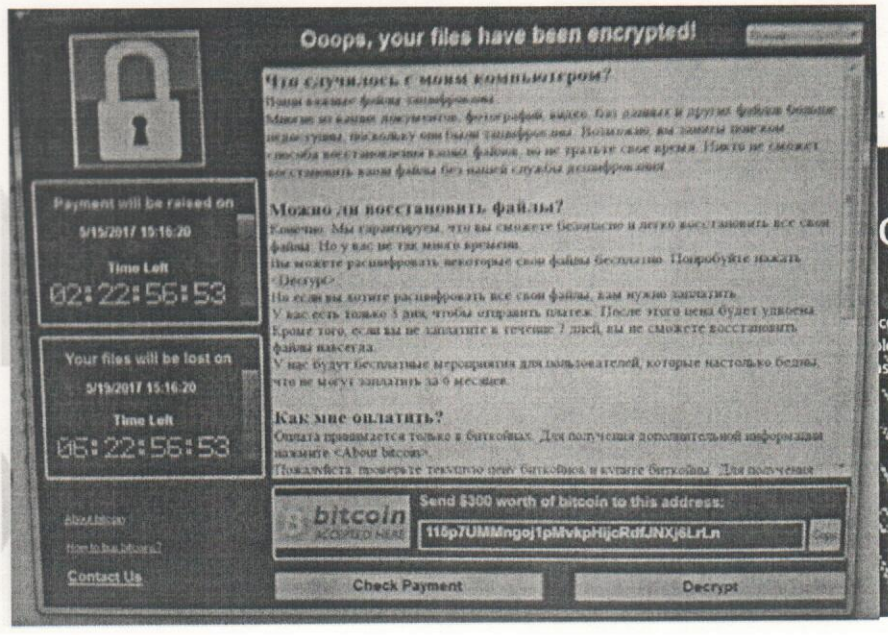
В случае заражения корпоративного компьютера вредоносным кодом оно может длительное время похищать ценную информацию оставаясь незамеченным. В дальнейшем утечка этой информации может нанести значительный ущерб для репутации и бизнеса организации.

Если в результате фишинга пользователь ввел на поддельном сайте свои учетные данных (логин и пароль), они используются злоумышленникам для доступа к личной и служебной переписке пользователя, похищения аккаунтов в социальных сетях и переводов денежных средств через системы интернет-банкинга.

Чем всё может закончится

DOCSHELL

Вирусы-шифровальщики WannaCry NotPetya



В 2017 году наиболее опасными оказались эпидемии вирусов шифровальщиков, таких как WannaCry и NotPetya, большая часть заражений которых пришлась на Российскую Федерацию. В результате запуска вредоносного кода вся доступная информация на компьютере и сетевых папках оказывается зашифрованной злоумышленником и заблокирована. За расшифровку и восстановление доступа к файлам требовали достаточно внушительную сумму выкупа. При этом для многих пользователей и организаций оказалась безвозвратно потерянной критичная информация, подготовленная за несколько месяцев.

DOCSHELL

Чем всё может закончится

Вредоносное использование ресурсов

В конце 2017 года из-за роста курса криптовалют, таких как bitcoin, существенное распространение получило вредоносное программное обеспечение, которые скрытно от пользователя и организации выполняет сложные вычисления, связанные с криптовалютами (майнинг). В результате этого существенно повышаются расходы на электроэнергию, а из-за сильной загрузки ресурсов компютера, затрудняется работа в приложениях, необходимых пользователю для выполнения его служебных обязанностей.

Обучение ИБ. Фишинг и другие угрозы ИБ для пользователей. Часть 2. Как распознать фишинг

Инструктаж для пользователей по угрозам, связанным с Фишингом, вирусами и другими актуальными угрозами

Как распознать фишинг

Как распознать Фишинг

DOCSHELL

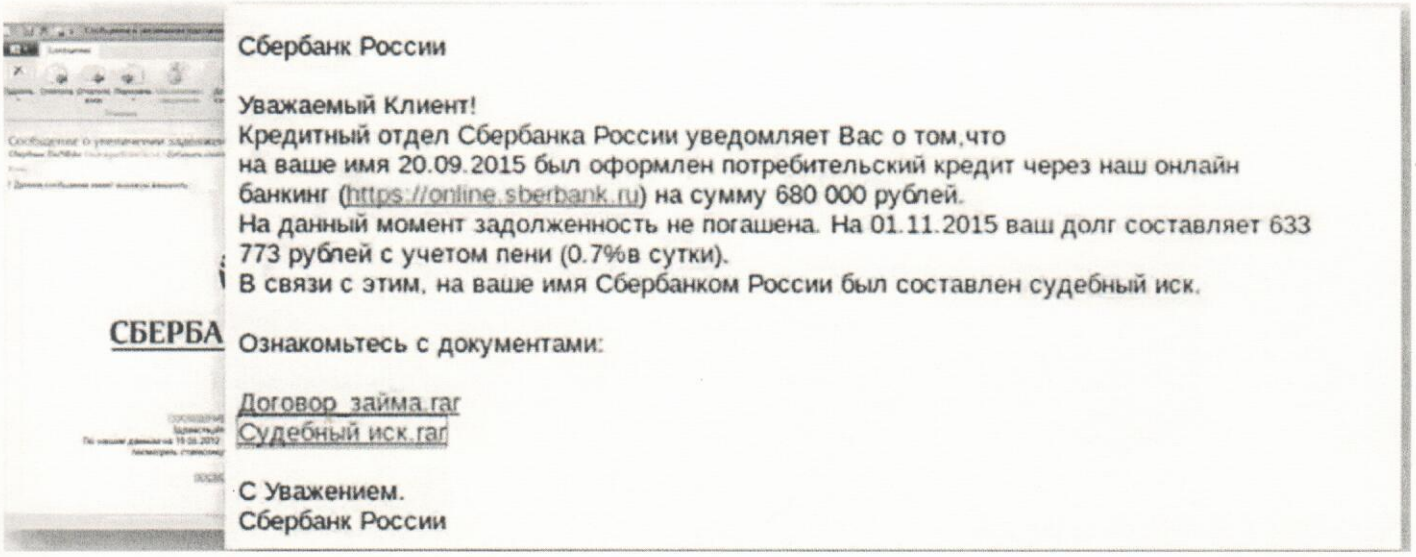
- Слабости
- Сильные эмоции
- Манипуляция

Мошенники стараются использовать Ваши слабости, для того чтобы достичь своих целей – получить информацию или побудить Вас сделать что-либо.
Слабости вызывают сильные эмоции (страх, гнев, любопытство и т.п.) и позволяют на секунду отключить критическое мышление.
Этой секунды как раз хватит чтобы кликнуть по ссылке или открыть вложенный файл.
Если вами **пытаются манипулировать –** скорее всего это мошенники.

