

# 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: КРИТИЧЕСКИЙ

TLP: AMBER

Цели	Актуальность угрозы	Описание
Коммерческие и государственные компании	Актуально по настоящему времени	<p>Специалистами Экспертного центра безопасности компании Positive Technologies (РТ Expert Security Center, РТ 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.</p> <p>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.</p> <p>В ходе исследования образцов ВПО специалисты РТ ESC обнаружили ссылку на фишинговое доменное имя <a href="http://inst.rsnet-devel[.]com">inst.rsnet-devel[.]com</a>, 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.</p>

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, направленные 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 НКЦИ.

---

**Рекомендации по  
нейтрализации  
угроз**

---

**Ссылки**

[https://www.ptsecurity.com/ru-ru/research/analytics/apt31-new\\_attacks/](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?



#### Что такое Фишинг?

- Фишинг – это разновидность мошенничества
- Распространяется по различным каналам
- Выделяют целевой фишинг (spear phishing)
- С фишинга начинаются 78-95% современных кибератак
- Ущерб от целевых атак по РФ в среднем составляет 90 млн. руб.

! **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 агентств, 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 закончиться

DOC SHELL

## 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 данные (логин и пароль), они используются злоумышленниками для доступа к личной и служебной переписке пользователя, похищения аккаунтов в социальных сетях и переводов денежных средств через системы интернет-банкинга.

# Чем всё может закончиться

DOC SHELL

## Вирусы-шифровальщики WannaCry NotPetya

**Oops, your files have been encrypted!**

**Что случилось с моим компьютером?**

Ваше важные файлы были зашифрованы. Многие из ваших документов, фотографий, видео, баз данных и других файлов становятся недоступны, поскольку они были зашифрованы. Возможно, вы заметили признаки атаки вируса восстановления ваших файлов, но не тратите свое время. Никто не сможет восстановить ваши файлы без нашей специальной дешифровки.

**Можно ли восстановить файлы?**

Конечно. Мы гарантируем, что вы сможете безопасно и легко восстановить все свои файлы. Но у вас не так много времени. Вы можете расшифровать некоторые свои файлы бесплатно. Попробуйте нажать «Decrypt». Но если вы хотите расшифровать все свои файлы, вам нужно заплатить. У вас есть только 3 дня, чтобы отдать платеж. После этого цена будет удвоена. Кроме того, если вы не заплатите в течение 7 дней, вы не сможете восстановить ваши файлы никогда.

У нас будут бесплатные мероприятия для пользователей, которые настолько бедны, что не могут заплатить за 6 месяцев.

**Как мне оплатить?**

Оплата производится только в биткоинах. Для получения дополнительной информации нажмите <About Bitcoin>. Пожалуйста, проверьте текущую цену биткоина и купите биткоины. Для получения

Send \$300 worth of bitcoin to this address:

**bitcoin**  
ACCEPTED HERE  
116p7UMMingoJ1pMvkPhIjcRafJNXj6LrLn

Check Payment      Decrypt

**computer has been encrypted**

computer have been encrypted with an military grade encryption. It's impossible to recover your data without an special key. This page will help you to understand what happened to your computer and how to get back your data. You can use this key and the complete decryption of your computer.

