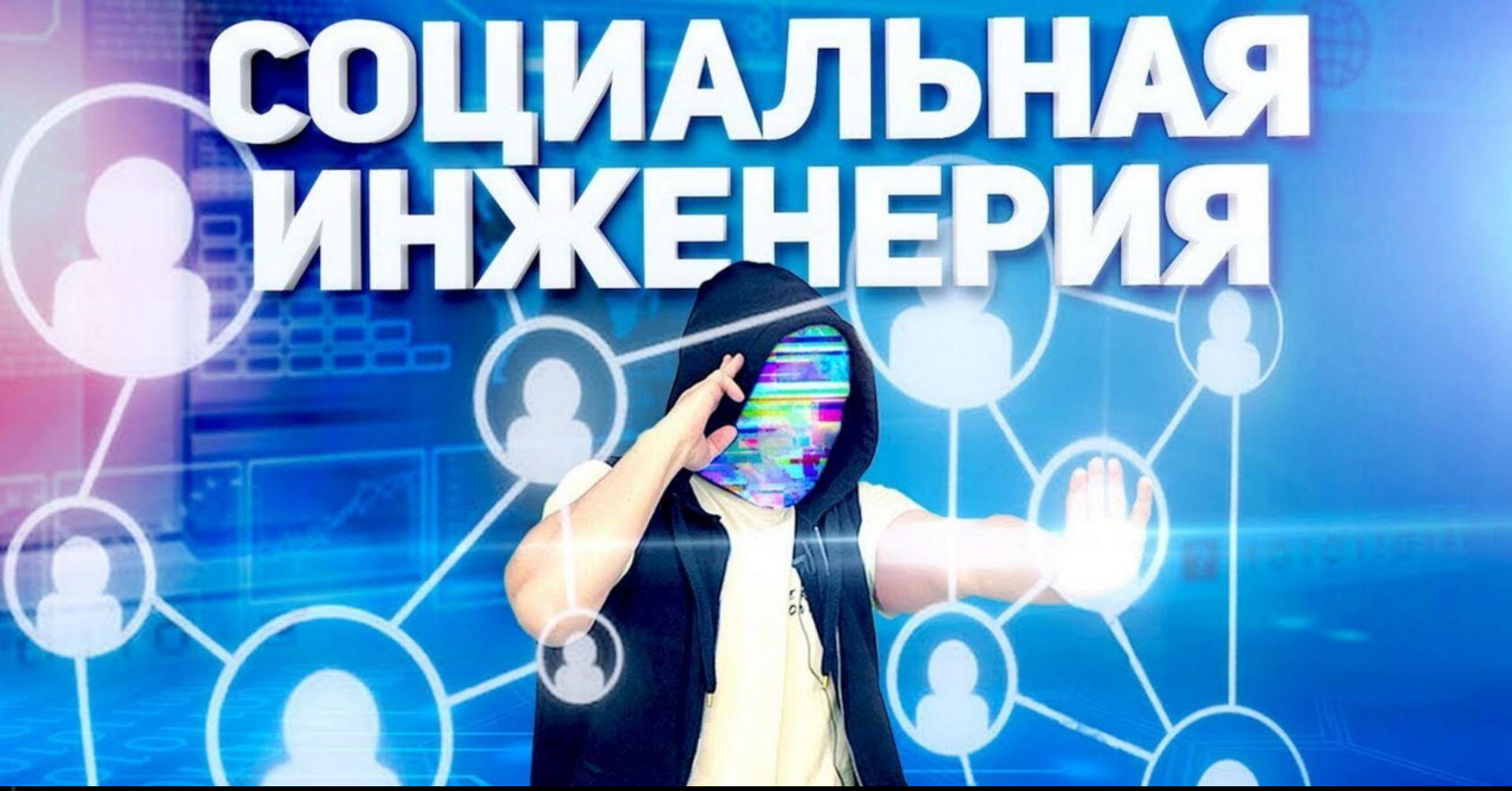

Социальная инженерия

Сейчас наши девайсы хранят очень много информации.
От безобидных заметок до персональных данных, секретных файлов и банковских карт



Социальная инженерия – метод получения необходимого доступа к информации, основанный на особенностях психологии людей