Как распознать Фишинг

DOCSHELL

Все что нужно злоумышленнику – чтобы вы запустили приложенный к письму файл



Сбербанк России

Уважаемый Клиент!
Кредитный отдел Сбербанка России уведомляет Вас о том,что
на ваше имя 20.09.2015 был оформлен потребительский кредит через наш онлайн банкинг (https://online.sberbank.ru) на сумму 680 000 рублей.
На данный момент задолженность не погашена. На 01.11.2015 ваш долг составляет 633 773 рублей с учетом пени (0.7%в сутки).
В связи с этим, на ваше имя Сбербанком России был составлен судебный иск.

СБЕРБА

Ознакомьтесь с документами:

Договор_займа.rar
Судебный иск.rar

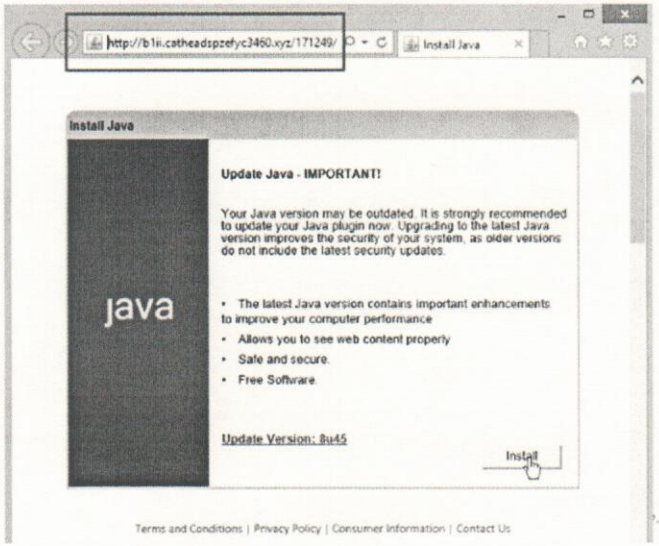
С Уважением.
Сбербанк России

При фишинге по электронной почте, злоумышленникам нужно чтобы вы запустили приложенный файл или перешли по внешней сслыке.

Как распознать Фишинг

DOCSHELL

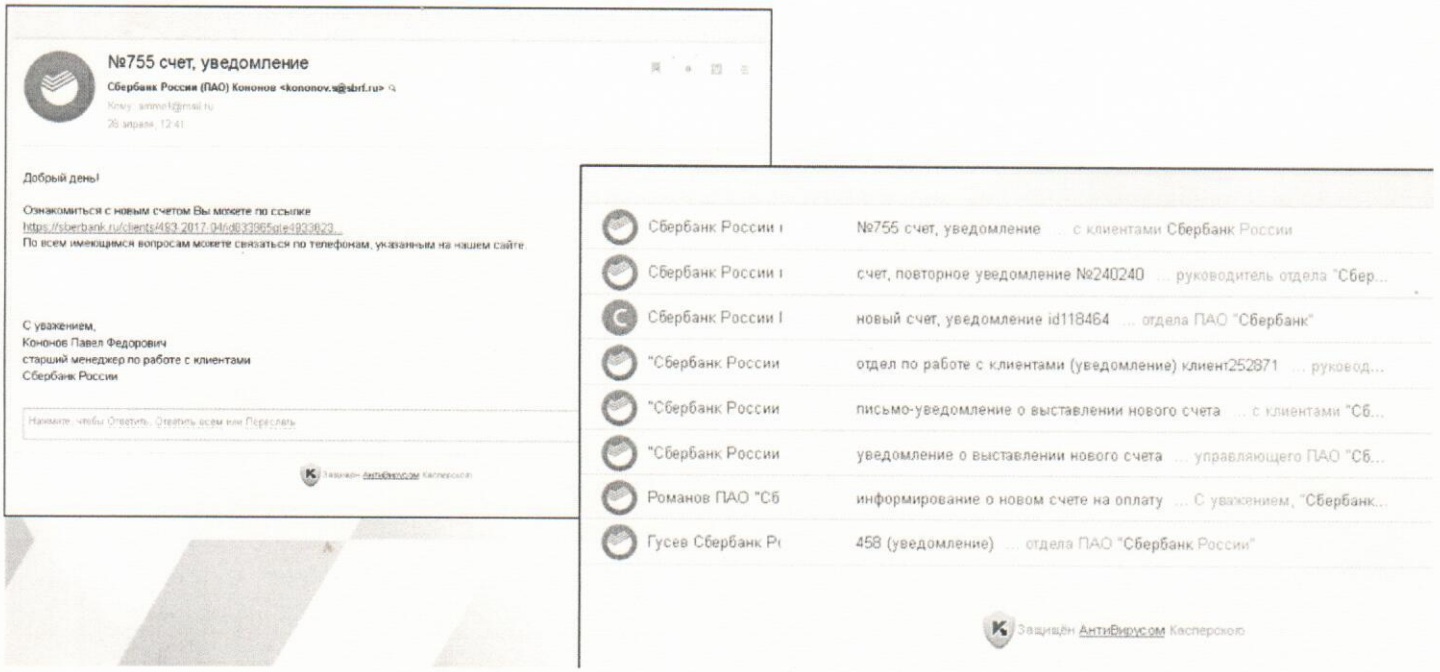
На фишинговом сайте - вас пытаются заставить скачать приложение или ввести свои учетные данные



На фишинговом сайте - Вас пытаются заставить скачать приложение или ввести свои учетные данные (логин и пароль).
Давайте посмотрим на несколько актуальных примеров фишинговых сообщений.

