Анлим

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

«Кибергигиена для всех»

Тюмень, 2020 год

СОДЕРЖАНИЕ

1. Определения

Аутентификация - процедура проверки подлинности, например, проверка подлинности пользователя путём сравнения введённого им пароля (для указанного логина) с паролем, сохранённым в базе данных пользовательских логинов.

Двухфакторная аутентификация — это метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов (например, пароль и код из СМС), что обеспечивает двухслойную, более эффективную защиту аккаунта от несанкционированного проникновения.

Социальная инженерия – метод получения необходимого доступа к информации, основанный на особенностях психологии людей. Основной целью социальной инженерии является получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам.

Фишинг — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации. Фишинг представляет собой пришедшие на почту поддельные уведомления от банков, провайдеров, платежных систем, партнеров, технической поддержки и других организаций о том, что по какой-либо причине получателю срочно нужно передать / обновить личные данные. Причины могут называться различные. Это может быть утеря данных, поломка в системе и др. Целью злоумышленника является получение защищаемой информации организации, учетных данных пользователя.

Fakenews (фейк-ньюс, фальшивые, поддельные, «фейковые», ложные новости) - это информационная мистификация или намеренное распространение дезинформации в социальных медиа и традиционных СМИ с целью введения в заблуждение, для того чтобы получить финансовую или политическую выгоду, для создания паники, продвижения своих интересов, побуждения к противоправным и опасным действиям.

Deepfake (deepface, дипфейк, дипфейс) — объединение слов «глубинное обучение» (англ. Deep learning) и подделка (англ. Fake), методика синтеза изображения, видео, голоса. Основана на искусственном интеллекте. Эта методика используется для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики. Может использоваться в корыстных целях для подделки видео, голоса и изображений.

2. Общие положения

Данный документ представляет собой методические рекомендации, необходимые для повышения осведомленности пользователей и сотрудников, перешедших на дистанционную работу, о кибергигиене.

В настоящем документе описываются актуальные угрозы и мошеннические схемы, которые могут затронуть любого человека. Также в данных методических рекомендациях рассмотрены методы защиты информации, которые позволят людям уберечь свои личные данные и средства от злоумышленников.

В настоящих методических рекомендациях имеются QR-коды (штрихкоды), которые представляют собой ссылки на статьи, содержащие более развёрнутую информацию о крупных инцидентах, возможных уязвимостях, видах мошенничества, а также дополнительную информацию в рамках тем, затрагиваемых в данном документе.

Для чтения QR-кода и последующего перехода к статье необходим мобильный телефон с тыловой или фронтальной камерой, и приложение, которое превратит камеру в сканер. Необходимо зайти в программу, навести камеру на QR-код. Результат – ссылка на нужную статью. Если Вы используете устройство с операционной системой Android, приложения для сканирования штрихкодов можно найти в официальном магазине - Google Play. В устройствах компании Apple данный функционал встроен в возможности камеры. Чтобы сканировать QR-код, необходимо выполнить следующие действия:

1. **выберите основную камеру;**
2. **удерживайте устройство так, чтобы QR-код находился в видоискателе программы «Камера»;**
3. **устройство распознает QR-код, о чем появится соответствующее уведомление;**
4. **коснитесь уведомления, чтобы открыть связанную с QR-кодом ссылку.**

Пример для тренировки

3. Злоумышленники и COVID-19

Злоумышленники не сидят на месте, и быстро адаптируются к изменяющемуся миру, и используют в своих целях актуальные проблемы. Исключением не стала и тема пандемии COVID-19.

По мере распространения коронавируса растет и число мошенников, активно эксплуатирующих всеобщий ажиотаж вокруг данной проблемы. Киберпреступники стали активно эксплуатировать тему COVID-19 для рассылки почтового спама, фишинговых писем и вредоносных программ с целью обмануть пользователей, заразить вредоносным ПО, или украсть их персональную информацию.

Какие «легенды» эксплуатируют злоумышленники:

- **прибегают к социальной инженерии, обзванивают потенциальных жертв и обещают им отсрочки по выплате кредитов, различные компенсации, пособия, возврат средств за авиационные билеты, услуги по диагностике заражения коронавирусной инфекцией, а также предлагают волонтерство;**
- **рассылают жертвам угрозы заразить их и членов их семей коронавирусом, если они откажутся заплатить выкуп;**
- **предлагают внести пожертвование на разработку вакцины;**
- **предлагают жертвам получить социальные выплаты и материальную помощь и под предлогом этого собирают данные их банковских карт и персональную информацию;**
- **создают поддельные сайты якобы по оказанию экстренной помощи предприятиям в условиях пандемии коронавирусной инфекции и похищают их персональные данные;**
- **звонят жертве и сообщают, будто она контактировала с зараженным COVID-19, поэтому сейчас приедут специалисты для проведения анализа. Однако анализ не бесплатный, поэтому необходимо перевести деньги. Затем злоумышленники могут сообщить, будто результаты анализов оказались положительными, и предложить дорогостоящее лечение. Получив деньги, мошенники скрываются;**
- **создают поддельные интернет-магазины по продаже экспресс-тестов и новейших лекарств от коронавируса, масок, антисептиков, перчаток, респираторов и др.;**