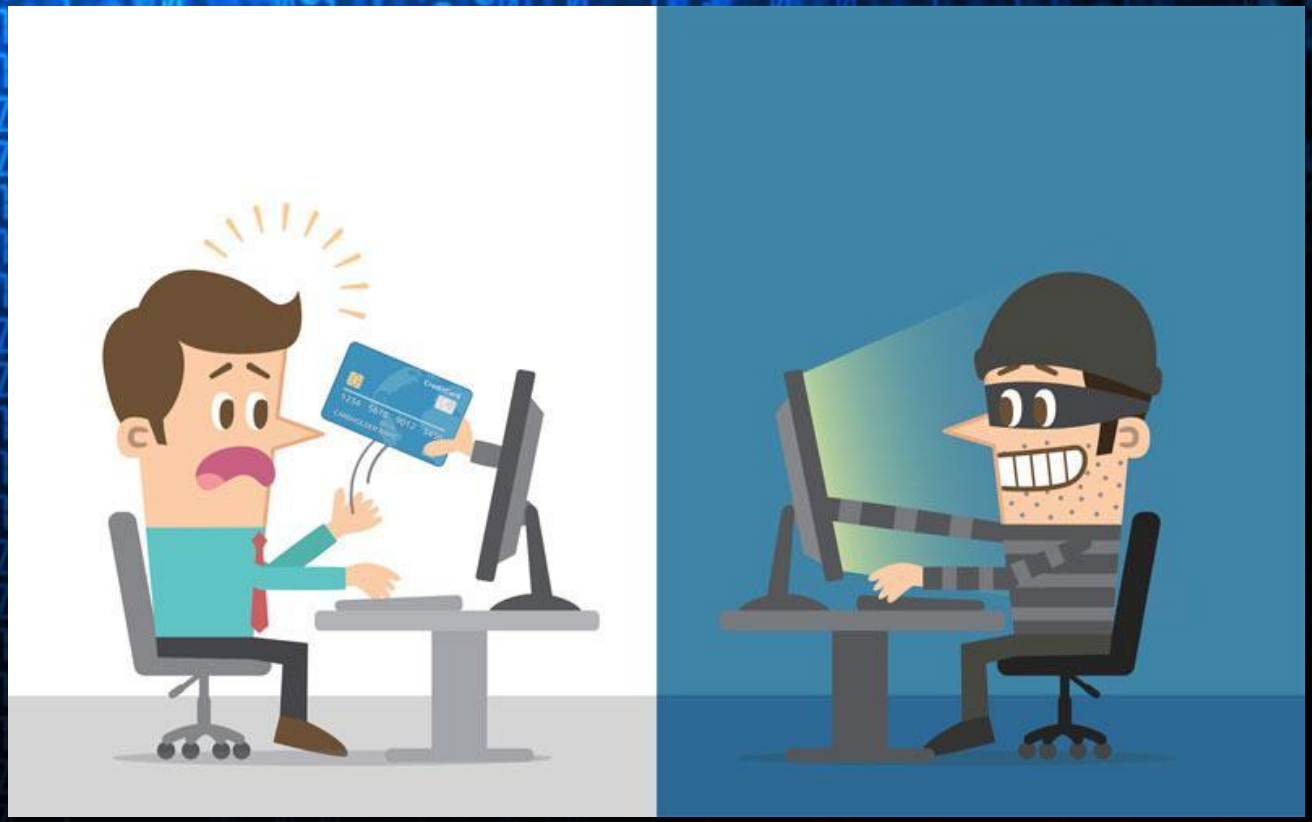
Конечно, сегодня социальную инженерию зачастую используют в интернете для получения закрытой информации или информации, которая представляет большую ценность.

Современные социальные инженеры используют свои навыки для повышения результатов в бизнесе и жизни.

Все техники социальной
искажениях.

Эти ошибки в поведении используются социальными инженерами для создания атак, направленных на получение конфиденциальной информации, часто с согласия жертвы.

Так, одним из простых примеров является ситуация, в которой некий человек входит в здание компании и вешает на информационном бюро объявление, выглядящее как официальное, с информацией об изменении телефона справочной службы интернет-провайдера. Когда сотрудники компании звонят по этому номеру, злоумышленник может запрашивать личные пароли и идентификаторы для получения доступа к конфиденциальной информации.



ФИШИНГ (англ. phishing, от fishing — рыбная ловля, выуживание) — это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