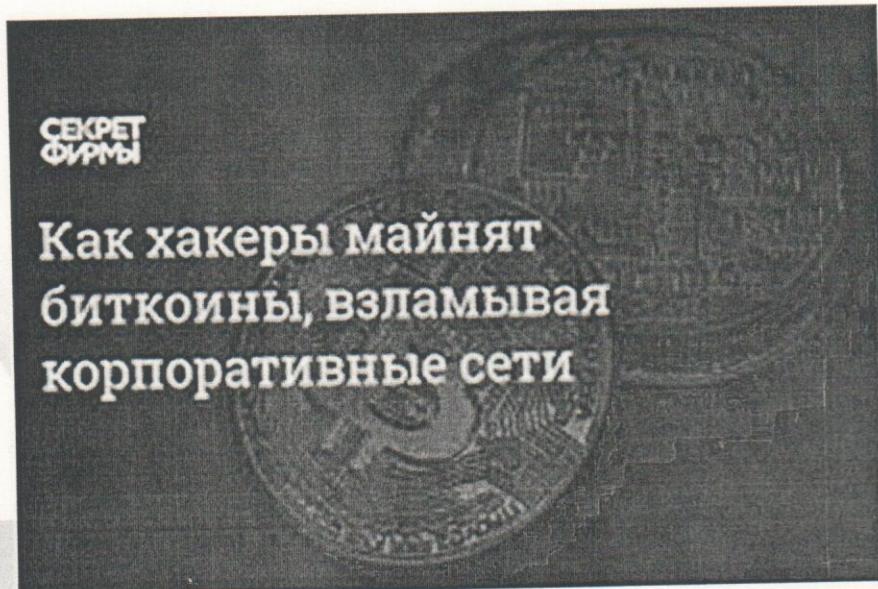
The price will be doubled in 7 days.

13 hours 43 minutes 10 seconds

Start the decryption process

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 потеряной критичная информация, подготовленная за несколько месяцев.

## Чем всё может закончиться 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 компьютера, 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



- Слабости
- Сильные эмоции
- Манипуляция



Мошенники стараются использовать Ваши слабости, для того чтобы достичь своих целей – получить информацию или побудить Вас сделать что-либо.

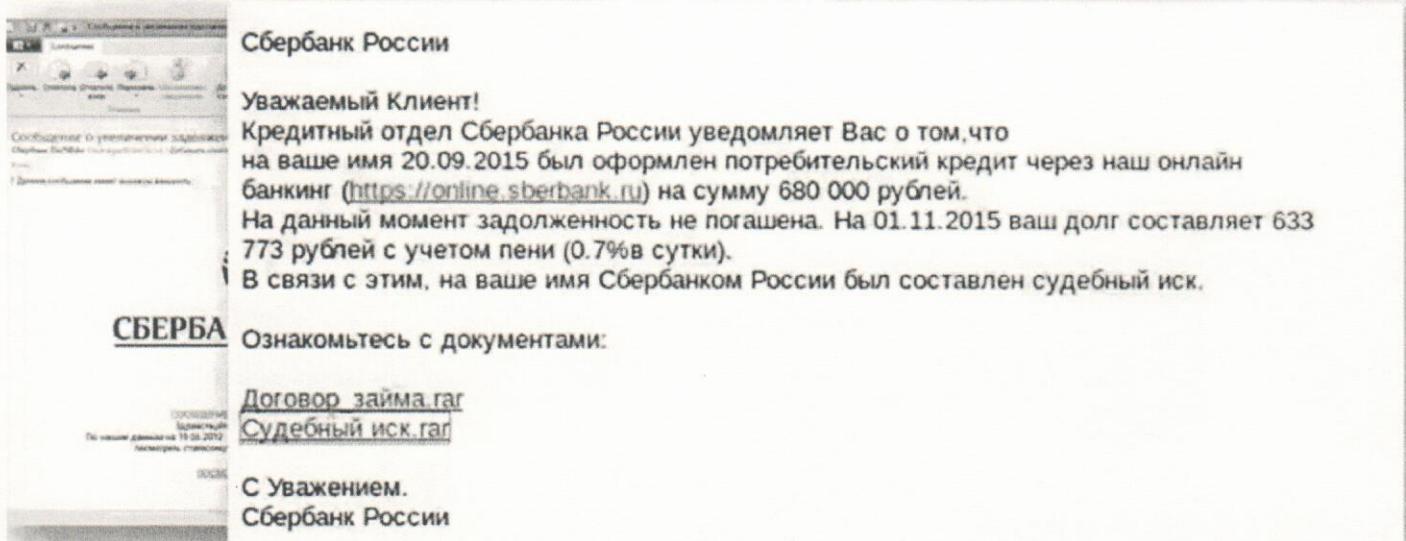
Слабости вызывают сильные эмоции (страх, гнев, любопытство и т.п.) и позволяют на секунду отключить критическое мышление.

