Муниципальное бюджетное общеобразовательное учреждение «Средняя общеобразовательная школа №8» г.Уссурийска

КИБЕРБЕЗОПАСНОСТЬ

Выполнил: Вишнепольский Михаил,
ученик 11 класса
Руководитель: Рева Т.А.,
учитель информатики

Уссурийск, 2023г.

Оглавление:

Введение

Актуальность: вопрос интернет безопасности с каждым годом становится более популярным из-за быстрого развития соответствующих технологий. Актуальность в создании собственной безопасности будет всегда, следовательно, актуальность моего проекта тоже.

Объект исследования: Кибербезопасность и злоумышленники в сети интернет

Предмет исследования: возможность защиты от неприятелей и создание надёжного пароля

Цель проекта: создать собственный пароль и проверить его надёжность

Задачи проекта:

- Собрать информацию из различных источников по данной теме для создания проекта;
- Проанализировать основные виды обмана в интернете;
- Обобщить полученные результаты и сделать выводы;
- Рассмотреть программное обеспечение для создания безопасности электронных устройств;
- Разработать защиту;
- Защитить проект.

Методы исследования:

- Изучение литературы и других источников информации;
- Анализ текста;

Практическая значимость моего проекта может быть использована в школе для осведомления учащихся об опасности интернет ресурсов, а также для осведомления взрослого поколения в опасности всемирной паутины. Разработанные материалы могут быть использованы для организации самостоятельной защиты учеников.

ГЛАВА 1. Информационная безопасность

1.1 Кибербезопасность – простым языком

Кибербезопасность (ее иногда называют компьютерной безопасностью) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.

Кибербезопасность борется с тремя видами угроз.

Киберпреступление– действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.

Кибератака – действия, нацеленные на сбор информации, в основном политического характера.

Кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

Как злоумышленникам удается получить контроль над компьютерными системами? Они используют различные инструменты и приемы – ниже мы приводим самые распространенные.

Вредоносное ПО

Название говорит само за себя. Программное обеспечение, которое наносит вред, – самый распространенный инструмент киберпреступников. Они создают его сами, чтобы с его помощью повредить компьютер пользователя и данные на нем или вывести его из строя. Вредоносное ПО часто распространяется под видом безобидных файлов или почтовых вложений. Киберпреступники используют его, чтобы заработать или провести атаку по политическим мотивам.

Вредоносное ПО может быть самым разным, вот некоторые распространенные виды:

- **Вирусы** – программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы компьютера, они копируют сами себя.

- **Троянцы**– вредоносы, которые прячутся под маской легального ПО. Киберпреступники обманом вынуждают пользователей загрузить троянца на свой компьютер, а потом собирают данные или повреждают их.
- **Шпионское ПО** – программы, которые втайне следят за действиями пользователя и собирают информацию (к примеру, данные кредитных карт). Затем киберпреступники могут использовать ее в своих целях.
- **Программы-вымогатели** шифруют файлы и данные. Затем преступники требуют выкуп за восстановление, утверждая, что иначе пользователь потеряет данные.
- **Рекламное ПО** – программы рекламного характера, с помощью которых может распространяться вредоносное ПО.
- **Ботнеты** – сети компьютеров, зараженных вредоносным ПО, которые киберпреступники используют в своих целях.

1.2. Методы обмана

В мире всегда существовали мошенники, которые умудрялись похищать средства и ценности в самых разнообразных масштабах. Постепенная информатизация мира привела к появлению нового вида злодеев – кибермошенников.

Схема с криптовалютами и ICO

Одним из самых популярных видов мошенничества в последние годы стали махинации с криптовалютами, в частности со сбором средств на запуск проектов в сфере блокчейн. Злоумышленники презентовали якобы хороший проект, на реализацию которого требовались средства. Для этого использовалось так называемое поддельное ICO (Initial Coin Offering). Это формат сбора средств на развитие проектов в сфере криптовалют. Прикрываясь этим инструментом, злодеи продавали фальшивую криптовалюту за биткоин или эфириум, которые имеют реальную стоимость. После нескольких раундов сбора средств «новаторы» пропадали без вести вместе с собранными средствами. При этом отследить их было практически невозможно т.к. всеми собранными средствами можно распоряжаться анонимно. Стоит отметить, что на рынке были и настоящие ICO, но таковых было не более 10-20%.