Популярные фишинговые схемы

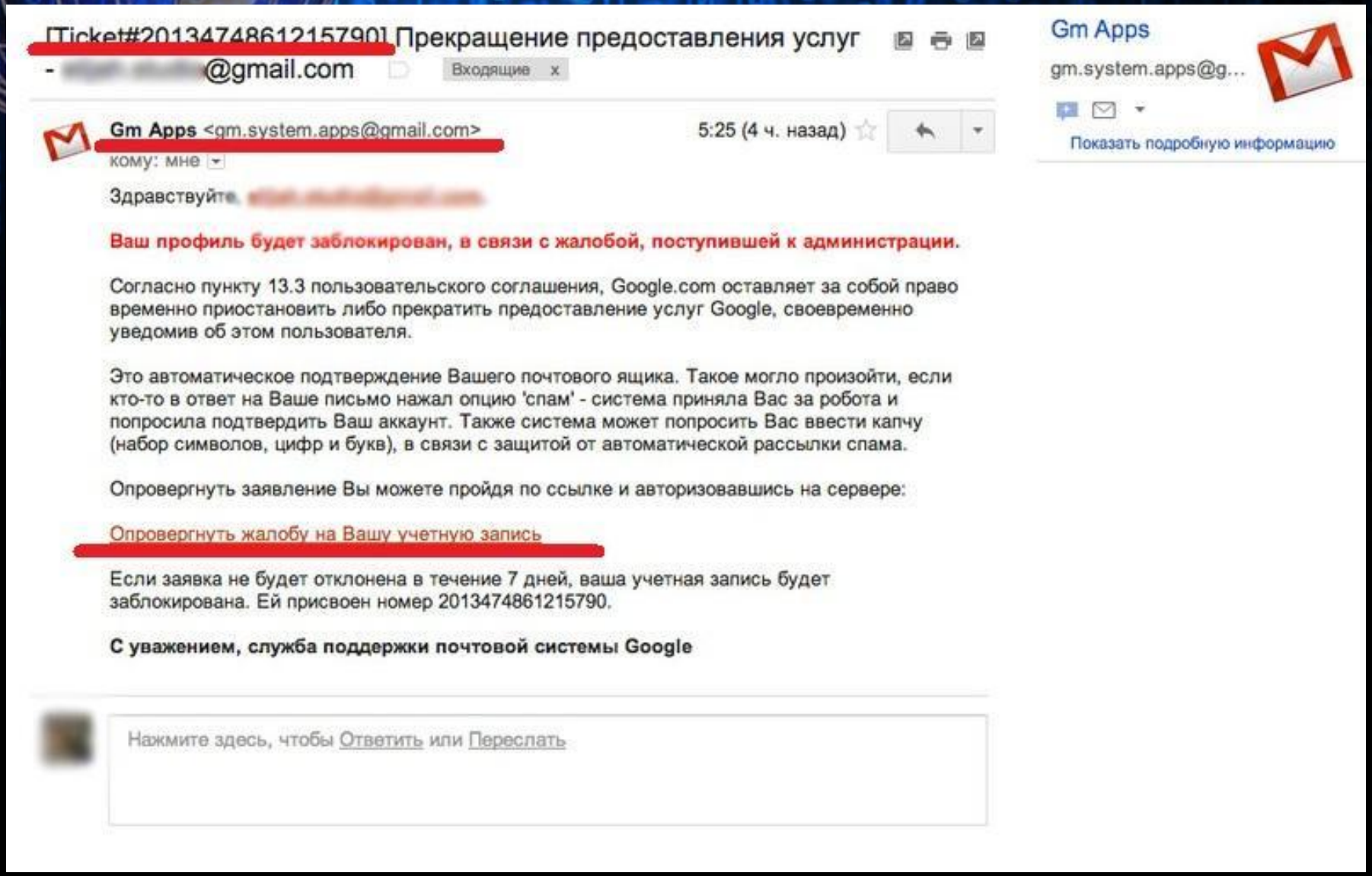
1) Несуществующие сотрудники
2) Мошенничество с использованием брендов известных корпораций
3) Поддельные лотереи
4) Ложные антивирусы и программы для обеспечения безопасности
5) IVR или телефонный фишинг
6) Телефонный фрикинг
7) Претекстинг
8) Квид про кво
9) «Дорожное яблоко»
10) Сбор информации из открытых источников
11) Плечевой серфинг

Несуществующие ссылки

Атака, которая заключается в отправлении письма с соблазнительной причиной посетить сайт и прямой ссылкой на него, которая лишь имеет сходство с ожидаемым сайтом, например, www.PayPai.com. Выглядит это, будто это ссылка на PayPal, мало кто заметит, что буква «l» заменена на «i». Таким образом, при переходе по ссылке жертва увидит сайт, максимально идентичный ожидаемому, и при вводе данных кредитной карты эта информация сразу направляется к злоумышленнику.

Подменное письмо

Письмо якобы от google с ссылкой на подменный сайт, с просьбой подтвердить данные аккаунта



[Ticket#2013474861215790] Прекращение предоставления услуг - [redacted]@gmail.com Входящие x

Gm Apps <gm.system.apps@gmail.com> 5:25 (4 ч. назад)

кому: мне

Здравствуйте, [redacted]

Ваш профиль будет заблокирован, в связи с жалобой, поступившей к администрации.

Согласно пункту 13.3 пользовательского соглашения, Google.com оставляет за собой право временно приостановить либо прекратить предоставление услуг Google, своевременно уведомив об этом пользователя.

Это автоматическое подтверждение Вашего почтового ящика. Такое могло произойти, если кто-то в ответ на Ваше письмо нажал опцию 'спам' - система приняла Вас за робота и попросила подтвердить Ваш аккаунт. Также система может попросить Вас ввести капчу (набор символов, цифр и букв), в связи с защитой от автоматической рассылки спама.

Опровергнуть заявление Вы можете пройдя по ссылке и авторизовавшись на сервере:

Опровергнуть жалобу на Вашу учетную запись

Если заявка не будет отклонена в течение 7 дней, ваша учетная запись будет заблокирована. Ей присвоен номер 2013474861215790.

С уважением, служба поддержки почтовой системы Google

Нажмите здесь, чтобы Ответить или Переслать

Gm Apps
gm.system.apps@g...
Показать подробную информацию

Подменное письмо

RU center

Уважаемый администратор домена!

Уведомляем Вас, что срок регистрации доменного имени [redacted] закончился. Вам необходимо оплатить услугу продления домена в течение одного рабочего дня с момента получения данного сообщения.

Оплатить

Если платеж не будет совершен в указанный срок, обслуживание доменного имени будет завершено. Домен будет удален из реестра и станет доступен для регистрации иным лицам.

Яндекс Деньги

Самое время напомнить о себе

Яндекс Деньги

Здравствуйте, [redacted].

В Яндекс.Деньгах меняются условия для неактивных пользователей — мы вводим абонентскую плату для счетов, которые не используются больше двух лет. Вы попадаете в число неактивных — со счетом *[redacted] очень давно ничего не происходит.