Статья про основные методы злоумышленников тему пандемии COVID-19

- **рассылают СМС, где говорится, что гражданин якобы нарушил карантинный режим. Мошенники ссылаются на действующую статью КоАП РФ, и требуют оплатить штраф, отправив 4000 рублей на указанный номер. В случае неуплаты грозят возбуждением уголовного дела;**
- **рассылают гражданам письма со ссылками на мошеннические сайты или вредоносными вложениями с целью выманить у них данные банковских карт от лица известных организаций, таких как Роспотребнадзор, Министерство здравоохранения, Всемирная Организация Здравоохранения (ВОЗ) и др.;**
- **распространяют вымогательское ПО под видом расширений для браузеров, мобильных и компьютерных приложений для отслеживания вспышек заражения коронавирусом (рисунок 1).**

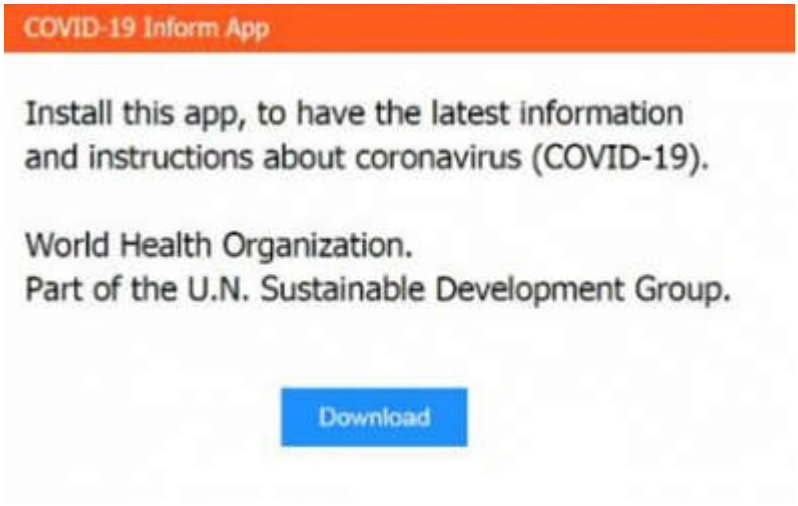

Рисунок 1. Пример фальшивого письма от лица ВОЗ

Вывод: у мошенников существует много разных легенд. Нужно сохранять самообладание при любой ситуации. Дать себе время на обдумывание и реакцию. Подходить к любой информации с подозрением, проверять ее.

Важно помнить: если Вы не среагируете экстренно на ситуацию, если Вы положите трубку, дадите себе время на обдумывание – ничего страшного не случится.

4. Угрозы безопасности и методы защиты

4.1. Вирусы

Вирусные и троянские программы долгое время были самым распространенным способом украсть или уничтожить информацию, снять деньги со счета. С переходом пользователей на дистанционную работу возросло число уязвимостей и угроз, которым подвергаются компании и рядовые пользователи, соответственно, возросло число атак.

Вредоносное ПО похищает персональные данные пользователей, в том числе логины, пароли, номера кредитных карт, хранящиеся в браузерах. Похищенную информацию злоумышленники затем используют в незаконных операциях (например, для похищения денежных средств с банковских счетов) или продают ее на подпольных торговых площадках.

Особую опасность представляют вирусы-шифровальщики. Данное вредоносное программное обеспечение делает недоступными Ваши личные и корпоративные файлы, которые хранятся на зараженном устройстве. Вернуть доступ к данной информации можно только при помощи специального ключа (пароля), который злоумышленники предлагаю в обмен на выкуп. Не следует платить злоумышленникам, т.к. никто не гарантирует Вам возврат файлов в прежнее состояние (рисунок 2).

Рисунок 2. Пример вируса-шифровальщика

Как защититься:

- **используйте лицензионные антивирусные решения, скаченные с официальных сайтов известных антивирусных компаний;**

- **не переходите по подозрительным ссылкам (на неизвестные сайты, навязчивую рекламу, сообщения о гарантированных выигрышах и пр.);**
- **не устанавливайте сомнительные программы на устройства (как на корпоративные, так и на личные);**
- **используйте только лицензионное программное обеспечение (не рекомендуется скачивать взломанные версии программ, так как они могут содержать вредоносные вложения);**
- **используйте средства антивирусной защиты на всех устройствах (домашнем, рабочем компьютере, планшете, телефоне);**
- **своевременно обновляйте используемое программное и системное обеспечение по мере выхода обновлений;**
- **наиболее важные файлы храните не только на жестком диске компьютера, но и на съемных носителях, внешних жестких дисках или в облачном хранилище;**
- **для повседневной работы за компьютером используйте учетную запись без прав администратора (тем самым, в случае заражения компьютера или получения доступа злоумышленником к нему, снижается вероятность нанесения значительного ущерба);**
- **не переходите по ссылкам из всплывающих окон, даже если рекламируемые компания или продукт вам знакомы (проверяйте информацию о акциях на официальных сайтах сервисов);**
- **будьте внимательны, устанавливая приложения/расширения: смотрите на разрешения, которые запрашивает ПО (рисунок 3), смотрите на отзывы и количества скачиваний (порой злоумышленники маскируют приложения под известные).**

Рисунок 3. Зловредное предложение запрашивает избыточные права

Вывод: будьте осторожны, не используйте взломанные версии приложений, пользуйтесь только лицензионными продуктами, скачивайте программное обеспечение с официальных сайтов. Не пренебрегайте средствами защиты. Обязательно используйте антивирус.