Совет: для начала изучите рынок криптовалют более детально, прежде чем вкладывать реальные деньги

Фейковые СМС от банка

Злоумышленники присылают на номер жертвы СМС с текстом о том, что ее карта заблокирована. В конце указывается номер телефона, по которому нужно связаться с якобы сотрудником банка. Доверчивый пользователь звонит по номеру и попадает в руки искусного мошенника, выполняя его просьбы и, сам того не замечая, передает свои конфиденциальные данные и деньги в чужие руки.

Совет: никогда и никому не сообщайте свои данные, а также любую банковскую информацию.

Дешевые товары на интернет-досках объявлений и онлайн-магазинах

Человеком часто движет желание сэкономить, чем пользуются коварные злодеи. Они регулярно размещают товары на сайте объявлений по очень выгодной цене, которая может быть на 30-40% ниже среднерыночной. Единственным условием покупки является внесение небольшого аванса на карту. После получения предоплаты исчезает не только «продавец», но и объявление с сайта.

Здесь нужно быть очень внимательным, заказывая товары в новом магазине, который продает по очень выгодным ценам. Очень часто наивные пользователи заказывают товар, внося предоплату и в итоге не получают ни посылки, ни денег. Проверяйте юридический адрес магазина, лицензии и ищите отзывы реальных покупателей.

Совет: если вы на 100% не уверены в честности продавца, то придерживайтесь покупок исключительно наложенным платежом.

Заражение вирусом-вымогателем

По всему миру активно распространяются вирусы-вымогатели, которые попадают на компьютер «жертвы» и зашифровывают все файлы, что ставит под угрозу всю хранившуюся информацию и парализует работу. Чтобы вернуть все ваши документы, вирус выдает сообщение с требованием перевести средства на криптовалютный кошелек, чтобы их невозможно было отследить. Только якобы после этого вы сможете возобновить доступ к файлам. К сожалению, в большинстве случаев вся информация так и остается зашифрованной даже после уплаты «выкупа».

Совет: регулярно обновляйте антивирус на всех своих устройствах.

Установка приложения на смартфон

Практически каждый современный человек пользуется смартфоном. Это еще одно поле деятельности для кибермошенников. Одним из вариантов хищения ваших личных данных является установка зловредных приложений под видом обычных программ.

Совет: никогда не загружайте приложения на телефон из других источников, кроме официальных магазинов приложений Google Play и App Store.

Кибермошенничество в соцсетях

Нужно быть максимально внимательным при участии в различных опросах. Очень часто мошенники проводят опросы под видом одного из популярных банков, предлагая в конце разыграть приз. Чтобы подтвердить получение выигрыша, грабители просят отправить определенную сумму на их счет для подтверждения, что вы якобы являетесь клиентом их банка. Никогда не отправляйте деньги третьим лицам под предлогом участия в розыгрыше призов. Банки никогда не требуют подобных действий.

Еще один способ выудить информацию у доверчивых пользователей - создание поддельных личных страничек с целью знакомства и получения личной информации, которая может послужить доступом к вашим реальным финансам.

Совет: в процессе общения злоумышленник постепенно переходит к более личным вопросам, поэтому будьте осторожны с онлайн-знакомствами и не раскрывайте своих персональных данных в сомнительных опросах в сети.

Обман на фриланс-услугах

Удаленная работа стала источником дохода для десятков миллионов людей по всему миру. Довольно часто можно встретить объявления и целые сайты, посвященные простому и быстрому заработку. Вам предлагается гибкий график, приличное вознаграждение и даже соцпакет. Чтобы начать работу, с вас могут потребовать небольшую плату за обучающие материалы или доступ к заказам. Когда мошенник получит деньги, то скорее всего вы не увидите ни работы, ни обучающих материалов.