Актуальные примеры фишинговых писем

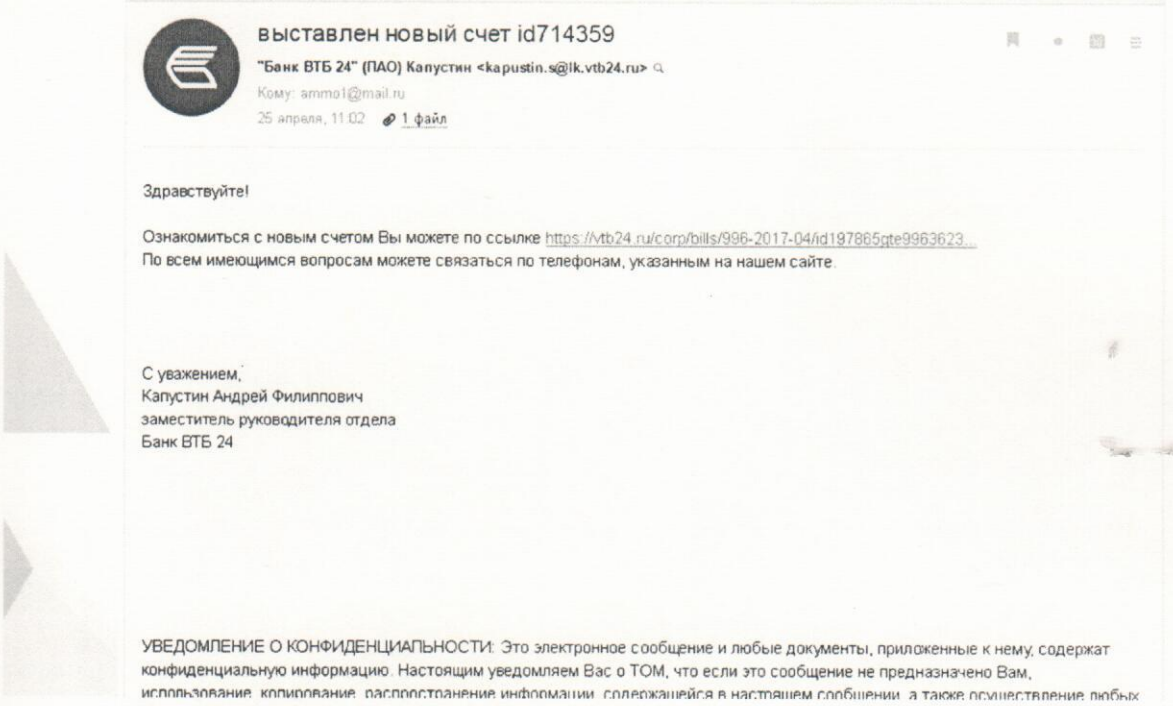
DOCSHELL



Традиционно злоумышленники предпочитают представляться Сбербанком, так больше шанс попасть в целевую аудиторию. Характерные признаки фишинга – обезличенное обращение говорит о массовости рассылки; короткий контактный телефон в подписи как правило не указывается, так как по нему легче проверить и найти злоумышленника.

Актуальные примеры фишинговых писем

DOCSHELL



Часто встречаются рассылки и от имени других популярных банков.

Актуальные примеры фишинговых писем

DOCSHELL

Госуслуги
Госпочта. Вам назначен штраф ГИБДД
Кому: Ilya Varlamov

Входящие - Google

ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО
ГОСУСЛУГИ

Госуслуги прозрачны как никогда

У Вас 1 новый штраф ГИБДД

Здравствуйте.
Вы подписались на уведомления о штрафах ГИБДД.
Мы нашли один штраф:

ШТРАФ ПО АДМИНИСТРАТИВНОМУ ПРАВОНАРУШЕНИЮ
ПОСТАНОВЛЕНИЕ
№1594372514948785
ОТ 05.02.2017г

250 руб.
со скидкой 50%

нужно заплатить до: 05.05.2017
со скидкой 50% до: 25.02.2017
подробности о штрафе

Фото

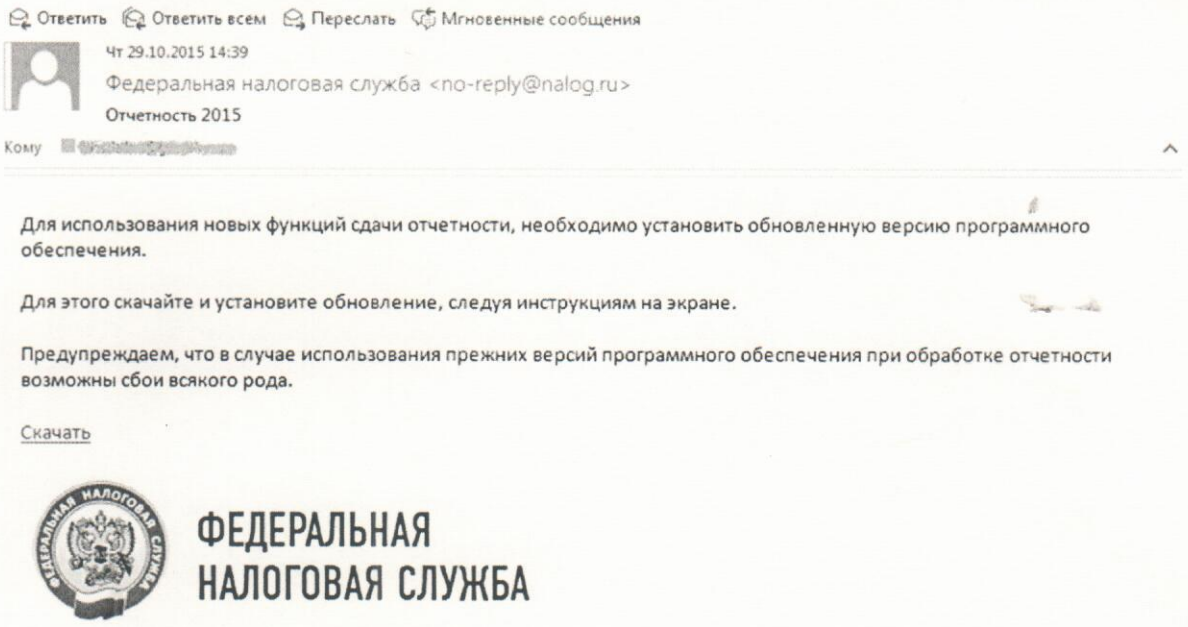
Обратная связь Помощь Отменить рассылку

госуслуги
Проще, чем кажется

Злоумышленники часто представляются государственными органами. В данном случае поддельное письмо было отправлено с адреса no-reply@gosuslugi-gov.ru, когда как письма от Госуслуг отправляются с адреса no-reply@gosuslugi.ru. Кроме того, мошенники забыли, что у Госуслуг сменился логотип.
Либо поддельные сайты и сообщения электронной почты содержат старые логотипы, опечатки и орфографические ошибки, чтобы избежать спам фильтров. Благодаря этому внимательный пользователь может определить подделку.