Размер абонентской платы — **270 руб.** в месяц, но не больше, чем есть на счете. Привязанных к счету карточек списания не коснутся.

Ваш баланс — **2 руб.** [redacted] **коп.** Можно пополнить его или потратить любую сумму на что-нибудь полезное. Не готовы сделать это прямо сейчас — отложите списание абонплаты. Забыли свой пароль — напишите службе поддержки.

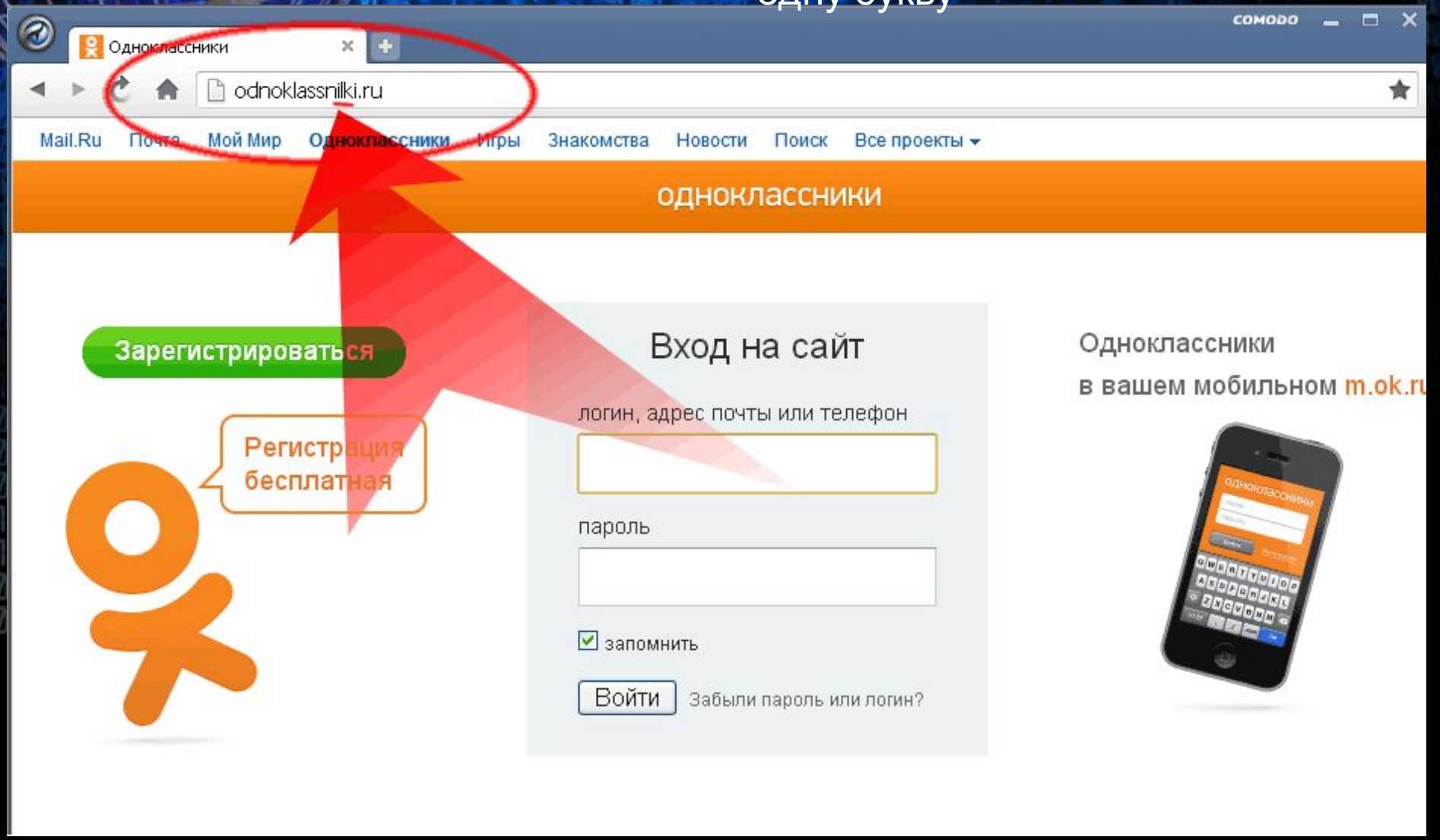
Если вы никак не откликнетесь, после 25 сентября мы спишем с вашего счета **2 руб.** [redacted] **коп.**

Мошенничество с использованием брендов известных корпораций

В таких фишинговых схемах используются поддельные сообщения электронной почты или веб-сайты, содержащие названия крупных или известных компаний. В сообщениях может быть поздравление с победой в каком-либо конкурсе, проводимом компанией,
о том, что срочно требуется изменить учётные данные или пароль. Подобные мошеннические схемы от лица службы технической поддержки также могут производиться по телефону.