Этой секунды как раз хватит чтобы кликнуть по ссылке или открыть вложенный файл.

**Если вами пытаются манипулировать – скорее всего это мошенники.**

# Как распознать Фишинг

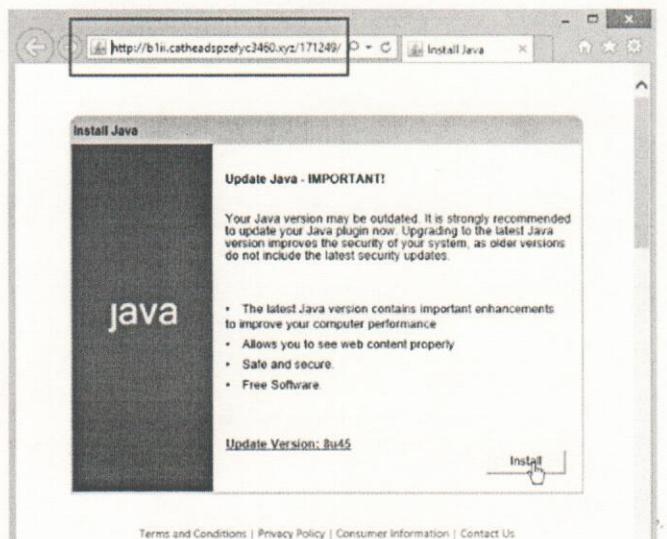
Все что нужно злоумышленнику – чтобы вы запустили приложенный к письму файл



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

## Как распознать Фишинг

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



№755 счет, уведомление  
Сбербанк России (ПАО) Кононов <kononov.v@sbirf.ru>   
Кому: ammo1@mail.ru  
26 апреля, 12:41

Добрый день!

Ознакомиться с новым счетом Вы можете по ссылке  
[https://sberbank.ru/clients/493\\_2017-04/d033965gtel4933623](https://sberbank.ru/clients/493_2017-04/d033965gtel4933623)  
По всем имеющимся вопросам можете связаться по телефонам, указанным на нашем сайте.

С уважением,  
Кононов Павел Федорович  
старший менеджер по работе с клиентами  
Сбербанк России

Нажмите, чтобы Ответить, Ответить всем или Переслать

 Защищен [Anti-Virus.com](#) Касперского

Сбербанк России	№755 счет, уведомление	с клиентами Сбербанк России
Сбербанк России	счет, повторное уведомление №240240	руководитель отдела "Сбер... Сбербанк"
Сбербанк России	новый счет, уведомление id118464	отдел по работе с клиентами (уведомление) клиент252871 ... руковод... письмо-уведомление о выставлении нового счета ... с клиентами "Сб... Сбербанк"
"Сбербанк России	"Сбербанк России	уведомление о выставлении нового счета ... управляющего ПАО "Сб... Сбербанк"
"Сбербанк России	Романов ПАО "Сб	информирование о новом счете на оплату ... С уважением, "Сбербанк... Сбербанк"
Гусев Сбербанк Р	458 (уведомление)	отдела ПАО "Сбербанк России"

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



выставлен новый счет id714359  
"Банк ВТБ 24" (ПАО) Капустин <kapustin.s@lk.vtb24.ru>   
Кому: ammo1@mail.ru  
25 апреля, 11:02  1 файл

Здравствуйте!

Ознакомиться с новым счетом Вы можете по ссылке <https://vtb24.ru/corp/bills/996-2017-04/d197865gtel9963623>  
По всем имеющимся вопросам можете связаться по телефонам, указанным на нашем сайте.