Актуальные примеры фишинговых писем

DOCSHELL



Ответить Ответить всем Переслать Мгновенные сообщения

Чт 29.10.2015 14:39
Федеральная налоговая служба <no-reply@nalog.ru>
Отчетность 2015

Кому [redacted]

Для использования новых функций сдачи отчетности, необходимо установить обновленную версию программного обеспечения.

Для этого скачайте и установите обновление, следуя инструкциям на экране.

Предупреждаем, что в случае использования прежних версий программного обеспечения при обработке отчетности возможны сбои всякого рода.

Скачать

ФЕДЕРАЛЬНАЯ НАЛОГОВАЯ СЛУЖБА

Популярны рассылки от органов государственного контроля – ФНС, ЦБ РФ и других. Пользователи под страхом получения штрафов не задумываясь скачивают и запускают файлы, приходящие якобы от официальных лиц и с пометкой “срочно”.

Также за последний год фиксировались следующие фишинговые рассылки:

от имени социальных сетей: facebook, вконтакте, одноклассники – рассылки о необходимости смены и восстановления паролей, рассылки о заблокированных учетных записях

от имени почтовых систем: mail.ru или google.com – про необходимость сменить пароль или разблокировать запись

от имени типографий – с просьбой подписать акты приема материалов

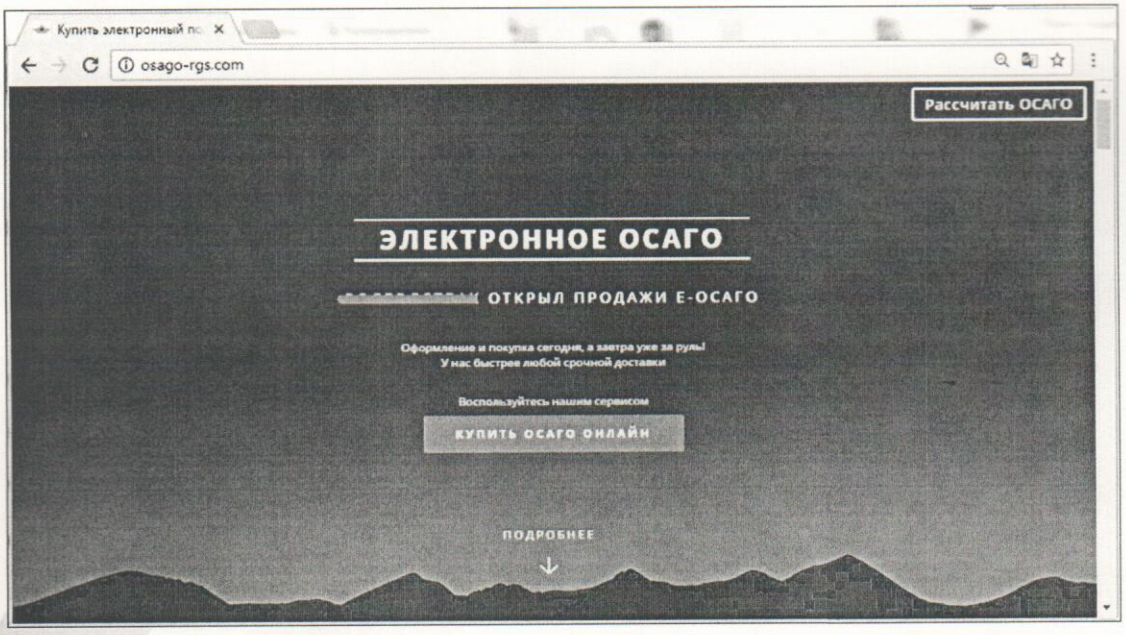
от имени партнеров – с просьбой провести сверку документов

Фишинговые сайты

Для поддельных сайтов злоумышленники обычно используют похожие имена. Например, подделка “s-mail-google.com” на официальный сайт “mail.google.com”. Подделка “online.sberblank.ru” на официальный сайт “online.sberbank.ru”. Также чтобы в вести в заблуждение пользователей применяется похожее оформление и фирменные цвета на сайте.
Давайте посмотрим на несколько актуальных примеров, обнаруженных в этом году.

Актуальные примеры фишинговых сайтов

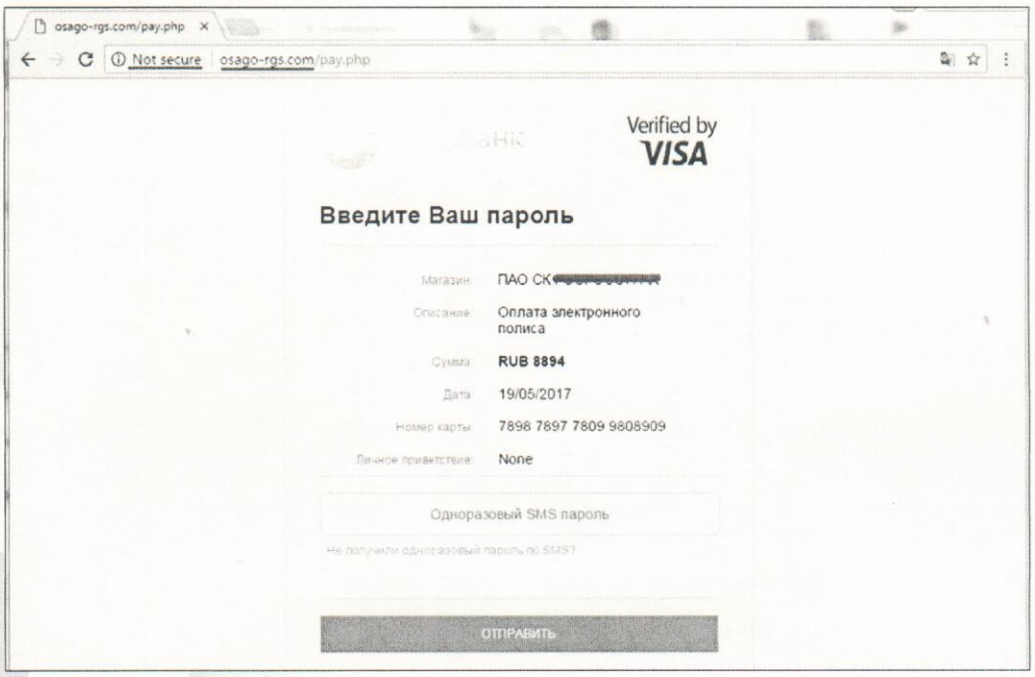
DOCSHELL



Главная страница фишингового сайта полностью копирует оформление сайта известной страховой компании. Как только посетитель изъявляет желание купить электронный полис ОСАГО и нажимает красивую кнопку в центре экрана, открывается