Совет: остерегайтесь таких предложений, ведь на большинстве фриланс-бирж начать работу можно абсолютно бесплатно.

Фальшивые интернет-аукционы

Интернет-аукцион является хорошей возможностью купить товар по более низкой цене, но и здесь можно попасться «на удочку».

Совет: прежде чем делать ставки на лот, проверьте рейтинг и отзывы о продавце. На аукционах – это важнейшие показатели честности. Не рекомендуется делать ставки на товары продавцов с маленьким количеством отзывов и сделок или нулевым рейтингом.

Мошенничество с любителями онлайн-игр

Многие дети и даже люди старшего поколения обожают игры. Желание быть лучшим порождает зависимость, которая проявляется в растрате денег на своих игровых персонажей для покупки виртуальных улучшений и предметов. Чтобы сэкономить, многие ищут, где это можно сделать подешевле, наталкиваясь на аферистов, которые берут предоплату, но не предоставляют виртуальные ценности.

Совет: следите за собственными детьми, если они играют в сети.

Мошенничество на бесконтактных платежах

Современные банковские карточки оснащаются чипом, позволяющим совершать быструю оплату, поднося карту к терминалу, который считывает информацию и списывает соответствующую сумму со счета. Теперь подобными устройствами считывания пользуются не только магазины, но и мошенники. Они носят в сумке самодельные портативные терминалы и прислоняются к «жертвам», чтобы украсть деньги с карты.

Совет: чтобы обезопасить себя, установите в лимит на дневные платежи или поставьте необходимость вводить пин-код для подтверждения любых транзакций.

1.3. Методы защиты

1. Антивирус

Это базовый софт, обеспечивающий безопасность. В задачи антивирусного ПО входит обнаружение шпионских программ, вирусов, фишинговых ресурсов, опасных серверов и подозрительного трафика. Популярные антивирусы справляются с большинством угроз, которые поступают на компьютер из сети или съёмных носителей. Правда, они не защищают от действий пользователя на

сайтах. То есть, если ресурс не вызвал у программы подозрений и открылся, нажатия на ссылки или действия с элементами уже не будут защищены.

2. VPN

VPN — это защищённая сеть, которая скрывает IP адрес и месторасположение. Она надёжно зашифрует весь трафик и данные, передаваемые с устройства. Если вам необходимо обойти блокировку сайта, получить анонимность в сети или подключиться к Wi-Fi в публичном месте, используйте VPN.

Сама технология работает так:

1. Информация шифруется на устройстве.
2. Передаётся на сервер VPN-провайдера.
3. Дешифруется на сервере.
4. Передаётся по назначению (на сервер сайта).

Таким образом, личная информация защищена от перехвата, она полностью зашифрована, персональные данные скрыты. Блокировки сайтов, например, от Роскомнадзора перестают работать. Присутствие в сети выглядит так, словно вы вышли в интернет не из России, а из другой страны (где размещён VPN сервер). Вот список VPN-сервисов, которыми можно пользоваться бесплатно.

3. Временная анонимная почта

Временная почта – это ящик со случайным адресом и ограниченным сроком жизни. Он удобен, когда нужен доступ к сервису с регистрацией, а вы не планируете им долго пользоваться. Кроме того, сами «времянки» обычно не просят логиниться или указывать личную информацию. Просто заходишь на сайт и применяешь.

Сервисов временной почты много и найти удобный вариант не трудно. Обратить внимание стоит на эти: Temp Mail и EmailOnDeck.

Такая почта не защищает от последствий после перехода по подозрительным ссылкам и не предотвращает «слив» данных на фишинговом ресурсе. Но она помогает снизить до минимума поступающий спам, в котором часто скрываются подобные опасности.