С уважением,  
Капустин Андрей Филиппович  
заместитель руководителя отдела  
Банк ВТБ 24

УВЕДОМЛЕНИЕ О КОНФИДЕНЦИАЛЬНОСТИ: Это электронное сообщение и любые документы, приложенные к нему, содержат конфиденциальную информацию. Настоящим уведомляем Вас о том, что если это сообщение не предназначено Вам, использование, копирование, распространение информации, содержащейся в настоящем сообщении, а также осуществление любых

Часто встречаются рассылки и от имени других популярных банков.

## Актуальные примеры фишинговых писем



Госуслуги Госпоста. Вам назначен штраф ГИБДД  
Кому: Ilya Varlamov

**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.

нужно заплатить до: 05.05.2017 со скидкой 50% до: 25.02.2017  
размерность штрафа: 250 руб. со скидкой 50%

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



Ответить Ответить всем Переслать Мгновенные сообщения

Чт 29.10.2015 14:39

Федеральная налоговая служба <no-reply@nalog.ru>

Отчетность 2015

Кому: [no-reply@nalog.ru](#)

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

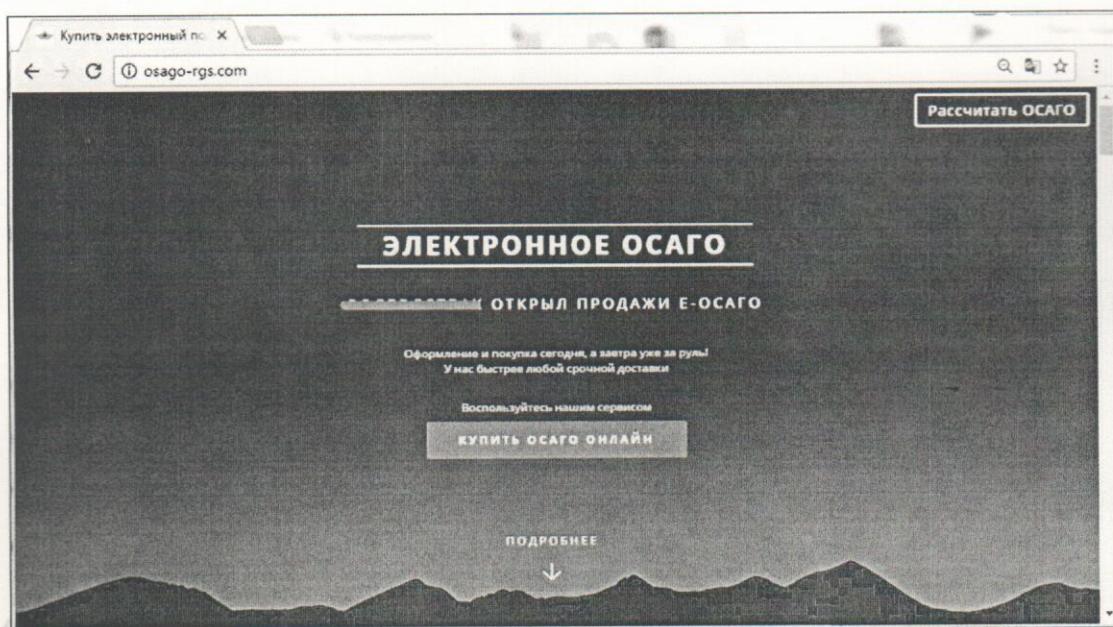
Для поддельных сайтов злоумышленники обычно используют похожие имена.

Например, подделка “s-mail-google.com” на официальный сайт “mail.google.com”.

Подделка “online.sberblank.ru” на официальный сайт “online.sberbank.ru”. Также чтобы ввести 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



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



osago-rgs.com/pay.php

Not secure osago-rgs.com/pay.php

Verified by  
VISA

Введите Ваш пароль

Магазин: ПАО СК

Описание: Оплата электронного полиса

Сумма: RUB 8894

Дата: 19/05/2017

Номер карты: 7898 7897 7809 9808909

Личное приветствие: None

Одноразовый SMS пароль

Не получил одиноразовый пароль по SMS?

