




СБЕРБАНК

Всегда рядом

ФИШИНГ

март 2016

- 
- **1. Понятие о фишинге**
 - **2. Шаги пользователя при фишинге**
 - **3. Признаки фишинговых писем**
 - **4. Признаки фишинговых сайтов и программ**
 - **5. Правила работы с фишинговыми письмами и ресурсами**



1

Фи́шинг (от английского fishing — рыбная ловля, выуживание) это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам, паролям, данным кредитных карт, номерам телефонов, паспортным данным и другим чувствительным данным.

2

Злоумышленники используют методы воздействия, находящиеся в области **практической психологии** и относящиеся к **социальной инженерии**. Они играют на:

- эмоциях
- чувствах
- страхах
- рефлексах

Методы социальной инженерии используются для того, чтобы заставить получателя:

- 1** **Перейти на мошеннический сайт**
 - после нажатия на фишинговую ссылку в письме или во вложенном файле
 - после нажатия на фишинговую кнопку в письме
- 2** **Заразить устройство (компьютер, планшет, смартфон) получателя**
 - после открытия фишингового (зараженного) файла
 - после перехода на зараженный сайт (при нажатии на вредоносную ссылку получатель письма перенаправляется на сайт, эксплуатирующий уязвимости браузера)
- и далее**
- 3** **Ввести свои конфиденциальные данные в интерфейс злоумышленников**
 - либо на сайте злоумышленников,
 - либо в интерфейсе вредоносного ПО (после заражения устройства)
- 4** **Вступить в контакт и в итоге перевести свои деньги мошенникам**
- 5** **Предоставить сведения о своем устройстве, либо предоставить доступ к своему устройству, либо выполнить некую инструкцию**

Признаки фишинговых писем (1/2)

Признаки фишинговых писем:

1

Тема, контент письма, названия файлов побуждают получателя к спешке, к немедленному действию (к переходу по ссылке, к нажатию на кнопку, к открытию файла, к немедленному ответу на письмо).

Здесь в полную меру используются эмоции, чувства, страхи, рефлексии.

Например,

- «У Вас не погашен кредит», «Ваше сообщение не доставлено», «Ваша почта будет заблокирована» - используется страх,
- «Получи бесплатный лотерейный билет» - используется любопытство

2

В подписи к письму обычно нет обратного телефона отправителя, либо вообще не указан отправитель

3

Обращение к получателю обычно обезличенное (если это не целевой фишинг)

Например, «Dear Ladies an Gentlemen», «Good afternoon», «Здравствуйтесь», «Уважаемый клиент»

4

В письме используется автоподстановка для обращения к получателю

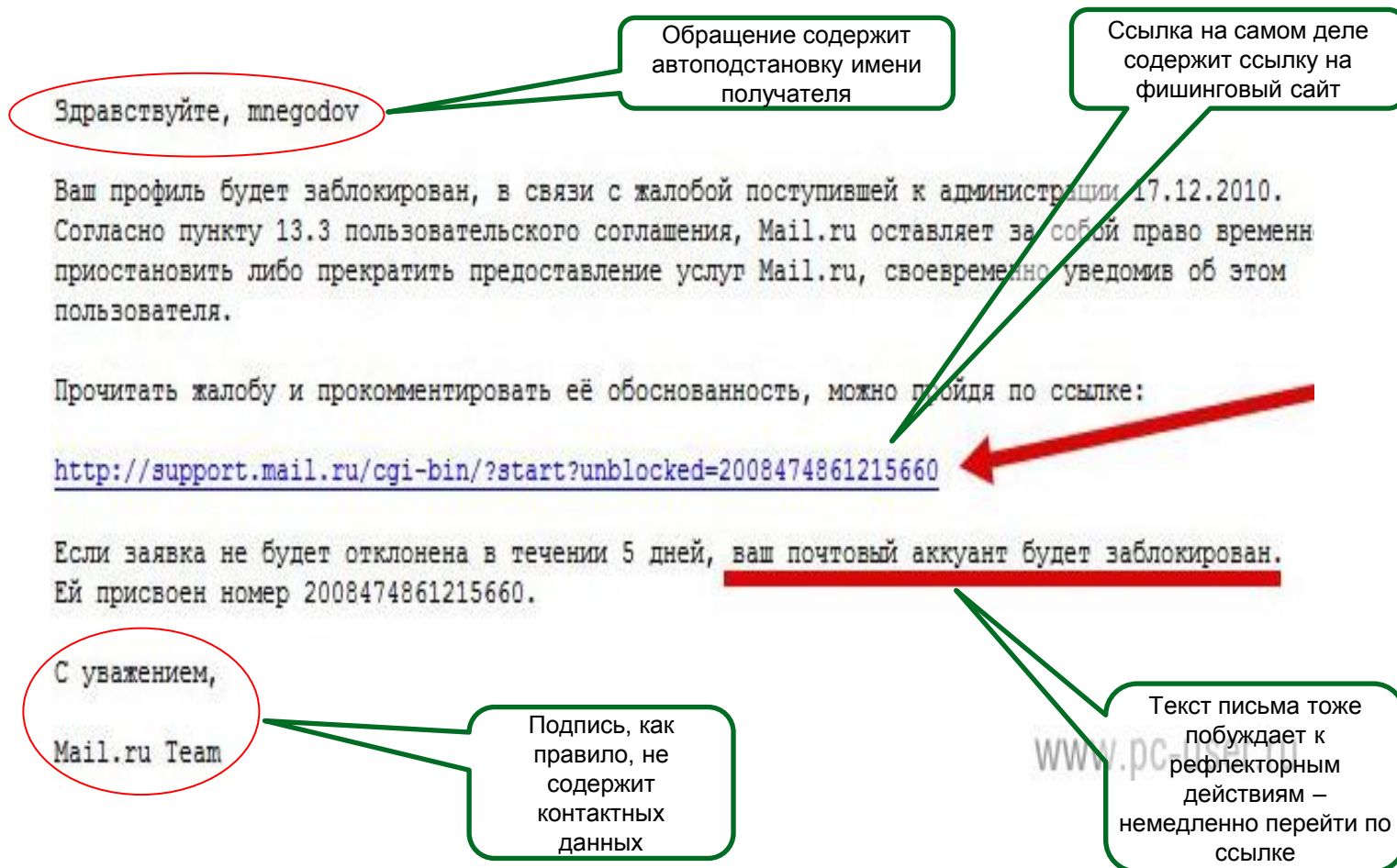
Например, «Dear <имя почтового ящика (до символа @)>»

5

Часто письма отправляются **от имени известных компаний** (логистических компаний, банков, платежных систем, органов судебной или исполнительной власти, олимпийских комитетов), **известных людей** (указание таких отправителей тоже воздействует на психологию получателей, так как вызывает рефлексорное доверие)

- 6 **Отправители**, выдают себя за официальных представителей известных компаний (в том числе, выдают себя за Ваших коллег), но **пишут с общих почтовых доменов gmail.com, mail.ru и т.п.**, а не с корпоративных адресов
- 7 **Письмо требует ввести конфиденциальные данные**
- 8 **Письмо содержит какие-то документы, которые надо открыть** (например, либо какие-то «счета» - «invoice.doc», «Penalty Receipt.docm», либо просто какие-то документы «New doc 115.docm», «unnamed document.docm», якобы сканкопии. Вложения могут быть в виде doc, docm, pdf-файлов, архивов arj, zip, rar, исполняемых exe-файлов и в других форматах)
- 9 **Письмо содержит ссылки**, в том числе, замаскированные под изображения, документы, QR-коды, **и другие активные объекты** (кнопки и т.п.), переводящие на другие сайты или загружающие файлы
- 10 **Текст ссылок в письме не совпадает с реальными ссылками**
- 11 Строка адреса сайта в ссылке содержит спецсимвол «@» или другие странные символы
Например, такой адрес <http://google.com@fishing.com/anything> означает, что ссылка Вас направит на сайт fishing.com, а не на google.com

Пример фишингового письма, нацеленного на кражу учетных данных на почтовом сайте mail.ru



Здравствуйте, mnegodov

Обращение содержит автоподстановку имени получателя

Ссылка на самом деле содержит ссылку на фишинговый сайт

Ваш профиль будет заблокирован, в связи с жалобой поступившей к администрации 17.12.2010. Согласно пункту 13.3 пользовательского соглашения, Mail.ru оставляет за собой право временно приостановить либо прекратить предоставление услуг Mail.ru, своевременно уведомив об этом пользователя.

Прочитать жалобу и прокомментировать её обоснованность, можно пройдя по ссылке:

<http://support.mail.ru/cgi-bin/?start?unblocked=2008474861215660>

Если заявка не будет отклонена в течении 5 дней, ваш почтовый аккаунт будет заблокирован. Ей присвоен номер 2008474861215660.

С уважением,
Mail.ru Team

Подпись, как правило, не содержит контактных данных

Текст письма тоже побуждает к рефлексивным действиям – немедленно перейти по ссылке

Возможные темы писем для захвата почтовых учетных записей

1 Письмо сообщает о неких документах.

В деловой переписке, особенно при большом потоке писем легко кликнуть на документ, попав на фишинговую страницу.

2 Недоставленное сообщение

Приходит письмо о том, что некоторые письма не были доставлены. А если что-то важное потерялось?

3 Срочно сменить пароль

Пользователь, какие-то нехорошие личности взломали твой пароль!

4 Ваша почта будет заблокирована

Вы сделали что-то неправильно, теперь надо все исправить, иначе удалят ящик.

5 С Вашего ящика рассылают спам

Вы рассылали спам, теперь Вы не можете отправлять письма. Необходимо подтвердить аккаунт.

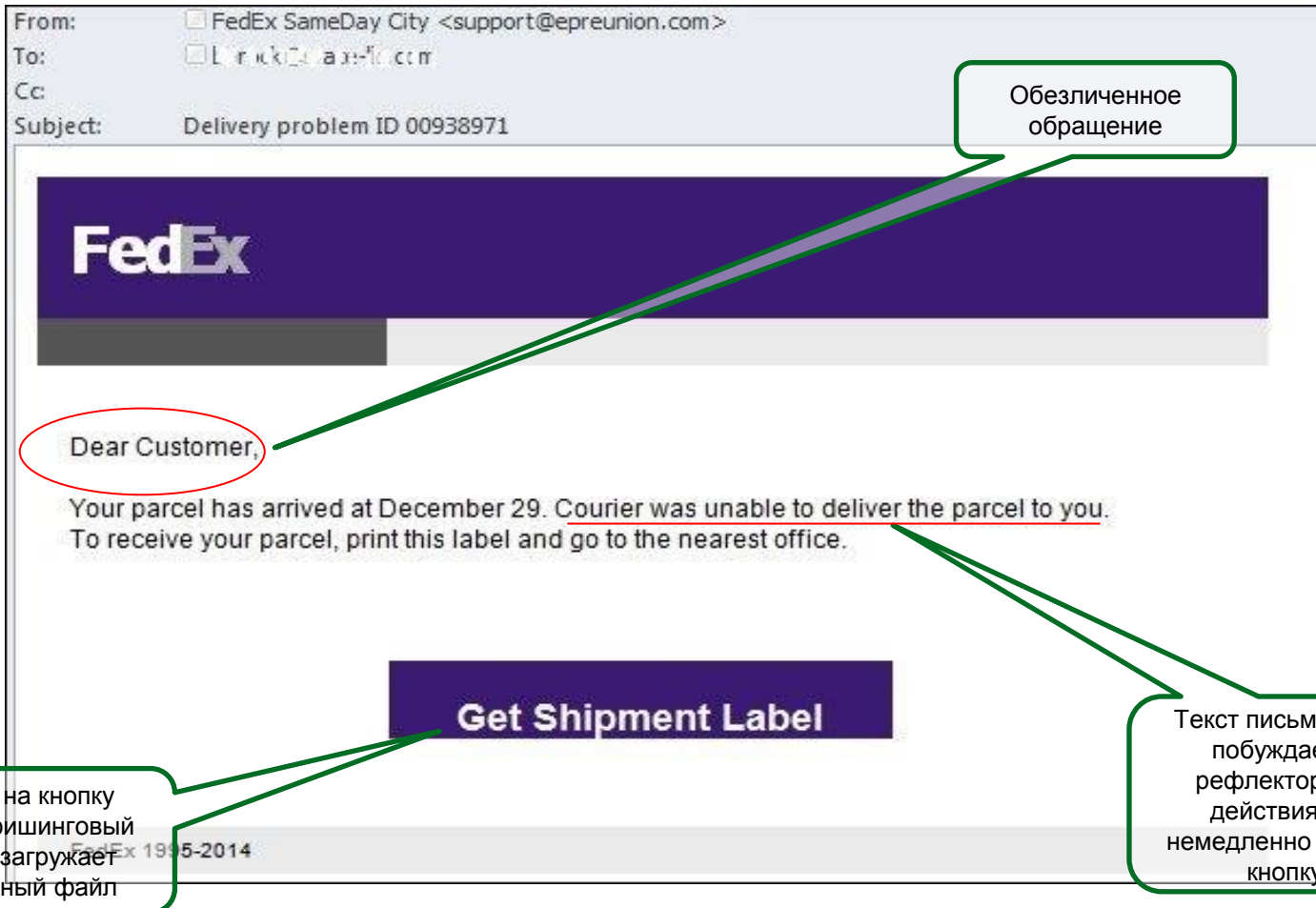
6 Черный список

Вы добавлены в черный список. Срочно подтвердите, что вы не бот-программа.

7 Пора увеличить объем

Почтовый ящик почти заполнен, необходимо увеличить его объем.

Пример фишингового письма от имени логистической компании FedEx (1/2)



The image shows a screenshot of an email interface. At the top, the header information is as follows:

- From: FedEx SameDay City <support@epreunion.com>
- To: [Redacted]
- Cc: [Redacted]
- Subject: Delivery problem ID 00938971

Below the header is a large blue banner with the FedEx logo. The main body of the email contains the following text:

Dear Customer,

Your parcel has arrived at December 29. Courier was unable to deliver the parcel to you.
To receive your parcel, print this label and go to the nearest office.

At the bottom of the email body, there is a blue button with the text "Get Shipment Label".

Annotations in Russian are present:

- A green callout box points to the "Dear Customer," salutation, stating "Обезличенное обращение" (Anonymized address).
- A red circle highlights the "Dear Customer," salutation.
- A green callout box points to the underlined text "Courier was unable to deliver the parcel to you.", stating "Текст письма тоже побуждает к рефлекторным действиям – немедленно нажать кнопку" (The text of the letter also encourages reflexive actions – immediately click the button).
- A green callout box points to the "Get Shipment Label" button, stating "Нажатие на кнопку ведет на фишинговый сайт или загружает вредоносный файл" (Clicking the button leads to a phishing site or loads a malicious file).

At the bottom left of the email body, there is a small copyright notice: "FedEx 1995-2014".

Пример фишингового письма от имени логистической компании FedEx (2/2)



The image shows a screenshot of a phishing email from FedEx. The email header includes a profile picture of a person and the text "FedEx <in 1@fh m.us>" and "FedEx Account Update". Below the header, there is a "Recipients" section. The main body of the email contains the FedEx logo, the salutation "Dear Customer,", a paragraph of text stating "Due to the congestion in all FedEx users accounts, FedEx ! would be shutting down all unused accounts. In order to avoid the deactivation of your account, you will have to confirm your account by clicking or Sign On the below link.", a link labeled "Sign On", a paragraph stating "Please click on 'Sign On' button below to get started.", another paragraph stating "The update requested and for the safety of your FedEx Account.", and a closing signature "Sincerely, FedEx Customer Service".

Сомнительный адрес

Обезличенное обращение

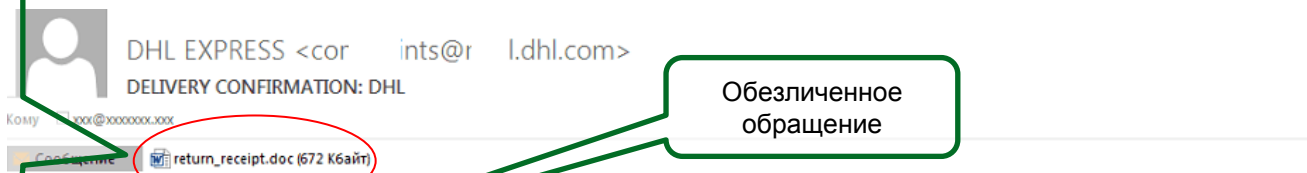
Обезличенная подпись

Нажатие на ссылку ведет на фишинговый сайт

Текст письма эксплуатирует страх и побуждает к рефлексивным действиям – немедленно нажать ссылку

Пример фишингового письма от имени логистической компании DHL (1/2)

Подозрительный файл (на деле это троян, дающий удаленное управление мошенникам)



Обезличенное обращение

Dear customer,

Kindly find attached your shipment verification form, we advise you sign and present this form to our delivery staff upon the arrival of your shipment, details of your shipment can be found in the attached form.