4.2. СМС и звонки

4.2.1. СМС

Самым распространенным видом мошенничества являются фальшивые сообщения злоумышленников от лица банков, партнеров, обслуживающих организаций, родственников.

Например, Вы получаете сообщение с просьбой перезвонить в «службу безопасности банка» из-за «подозрительной активности» или «попытки хищения» денег, либо с просьбой предоставить срочно информацию по работе.

Статья про виды банковского мошенничества

В первом случае жертве сообщают, что в банковском личном кабинете были зафиксированы подозрительные действия. Например, перевод в другой город внушительной суммы, или блокировка карты из-за подозрительной активности (рисунок 4). Поэтому необходимо произвести определенные процедуры для

того, чтобы обезопасить счёт. Для этого необходимо позвонить на указанный в СМС номер.

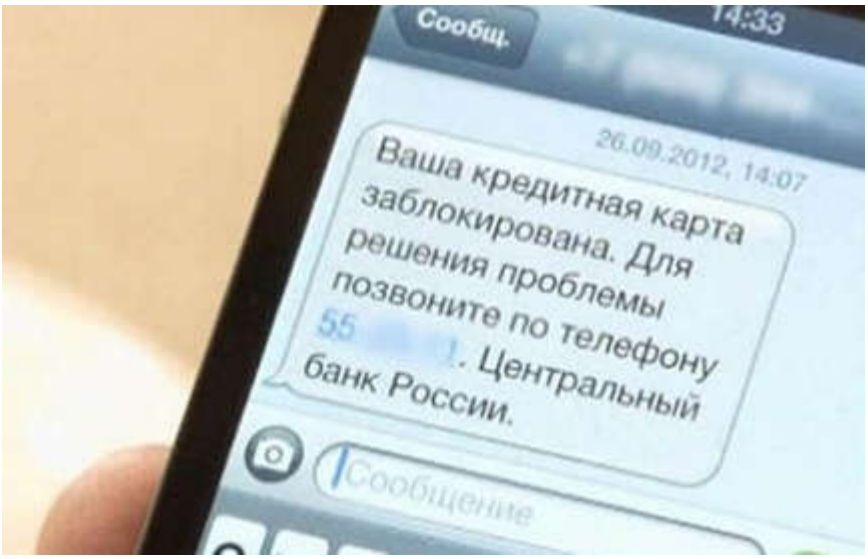

Рисунок 4. Пример мошеннического СМС

Во втором случае злоумышленники могут представиться сотрудниками компании-клиента, технической службой, занимающейся обслуживанием, специалистами либо партнерами. Мошенники попытаются выведать конфиденциальную информацию, связанную с компанией, в которой работает жертва (корпоративную и служебную тайну, персональные данные, аутентификационные данные для дистанционной работы).

В СМС может быть указан номер, похожий на телефон банка, либо компаний, связанных с местом работы жертвы мошенников. Кого-то смутит несоответствие номеров даже на пару цифр, а кто-то думает, что, например, у службы безопасности вполне может быть собственный номер. И с полной уверенностью сам звонит злоумышленникам.

Мошенники, отвечающие на звонки по указанному в рассылке телефону, узнают у доверчивых граждан всё, что необходимо для совершения атаки, кражи, и любых других противоправных действия. Масштабы этой деятельности огромны — в основном из-за недостаточной осведомлённости потенциальных жертв.

Статья про СМС-мошенничестве на тему COVID-19

Помимо выше указанного не стоит забывать и об обычном мошенничестве с переводом денег. Такие СМС обычно содержат просьбы о финансовой помощи якобы

от родственника ввиду тяжелой жизненной ситуации, либо спекуляции на тему каких-либо нарушений законодательства РФ (рисунок 5).

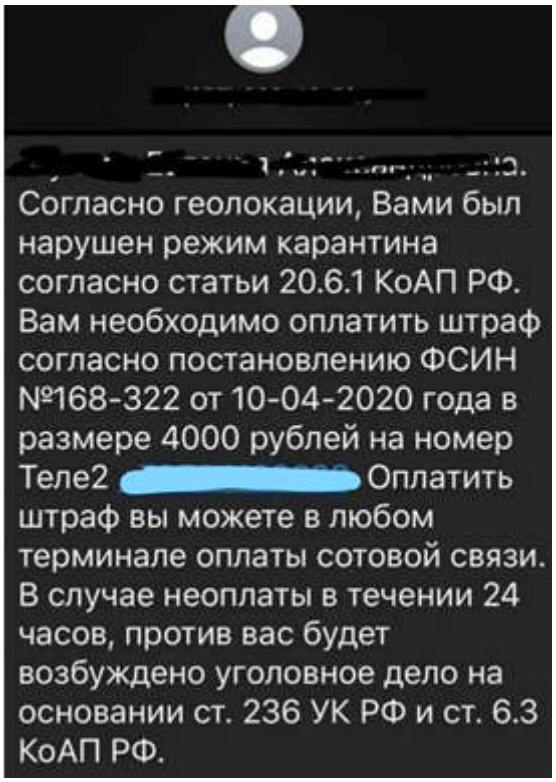

Рисунок 5. Пример мошеннического СМС на тему COVID-19

Как вычислить мошенников: **во-первых, обратите внимание на номер, с которого прислали СМС, — он должен совпадать с официальным номером Вашего банка, партнеров. Во-вторых, обратите внимание на телефон, по которому Вас просят перезвонить — требование к нему то же самое. Если Вы все-таки перезвонили по телефону, то помните главное правило: никаких личных данных не нужно сообщать. Опасайтесь подозрительных СМС, а также сообщений в мессенджерах.**