страница, на которой предлагается рассчитать стоимость страхования. Для этого нужно заполнить небольшую анкету, в том числе указать имя, дату рождения, номер водительского удостоверения и данные об автомобиле.
После завершения всех «формальностей» жертве предлагают оплатить электронный полис ОСАГО с помощью банковской карты. Для этого нужно указать в соответствующих полях номер карты, дату окончания ее действия и CVC/CVV-код.
В результате вышеописанных действий в руки мошенников попадает достаточно информации, которую можно использовать для развития атаки на жертву или, что происходит чаще, продать третьим лицам. В последнем случае кража средств происходит через некоторый промежуток времени; распространенный способ вывода денег – покупка товаров в онлайн-магазине с последующей перепродажей. Не все банки поддерживают двухфакторную аутентификацию по протоколу 3-D Secure, поэтому многие товары и услуги можно оплатить картой без кода подтверждения, а следовательно — без участия жертвы.

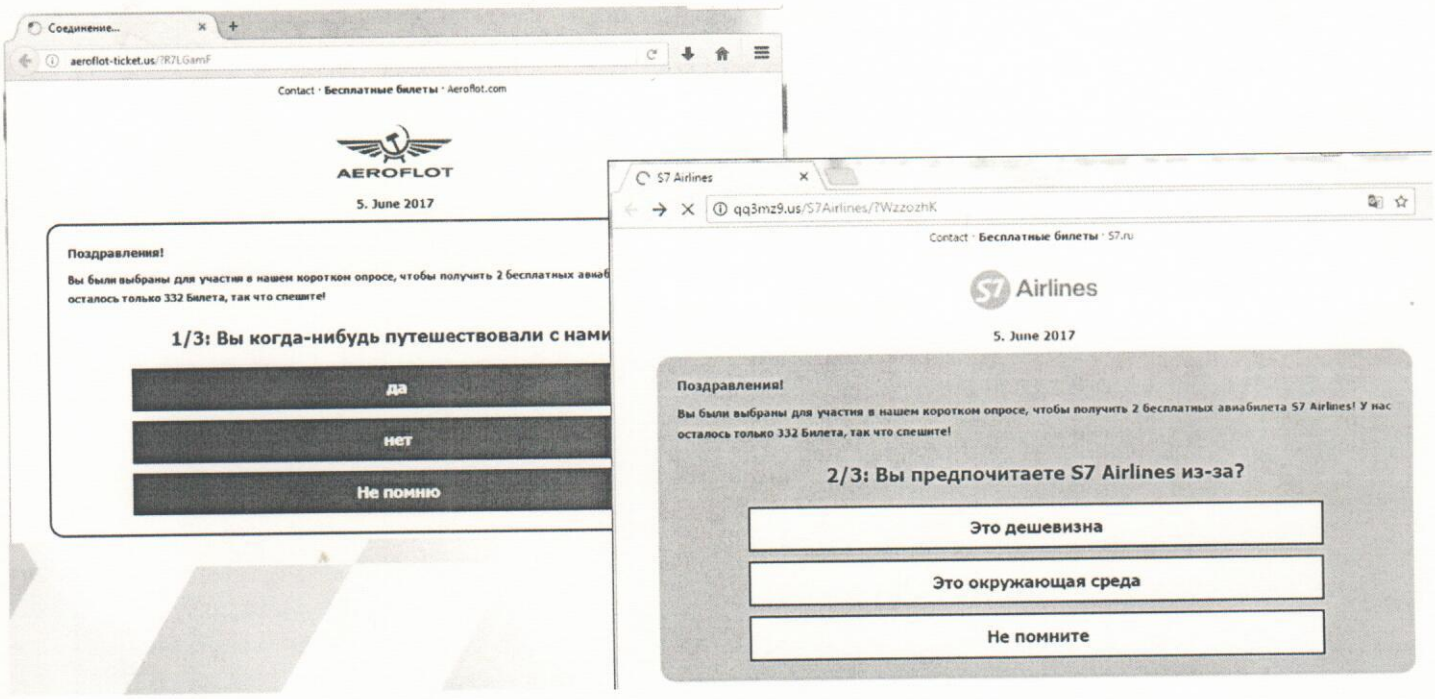
Актуальные примеры фишинговых сайтов



Однако в рассматриваемом примере мошенники пытаются украсть деньги самостоятельно и «не отходя от кассы». Для этого они перенаправляют жертву на поддельную страницу подтверждения оплаты, где просят ввести код из SMS, полученной от банка. В случае успеха злоумышленники обходят двухфакторную аутентификацию и получают деньги без каких-либо дополнительных усилий.
Обратите внимание на отсутствие защищенного соединения при открытии данной страницы, а также на то, что в ходе оплаты домен не изменился – обычно запрос кода из SMS происходит уже на защищенной странице платежной системы. Естественно, фишинговая страница не имеет никакого отношения к банку, упоминаемому на ней для введения жертвы в заблуждение.