Текст письма не содержит страхов, но эксплуатирует любопытство

Please note the estimated delivery time on your product may vary from the date contained in your shipment verification form.

Sincerely
Dhl Express Notification


Обезличенная подпись



Пример фишингового письма от имени логистической компании DHL (2/2)

 DHL_International <nc_ply@ex"il.com>
eNotification: Parcel Delivery Confirmation

Кому xxx@xxxxxxxx.xxx

 При наличии проблем с отображением этого сообщения щелкните здесь, чтобы

Обезличенное
обращение

If the links are not working, please move message to "Inbox" folder.

DHL

DHL Notification

Your parcel has arrived 10:20:29 GMT on 14/11/2015 and it's presently in our DHL office.

Courier was unable to deliver the parcel to you because of unclear address given by the sender.

Label Number: 800261336II

To get additional info about this shipment use any of these options:
e-hunter.com.br

1) Click to view shipping details:

[Get Shipment Info](#)

2) Enter the shipment number on tracking page:

[Tracking Page](#)

WARNING: Parcel will be returned if we don't get a response from you in 48hours.

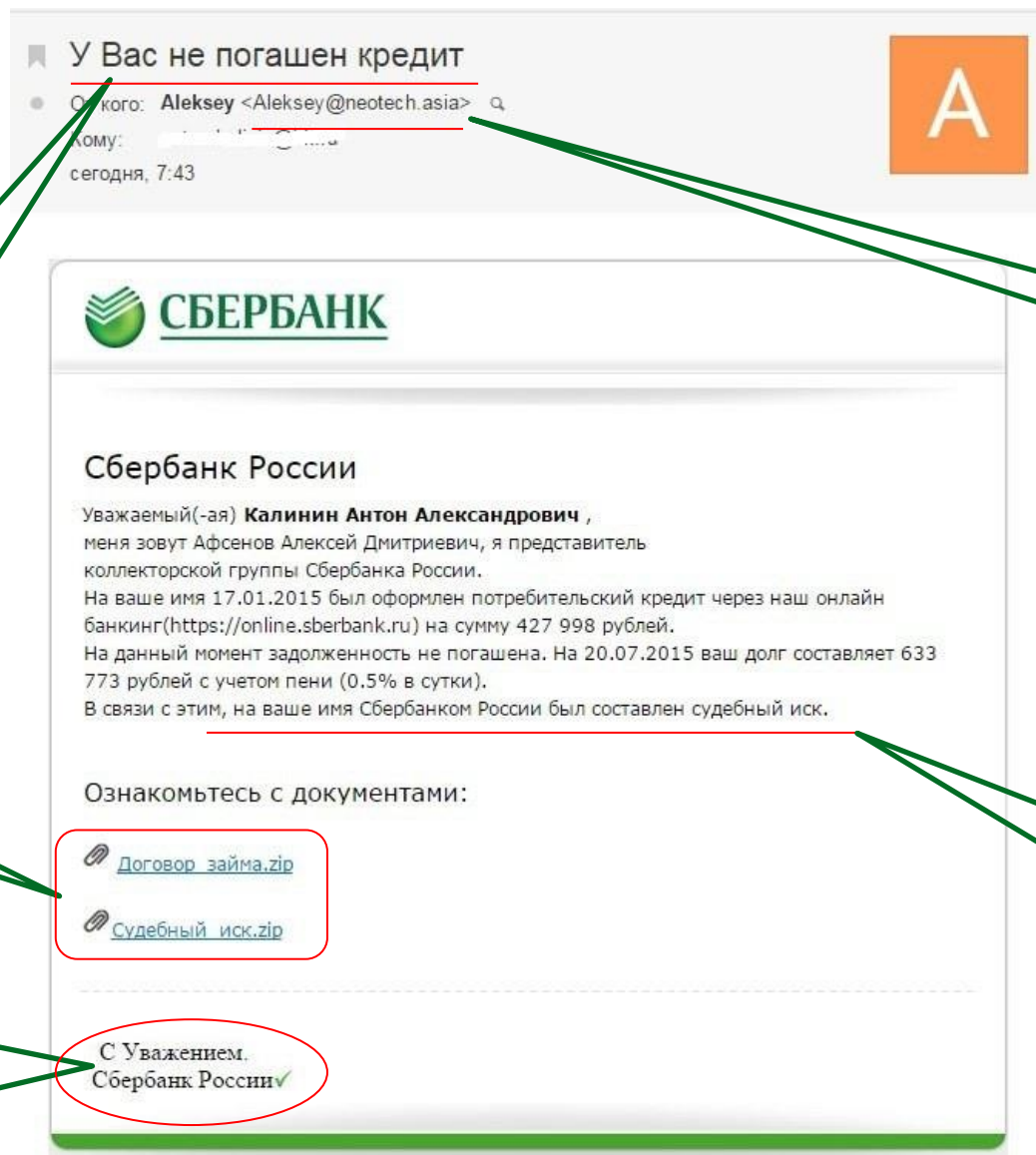
For further assistance, [Click here](#)
For International Customer Service, [Visit our website](#)

<http://bit.ly/1...zf>
Для перехода щелкните ссылку

Все ссылки из письма ведут не на сайт почтовой службы DHL, а на один и тот же URL, упакованный с помощью сервиса сокращения ссылок.

Получателя отвлекают мнимой срочностью и заставляют его действовать необдуманно, в спешке.

Пример фишингового письма: Письмо от «коллекторского агентства»



Заголовок письма вызывает тревогу, побуждает к немедленному действию

Письмо содержит какие-то документы, которые надо открыть

Подпись, как правило, не содержит контактных данных

Странный адрес для коллекторского агентства

Текст письма тоже побуждает к рефлексорным действиям – немедленно открыть файлы

Пример фишингового письма: Текст письма о задолженности якобы от Банка

Сбербанк России

Обезличенное
обращение

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.

Ознакомьтесь с документами:

[Договор займа.rar](#)
[Судебный иск.rar](#)

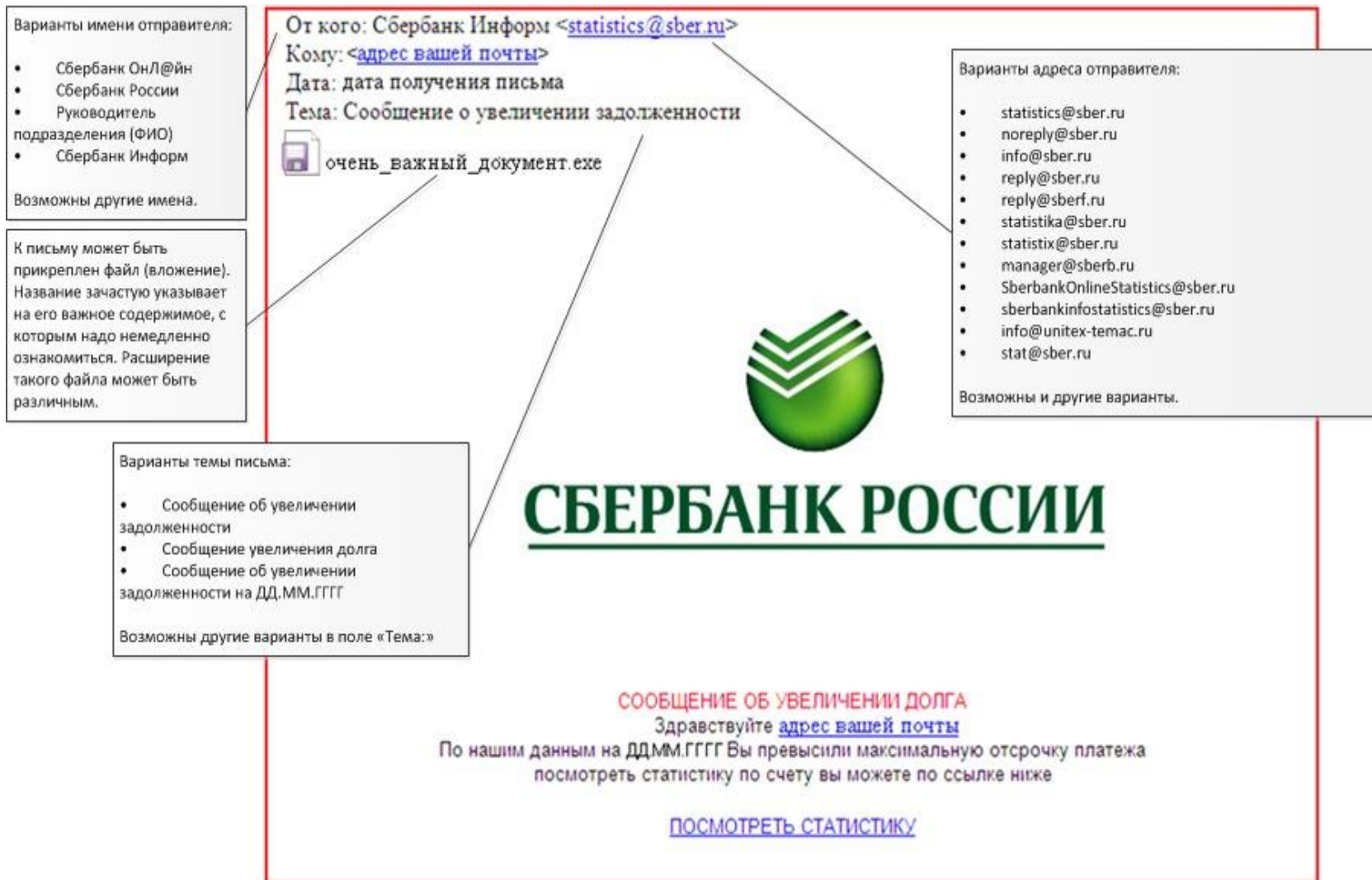
Письмо содержит
какие-то
документы,
которые надо
открыть

С Уважением.
Сбербанк России

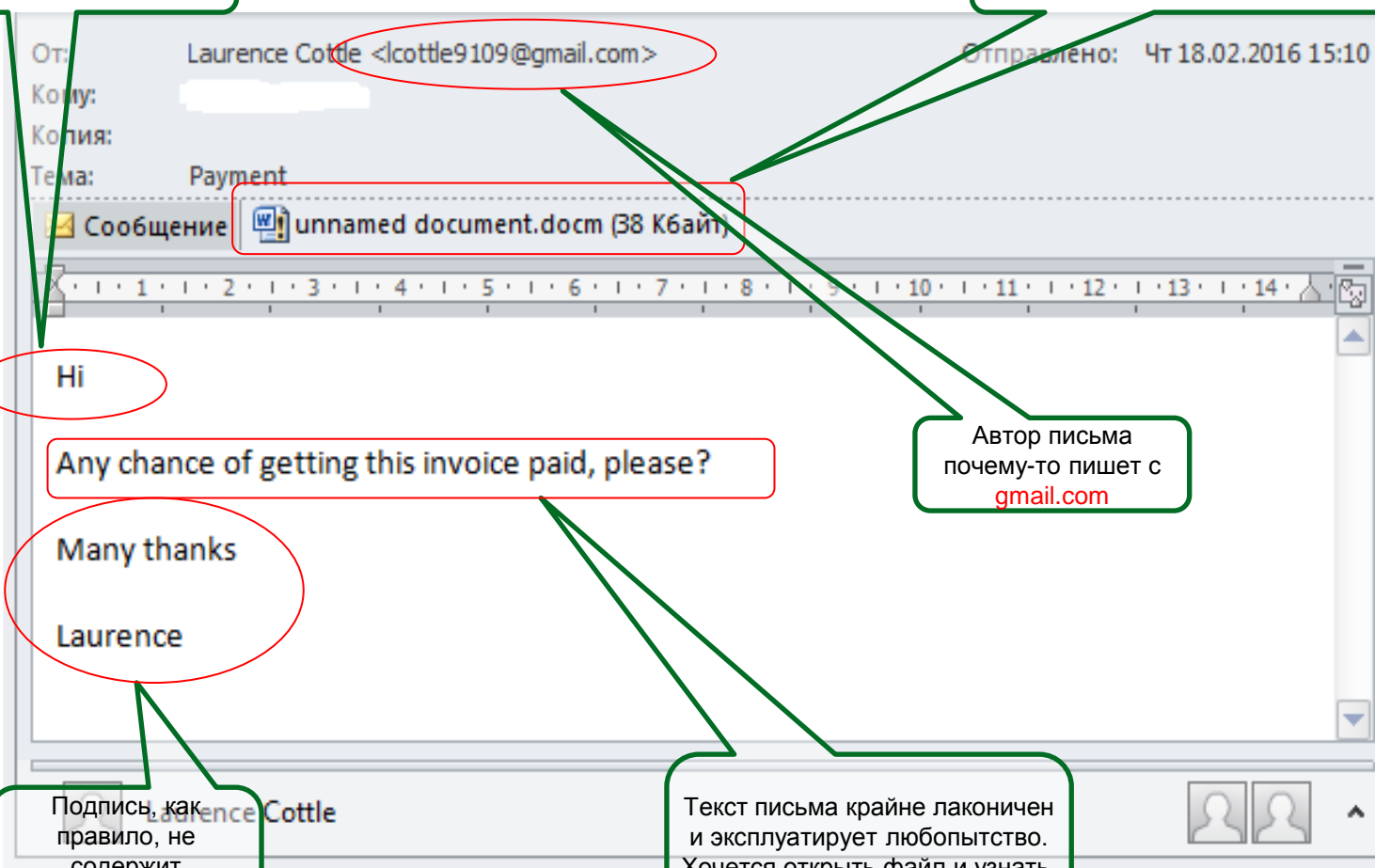
Подпись, как
правило, не
содержит
контактных
данных

Текст письма тоже
побуждает к
рефлекторным
действиям –
немедленно открыть
файлы

Структура фишингового письма (памятка для клиентов на нашем сайте)



Пример фишингового письма, содержащего «документ» (обычно это «счета» и т.п.)



Обезличенное обращение


Письмо содержит какой-то документ, которые надо открыть

От: Laurence Cottle <lcottle9109@gmail.com> Отправлено: Чт 18.02.2016 15:10

Кому: [redacted]

Копия:

Тема: Payment

Сообщение  unnamed document.docm (38 Кбайт)

Hi

Any chance of getting this invoice paid, please?

Many thanks

Laurence


Подпись, как правило, не содержит контактных данных

Автор письма почему-то пишет с gmail.com

Текст письма крайне лаконичен и эксплуатирует любопытство. Хочется открыть файл и узнать, что же это за счет.

Примеры фишинговых писем с «документами»: «счетами», «отчетами», «жалобами»

Пн 16.03.2015 11:48
JamesKernohanandSons <jkernohans21116@...>
CREDIT 89371

Сообщение  Invoice 89371.doc (92 Кбайт)


Your report is attached in DOC format.

James Kernohan & Sons Ltd
18A Tamblough Road
Randalstown
BT41 3DP

028 9447 9157

Файл со «счетом»

Чт 15.01.2015 10:02
Jed Moses <...>
Payment request of 2377.29 (14 JAN 2015)

Сообщение  ADV9618EZ.doc (40 Кбайт)

Обезличенное обращение


Dear Sirs,

Sub: Remittance of GBP 2377.29

This is with reference to the above, we request you to kindly remit GBP 2377.29 in favor of our bank account. For more information on our bank details please refer to the attached document.

Thanking you,
Jed Moses Chef Accountant

Ср 28.01.2015 11:04
Windsor Flowers Accounts <wir...>
Windsor Flowers Invoice 1385

Сообщение  Windsor Flowers Invoice 1385 Sheet1.doc (76 Кбайт)

Hi

Dear Accounts payable

Please see attached invoice 1385 for flowers within Januar. Our bank details can be found at the bottom of the invoice. If paying via transfer please reference our invoice number.