4. Постоянное шифрование

Чтобы результатом действий на сайте не стала утечка личных данных или спам-атака на почту, пользуйтесь ресурсами, сетевой адрес которых начинается с HTTPS. Это значит, что соединение между вами и сервером шифруется – информацию не получится перехватить.

Современные браузеры напоминают о риске нешифрованного соединения. Если при проверке сертификата данные не совпадают, на экране появляется предупреждение. Правда, его можно проигнорировать, нажав «Я принимаю риск, всё равно перейти».

Чтобы повысить уровень защиты, зашифруйте столько интернет-трафика, сколько сможете, с помощью расширения HTTPS Everywhere. Оно автоматически заставляет сайты использовать HTTPS протокол вместо HTTP. Его можно бесплатно установить в браузеры Google Chrome, Mozilla Firefox и Opera, в том числе и на мобильных устройствах.

Информации в облачных хранилищах тоже не мешает добавить защиты. Установите программу для шифрования данных в облаке, например, Boxcryptor.

5. Сложные пароли

Люди древности пытались закодировать свои сообщения. Так зародилась криптография.

Сложность паролей напрямую определяет их надёжность, поэтому рекомендуется использовать длинные случайные комбинации символов. Во-первых, их почти невозможно взломать перебором. Во-вторых, они не имеют привязки к личности пользователя.

Пароль в виде имени супруга или ребёнка, даты рождения, клички собаки, названия любимой команды непосредственно связаны с вами. Это та

информация, которую злоумышленники смогут подобрать, если получат доступ к социальной сети, почте или компьютеру.

Поэтому 17041991 – это плохой пароль. Masha17041991 или 1704masha1991 — тоже. А Vy0@$e6#Omx6 – сильный пароль. Его невозможно собрать исходя из данных о человеке, а найти перебором сложно технически.

Не используйте одинаковые пароли. В идеале для каждого случая должна быть своя комбинация. Применять для всех почтовых аккаунтов, соцсетей и банковских сервисов один и тот же код — опасно.

Всё запомнить будет трудно. Поэтому установите для хранения менеджер паролей:

- KeePass
- LastPass
- RoboForm
- Protect (дополнение Яндекс.Браузера)

6. Двухфакторная авторизация (аутентификация)

Чтобы защитить себя в интернете используйте двухфакторную аутентификацию. Это означает, что при попытке авторизоваться на сервисе будет необходимо указать два секретных параметра-доказательства. При стандартном входе такой параметр только один – пароль. В случае с двухфакторной авторизацией нужно будет ввести ещё один. Чаще всего это случайный сгенерированный код, который отправляется в SMS на телефон. Если злоумышленник завладел паролем, то он не сможет войти в аккаунт.

Сейчас двухфакторная аутентификация используется большинством крупных сервисов: Microsoft, Google, Yandex, Dropbox, ВКонтакте. Для подтверждения они применяют SMS, мобильные приложения, токены (редко), резервные ключи.

7. Осторожность с почтой

Будьте аккуратны с файлами, приложенными к письмам в электронной почте. Никогда не открывайте и не запускайте их, если источник неизвестен. В

противном случае убедитесь, что он действительно прислал вам важный документ. Не забудьте также проверить файл антивирусом – вдруг отправитель распространяет угрозы, но не подозревает об этом сам.

8. Своевременное обновление ПО

Преступники совершенствуют свои инструменты, а разработчики со «светлой» стороны – укрепляют оборону. Оба соперника изучают методы друг друга и стараются своевременно реагировать на изменения. Новые варианты взлома и слежки попадают в сеть ежедневно, поэтому для снижения рисков до минимума надо регулярно обновлять программное обеспечение. К нему относится и антивирус, и операционная система, и браузер.

9. Безопасность среды

Угроза может проникнуть на компьютер не только напрямую из сети или файла, полученного на почту. Источником способна послужить локальная сеть на работе, заражённое устройство одного из членов семьи, уязвимая точка Wi-Fi в общественном месте.