4.2.2. Звонки с номера, похожего на банковский, либо с незнакомого номера

Наравне с СМС-мошенничеством распространены схемы со звонками. Подход такой же, как и в случае с сообщениями на телефон. Далее будут рассмотрены ситуации, с которыми может столкнуться каждый.

Ситуация №1: Вам звонят, представляются работниками банка, либо другой организации и просят предоставить конфиденциальную информацию. А дальше просят по телефону назвать секретные данные: пароли, логины, электронную почту, ФИО, адрес проживания.

Ситуация №2: Сначала Вам звонят с неизвестного номера, отличного от официальных номеров, пытаются выведать данные, но вы понимаете, что это мошенники, и кладете трубку. После этого они тут же перезванивают с подменного номера, у Вас высвечивается телефон, например, официальной горячей линии банка, говорят, что это служба безопасности Вашей кредитной организации, что вас только что пытались взломать мошенники, и под предлогом обезопасить счет все равно выведывают данные.

Метод называется социальной инженерией: к каждому звонку преступники тщательно готовятся, так что их действия могут быть почти неотличимы от работы реального сотрудника банка: они могут знать ваше имя и отчество, паспортные данные, адрес проживания, ФИО родственников, даже срок действия карты и ее номер. Эти данные злоумышленники получают из утекших в интернет баз данных различных компаний (в том числе банков), открытых источников (Ваши социальные сети), с помощью предварительных звонков от лица обслуживающих компаний (мошенники звонят от лица интернет провайдеров, сервисных компаний, которые, например, занимаются окнами, сотовых операторов). Существует множество источников, из которых мошенники получают всю необходимую информацию.

Как вычислить мошенников: **Вам позвонят рано утром, или под вечер, или даже на выходных — словом, тогда, когда вы будете готовы к этому меньше всего. Обращайте внимание на необычное поведение собеседников: мошенники будут требовать принять решение немедленно — это должно вас насторожить. И наконец, главное правило: настоящий сотрудник банка не будет у вас спрашивать данные карты — на кого оформлена, CVV-код с обратной стороны, одноразовый пароль. Он уже знает, как вас зовут, и ваши коды-пароли ему не нужны. Компаниям-партнерам тем более не должны узнавать у Вас конфиденциальную информацию.**

Вывод: не стоит поддаваться панике, не принимайте поспешных решений. Успокойтесь, и обдумайте всё. Позвоните по официальному номеру банка, компании, личному номеру родственника, и уточните информацию. Если Вам звонят от лица какой-либо компании, уточните ФИО и должность звонящего. Позвоните в компанию, проверьте информацию. Не сообщайте кодовые слова, ПИН, защитные коды, пароли из СМС, данные банковских карт, и персональные данные.

4.3. Фишинг

Злоумышленники используют ещё один не новый, но распространенный и эффективный метод мошенничества, который называется фишинг.

Мошенниками применяется ряд методов, которые позволяют получить ценную информацию. Однако одна тактика фишинга является наиболее распространенной: жертва получает электронное письмо или текстовое сообщение, отправитель которого представляется определенным лицом или организацией, которым пользователь доверяет. Например, злоумышленник в сообщении представляется сотрудником банка или за представителем государственного учреждения (налоговая, администрация и пр.).

Когда ничего не подозревающий получатель открывает это электронное письмо или сообщение, то он обнаруживает пугающий, либо заманчивый текст, где требуется перейти на веб-сайт, либо установить вредоносное приложение, и немедленно выполнить определенные действия, чтобы избежать опасности или каких-либо серьезных последствий, либо чтобы получить какой-нибудь выигрыш, воспользоваться какой-то полезной услугой.

Если пользователь «клюет на наживку» и переходит по ссылке, то он попадает на веб-сайт, имитирующий тот или иной законный интернет-ресурс. На этом веб-сайте пользователя просят «войти в систему» (личный кабинет в банке, социальные сети, интернет-магазин и др.), используя имя своей учетной записи (логин, адрес электронной почты) и пароль, либо просят предоставить данные банковской карты (рисунки 6-7). Если жертва оказывается достаточно доверчивой и соглашается, то введенные данные попадают напрямую к злоумышленникам, которые затем используют их для кражи конфиденциальной информации или денежных средств с банковских счетов. Кроме того, они могут продавать полученные личные данные на черном рынке.