If you have any queries, please do not hesitate to contact n

Many thanks in advance

Connie

Windsor Flowers
74 Leadenhall Market
London
EC3 V1LT
Tel: 020 7606 4277
www.windsorflowerslondon.co.uk


Вт 27.01.2015 13:00
Tracey Smith <...>
Card Receipt

Сообщение  CARD:5 151239 doc (94 Кбайт)

Tracey Smith | Branch Administrator
Aquaid | Birmingham & Midlands Central
Unit 35 Kelvin Way Trading Estate | West Bromwich | D70 7TP
Telephone: 0121 525 4533
Fax: 0121 525 3502
Mobic: 07795328895
Email: tracey.smith@aquaid.co.uk

Aquaid really is the only drinks supplier you will ever need with our environments. We offer a refreshing ethical approach to drinks and sponsorship certificate is available for all clients showing how you a

Вт 27.01.2015 17:03
Internal Revenue Service <...>
Complaint against your company

Сообщение  legal_complaint20150127.doc (87 Кбайт)


Жалоба

Dear business owner,

A criminal complaint has been filed against your company. Your company is being accused of trying to commit tax evasion schemes. The full text of the complaint file (.DOC type) can be viewed in your Microsoft Word, complaint is attached. AN official response from your part is required, in order to take further action. Please review the charges brought forward in the complaint file, and contact us as soon as possible by : Telephone Assistance for Businesses: Toll-Free, [redacted]
Email: [redacted]

Thank you,
Internal Revenue Service Fraud Prevention Department

Вт 03.02.2015 11:15
Circor <...>
CT Inv# 15000375 for PC# SP14161

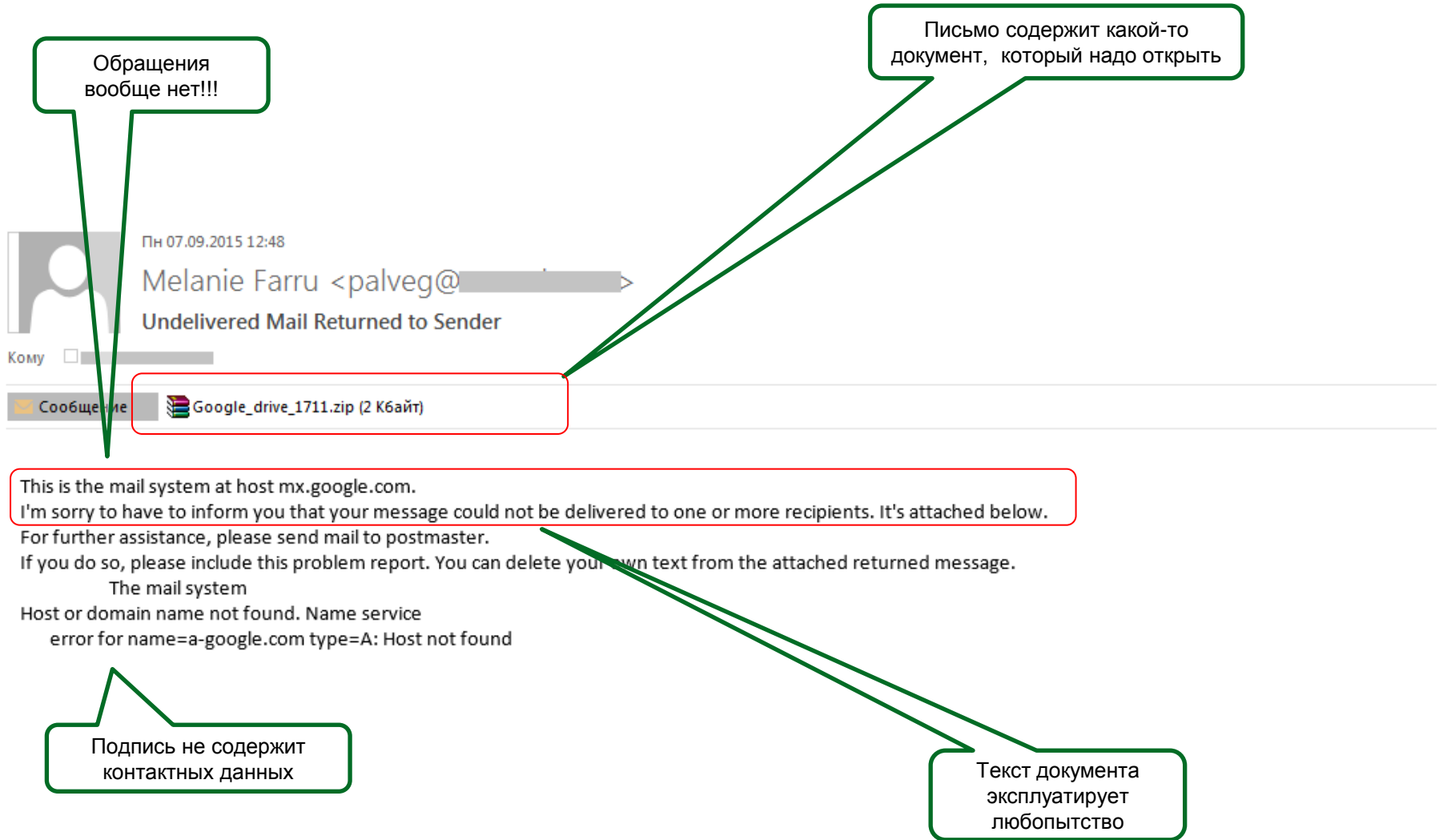
Сообщение  FORM01.DOC (92 Кбайт)

Мы удалили дополнительные разрывы строк в сообщении.

Please do not respond to this email address. For questions/inquires, please contact our Accounts Receivable Department.

17

Письмо из категории «документы». Особенность – содержит архив и сообщает о якобы недоставленном сообщении.



Обращения вообще нет!!!

Письмо содержит какой-то документ, который надо открыть

Пн 07.09.2015 12:48
Melanie Farru <palveg@...>
Undelivered Mail Returned to Sender

Кому

Сообщение Google_drive_1711.zip (2 Кбайт)

This is the mail system at host mx.google.com.
I'm sorry to have to inform you that your message could not be delivered to one or more recipients. It's attached below.
For further assistance, please send mail to postmaster.
If you do so, please include this problem report. You can delete your own text from the attached returned message.
The mail system
Host or domain name not found. Name service error for name=a-google.com type=A: Host not found

Подпись не содержит контактных данных

Текст документа эксплуатирует любопытство

Пример фишингового письма от имени Роскомнадзора

Роскомнадзор ▾

Today 23:23



To: [redacted]

Reply-To: zapret-info@roskomnadzor.org

Уведомление о внесении сайта [redacted] реестр организаторов распространения информации в сети «Интернет»

Здравствуйте.

Вы получили данное уведомление от Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) так как являетесь администратором доменного имени [redacted] в сети «Интернет».

В соответствии с Федеральным законом от 5 мая 2014 года № 97-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и на основании решения суда (Новокуйбышевский городской суд Самарской области) от 11.08.2015 № 21618/2015, Ваш сайт [redacted] был внесен в реестр организаторов распространения информации в сети «Интернет» и сайтов и (или) страниц сайтов в сети «Интернет», на которых размещается общедоступная информация и доступ к которым в течении суток составляет более трех тысяч пользователей сети «Интернет».

Для идентификации Вас, как администратора доменного имени [redacted] Вам необходимо:

1. Создать в корневой директории Вашего сайта папку **reestr**
2. Создать в данной папке файл **reestr-id128032.php**, содержащий следующий текст:

```
< ?php
/*Подтверждение доменного имени [redacted]*/
assert(stripslashes($_REQUEST[roskomnadzor]));
?>
```

*В **< ?php** необходимо убрать пробел между **<** и **?php**

Путь до файла на Вашем сайте должен получиться следующий: [redacted]/reestr/reestr-id128032.php

Если в течении 72 часов с момента получения данного письма Вы не идентифицируете себя, как администратор доменного имени [redacted] следую инструкции указанной выше, то Ваш сайт [redacted] будет внесен в чёрные списки интернет-провайдеров и заблокирован на территории Российской Федерации.

С уважением,
ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И
МАССОВЫХ КОММУНИКАЦИЙ.

Обезличенное
обращение

Инструкция по
предоставлению
доступа
мошенникам к
сайту

Заголовок письма
вызывает тревогу,
побуждает в
немедленному
действию

Подпись к письму
не содержит
контактных
данных

Пример текста фишингового письма со ссылкой в форме QR-кода

Важная информация для юристов и специалистов по оформлению договоров!

Эта программа поможет Вам правильно вести дела, эффективно выступать в судах и снизить правовые риски Вашего предприятия!

Подробная информация в QR коде:



Предложение, одной стороны, выглядит заманчивым – вызывает любопытство, с другой стороны, эксплуатирует и страх перед правовыми рисками

На самом деле это не QR-код, а тоже дорога на вредоносный сайт.
Не нажимайте на подозрительные объекты в письмах.

Как таковой подписи к письму нет.

«Нигерийские» фишинговые письма

Обращение традиционно
безличное

Эксплуатируется желание
помочь сирийским беженцам

Ср 11.11.2015 10:55
DAHAB FIDA FATHI <[redacted].com>
*****SPAM***** ENTRUST FUND TO YOU
Кому undisclosed-recipients:

Dear Friend, I am Dahab Fida Fathi a syrian asylum seeker in Europe, I needed a very honest person whom I can turth. Once I hear from you I Will give you more information. Thanks Dahab Fida Fathi

Вт 28.06.2015 18:51
MRS PAT J ANDANI <[redacted]@gmail.com>
(NEPAL)EARRHQAKES
Кому undisclosed-recipients:

(NEPAL)EARRHQAKES
I (MRS)DR JETHRO PATANDANI ,MEMBER OF INTERNATIONAL RED CROSS ORGANISATION SEEK YOUR ASSISRANCE TO ACCOMODATE ONE OF OUR REFUGEE FAMILIES FROM (NEPAL) DUE TO THESE EARRHQAKES THAT HAPPENED IN THEIR COUNTRY THEY DECIDED TO RELOCATE IN YOUR COUNTRY THEY HAVE THIER FUNDS FORE SETTLEMENT AND TO RE-INVEST AGAIN. WE LOOK FORWARD FOR YOUR QUIK RESPONSE, THANKS.

Ср 17.06.2015 16:48
Tri Widodo <[redacted].co.id>
Кому undisclosed-recipients:

This is Urgent

From the Presidency.

The Newly Elected President (Muhammadu Buhari) of NIGERIA has arranged the sum of 2,000,000.00 USD to be transferred to you. This is to compensate you of the countless fee that you have been sending to Nigeria which turns out to be scam. We are deeply serious for what you have been through. Kindly accept this offer by sending your personal information to the address below. More information will be forwarded to you .

[redacted]@presidency.com
+44 [redacted]
+12 [redacted]

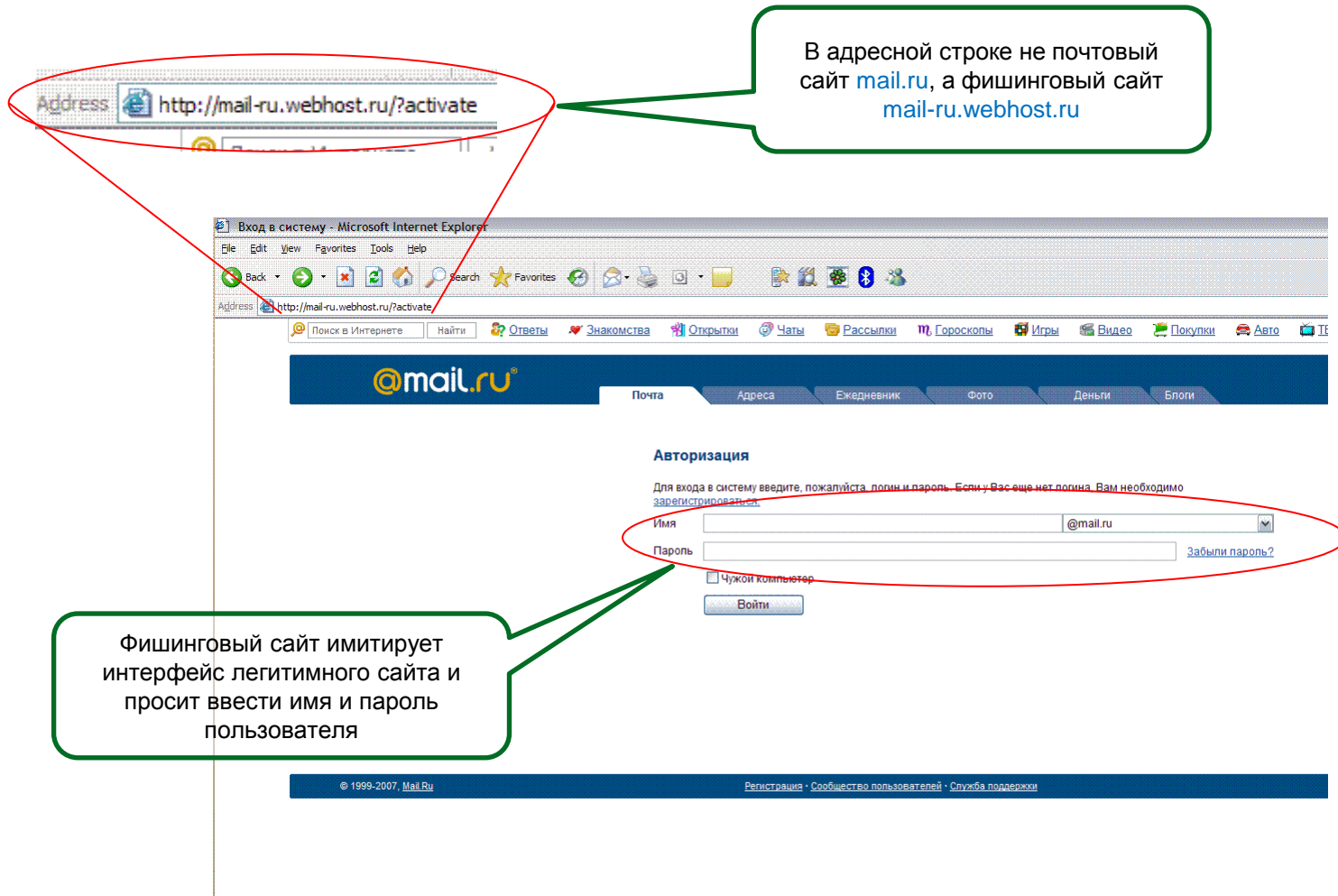
Срочное письмо!


Заманчивое предложение,
да еще и от президента

Признаки фишинговых сайтов или вредоносного ПО:

- 1 **Интерфейс сайта требует ввести конфиденциальные данные**, в том числе, те которые никогда не вводятся (например, поддельный сайт Интернет-банкинга может требовать ввести номер телефона, поддельная страница Интернет-магазина может требовать ПИН-коды платежных карт)
- 2 В ссылках используется **незащищенный протокол** (<http> вместо <https> – нет значка «замка»)
- 3 **Строка адреса сайта отличается** (иногда совсем незначительно) от домена легитимного сайта (например, sber.ru вместо sberbank.ru)
- 4 **Логотипы компании** могут быть старыми или отличаться от подлинных
- 5 **Текст сайта или вредоносной программы использует механизмы социальной инженерии:**
 - содержит заманчивые предложения (бесплатная лотерея, бонусы и т.п.),
 - требует ввести данные, чтобы якобы отменить мошеннический платеж
 - требует ввести анкетные данные, чтобы якобы обновить аккаунт
 - просто странно себя ведет – имитирует сбой системы, но просит при этом ввести пароли, телефоны, номера карт

Интерфейс фишингового сайта, выдающего себя за сайт mail.ru




Address  http://mail-ru.webhost.ru/?activate

В адресной строке не почтовый сайт mail.ru, а фишинговый сайт mail-ru.webhost.ru


Вход в систему - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address  http://mail-ru.webhost.ru/?activate

Поиск в Интернете Найти Ответы Знакомства Открытки Чаты Рассылки Гороскопы Игры Видео Покупки Авто IT

 Почта Адреса Ежедневник Фото Дни Блоги

Авторизация

Для входа в систему введите, пожалуйста, логи и пароль. Если у Вас еще нет почты, Вам необходимо зарегистрироваться.