ОТПРАВИТЬ

Однако в рассматриваемом примере мошенники пытаются украдь 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



Contact · Бесплатные билеты · Aeroflot.com

AEROFLOT

5. June 2017

Поздравления!

Вы были выбраны для участия в нашем коротком опросе, чтобы получить 2 бесплатных авиабилета! У нас осталось только 332 Билета, так что спешите!

1/3: Вы когда-нибудь путешествовали с нами

да

нет

Не помню

S7 Airlines

5. June 2017

Поздравления!

Вы были выбраны для участия в нашем коротком опросе, чтобы получить 2 бесплатных авиабилета S7 Airlines! У нас осталось только 332 Билета, так что спешите!

2/3: Вы предпочитаете S7 Airlines из-за?

Это дешевизна

Это окружающая среда

Не помните

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

## Актуальные примеры фишинговых сайтов



Навигация | <https://checkin-snils.ru>

МЕЖРЕГИОНАЛЬНЫЙ  
ОБЩЕСТВЕННЫЙ  
ФОНД РАЗВИТИЯ

Всего свободных средств: 389 100 322 руб.  
Выплачено за сегодня: 47 56  
Всего СНИЛС в базе: 37 1

Главная | Выплаты | Проверка | Комментарии | О нас

Содиняемся с базами страхователей. Следуйте инструкциям...

Ваш номер СНИЛС: 128-456-895-65

Проверьте Ваш СНИЛС за 3 минуты на наличие денежных выплат со стороны частных страховых фондов.

Подключение к свободному оператору

Здравствуйте! Меня зовут Ирина. Я буду сопровождать Ваши выплаты по СНИЛС 128-456-895-65.

Для доступа к базам данных частных страховщиков, Единый Расчетный Центр взимает фиксированную плату, которая для Вас составляет всего 195 руб.

Оплата доступа производится один раз и позволяет в дальнейшем беспрепятственно получать сведения по начислениям страховых выплат через наш сайт. Для подключения базы данных, оплатите указанную сумму, после чего Вам будет моментально выведено 161454 руб. Для оплаты нажмите ниже кнопку "ОПЛАТИТЬ ДОСТУП" и следуйте дальнейшим инструкциям. Оплату можно произвести с использованием пластиковых карт или электронных денег.

По всем вопросам, обращайтесь в службу поддержки по адресу: snilshelp6@gmail.com

ПОЧЕМУ ВАМ ПОЛОЖЕНЫ СТРАХОВЫЕ ВЫПЛАТЫ ОТ ВНЕБЮДЖЕТНЫХ ФОНДОВ

Согласно Постановлению Правительства РФ № 192н страховые фонды обязаны предоставлять отчет ведомственные органы по страховым начислениям граждан, а также резидентам других стран, находящихся временно или постоянно на территории России, равно как и за ее территорией, но осуществляющих деятельность (в том числе через Интернет), прямо или косвенно относящуюся к получению доходов в РФ. По программе софинансирования частных страховых фондов, бюджетом РФ выделяются субсидии на выплаты, которые должны быть израсходованы в полном объеме. Но, частные фонды стараются не афишировать получение этих сумм (предназначенных напрямую для выплат гражданам), проводя их с

ОПЛАТИТЬ ДОСТУП

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



мошенники в  
Альфа.Клик



правильный сайт  
Альфа.Клик



лишняя буква "t" сайт  
ВКонтакте



должно быть rzd.ru сайт РЖД

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

DOC SHELL

The screenshot shows a website for 'МЕНДЕЛЕЕВСКАЗОТ' (Mendeleevskazot) with a background image of industrial equipment. The navigation menu on the left includes links for Главная, Продукция, Сертификаты качества, АСУП, Система менеджмента, Экология, Культурная деятельность, Карьера, and Контакты. A warning message 'Осторожно мошенники!' is prominently displayed. The page also contains contact information: Телефон: +7 (85522) 0-53-14 and E-mail: m-azot@amonni.ru.