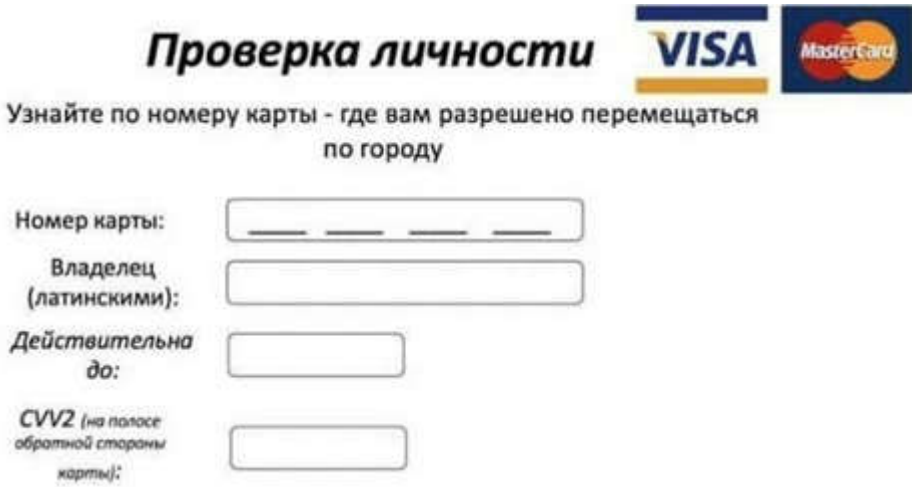

Рисунок 6. Фишинговая страница, где запрашиваются данные банковской карты

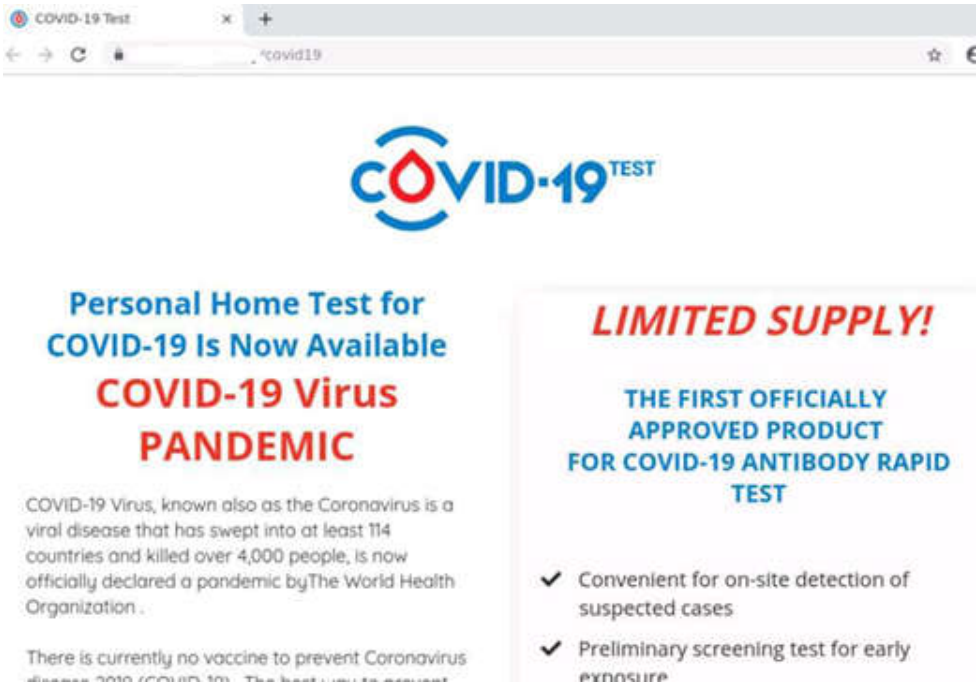

Рисунок 7. Фишинговая страница о продаже услуги экспресс-тестов на выявление COVID-19

Как распознать фишинговое письмо, и как защититься:

- **Подвергайте все сомнению. Адрес отправителя можно подделать. Знакомая компания? Реально ли она существует? Соответствует ли подпись реальности: телефоны, физический адрес, форма собственности и т.д. Ни в коем случае не связывайтесь по контактным данным, указанным в письме. Позвоните в компанию, от которой получили письмо, по публичным телефонам с официального сайта, и уточните, действительно ли Вам писали.**
- **Проверяйте текст, если письмо на иностранном языке. Фишинг – интернациональное явление, но далеко не всем мошенникам доступны услуги профессиональных переводчиков, поэтому в тексте письма могут встречать серьёзные ошибки.**
- **Не переходите по подозрительным ссылкам. Скорее всего, это атака. Наведите курсор на ссылку, чтобы увидеть реальный адрес, куда она ведет. Бывает, что местами переставлены всего две буквы в адресе и это не сразу заметно для человеческого глаза.**
- **Не открывайте сомнительные вложения. Для проверки вложений есть бесплатные сервисы, например, virustotal.com. Он проанализирует вложенный файл сразу через несколько десятков антивирусов. Лучше не скачивать подобные файлы, а отправлять подозрительные письма ИТ-специалистам с соответствующими замечаниями.**

- **Не пренебрегайте антивирусной защитой. Многие популярные антивирусы проверяют не только ваш ПК, но и почту – не отключайте эту опцию и внимательно относитесь к предупреждениям антивируса.**
- **Не покупайте ничего на неизвестных сайтах, не вводите там учётные данные для входа в различные системы (будь то социальные сети, либо сайты, связанные с работой) и банковские данные. Если же сайт вам знаком — проверьте его адрес и убедитесь, что там нет лишних букв и цифр.**
- **Будьте предельно внимательны при вводе учетных данных на сайтах и во время работы с онлайн-платежами.**
- **С осторожностью относитесь к сайтам с некорректными сертификатами и учитывайте, что введенные на них данные могут быть перехвачены злоумышленниками (рисунок 8).**