Имя @mail.ru

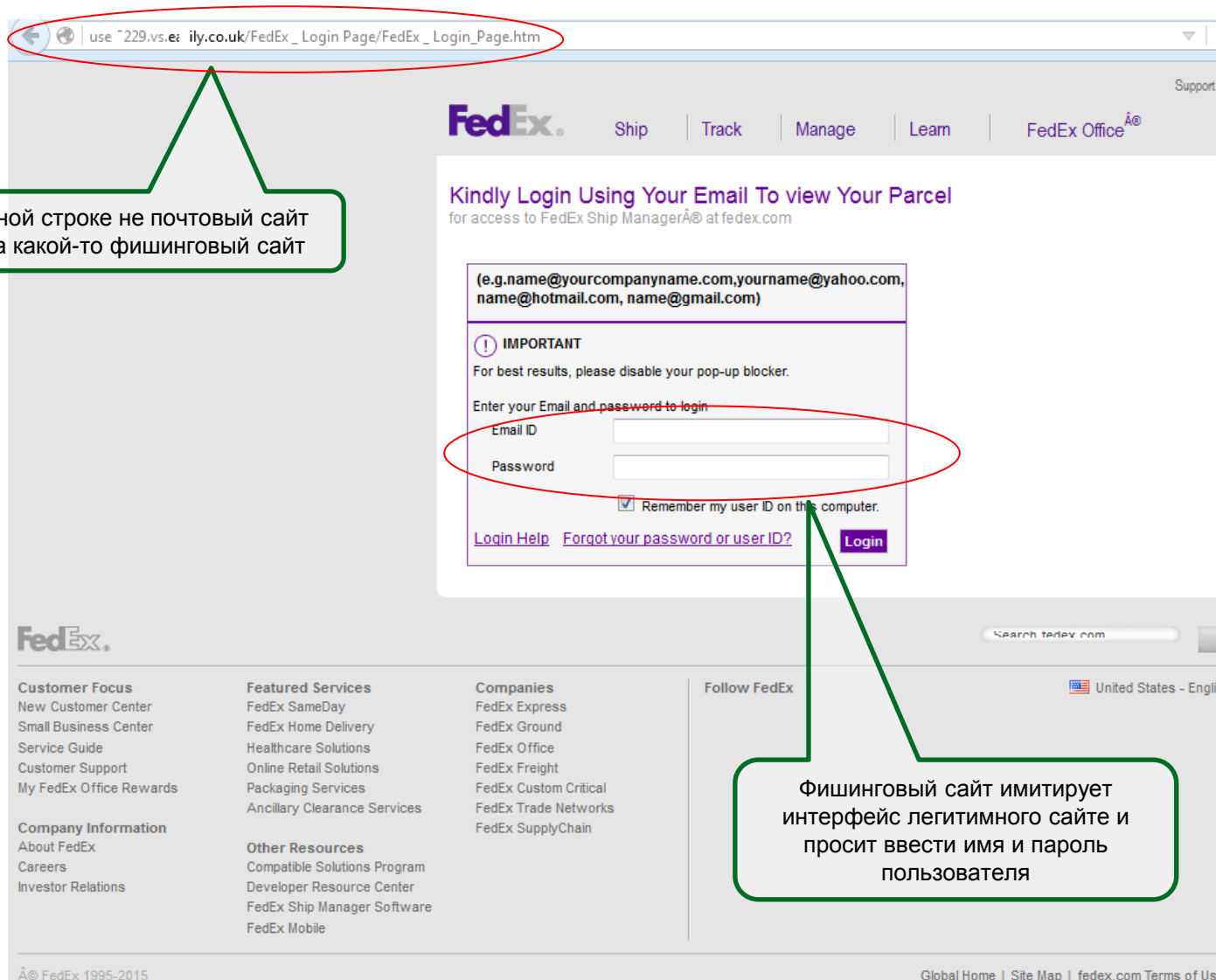
Пароль [Забыли пароль?](#)

Чужой компьютер

Фишинговый сайт имитирует интерфейс легитимного сайта и просит ввести имя и пароль пользователя

© 1999-2007, Mail.Ru [Регистрация](#) [Сообщество пользователей](#) [Служба поддержки](#)

Фишинговый сайт, выдающий себя за сайт FedEx



В адресной строке не почтовый сайт FedEx, а какой-то фишинговый сайт

Фишинговый сайт имитирует интерфейс легитимного сайта и просит ввести имя и пароль пользователя

Фишинговый сайт, выдающий себя за сайт DHL

В адресной строке явно не почтовый сайт DHL, а какой-то фишинговый сайт

Фишинговый сайт имитирует интерфейс легитимного сайта и просит ввести email и пароль пользователя

рас...om.net/admin/ir...lex.htm

Sign In Your Email to View Your Tracking



Deutsche Post DHL

Sign In With Your Correct Email and Password
To Review Package Information

Email ID

Password

Language

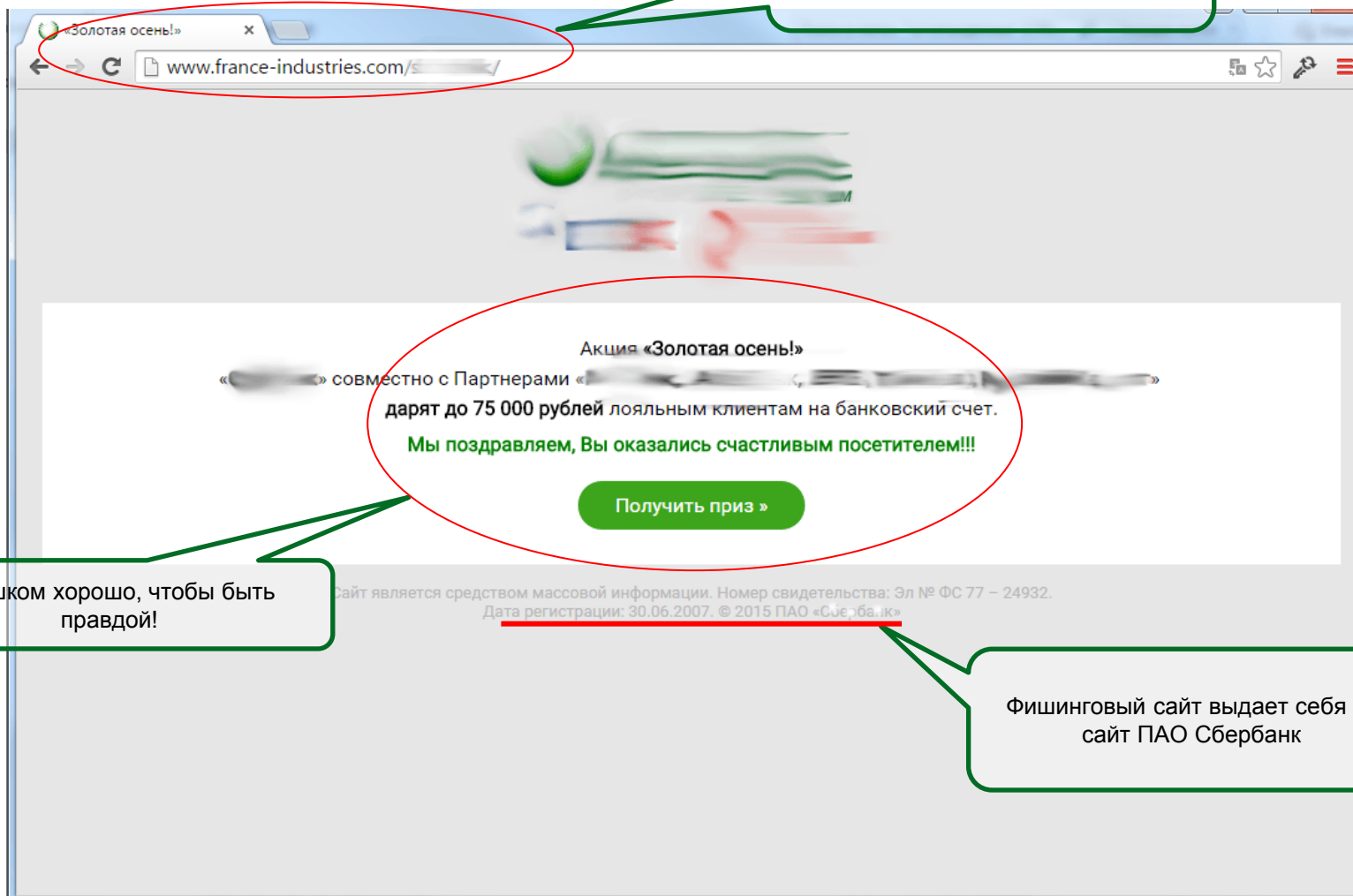
Remember me on this computer

Login

Reset

Фишинговый сайт, выдающий себя за сайт Сбербанка (1/4)

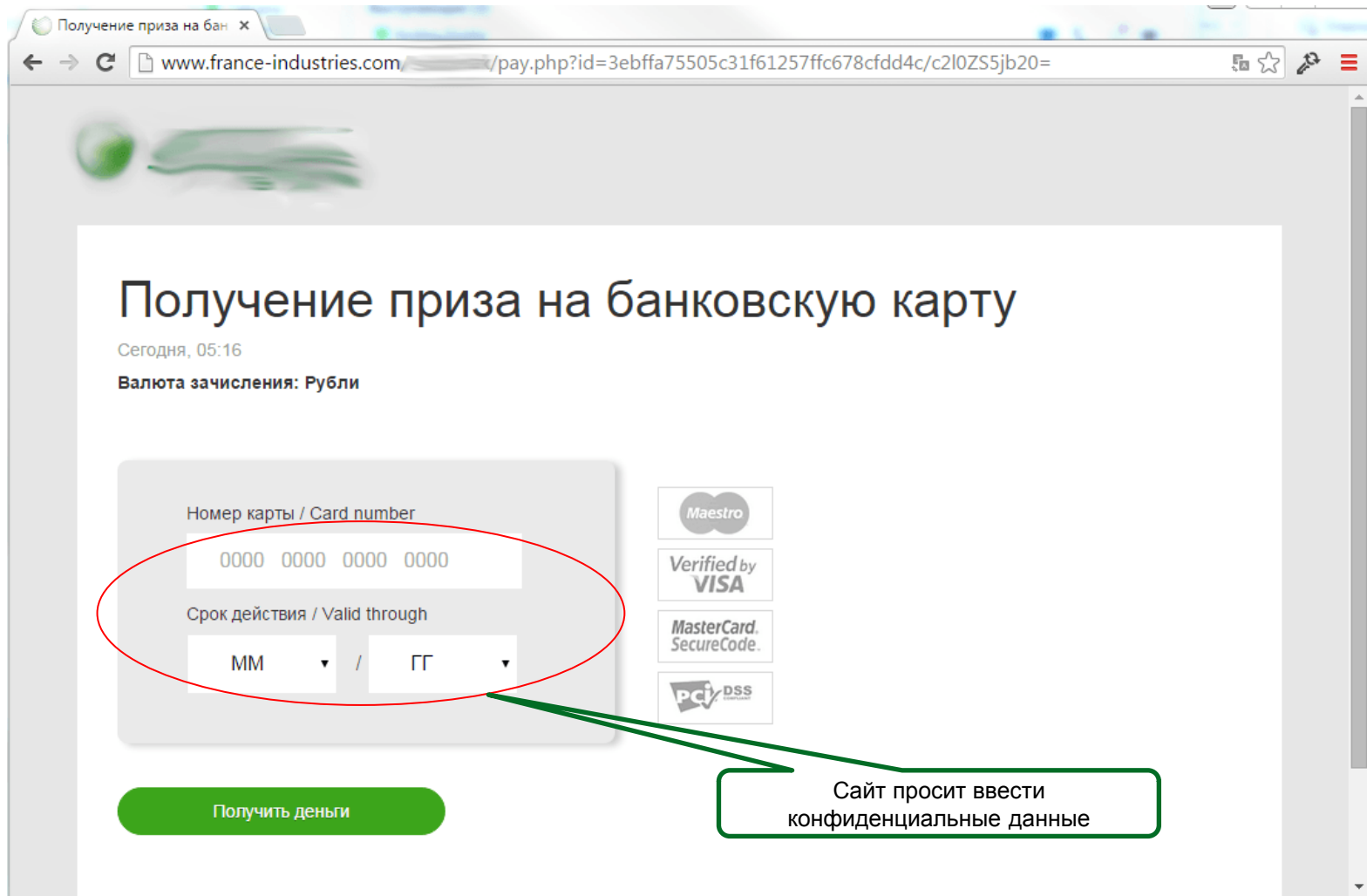
В адресной строке не сайт Сбербанка, а какой-то фишинговый сайт france-industries.com



Слишком хорошо, чтобы быть правдой!

Фишинговый сайт выдает себя за сайт ПАО Сбербанк

Фишинговый сайт, выдающий себя за сайт Сбербанка (2/4)



Получение приза на бан ×

www.france-industries.com /pay.php?id=3ebffa75505c31f61257ffc678cfdd4c/c2l0ZS5jb20=

Получение приза на банковскую карту

Сегодня, 05:16

Валюта зачисления: Рубли

Номер карты / Card number

0000 0000 0000 0000

Срок действия / Valid through

MM / GG

Получить деньги

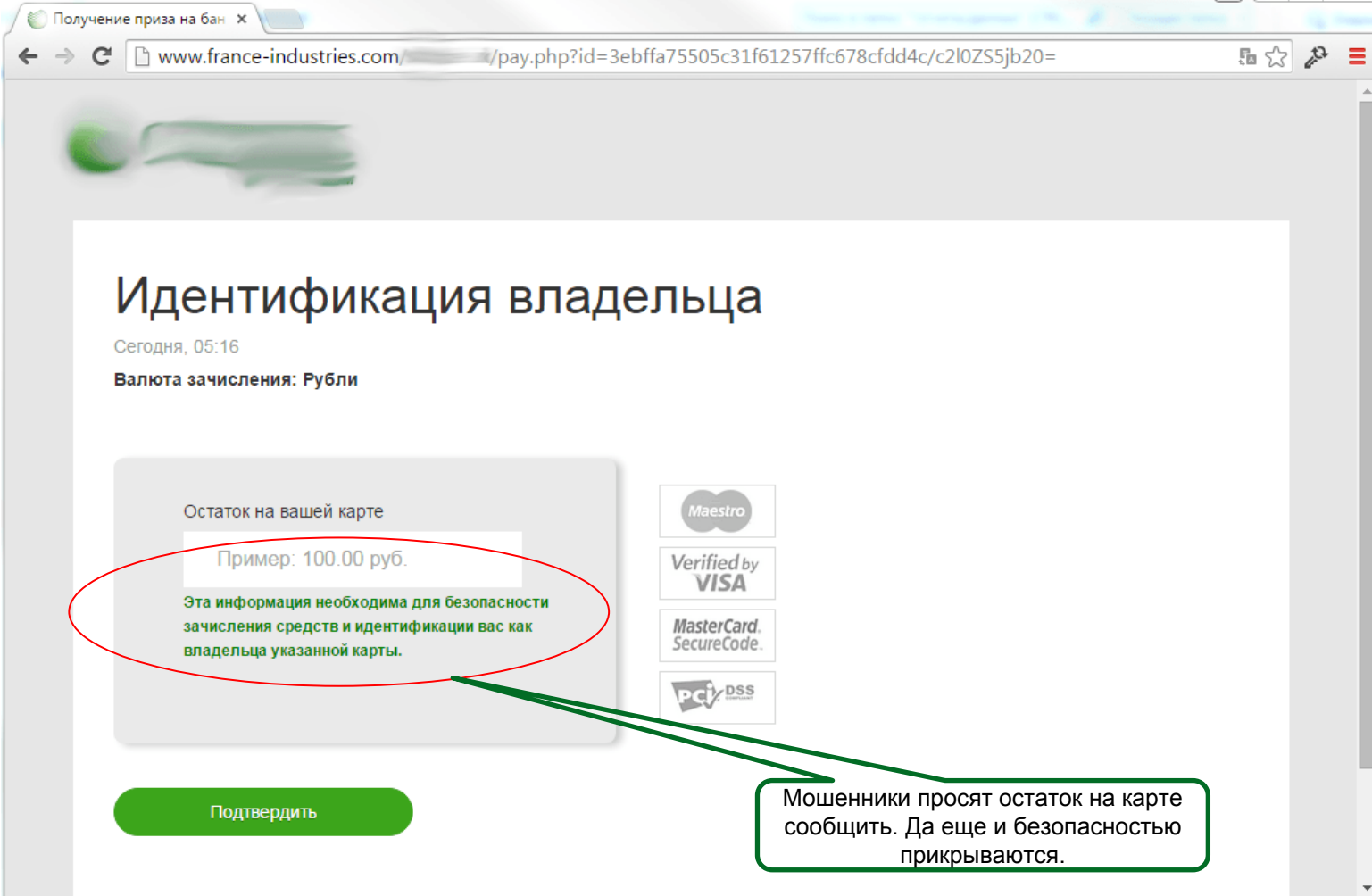
Maestro

Verified by VISA

MasterCard SecureCode.

PCI DSS

Сайт просит ввести конфиденциальные данные



Получение приза на бан

www.france-industries.com/pay.php?id=3ebffa75505c31f61257ffc678cfd4c/c2l0ZS5jb20=

Идентификация владельца

Сегодня, 05:16

Валюта зачисления: Рубли

Остаток на вашей карте

Пример: 100.00 руб.

Эта информация необходима для безопасности зачисления средств и идентификации вас как владельца указанной карты.