Подменный сайт

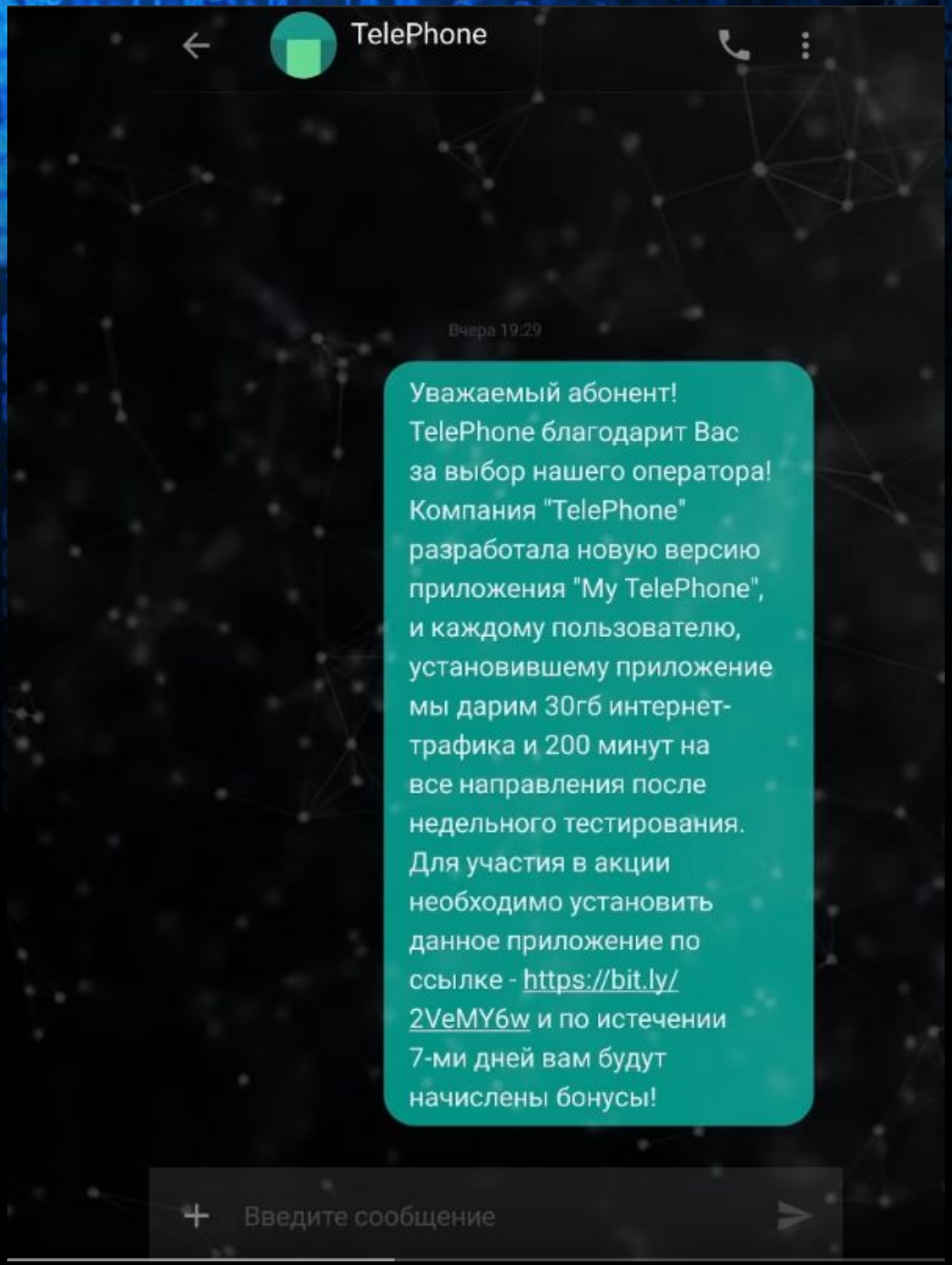
Сам подменный сайт адрес которого отличается, лишь на одну букву



Подложные лотереи

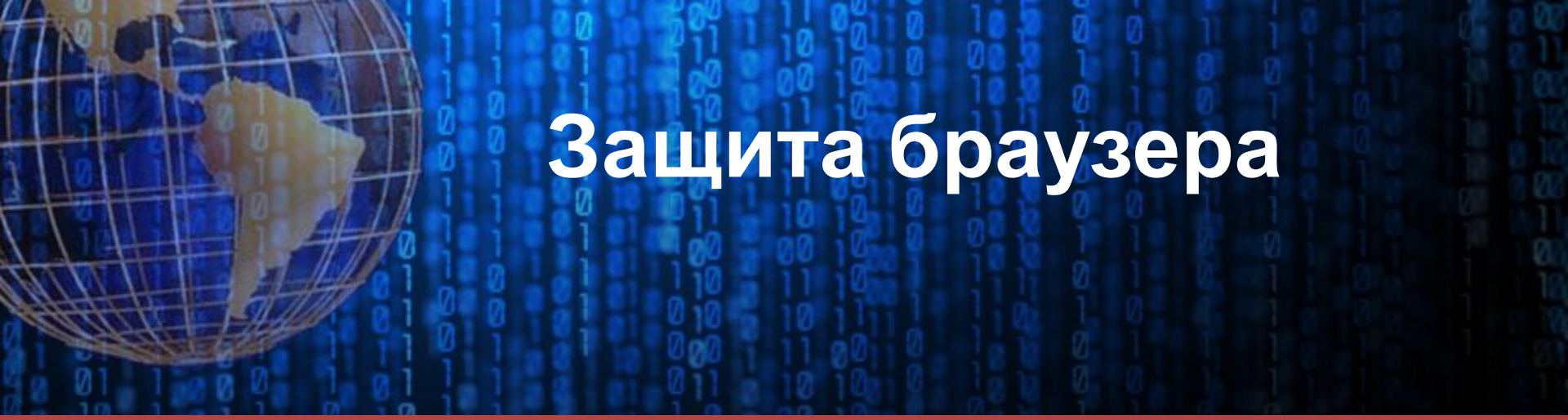
Пользователь может получить сообщения, в которых говорится о том, что он выиграл в лотерею, которая проводилась какой-либо известной компанией. Внешне эти сообщения могут выглядеть так, как будто они были отправлены от лица одного из высокопоставленных сотрудников корпорации