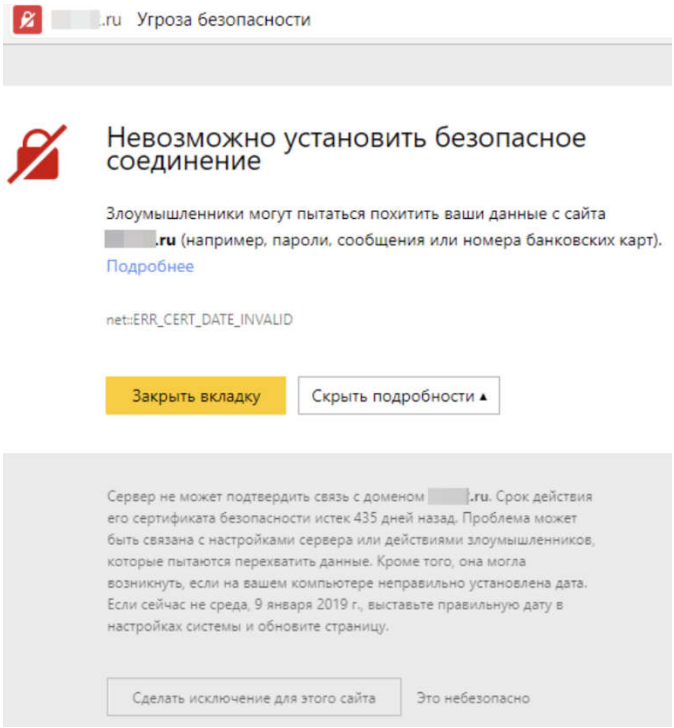

Рисунок 8. Сайт с некорректным сертификатом

Вывод: не переходите по ссылкам в письмах, СМС, сообщениях в мессенджерах. Проверяйте адрес сайта, на который Вы перешли. Не вводите конфиденциальную информацию на сайте, если сомневаетесь в его надежности

4.4. Удаленный доступ и пароли

Важным аспектом защиты являются стойкие, сложные пароли для доступа к различным сервисам. Рекомендации:

- **используйте сложные пароли, состоящие из незначащих комбинаций букв, цифр и знаков, длиной не менее 8 символов;**
- **для создания и хранения паролей можно воспользоваться менеджером паролей (защищенным хранилищем с функциями генерации новых паролей). Помните, что злоумышленники об этом знают, и создают и распространяют поддельные менеджеры паролей;**
- **используйте двухфакторную аутентификацию там, где это возможно. Это Ваш второй уровень защиты. Первый фактор — это пароль, второй — устройство. Не используйте СМС в качестве второго фактора. Перехват СМС — хорошо известный и популярный способ взлома;**
- **не используйте один и тот же пароль для разных систем (для сайтов, электронной почты и др.). Данная ошибка приводит к тому, что сворованный пароль с одного вредоносного, или слабозащищенного сайта позволит злоумышленнику получить доступ ко всем остальным вашим ресурсам (почте, социальным сетям, компьютеру);**
- **меняйте все пароли хотя бы раз в полгода, а лучше — каждые два-три месяца.**

Надёжный пароль – залог безопасности сервисов, которыми Вы пользуетесь.

Защиту от компрометации учетной записи, даже если мошенником был получен Ваш пароль, гарантирует двухфакторная аутентификация. Без специального сгенерированного кода, атакующий не сможет получить доступ к Вашим сервисам, если даже он знает логин и пароль.

Статьи про возросшее количество доступных удаленных рабочих столов и серверов

Используя для работы интернет-подключения, будьте осторожны: не подключайтесь к неизвестным, открытым точкам доступа. Используйте только те выходы в сеть, которые принадлежат Вам. Настройте доступ к WiFi-сети по паролю. Не стоит забывать и о доступе к настройкам Вашего оборудования: не забудьте изменить логин и пароль по умолчанию (чаще всего это: логин - admin, пароль - admin) на Wi-Fi-устройстве, и включите шифрование. Если Вы не знаете, как это сделать, то обратитесь к доверенному IT-специалисту.

Зачастую сотрудники различных компаний используют сторонние сервисы для дистанционного доступа к своим рабочим компьютерам. Необходимо узнать у руководства Вашей компании, разрешен ли данный вид доступа. Помимо этого, не

устанавливайте нелицензионное программное обеспечение для удаленного доступа к рабочему столу, т.к. злоумышленники могут воспользоваться этим, и попасть в корпоративную сеть.

Необходимо следовать следующим правилам:

1. **При любой возникшей нештатной ситуации обращайтесь к IT-специалисту, подробно объяснив, что и как произошло. Данный сотрудник поможет Вам решить проблему.**
2. **Объясните близким людям, проживающим с Вами, что нельзя пользоваться компьютером – это позволит избежать случайного заражения устройства или потери данных.**
3. **Не передавайте защищаемую информацию, а также учетные данные для дистанционного доступа третьим лицам.**
4. **Не публикуйте в социальных сетях фотографии с Вашим рабочим местом, фотографии рабочего стола и документов: велика вероятность того, что злоумышленник может обнаружить на фотографиях конфиденциальную информации (в том числе логины и пароли для удаленного доступа).**

4.5. Deepfake

Фейковые видео, голоса, изображения становятся все убедительнее и появляются всё чаще (рисунок 9).