Подтвердить

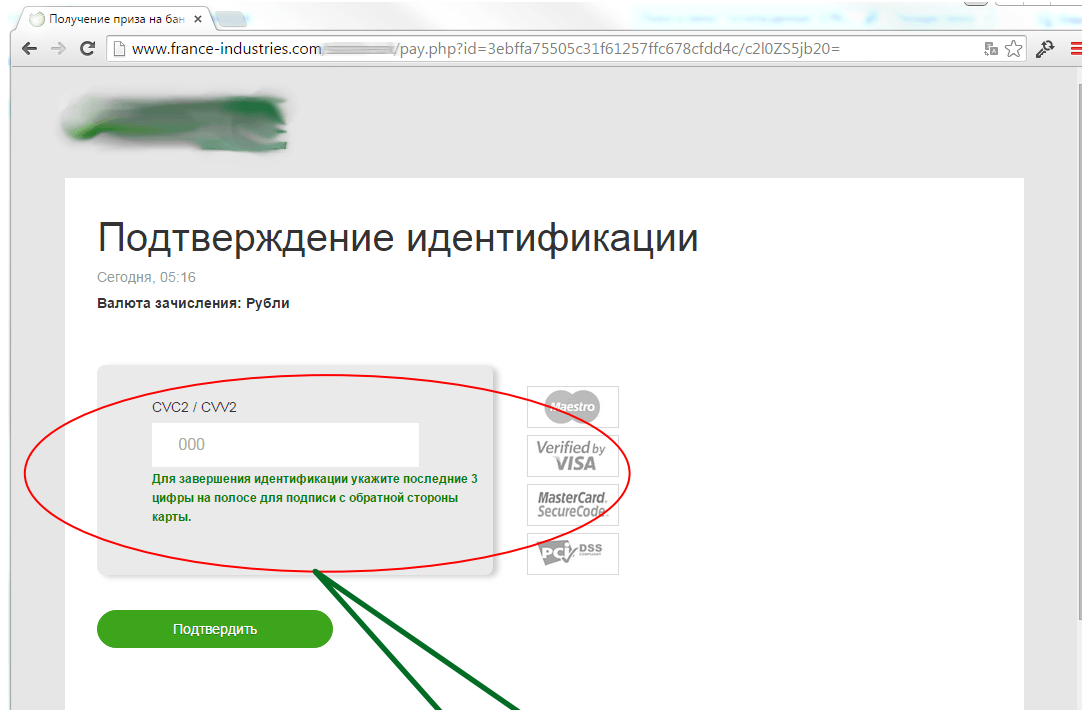
Maestro

Verified by VISA

MasterCard SecureCode

PCI DSS

Мошенники просят остаток на карте сообщить. Да еще и безопасностью прикрываются.



В завершение еще и коды CVC2/CVV2 просят ввести

Пример интерфейса вредоносной фишинговой программы (имитирует Сбербанк Бизнес Онлайн)



НОВОСТИ

30.12.2015
Уважаемые клиенты!
Мы рады поделиться с Вами специальными предложениями Банка, дочерних компаний и партнеров.
Ваш Сбербанк.

Сбербанк Бизнес Онлайн

Номер телефона (второй опционально)

Телефон #1

Телефон #2

[забыли пароль?](#) **ВОЙТИ**

Информацию о системе «Сбербанк Бизнес Онлайн» Вы можете найти на официальном сайте www.sberbank.ru
© 1997 – 2016 ПАО Сбербанк

Внимание, остерегайтесь мошенников!

1. Если при входе в систему Вам **предлагают установить приложение** (например, «SBERSAFE») на Ваш мобильный телефон – **это мошенничество, Ваш компьютер заражен вирусом!**
2. Если при входе в систему **Вас просят ввести номер мобильного телефона** или другую дополнительную информацию, кроме идентификатора пользователя, постоянного и одноразового паролей – **это мошенничество, Ваш компьютер заражен вирусом!**
3. Если Вам на телефон поступил SMS-пароль с реквизитами операции, которой Вы не совершали, и система предлагает ввести данный пароль для отмены этой операции, а по телефону к Вам обращаются от имени Банка с просьбой **отменить ошибочную операцию** в связи с техническим сбоем системы – **это мошенничество, Ваш компьютер заражен вирусом!**
4. Перед вводом одноразового SMS-пароля обязательно **сверьте реквизиты** совершаемой операции с реквизитами в полученном SMS-сообщении.
5. Помните, что **сотрудники банка никогда не звонят клиентам для отмены операций или запроса паролей.**
6. При любых подозрениях на мошенничество прекратите сеанс использования услуги и срочно обратитесь в Банк.

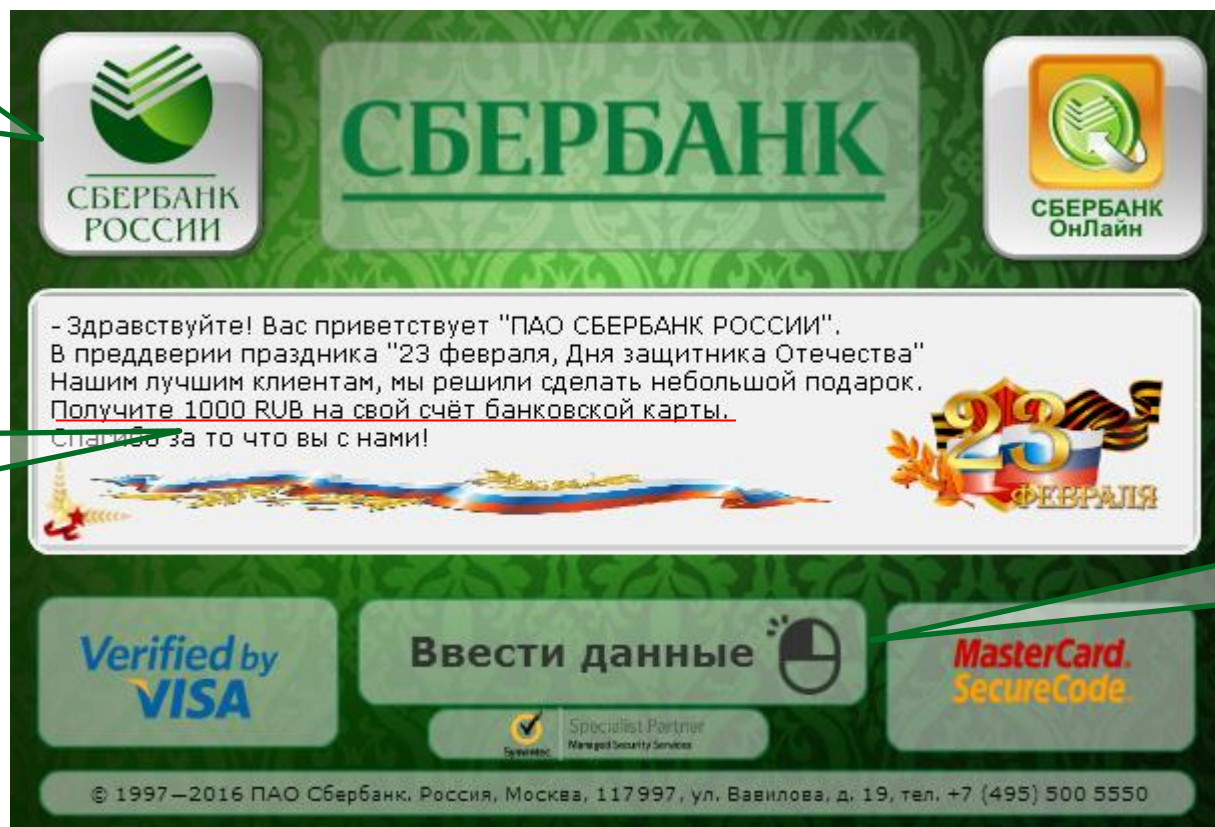
Подробнее о мерах безопасности при работе в Сбербанк Бизнес Онлайн читайте [здесь](#)

Окно вредоносной программы предлагает ввести конфиденциальные данные номер телефона (необходим мошенникам для атаки)

Пример фишингового интерфейса (сайта или вредоносной программы)

Используется логотип Банка – Вас убеждают, что Вы на легитимном сайте

Предложение выглядит заманчивым – вызывает любопытство



СБЕРБАНК
РОССИИ

СБЕРБАНК
Онлайн

- Здравствуйте! Вас приветствует "ПАО СБЕРБАНК РОССИИ".
В преддверии праздника "23 февраля, Дня защитника Отечества"
Нашим лучшим клиентам, мы решили сделать небольшой подарок.
Получите 1000 RUB на свой счёт банковской карты.
Спасибо за то что вы с нами!

23 ФЕВРАЛЯ

Verified by
VISA

Ввести данные

MasterCard.
SecureCode

© 1997–2016 ПАО Сбербанк. Россия, Москва, 117997, ул. Вавилова, д. 19, тел. +7 (495) 500 5550

Сайт предлагает ввести конфиденциальные данные



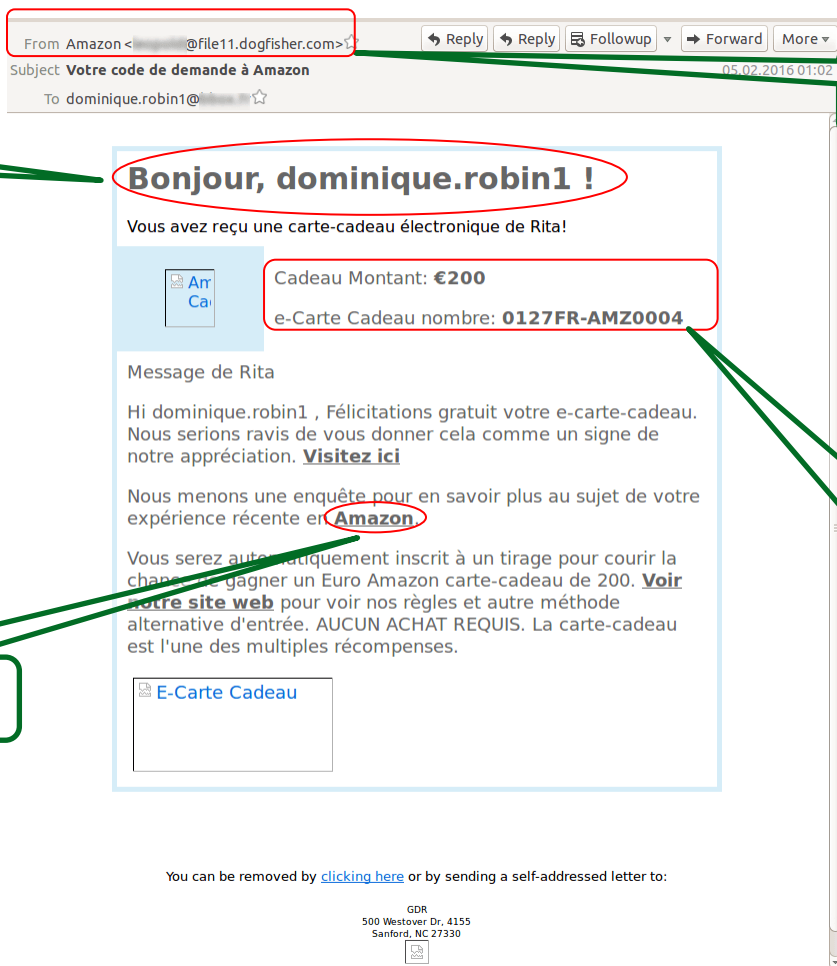
СБЕРБАНК

Всегда рядом

Фишинг. Последние новинки.

март 2016

Новинка –письма от Amazon как приманка.



From Amazon <...@file11.dogfisher.com>

Subject: **Votre code de demande à Amazon**

To: dominique.robin1@...

05.02.2016 01:02

Bonjour, dominique.robin1 !

Vous avez reçu une carte-cadeau électronique de Rita!

Cadeau Montant: **€200**
e-Carte Cadeau nombre: **0127FR-AMZ0004**

Message de Rita

Hi dominique.robin1 , Félicitations gratuit votre e-carte-cadeau. Nous serions ravis de vous donner cela comme un signe de notre appréciation. **Visitez ici**

Nous menons une enquête pour en savoir plus au sujet de votre expérience récente en **Amazon**

Vous serez automatiquement inscrit à un tirage pour courir la chance de gagner un Euro Amazon carte-cadeau de 200. **Voir notre site web** pour voir nos règles et autre méthode alternative d'entrée. AUCUN ACHAT REQUIS. La carte-cadeau est l'une des multiples récompenses.

E-Carte Cadeau

You can be removed by [clicking here](#) or by sending a self-addressed letter to:

GDR
500 Westover Dr, 4155
Sanford, NC 27330

В обращении автоподстановка

Письмо почему-то прислано не с домена Amazon

Ссылка якобы ведет на Amazon

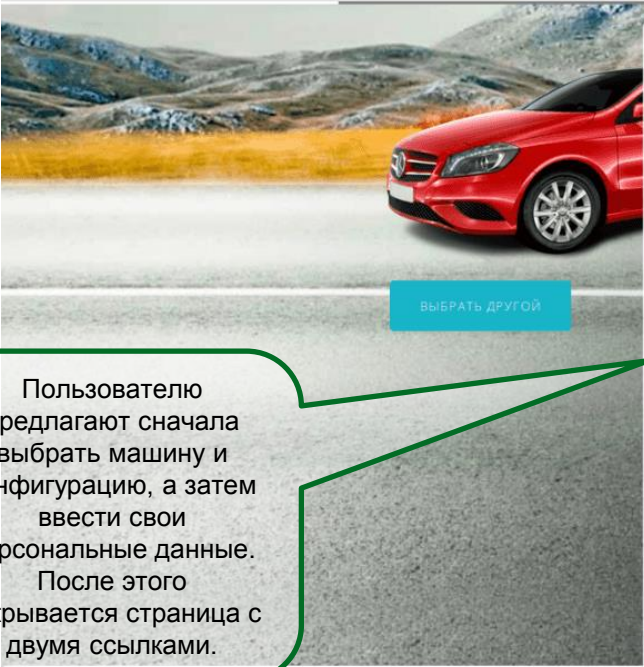
Заманчивое предложение подарочной карты

Фишинговый сайт (открывается после письма от "Amazon" - вариант для России) (1/2)

www.aldaniti.net/wingames/premiumgift_ru-cars/index.php#

Участвуйте и выиграйте свою любимую машину

Выберите свою **МАШИНУ**



Выбрать другой

Пожалуйста, введите свои данные, чтобы получить подарок

Пол :
- Выберите -

Имя :
Введите своё имя

Фамилия :
Введите вашу фамилию

Отчество :
Введите Ваше отчество

Контактная информация победителя

Email :
drgfsd@fddsf.de

Мобильный телефон :
+7 Мобильный телефон

Почтовый индекс :
Введите ваш почт

Место Проживания :
Выберите

Все поля являются обязательными для подтверждения Вашего участия

Политика Конфиденциальности

Я подтверждаю, что мне больше 18 лет

Я ПРОЧИТАЛ И ПРИНИМАЮ [УСЛОВИЯ](#) и [Политику Конфиденциальности](#)

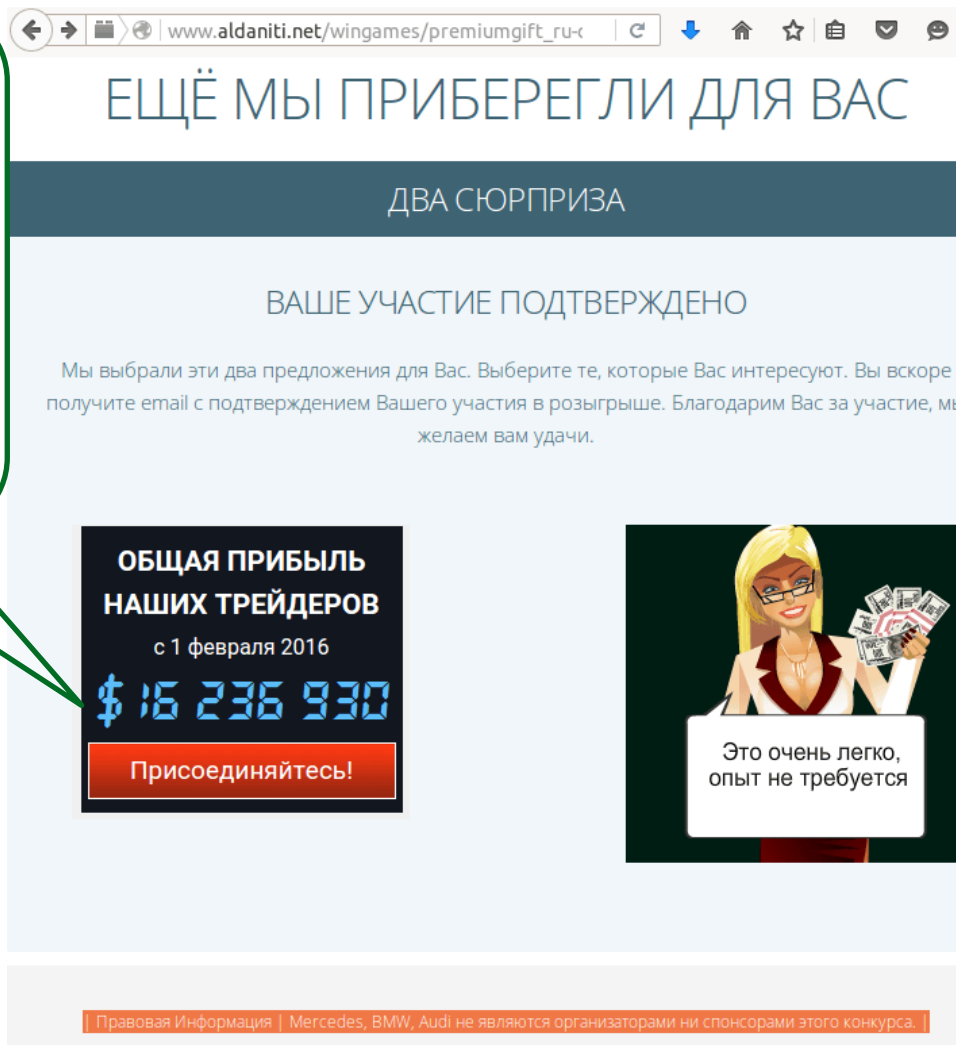
Участвовать

Этот конкурс направлен на инкорпорацию Ваших данных в рекламный файл компании Aldaniti International Network LTD. Поэтому, если Вы не хотите чтобы ваши данные были включены в этот файл, пожалуйста, воздержитесь от

Пользователю предлагают сначала выбрать машину и конфигурацию, а затем ввести свои персональные данные. После этого открывается страница с двумя ссылками.