Актуальные примеры фишинговых сайтов

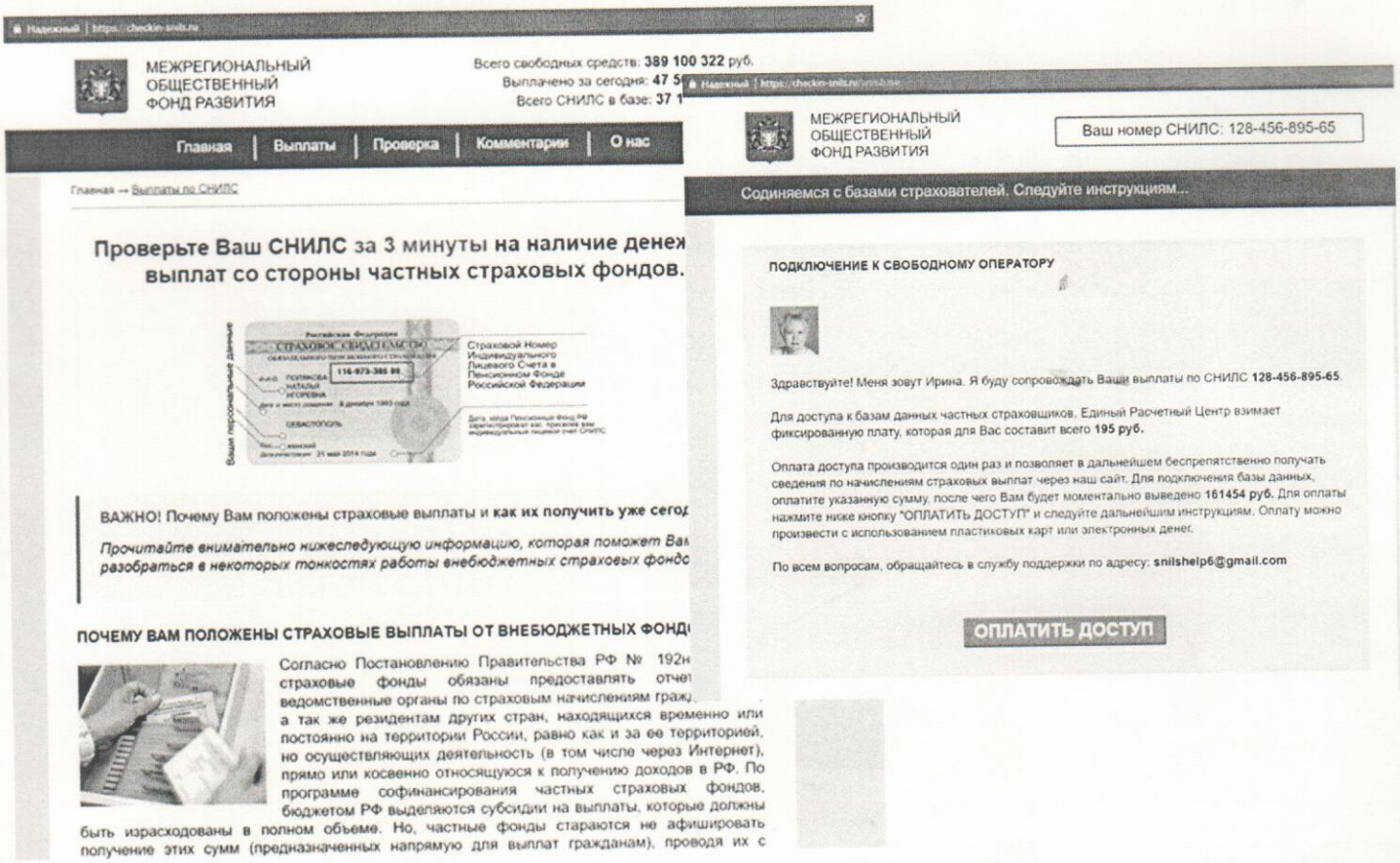
DOCSHELL



Ещё один свежий пример – раздача бесплатных авиабилетов. Использовалась символика «Аэрофлот» и S7 Airlines. Ответив на вопросы пользователям предлагалось поделится с друзьями информацией об акции на своей странице в соц.сетях, а для получения билетов необходимо было подтворить свой номер телефона – в результате чего пользователь оказывался подписан на платную услугу стоимостью 30 руб. в сутки.

Актуальные примеры фишинговых сайтов

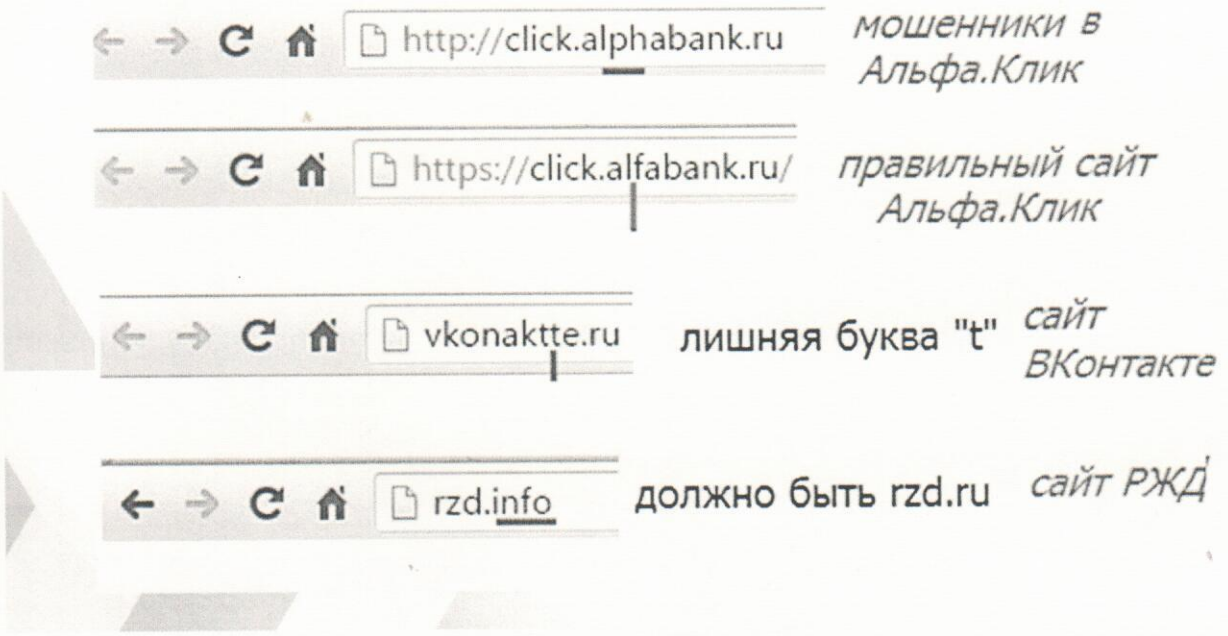
DOCSHELL



Ещё в одном недавнем случае, мошенники представлялись страховыми фондами. Всего было зарегистрировано более 50 поддельных сайтов, действующих от имени "Внебюджетного финансового фонда развития", "Социального фонда общественной поддержки" либо "Межрегионального общественного фонда развития". Предлагалось произвести проверку по своему номеру СНИЛС в результате которого необходимо пользователю сообщалось о возможности получения от фондов, якобы положенных гражданину начислений общей суммой более 150 тыс. руб. Для получения денег необходимо было оплатить единую пошлину в размере 195 руб.