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:

[mendeleevscazot.ru](http://mendeleevscazot.ru) (фальшивка) вместо [mendeleevskazot.ru](http://mendeleevskazot.ru) (настоящий сайт)

[kyazot.ru](http://kyazot.ru) (фальшивка) и [kuazot.ru](http://kuazot.ru)

[amonni.ru](http://amonni.ru) (фальшивка) и [ammoni.ru](http://ammoni.ru)

[tender-rosneft.ru](http://tender-rosneft.ru) (фальшивка) и [tender.rosneft.ru](http://tender.rosneft.ru)

[sibur.info](http://sibur.info) (фальшивка) и [sibur.ru](http://sibur.ru)

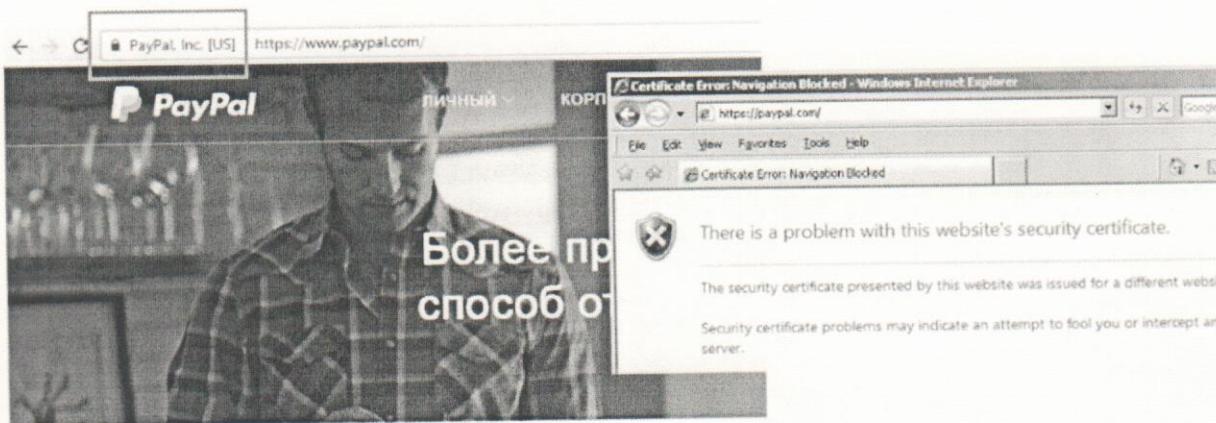
# Обучение ИБ. Фишинг и другие угрозы ИБ для пользователей. Часть 3. Памятка пользователя

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

### Памятка пользователю



#### Значок безопасного сайта

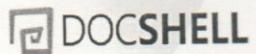


- Всегда HTTPS в адресной строке.
- Без ошибок или предупреждений безопасности.

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



#### Настоящий адрес сайта

НАПИСАТЬ

Входящие  
Важные  
Отправленные  
Черновики (2)  
Вся почта  
Спам (10)  
Корзина  
Круги  
admin@... .ru  
...@gmail....  
Дмитрий

Блокировка счета

Яндекс.Деньги <support@money-ver.zz.vc>  
кому: мне

Здравствуйте!

На вашем счете: 9 133,48 Р.

В связи с участвующими случаями мошенничества.  
Крайне необходима повторная активация Вашего счета.