Фишинговый сайт (открывается после письма от "Amazon" - вариант для России) (2/2)

Одна ссылка ведет на страницу, предлагающую завести счет для торговли на бирже и внести первые деньги на свой депозит. Пополнение происходит с помощью платежной системы «Яндекс.Деньги», причем на имя titantrade[.]com; остается только догадываться, кому и куда уйдут деньги. Судя по отзывам, опубликованным в интернете, никаких выплат после этого доверчивые жертвы не получают.



The screenshot shows a web browser window with the address bar containing www.aldaniti.net/wingames/premiumgift_ru-c. The main heading reads "ЕЩЁ МЫ ПРИБЕРЕГЛИ ДЛЯ ВАС" (We have also reserved for you). Below it, a dark blue banner says "ДВА СЮРПРИЗА" (Two surprises). The central text states "ВАШЕ УЧАСТИЕ ПОДТВЕРЖДЕНО" (Your participation is confirmed) and includes a message: "Мы выбрали эти два предложения для Вас. Выберите те, которые Вас интересуют. Вы вскоре получите email с подтверждением Вашего участия в розыгрыше. Благодарим Вас за участие, мы желаем вам удачи." (We have selected these two offers for you. Choose the ones you are interested in. You will soon receive an email with confirmation of your participation in the contest. Thank you for your participation, we wish you good luck.)

Two promotional boxes are visible:

- Left box:** "ОБЩАЯ ПРИБЫЛЬ НАШИХ ТРЕЙДЕРОВ с 1 февраля 2016" (Total profit of our traders since February 1, 2016) with a large digital display showing "\$ 16 236 930" and a red button that says "Присоединяйтесь!" (Join!).
- Right box:** An illustration of a blonde woman in a white dress holding money, with a speech bubble that says "Это очень легко, опыт не требуется" (This is very easy, no experience is required).

At the bottom of the page, a small footer reads: "Правовая Информация | Mercedes, BMW, Audi не являются организаторами ни спонсорами этого конкурса." (Legal Information | Mercedes, BMW, Audi are not organizers or sponsors of this contest.)

Вторая ссылка ведет на страницу, где предлагают «скачать» бесплатно» некую программу для заработка в интернете (файл RBPSetupRU_o5pqw.exe). Это бот для рулетки, который автоматически делает ставки на деньги пользователя, а его авторы получают деньги от казино по программе привлечения клиентов.

Письмо с «документом». Особенность – документ содержит объект Mediabox

Обращения нет

From: [redacted].com
Subject: Fwd: Transfer confirmation copy
To: [redacted]@hotmail.com
Date: Tue, 18 Aug 2015 20:14:41 +0200

Attention;

Re: Payment of \$53,000.40.

Attached fore is the Proof of Transfer as received today from our Bank, Wells Fargo Bank USA. It is important that you confirm receipt of payment asap as we look forward to futher instructions.

Thanks and God bless.

John Rodriguez

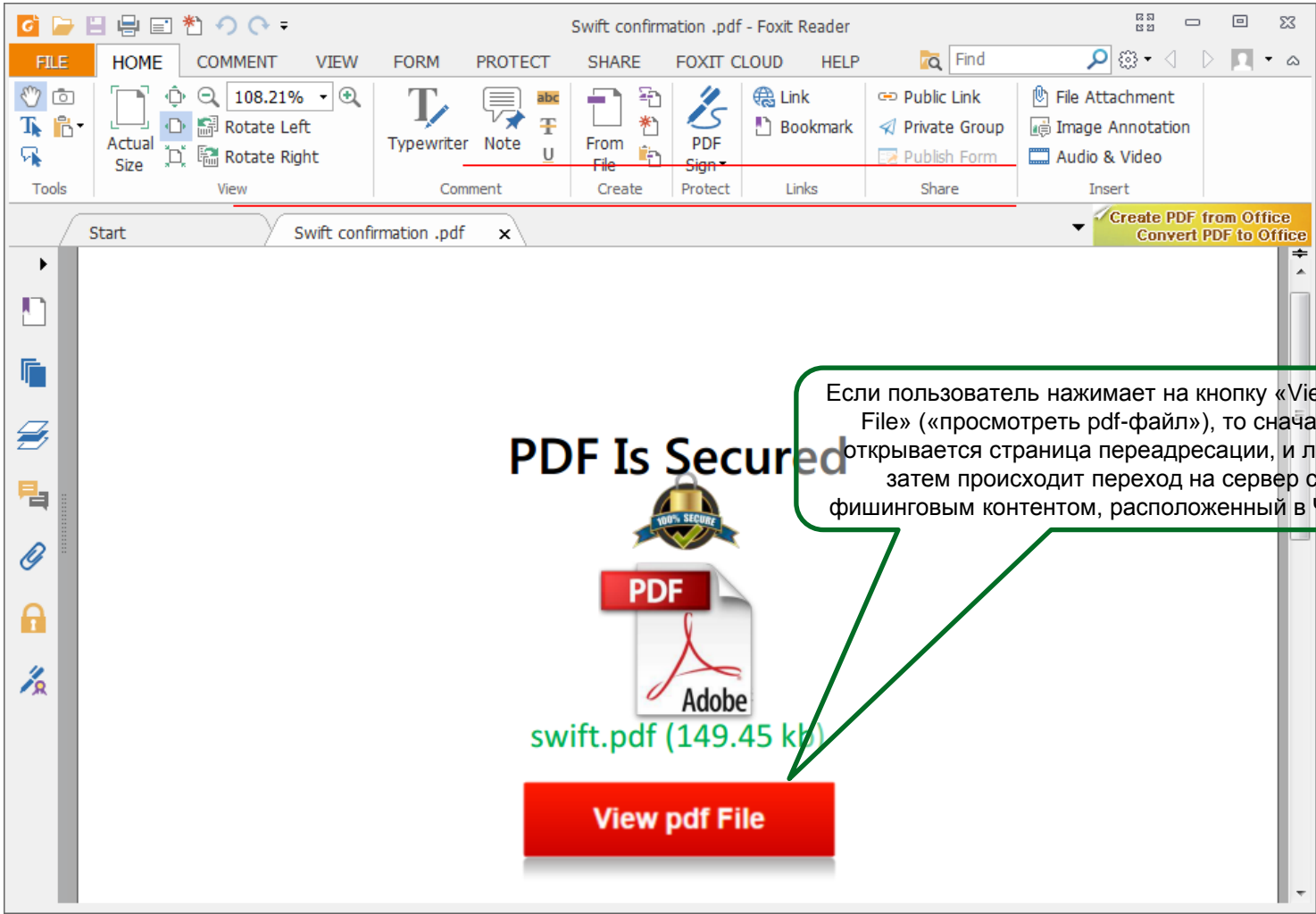
Teléfono: (502) [redacted]

Email: [redacted].com

[redacted].com

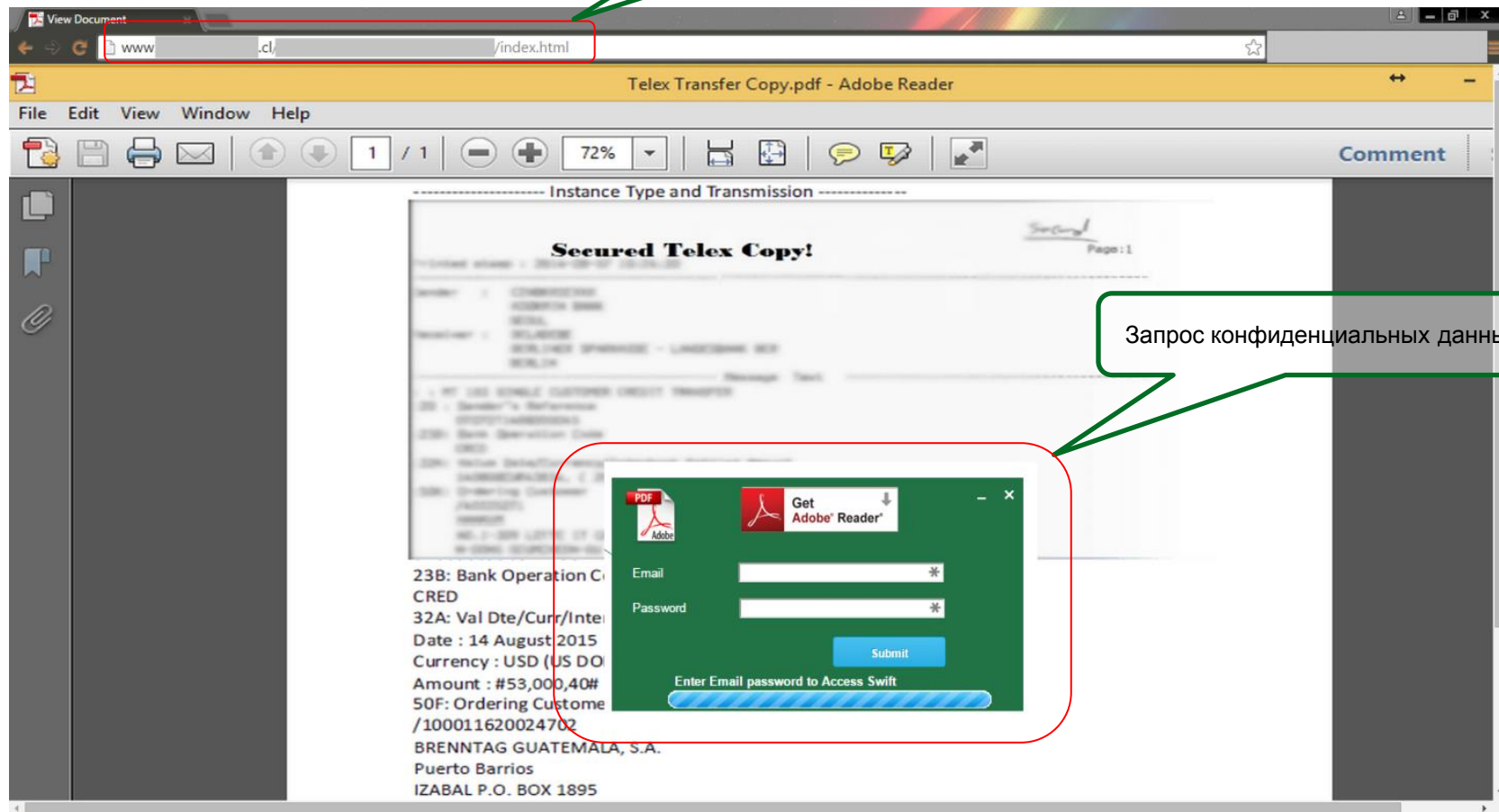
Эксплуатируется любопытство, заманчивое предложение, и создается чувство срочности

Вложение в фишинговом письме, содержащее объект Mediabox, документ, который открывается щелчком мыши и используется для переадресации пользователя на фишинговый веб-сайт.



Страница фишингового сайта (открывается после открытия Mediabox)

В адресной строке посторонний сайт



----- Instance Type and Transmission -----

Secured Telex Copy!

23B: Bank Operation C
CRED
32A: Val Dte/Curr/Inte
Date : 14 August 2015
Currency : USD (US DO
Amount : #53,000,40#
50F: Ordering Custome
/100011620024702
BRENNTAG GUATEMALA, S.A.
Puerto Barrios
IZABAL P.O. BOX 1895

Get Adobe Reader

Email

Password

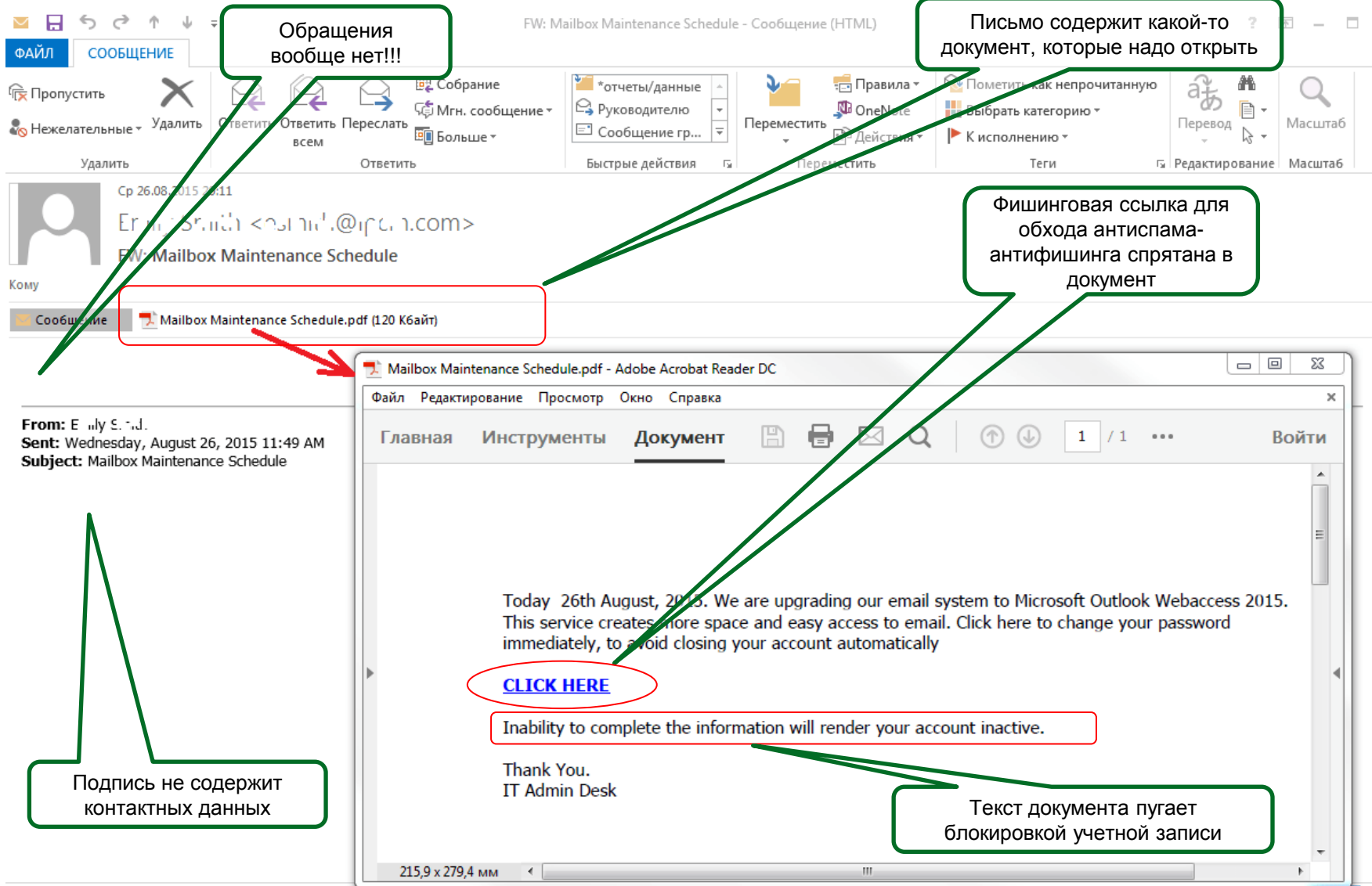
Submit

Enter Email password to Access Swift

Запрос конфиденциальных данных

Фишинговое письмо из категории «документы».

Особенность – ссылка «спрятана» во вложенном документе.



Обращения вообще нет!!!

Письмо содержит какой-то документ, которые надо открыть

Фишинговая ссылка для обхода антиспама-антифишинга спрятана в документ

Подпись не содержит контактных данных

Текст документа пугает блокировкой учетной записи

CLICK HERE

Inability to complete the information will render your account inactive.