Рисунок 9. Пример Deepfake: лицо актера Билла Хейдера заменили на лица других знаменитых актеров

Алгоритм Deepfake обучается на фотографиях настоящих людей. В результате создается сеть, способная генерировать неограниченное количество поддельных, но очень убедительно выглядящих изображений того или иного человека. Остается лишь

склеить эти отдельные кадры в видео — и дипфейк готов. Аналогичные методы позволяют создавать фейковое аудио.

Один из ярких примеров из 2018 года — поддельное видео с Бараком Обамой, в котором он рассказал, собственно, о дипфейках, и заодно бросил пару оскорблений в адрес действующего президента США.

Наглядным примером подделки голоса является статья Wall Streat Journal со ссылкой на страховую фирму Euler Hermes Group SA, в которой описывается следующий инцидент, произошедший в 2019 году:

1. Руководителю британской энергетической компании позвонил его непосредственный начальник из немецкого головного офиса. Он попросил в течение часа перевести 220 000 евро на счет вымышленного венгерского поставщика.

Статья про имитацию голоса

2. Британец перевел требуемую сумму.

3. Злоумышленники позвонили еще раз и сообщили, что головная компания переводит средства для возмещения этих расходов.

4. Позже в тот же день поступил новый звонок от «директора», который попросил провести еще один платеж.

5. Поскольку средства из головного офиса так и не поступили, а звонили мошенники с австрийского номера, а не с немецкого, руководитель британского отделения заподозрил неладное и не стал переводить деньги.

Вывод:

- **не распространяйте в большом количестве личную информацию и фотографии;**
- **закройте доступ к своим страницам в социальных сетях людям, не входящим в Ваш круг знакомств;**
- **не используйте определение по голосу в банках и других сервисах, не используйте биометрию для разблокировки устройств;**
- **относитесь скептически к различным видеозаписям, изображениям и аудиозаписям, публикуемым в сети Интернет. Обращайте внимание на возможные «артефакты»: искажения на видео и изображениях, неестественность движений. Скорее всего, Вас пытаются ввести в заблуждение.**

4.6. Fakenews

Несмотря на то, что посты в социальных сетях нередко вводят нас в заблуждение, они становятся одним из главных источников информации в современном мире, и даже фейковые новости быстро набирают тысячи просмотров. Такой феномен называется Fakenews (Фейк-ньюс). Помимо социальных сетей, фейковые новости активно распространяются в мессенджерах (рисунок 10).

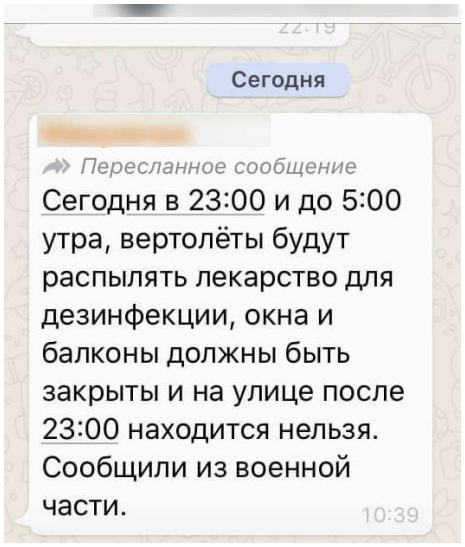

Рисунок 10. Пример распространяемого фейка в мессенджере WhatsApp

Некоторые фейк-ньюс могут быть по-настоящему опасными. Например, советы, касающиеся здоровья.

Данный метод используется с целью введения в заблуждение, для того чтобы получить финансовую или политическую выгоду, для создания паники, продвижения собственных интересов, побуждения к противоправным или опасным действиям.

Подробные статьи о распространенных фейковых новостях на тему пандемии Covid-19

В эпоху пандемии COVID-19 в сети начали появляться fakenews о коронавирусе. Вот самые яркие из них:

1. ***На самом деле, заболевших в России сотни тысяч, и власти скрывают это;***
2. ***Коронавирус передается при помощи комариных укусов;***
3. ***Частицы коронавируса могут долго сохраняется в воздухе;***
4. ***В некоторых странах придумали вакцину и лекарство от коронавируса;***
5. ***Алкоголь, табак и климат;***

6. Воздействие новых технологий;

7. Конспирологические теории о создании коронавируса (придумала определенная страна).

Стоит напомнить о том, что за распространение фейковых новостей следует уголовная ответственность: 31 марта 2020 года были ужесточены наказания за публичное распространение ложной информации. Был принят закон, предусматривающий наказание за распространение недостоверных новостей о чрезвычайных ситуациях, в том числе о распространении коронавируса COVID-19. За такие нарушения будет грозить наказание от штрафа 300 тыс. руб. до пяти лет лишения свободы.