Актуальные примеры фишинговых сайтов

DOCSHELL



Традиционно мошенники пытались подделывать популярные сайты банков, социальных сетей, почтовых службы, РЖД у других сервисов. Как видно в большинстве поддельных сайтов используется незащищенное соединение HTTP, так как получение SSL-сертификата дорогая и долгая процедура, а среднее время жизни мошеннических сайтов составляет несколько дней.

Актуальные примеры фишинговых сайтов

В корпоративной среде также фиксировались фишинговые сайты. Мошенники регистрировали похожие доменные адреса и создавали поддельные сайты, на которых были размещены ложная контактная информация и реквизиты счетов. Например, такие сайты:

mendeleev**sc**azot.ru (фальшивка) вместо mendeleevs**k**azot.ru (настоящий сайт)

k**y**azot.ru (фальшивка) и k**u**azot.ru

amo**nn**i.ru (фальшивка) и a**mm**oni.ru

tender-rosneft.ru (фальшивка) и **tender.**rosneft.ru

sibur.**info** (фальшивка) и sibur.ru

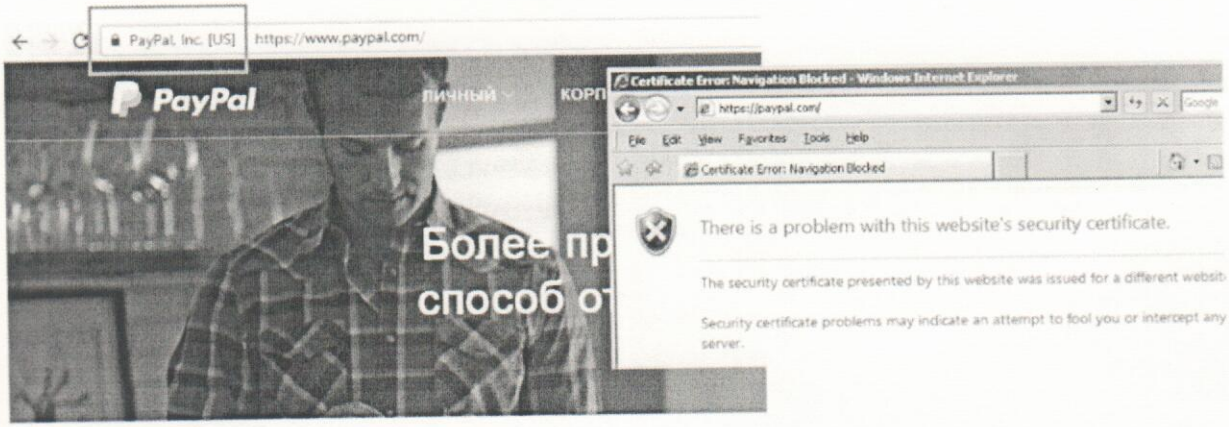
Обучение ИБ. Фишинг и другие угрозы ИБ для пользователей. Часть 3. Памятка пользователя

Инструктаж для пользователей по угрозам, связанным с Фишингом, вирусами и другими актуальными угрозами
Памятка пользователю

Памятка пользователю

DOCSHELL

Значок безопасного сайта



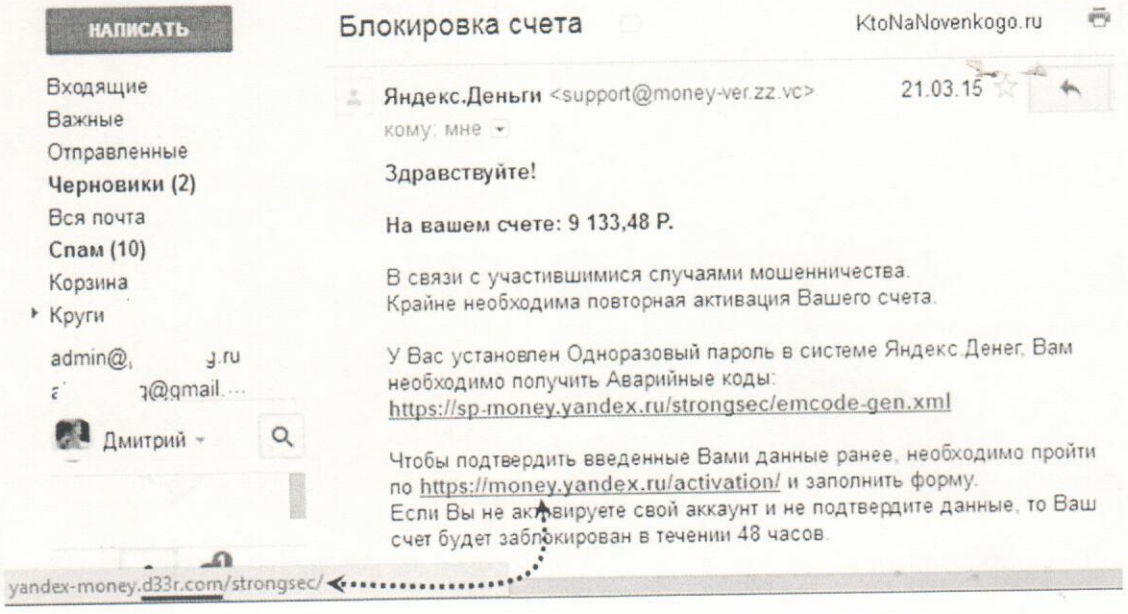
- Всегда HTTPS в адресной строке.
- Без ошибок или предупреждений безопасности.

При вводе логина, пароля или другой ценной информации на сайте убедитесь, что используется защищенное HTTPS соединения и действительный сертификат сайта – зеленый “замочек” слева от адреса сайта.
Кроме того, отсутствие сертификата сайта – один из признаков фишинга.