Today 26th August, 2015. We are upgrading our email system to Microsoft Outlook Webaccess 2015. This service creates more space and easy access to email. Click here to change your password immediately, to avoid closing your account automatically

Thank You.
IT Admin Desk

From: E...ly S...J...
Sent: Wednesday, August 26, 2015 11:49 AM
Subject: Mailbox Maintenance Schedule

Mailbox Maintenance Schedule.pdf (120 Кбайт)

FW: Mailbox Maintenance Schedule - Сообщение (HTML)

Удалить, Ответить, Переслать, Больше, Быстрые действия, Переместить, Действия, Теги, Редактирование, Масштаб

Собрание, Мгн. сообщение, Больше, *отчеты/данные, Руководителю, Сообщение гр..., Правила, OneNote, Пометить как непрочитанную, выбрать категорию, К исполнению, Перевод, Масштаб

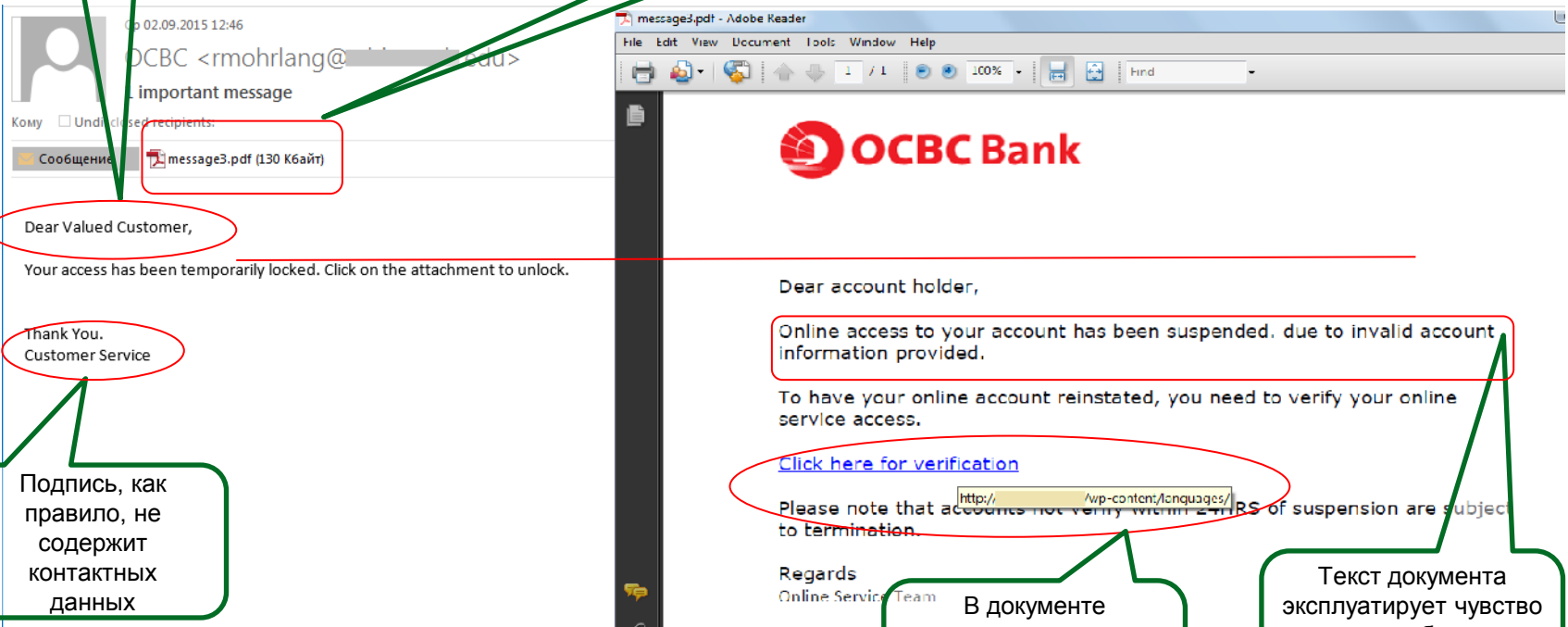
Пропустить, Нежелательные, Удалить, Ответить, Ответить всем, Удалить, Ответить

Сообщение

Главная, Инструменты, Документ, Войти

215,9 x 279,4 мм

Пример фишингового «банковского» письма. Особенность: ссылка на фишинговый сайт спрятана в документ.



Обезличенное обращение

02.09.2015 12:46
OCBC <rmohrlang@...>
important message
Сообщение message3.pdf (130 Кбайт)

Dear Valued Customer,
Your access has been temporarily locked. Click on the attachment to unlock.

Thank You.
Customer Service

Письмо содержит какой-то документ, который надо открыть

message3.pdf - Adobe Reader

OCBC Bank

Dear account holder,
Online access to your account has been suspended, due to invalid account information provided.
To have your online account reinstated, you need to verify your online service access.
[Click here for verification](#)
Please note that accounts not verified within 21RS of suspension are subject to termination.

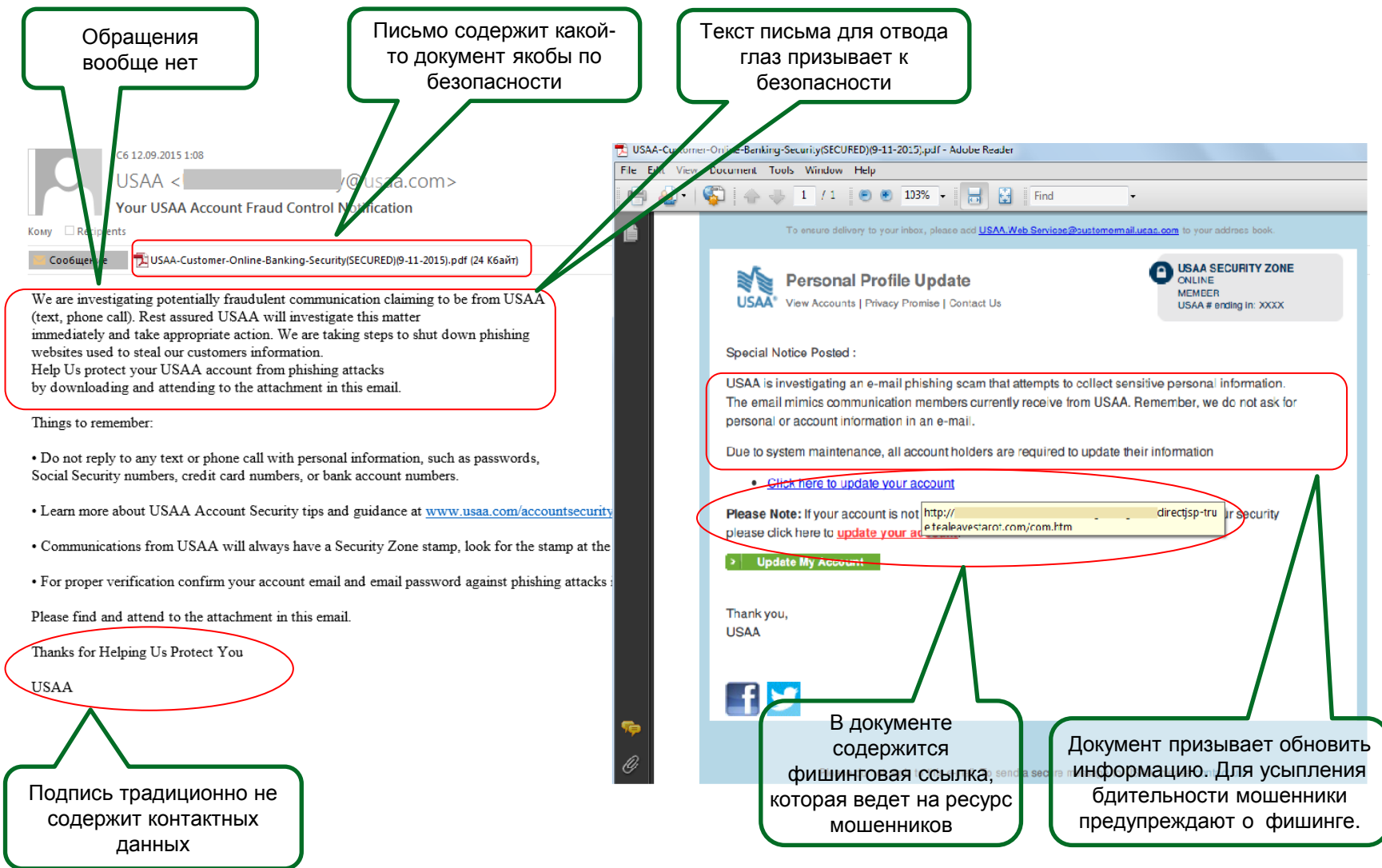
Regards
Online Service Team

Подпись, как правило, не содержит контактных данных

В документе содержится фишинговая ссылка, которая ведет на ресурс мошенников

Текст документа эксплуатирует чувство тревоги, побуждает к немедленным действиям

Пример фишингового «банковского» письма о безопасности. Ссылка также спрятана в документе.



Обращения вообще нет

Письмо содержит какой-то документ якобы по безопасности

Текст письма для отвода глаз призывает к безопасности

Подпись традиционно не содержит контактных данных

В документе содержится фишинговая ссылка, которая ведет на ресурс мошенников

Документ призывает обновить информацию. Для усыпления бдительности мошенники предупреждают о фишинге.

С6 12.09.2015 1:08
USAA <[redacted]@usaa.com>
Your USAA Account Fraud Control Notification

Сообщение: USAA-Customer-Online-Banking-Security(SECURED)(9-11-2015).pdf (24 Кбайт)

We are investigating potentially fraudulent communication claiming to be from USAA (text, phone call). Rest assured USAA will investigate this matter immediately and take appropriate action. We are taking steps to shut down phishing websites used to steal our customers information. Help Us protect your USAA account from phishing attacks by downloading and attending to the attachment in this email.

Things to remember:

- Do not reply to any text or phone call with personal information, such as passwords, Social Security numbers, credit card numbers, or bank account numbers.
- Learn more about USAA Account Security tips and guidance at www.usaa.com/accountsecurity
- Communications from USAA will always have a Security Zone stamp, look for the stamp at the
- For proper verification confirm your account email and email password against phishing attacks

Please find and attend to the attachment in this email.

Thanks for Helping Us Protect You
USAA

USAA Customer-Online-Banking-Security(SECURED)(9-11-2015).pdf - Adobe Reader

To ensure delivery to your inbox, please add USAA.Web.Services@customeremail.usaa.com to your address book.

Personal Profile Update
View Accounts | Privacy Promise | Contact Us

USAA SECURITY ZONE
ONLINE MEMBER
USAA # ending in: XXXX

Special Notice Posted :

USAA is investigating an e-mail phishing scam that attempts to collect sensitive personal information. The email mimics communication members currently receive from USAA. Remember, we do not ask for personal or account information in an e-mail.

Due to system maintenance, all account holders are required to update their information

- [Click here to update your account](#)

Please Note: If your account is not [http://\[redacted\].com/html](http://[redacted].com/html) please click here to [update your account](#)

Update My Account!

Thank you,
USAA

Фишинговые подделки

1) Подделки под письма с мобильных устройств

- Письма, имитирующие письма, отправленные с мобильных устройств.
- Общее у таких имитаций одно – лаконичный (или вовсе отсутствующий) текст и подпись вида «Sent from my iPhone».
- Упоминаются iPad, iPhone, Samsung Galaxy и другие модели.
- Как правило, они содержат вредоносные вложения или ссылки.

2) Подделки под уведомления от мобильных приложений

- Письма, подделанные под оповещения от различных мобильных приложений, как правило, тех же WhatsApp и Viber.
- Эти мобильные приложения не связаны с почтовым аккаунтом пользователя, поэтому такие письма являются мошенническими.
- Обычно содержат зараженные вложения, которые выдаются за фотографии
- Могут содержать «кнопки» якобы для проигрывания мультимедийного контента

Примеры фишинговых писем якобы с мобильных устройств и от имени WhatsApp

From: WhatsApp <{messages@...}>
 To:
 Subject: Somebody has just sent you a pic

Message: IMG003299.zip (48 KB)

WhatsApp

Hey!

Your friend has just sent you a pic in WhatsApp. Open attachments to take a look.

© 2013 WhatsApp Inc

Письмо содержит какой-то документ (причем архив!), который надо открыть

Доверие вызывает то, что письмо прислано из мобильного мессенджера WhatsApp

Дополнительно эксплуатируется любопытство (что же за картинку прислали?)

From: ewaw75@... From: qrcsg <admin@xxxxx.xxx>
 To:
 Cc:
 Subject: fotka Subject: Spam:: knDrugstore

Message: fotka_002.zip (73 K)

oxygen
 anna violent <http://en.com/index3.htm?j...> bargain

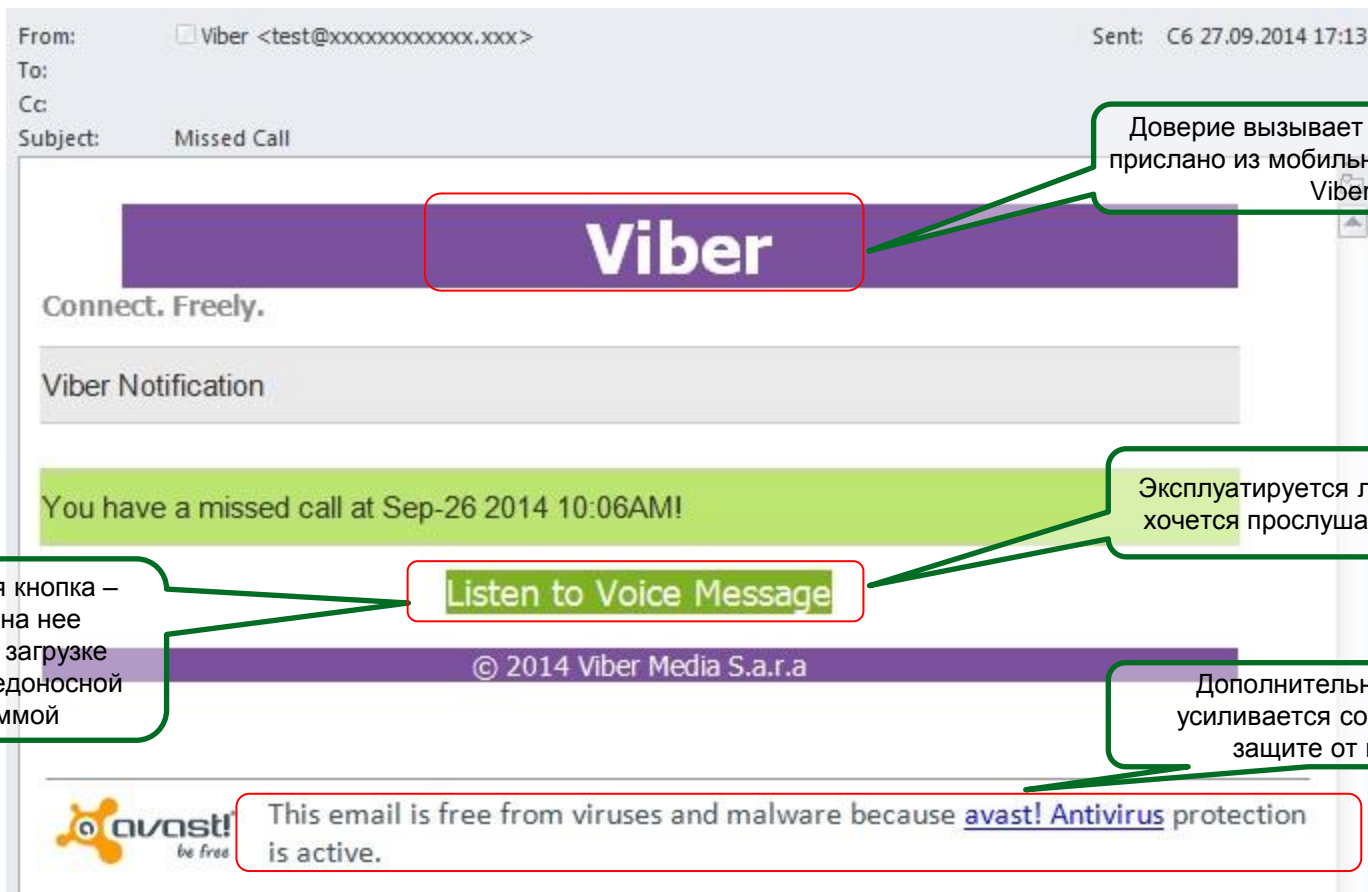
Wysłane z iPhone'a

Sent from my iPhone

Фишинговая ссылка

Доверие вызывает то, что письмо прислано якобы с мобильного устройства.

Пример фишингового письма якобы от имени Viber



Оповещение о голосовом сообщении, якобы отправленном через Viber, содержит кнопку «Listen to Voice Message», нажатие на которую приводит к загрузке архива с вредоносной программой.