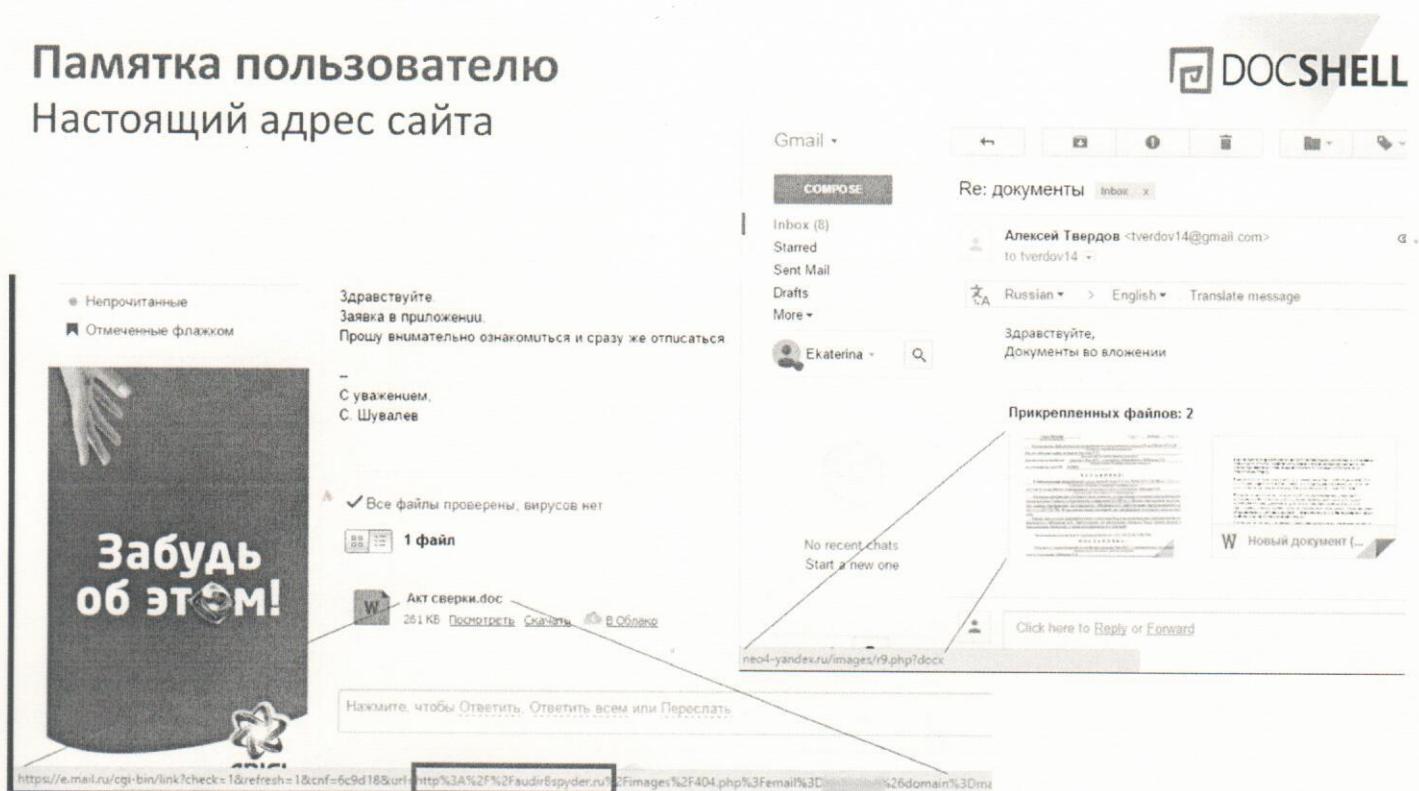
У Вас установлен Одноразовый пароль в системе Яндекс.Денег. Вам необходимо получить Аварийные коды:  
<https://sp-money.yandex.ru/strongsec/emcode-gen.xml>

Чтобы подтвердить введенные Вами данные ранее, необходимо пройти по <https://money.yandex.ru/activation/> и заполнить форму.  
Если Вы не активируете свой аккаунт и не подтвердите данные, то Ваш счет будет заблокирован в течении 48 часов.