Смс с ссылкой



Ложные антивирусы и программы для обеспечения безопасности

Подобное мошенническое программное обеспечение, также известное под названием «scareware», — это программы, которые выглядят как антивирусы, хотя, на самом деле, все обстоит совсем наоборот. Такие программы генерируют ложные уведомления о различных угрозах, а также пытаются завлечь пользователя в мошеннические транзакции. Пользователь может столкнуться с ними в электронной почте, онлайн объявлениях, в социальных сетях, в результатах поисковых систем и даже во всплывающих окнах на компьютере, которые имитируют системные сообщения.



Защита браузера

Поддельный сайт!

Имеется информация о том, что веб-страница на www.royalquest.ru является поддельным сайтом. В соответствии с вашими настройками безопасности она была заблокирована.

Поддельные сайты разработаны, чтобы обманным путем заставить вас сделать что-либо опасное, например установить программу или раскрыть свою личную информацию, такую как пароли, телефонные номера или данные кредитных карт.

Ввод на этой веб-странице любой информации может привести к краже личности или мошенничеству.

Уходим отсюда!

Почему эта страница была заблокирована?

Игнорировать это предупреждение

IVR или телефонный фишинг

Телефонный фишинг — Вишинг (англ. vishing — voice fishing) назван так по аналогии с фишингом. Данная техника основана на использовании системы предварительно записанных голосовых сообщений с целью воссоздать «официальные звонки» банковских и других IVR систем. Обычно жертва получает запрос (чаще всего через фишинг электронной почты) связаться с банком и подтвердить или обновить какую-либо информацию. Система требует аутентификации пользователя посредством ввода PIN-кода или пароля. Поэтому, предварительно записав ключевую фразу, можно выведать всю нужную информацию.

Подменное письмо

[all] выставлен счет id73205

Сбербанк России Константинов <konstantinov.s@sberbank.ru>

Кому: all@rocit.ru

сегодня, 13:01 1 файл

Мы не можем проверить подлинность отправителя. Рекомендуем вам быть внимательнее при совершении действий, указанных в письме. Подробнее

Здравствуйте!

Вам выставлен счет. Просмотреть его можете во вложении или загрузить с нашего сайта по ссылке
http://online.sberbank.ru/ru/legal/docs/343-03-17/2814300de5728gf.html

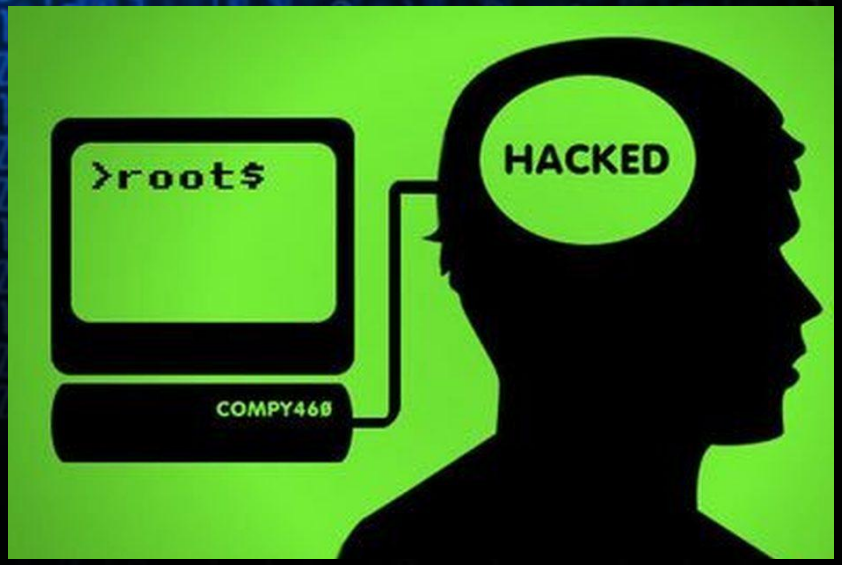
В случае возникновения вопросов Вы можете позвонить в отдел по работе с юридическими (физическими) лицами по телефонам, указанным на нашем сайте.