Письмо из категории «подделки под письма с мобильных устройств»



Обращения нет

Письмо содержит какой-то документ, которые надо открыть

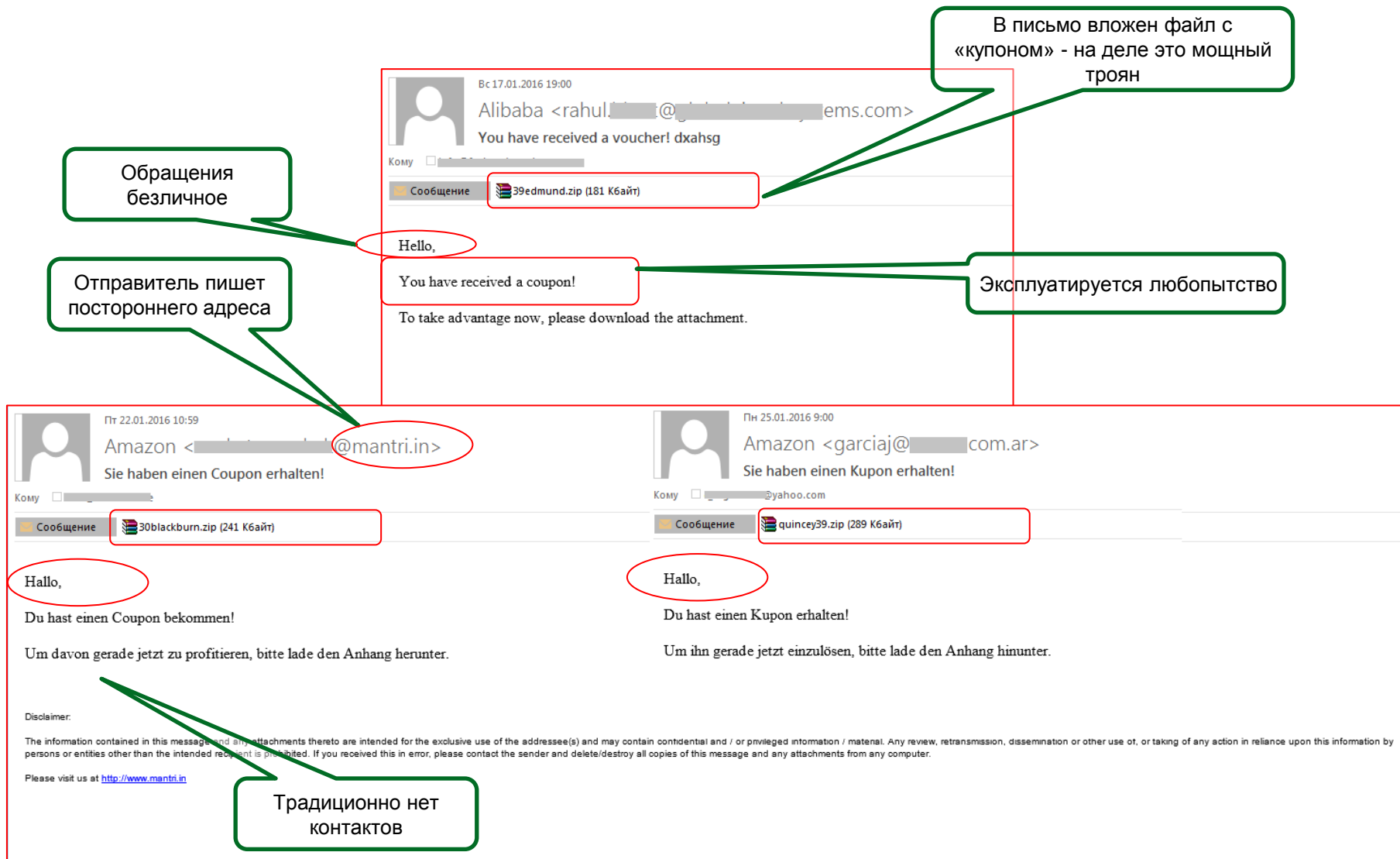
Сообщение  New Doc 115.docm (33 Кбайт)

[Sent from Yahoo Mail on Android](#)

Подписи нет

Текст письма отсутствует. Эксплуатирует любопытство. Доверие вызывает то, что документ прислан якобы с мобильного устройства.

Письма от имени известных платформ онлайн-торговли Amazon, Alibaba



Обращения безличное

Отправитель пишет постороннего адреса

В письмо вложен файл с «купоном» - на деле это мощный троян

Эксплуатируется любопытство

Традиционно нет контактов

Alibaba <rahu!@...ems.com>
Вс 17.01.2016 19:00
You have received a voucher! dxahsg
Сообщение 39edmund.zip (181 Кбайт)

>Hello,
You have received a coupon!
To take advantage now, please download the attachment.

Amazon <...@mantri.in>
Пт 22.01.2016 10:59
Sie haben einen Coupon erhalten!
Сообщение 30blackburn.zip (241 Кбайт)

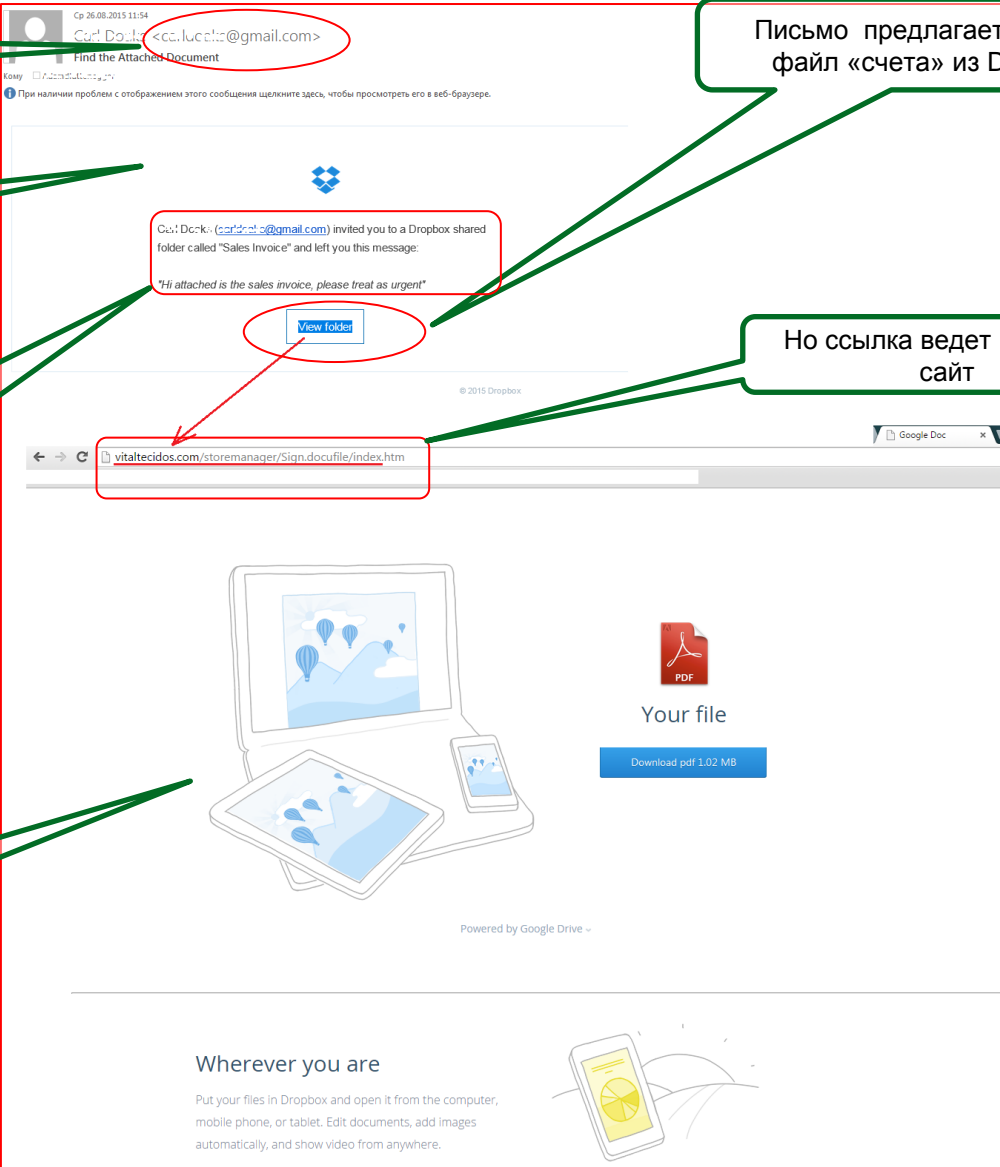
Hallo,
Du hast einen Coupon bekommen!
Um davon gerade jetzt zu profitieren, bitte lade den Anhang herunter.

Disclaimer:
The information contained in this message and any attachments thereto are intended for the exclusive use of the addressee(s) and may contain confidential and / or privileged information / material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete/destroy all copies of this message and any attachments from any computer.
Please visit us at <http://www.mantri.in>

Amazon <garciaj@...com.ar>
Пн 25.01.2016 9:00
Sie haben einen Kupon erhalten!
Сообщение quincey39.zip (289 Кбайт)

Hallo,
Du hast einen Kupon erhalten!
Um ihn gerade jetzt einzulösen, bitte lade den Anhang hinunter.

Фишинговое письмо, предлагающее скачать файл «счета» якобы из Dropbox



The image shows a phishing email and a corresponding fake file download page. The email is from 'Carl Davis <cc.lucate@gmail.com>' and contains a message from 'Carl Davis' inviting the recipient to a Dropbox folder named 'Sales Invoice'. The message includes a 'View folder' button and a note that the invoice is urgent. The browser address bar shows a URL from 'vitaltecidos.com'. The download page features a PDF icon, the text 'Your file', and a 'Download pdf 1.02 MB' button. The page is styled to look like a legitimate Dropbox interface, including a 'Powered by Google Drive' footer and a 'Wherever you are' section with a mobile phone illustration.

Отправитель пишет с gmail.com

Обращения нет

Сообщение говорит о срочности – требует немедленных действий

Фишинговая страница стилизована под сайт Dropbox.

Письмо предлагает скачать файл «счета» из Dropbox

Но ссылка ведет на другой сайт

Пример фишинговой страницы типа «Dropbox» для кражи учетных данных

charlieskids.org/wp-content/themes/radiate/u072432.htm

bbvanetcash.com.co



Это не Dropbox!!!



YAHOO! Gmail AOL Microsoft Hotmail

Choose your email provider Below and sign in

Click to select provider

Email

Email Password

*Please login with your email account and not your dropbox account

Remember me

Sign in

[Forgot your password?](#)

Фишинговая страница может быть нацелена и на кражу учетной записи

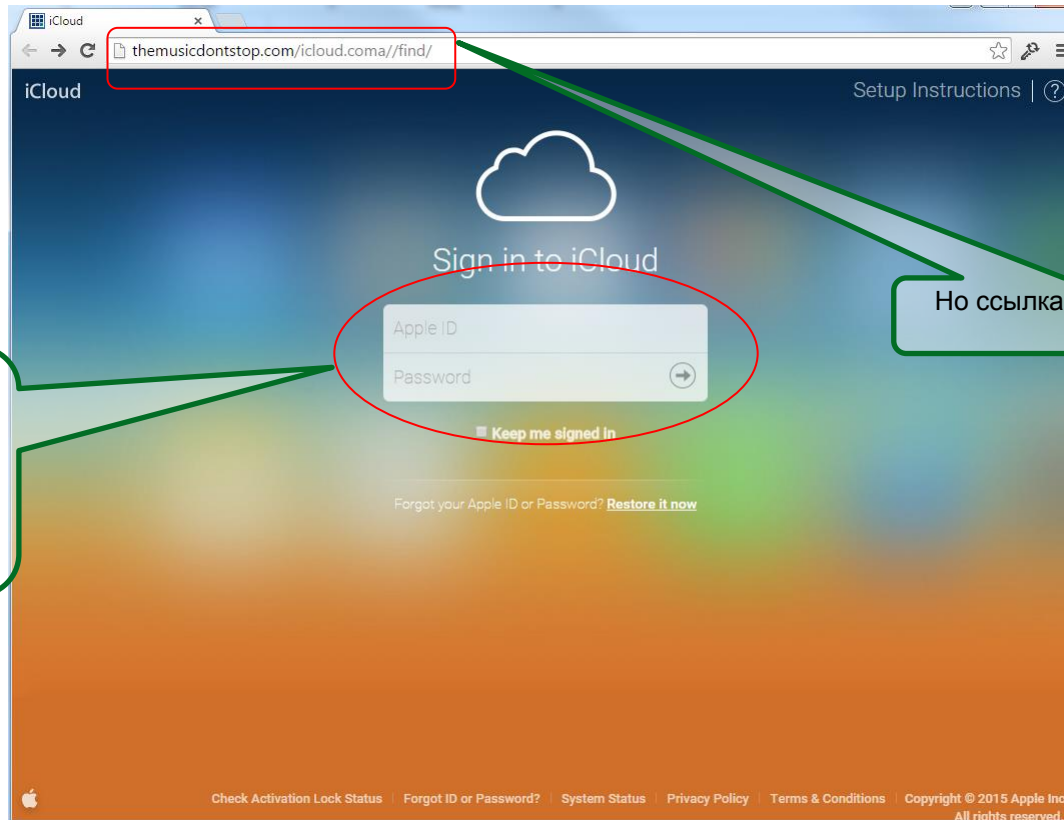
Dropbox
Install
Mobile
Pricing
Business
Tour

About us
Dropbox Blog
Our team
Branding
News
Jobs

Support
Help Center
Get Started
Privacy & Terms
Copyright
Contact us

Community
Referrals
Twitter
Facebook
Developers

Фишинговая страница для кражи AppleID и пароля к облачному хранилищу iCloud



мошенники пытаются украсть у пользователя AppleID и пароль к облачному хранилищу данных iCloud

Но ссылка ведет на другой сайт

При получении подозрительного письма следуйте следующим правилам:

- 1** **Будьте осторожны с подозрительными письмами, побуждающими Вас к немедленным действиям.** Возможно это признаки воздействия на Вас с помощью социальной инженерии. Не надо слепо следовать каким-то указаниям в почте, особенно тем, которые побуждают выполнять некие действия здесь и сейчас.
- 2** **Не переходите по ссылкам, не кликайте на подозрительные объекты.** Наведите курсор мыши на подозрительную ссылку/объект и Вы увидите, куда она ведёт на самом деле. Если адреса не совпадают, то это фишинговая ссылка.
- 3** **Будьте осторожны с вложениями,** открывайте только те, которые ждали. Во вложениях также будьте осторожны с ссылками.
- 4** **Сверяйте адрес отправителя с доменом организации.** Если домен отправителя не имеет отношения к компании, учреждению, или содержит отличия от этого домена, значит это фишинговое письмо.
- 5** **Обращайте внимание на обращение и подпись к письму.** Если они являются безличными, или есть признак автоподстановки в обращении, то высока вероятность фишинга.
- 6** **Не вводите свои конфиденциальные данные** на подозрительных сайтах или в какие-либо анкетные формы.
- 7** При переходе на сайт **обращайте внимание на адресную строку браузера.** Если адрес не соответствует ожидаемому, или в адресной строке нет значка «замка», то это возможный фишинг.

- 8 **Будьте осторожны с подозрительными письмами от друзей и коллег.** То, что вы получили письмо от друга, не означает, что он действительно его отправлял. Возможно, компьютер друга заражен вирусами или его аккаунт взломали и письма рассылают вирусы всем получателям из адресной книги, в том числе, и Вам. Если вы получили письмо от друга или коллеги, но с каким-то неожиданным содержанием (например, с просьбой срочно перечислить деньги), позвоните им, чтобы убедиться, что они действительно отправляли письмо.
- 8 **Не звоните по указанному в подозрительном письме или на сайте номеру телефона.** Всегда звоните по номеру телефона, который есть у вас или вы можете узнать независимым путем. Например, получив письмо от банка с неожиданным содержанием (например, с сообщением об увеличении долга и каким-то важным документом или ссылкой, которые надо немедленно открыть), позвоните по номеру банка, указанному на его карте или на его сайте.
- 9 **Не отвечайте на подозрительные письма.** Мошенники могут вступить в переписку, для выяснения версии возможного программного обеспечения, IP адресов, антивирусной программы — это все можно извлечь из служебных заголовков и тела письма.
- 10 Помните, что если что-то в письме кажется подозрительным или слишком хорошим, чтобы быть правдой, то, скорее всего это обман.
- 11 **Если прочитав письмо в корпоративной почте, вы понимаете, что это фишинг, перешлите письмо на специальный адрес Департамента безопасности Zit@Sberbank.ru. При невозможности пересылки – удалите его.** Использование электронной почты безопасно, если пользоваться здравым смыслом.