Памятка пользователю

DOCSHELL

Настоящий адрес сайта

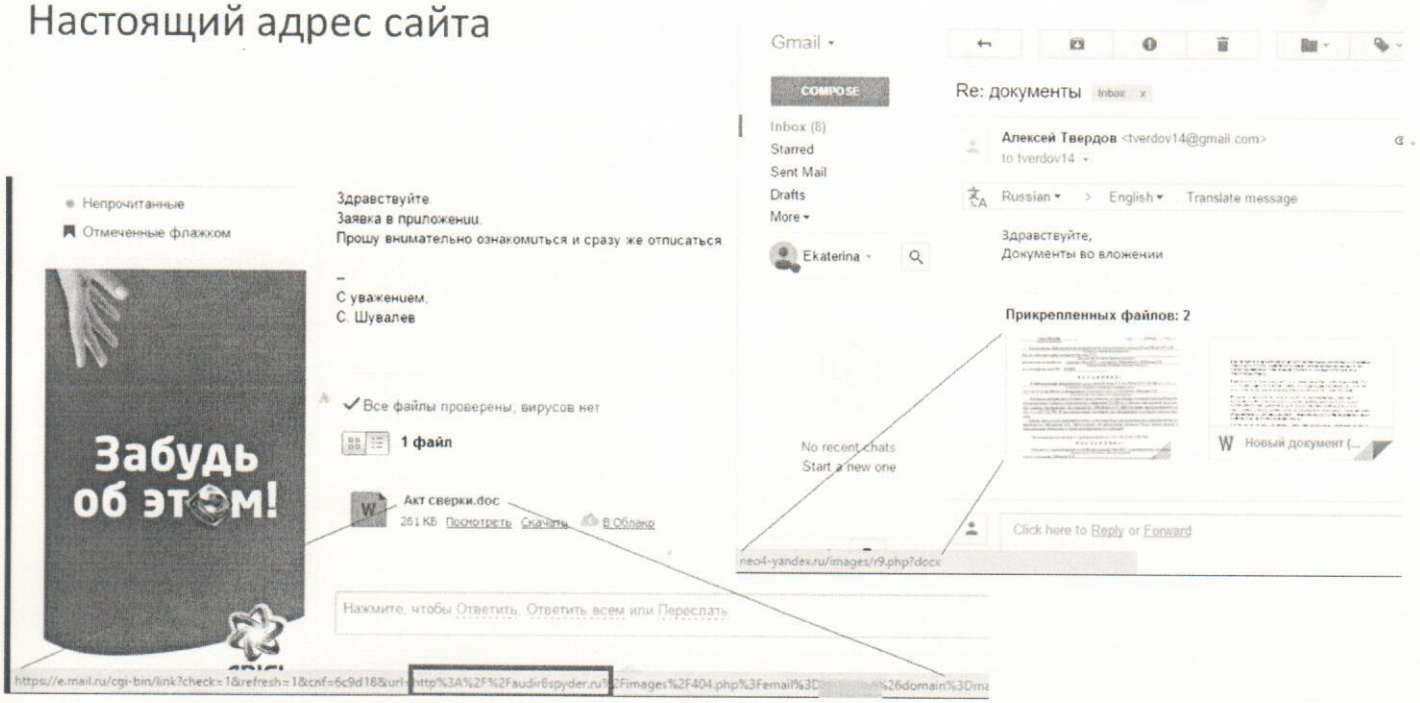


Всегда проверяйте какой настоящий адрес скрывается за ссылками в письме и на сайте. Для этого наведите мышку на ссылку в письме не нажимая её. В нижнем левом углу браузера вы увидите настоящий адрес сайта в сети Интернет. В данном примере это домен d33r.com

Памятка пользователю

DOCSHELL

Настоящий адрес сайта

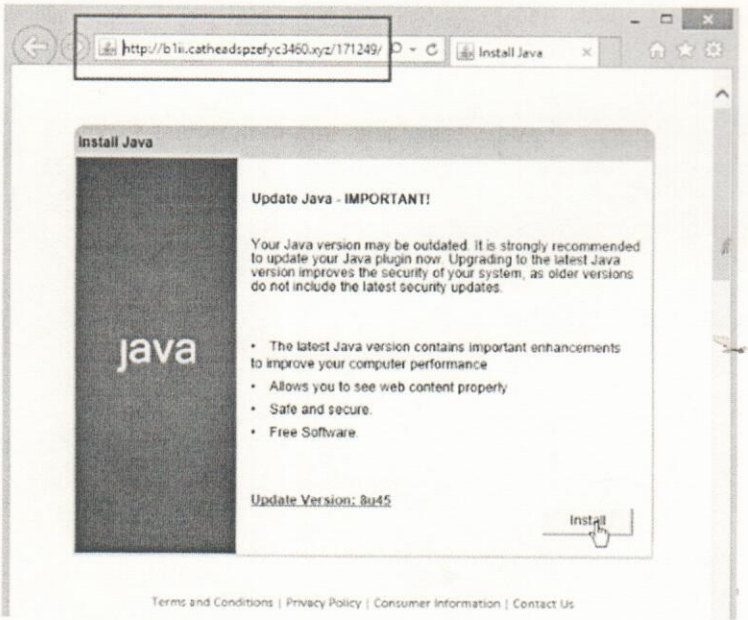


Ещё несколько примеров как под файлами или картинками скрываются ссылки на фишинговые сайты.

Памятка пользователю

DOCSHELL

Не скачивайте неизвестные файлы



Часто фишинговые сайты сообщают об обновлении и проблеме, которую надо решить – для этого вам предлагают скачать файл или установить программу, в которой как правило содержится вредоносный код.

Будьте осторожны и не переходите по необычным ссылкам во время работы в сети Интернет, не скачивайте файлы или не открывайте вложения электронной почты, если вы не уверены в их надежности.

Для проверки безопасности вложений, пришедших по электронной почте, обращайтесь к администратору антивирусной защиты, а установку нового программного обеспечения проводите только при участии системного администратора вашей организации. Для проверки надежности сайтов сети Интернет используйте сервисы: *https://virustotal.com/* и *https://rescan.pro*

Зачастую мошенники просят отключить антивирус для того чтобы он не помешал установке важного программного обеспечения. Это один из признаков фишинга. Не отключайте защитные механизмы антивируса и не препятствуйте получению обновлений антивирусных программ. Не отключайте персональный межсетевой экран и иные средства защиты информации, установленные на вашем компьютере.

Создавайте свой пароль с применением заглавных и строчных букв, а также цифр, не используя простые для угадывания варианты.

Не используйте во внешних сервисах сети Интернет те же пароли, которые используете в служебной деятельности. Никогда не сообщайте свой пароль по электронной почте или телефону.