С уважением,
"Сбербанк России"
отдел по работе с клиентами
Константинов Павел Богданович
Тел.: 8 (800) 555-55-50 (звонки по России бесплатно)

✔ Все файлы проверены, вирусов нет

1 файл

Телефонный фрикинг



Телефонный фрикинг (англ. phreaking) — термин, описывающий эксперименты и взлом телефонных систем с помощью звуковых манипуляций с тоновым набором. Эта техника появилась в конце 50-х в Америке. Телефонная корпорация Bell, которая тогда покрывала практически всю территорию США, использовала тоновый набор для передачи различных служебных сигналов. Энтузиасты, попытавшиеся повторить некоторые из этих сигналов, получали возможность бесплатно звонить, организовывать телефонные конференции и администрировать телефонную сеть.

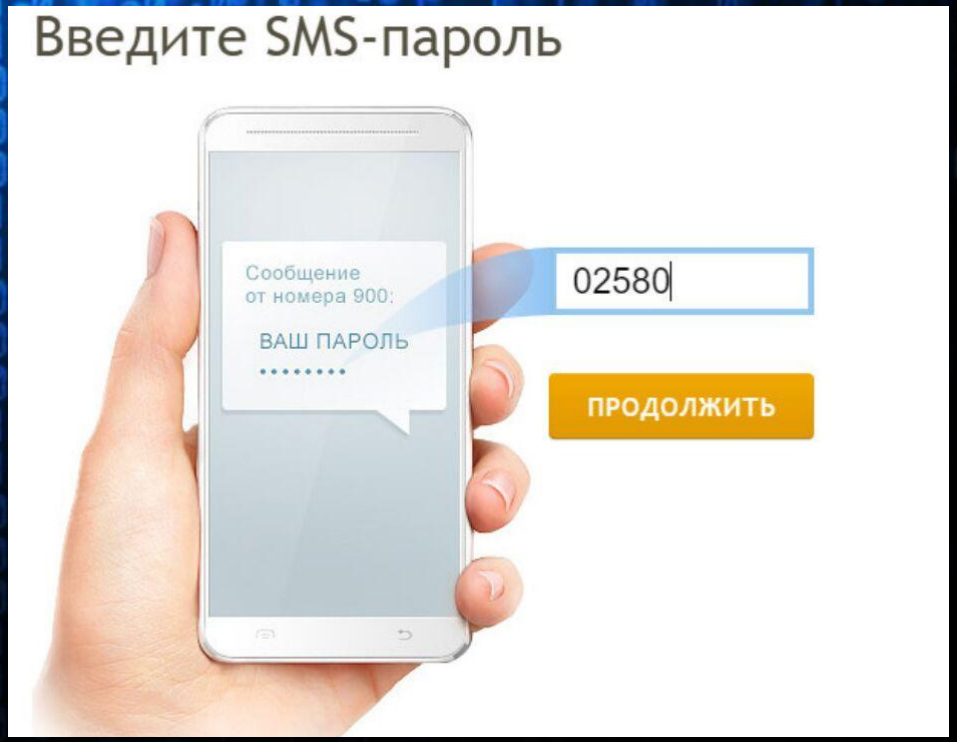
Претекстинг

Претекстинг (англ. pretexting) — атака, в которой злоумышленник представляется другим человеком и по заранее подготовленному сценарию выуживает конфиденциальную информацию.

Претекстинг – по сути это техника актерской игры, где всё происходит по сценарию. В результате жертва самая даёт нужную злоумышленнику информацию сам того не подозревая.

pretext

Допустим если злоумышленник играет роль сотрудника банка, он должен знать ФИО жертвы и примерно знать операции, которые он недавно совершал. И имея такой базовый набор, человек по ту сторону вполне может узнать пинкод карты, пароль из смс, реквизиты и многое другое, что даст ему

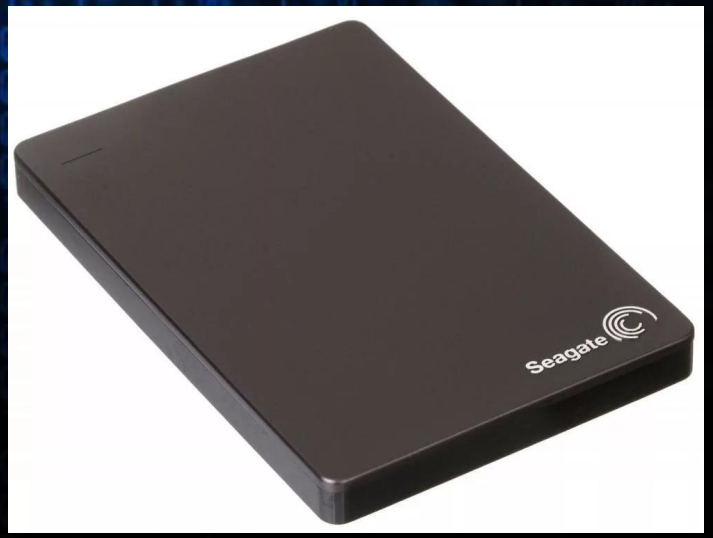


Так как этот метод очень неэффективен, то и защита от этой техники тоже проста, просто не сообщать важные данные операторам так, как настоящий оператор никогда не попросит информацию, которую нельзя разглашать