yandex-money.d33r.com/strongsec/

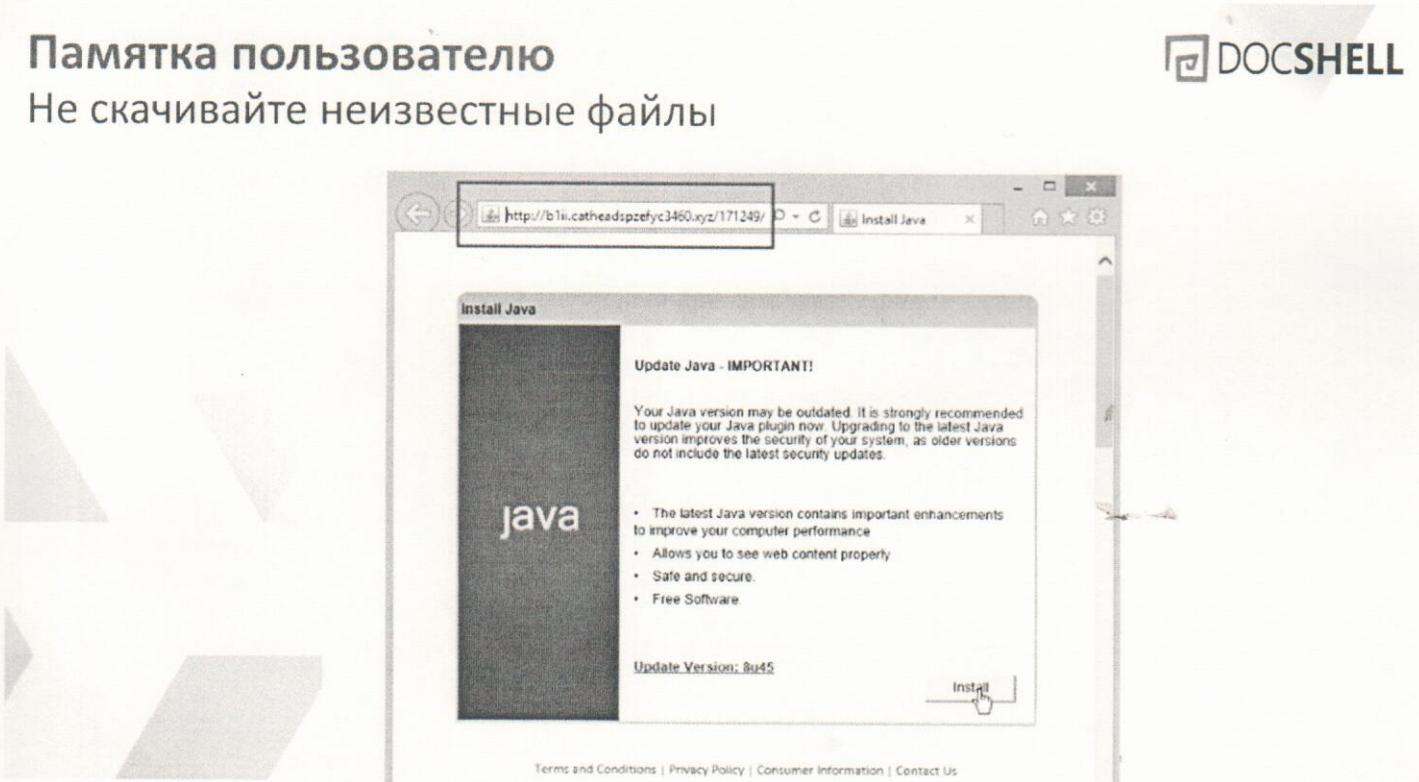
Всегда проверяйте какой настоящий адрес скрывается за ссылками в письме и на сайте. Для этого наведите мышку на ссылку в письме не нажимая её. В нижнем левом углу браузера вы увидите настоящий адрес сайта в сети Интернет. В данном примере это домен d33r.com

## Памятка пользователю Настоящий адрес сайта



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

## Памятка пользователю 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.