Вывод: с развитием интернета отличить, где правда, а где ложь, становится все сложнее. Для этого необходимо следовать следующим правилам, которые помогут распознать fakenews, и не понести ответственность за их распространение:

- **первое, что Вы можете сделать для борьбы с дезинформацией - остановиться и подумать: прежде чем пересылать сообщение, подумайте, какова вероятность того, что это фейк, и, если у вас возникают сомнения, не пересылайте информацию;**
- **перед тем, как переслать сообщение, задайте себе простой вопрос: откуда идет эта информация? недостоверная информация часто происходит от "подруги моего друга" или "соседа коллеги по работе". Это почти всегда значит, что информация - выдумка. Нужно обращать внимание только на официальные заявления уполномоченных органов (организаций);**
- **в соцсетях за информацией нужно обращаться только к проверенным аккаунтам новостных, правительственных и известных общественных организаций. Информацию, которую вы получаете в соцсетях, тоже лучше всего всегда сверять с информацией в надежных источниках. Если вам пришел пост или видео, которое выглядит подозрительно, то лучше их проверить;**
- **вирусной становится информация, которая вызывает у нас эмоции - страх, беспокойство, огорчение или радость – остерегайтесь эмоций, и не впадайте в панику.**

4.7. Настройки личных интернет ресурсов

Немаловажно уделить внимание своим личным интернет ресурсам, т.к. они могут стать причиной утечки важной информации.

К личным интернет ресурсам относятся: мессенджеры, электронная почта, социальные сети, приложения для видеоконференцсвязи, личный кабинет на каком-либо сайте.

Важно помнить, что слабые настройки защиты (простые пароли, отсутствие двухфакторной аутентификации, простые контрольные вопросы для восстановления доступа к аккаунтам), публикация конфиденциальной информации в открытом доступе, отправка важной личной информации в социальных сетях – всё это может сыграть с Вами злую шутку. Злоумышленник сможет заполучить доступ к чему угодно, не приложив каких-либо усилий.

Сценарий №1: у Вас установлены слабые пароли на почте, не установлена двухфакторная аутентификация. Злоумышленник с помощью специальных программ сможет подобрать Ваш пароль, и получить доступ к почте, на которой могут храниться Ваши личные и деловые переписки, отправленные документы (сканы паспортов, медицинские справки и др.) с персональными данными, пароли от некоторых ресурсов. Заполучив доступ к электронному ящику, злоумышленнику не составит труда сбросить пароли с сервисов, которые привязаны к Вашей почте.

Сценарий №2: Вы отправляете фотографии из личного архива другу в социальной сети ВКонтакте. При загрузке файлов в социальной сети, они индексируются и имеют определенный адрес. Злоумышленник может подобрать этот адрес, и получить доступ к фотографии.

Сценарий №3: на Вашем мессенджере и устройстве не установлен пароль на вход. Соответственно, если устройство попадет в руки третьим лицам, то они смогут прочитать все переписки.

Вывод: будьте внимательны. Подходите к защите личных интернет ресурсов с умом, и не пренебрегайте защитой.

4.8. Договоры

Мы постоянно подписываем договоры: со страховой компанией, банком, фитнес-клубом, турагентством или оператором сотовой связи. Договоры важные и не очень, для себя или близких. Единственное, что объединяет эти договоры — их мало кто читает.

В связи с переходом на дистанционную работу многие компании, скорее всего, перейдут к договорам в электронном виде. Поэтому, как и при подписании обычного договора, необходимо следовать главному правилу: сначала читайте, а потом подписывайте.

Это простое правило, которому следуют единицы. Каждый день кто-нибудь подписывает договор, не глядя на условия. Большинство людей подписывает договор не читая, по двум причинам: боятся выглядеть глупо и не хотят затруднять собеседника (отнимать его время).

Наглядным примером является случай, который произошел в Сургуте. На молодых матерей были оформлены фирмы. Произошло это без их ведома. Они подписали множество договоров, не ознакомившись с условиями.

Репортаж телепередачи «Человек и Закон» о данном происшествии

Соблюдать это правило просто: возьмите тайм-аут и спокойно почитайте договор. От договора зависит многое: Вы можете понести ответственность за неисполнение условий, качество предоставляемых услуг, сроки, которые должны соблюдаться Вами и другой стороной, штрафы и пени, которые придется заплатить, порядок урегулирования вопросов, а также проблемы, которые может повлечь Ваша неосторожность.

5. Выводы

Мир ИТ многообразен. С каждым днем растет количество устройств, сервисов, ресурсов, технологий. Ценность информации растет в связи с тем, что всё автоматизируется. Соответственно, видов мошенничества и хакерских атак с каждым днем становится всё больше. А поймать злоумышленника крайне сложно.

Кибергигиена становится обязанностью каждого пользователя. Без неё будет сложно адаптироваться в растущем мире информационных технологий – ведь на каждом углу поджидают опасности, которые могут привести к потере или же краже Ваших личных данных.

Кибергигиене нужно учиться: усваивать знания, повторять, закреплять, проверять самих себя, и делать это на периодической основе. Многократное повторение позволяет закрепить полученные навыки.

Поделитесь знаниями с близкими. Если Вы научитесь не попадаться на уловки злоумышленников, на них может попасться Ваш близкий человек, в том числе и с вашего компьютера. Поэтому необходимо чтобы близкие люди тоже были осведомлены о кибергигиене.

Методические рекомендации разработаны: ООО «Анлим-ИТ»

По любым интересующим вопросам обращайтесь:

тел.: +7 (3452) 58-58-37

e-mail: info@unlim.group