Квид про кво

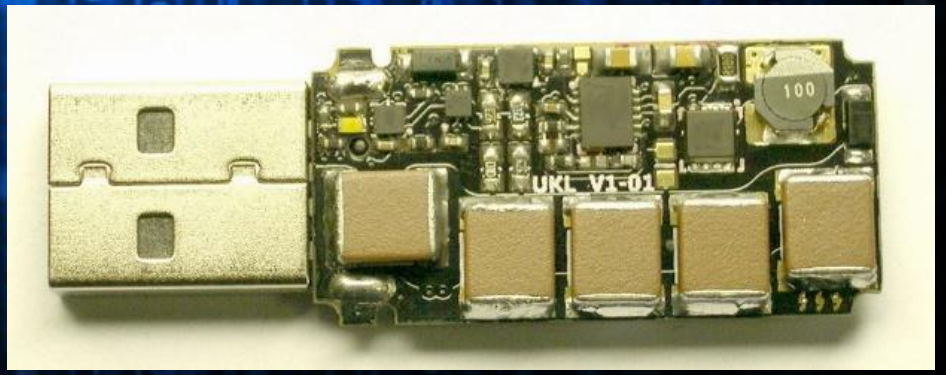
Квид про кво (от лат. *Quid pro quo* — «то за это») — в английском языке это выражение обычно используется в значении «услуга за услугу». Данный вид атаки подразумевает обращение злоумышленника в компанию по корпоративному телефону (используя актёрское мастерство) или электронной почте. Зачастую злоумышленник представляется сотрудником технической поддержки, который сообщает о возникновении технических проблем на рабочем месте сотрудника и предлагает помощь в их устранении. В процессе «решения» технических проблем злоумышленник вынуждает цель атаки совершать действия, позволяющие атакующему запускать команды или устанавливать различное программное обеспечение на компьютере жертвы.

«Дорожное яблоко»



Этот метод атаки представляет собой адаптацию троянского коня, и состоит в использовании физических носителей. Злоумышленник подбрасывает «инфицированные» носители информации в местах общего доступа, где эти носители могут быть легко найдены, такими как туалеты, парковки, столовые, или на рабочем месте атакуемого сотрудника

USB Killer – это на первый взгляд обычная флешка которая заставит вас плакать когда вы вставите ее в usb порт вашего персонального компьютера. После не громкого щелчка, который вы запомните на всю жизнь, вашему ПК понадобится в лучшем случае замена порта usb, а в худшем целых комплектующих.



BadUSB – метод атаки, включающий перепрошивку USB-устройства так, чтобы оно воспринималось компьютером как иное устройство. Например, USB-флешку компьютер будет видеть как клавиатуру или внешнюю сетевую карту, тем самым BadUSB сможет исполнять на компьютере заложенный в нее вредоносный код.

Сбор информации из открытых источников

Применение техник социальной инженерии требует не только знания психологии, но и умения собирать о человеке необходимую информацию. Относительно новым способом получения такой информации стал её сбор из открытых источников, главным образом из социальных сетей. К примеру, такие сайты как livejournal, «Одноклассники», «ВКонтакте», содержат огромное количество данных, которые люди и не пытаются скрыть. Как правило, пользователи не уделяют должного внимания вопросам безопасности, оставляя в свободном доступе данные и сведения, которые могут быть использованы злоумышленником.

Плечевой серфинг

(англ. *shoulder surfing*) включает в себя наблюдение личной информации жертвы через её плечо. Этот тип атаки распространён в общественных местах, таких как кафе, торговые центры, аэропорты, вокзалы, а также в общественном транспорте.

Как определить атаку социального инженера

Ниже перечислены методы действий социальных инженеров:

представление себя другом-сотрудником либо новым сотрудником с просьбой о помощи;
представление себя сотрудником поставщика, партнерской компании, представителем закона;
представление себя кем-либо из руководства;
представление себя поставщиком или производителем операционных систем, звонящим, чтобы предложить обновление или патч жертве для установки;
предложение помощи в случае возникновения проблемы и последующее провоцирование возникновения проблемы, которое принуждает жертву попросить о помощи;
использование внутреннего сленга и терминологии для возникновения доверия;
отправка вируса или троянского коня в качестве приложения к письму;
использование фальшивого pop-up окна, с просьбой аутентифицироваться еще раз, или ввести пароль;
предложение приза за регистрацию на сайте с именем пользователя и паролем;
записывание клавиш, которые жертва вводит на своём компьютере или в своей программе (кейлоггинг);
подбрасывание различных носителей данных (флэш-карт, дисков и т. д.) с вредоносным ПО на стол жертвы;
подброс документа или папки в почтовый отдел компании для внутренней доставки;
видоизменение надписи на факсе, чтобы казалось, что он пришел из компании;
просьба секретаря принять, а затем отослать факс;
просьба отослать документ в место, которое кажется локальным (то есть находится на территории организации);
подстройка голосовой почты, чтобы работники, решившие перезвонить, подумали, что атакующий — их сотрудник;

ЗАДАНИЕ 1

На приведите примеры социальной инженерии, которые случались в вашей жизни, с вашими знакомыми, родственниками (не менее 5).

Определите к какой из фишинговых схем они относятся.

ЗАДАНИЕ 2

Составьте список мероприятий по противодействию методов социальной инженерии (не менее 10).

ЗАДАНИЕ 3

Пройдите тест
по информационной
безопасности:

https://kgnic.ru/news/2020/test-na-znanie-osnov-po-informatsionnoj-bezopasnosti/