Старайтесь проверять степень защищённости всех устройств и сетей, к которым подключаетесь. А в общественных местах лучшее вообще не использовать открытые сети для онлайн-оплаты или авторизации в веб-сервисах (если нет VPN).

10. Телефон и планшет

Любое устройство, которое легко теряется, необходимо дополнительно защитить, то есть установить графический или цифровой код для разблокировки. Этого достаточно, чтобы предотвратить большинство опасностей. Только не выбирайте для блокировки даты или простейшие комбинации.

ГЛАВА 2. Немного о прочем

2.1. Что такое даркнет

Чтобы понять это, нужно разобраться в структуре интернета. Глобальную сеть условно делят на три слоя:

- **Поверхностный, или видимый**. Сюда относят общедоступные, открытые веб-ресурсы. То есть любые сайты, которые можно посетить по стандартной ссылке и найти в поисковиках.
- **Глубокий**. Включает контент, который не попадает в поисковые системы. Содержимое частных облачных хранилищ, корпоративных сетей и различных закрытых баз данных — всё это глубокий интернет. Чаще всего доступ к таким ресурсам защищён логином и паролем.
- **Тёмный, даркнет**. Это собирательное название компьютерных сетей, предназначенных для анонимной передачи информации. Там тоже есть сервисы для торговли, общения и обмена контентом, но их нельзя открыть через стандартный браузер или найти в обычном поисковике.

Архитектура скрытых сетей препятствует слежке за пользователями и контролю над передачей информации. Поэтому даркнет может быть как орудием против цензуры, так и ширмой для преступлений.

В России, как и в большинстве других стран, использовать скрытые сети разрешено. Но под запретом находятся многие активности, происходящие в даркнете. После появления биткоина, который позволяет пересылать деньги анонимно, скрытый интернет превратился в виртуальный чёрный рынок. Помимо легальных сайтов, даркнет наводнили площадки, где продают, украденные данные, наркотики, оружие и другие незаконные товары.

Как устроен даркнет

Скрытые сети существуют параллельно друг другу и обеспечивают анонимность разными техническими средствами. Например, крупнейшая из них построена на принципах TOR (The Onion Router), или луковой маршрутизации.

Это технология шифрования и передачи данных, созданная сотрудниками исследовательской лаборатории военно-морского министерства США.

Работает это так. Сообщение оборачивают в несколько слоёв шифрования, из-за чего напрашивается аналогия с луком. Затем его передают через множество сетевых узлов — так называемых луковых маршрутизаторов. Каждый из них снимает защитный слой, чтобы узнать следующий узел в цепочке. В результате ни один посредник не видит ни содержимое, ни весь маршрут сообщения. Полная расшифровка происходит только на стороне получателя.

Проект создавали в 1990-е годы для военных целей. Но позже авторы сделали код TOR общедоступным, чтобы технология послужила для защиты прав и свобод обычных людей. Теперь её можете использовать и вы для доступа к даркнету.

Сейчас разработкой TOR занимается организация TOR Project. У проекта много спонсоров среди обычных пользователей и различных научных, технологических и других учреждений. Постоянное развитие и относительная простота использования сделали технологию популярной. Поэтому в массовой культуре даркнет в первую очередь ассоциируется с этой скрытой сетью.

Журналисты часто связываются через TOR с информаторами. Facebook*, The New York Times и BBC используют её, чтобы вопреки блокировкам оставаться доступными в тоталитарных странах. Для этого компании создали TOR-версии своих сайтов в даркнете.

Скриншот: официальный сайт I2P

Другая относительно известная анонимная сеть — I2P (Invisible Internet Project). Энтузиасты со всего мира разрабатывают её с 2004 года. Техническая основа проекта обеспечивает более высокую скорость, чем TOR, и теоретически ещё большую защищённость.

Вместе с тем у I2P нет средств для быстрого развития. А в текущем состоянии инструменты для использования этой сети недостаточно удобны и просты для широкой аудитории. По количеству пользователей I2P значительно уступает TOR.

Есть и другие скрытые сети, но они ещё менее популярны.

Как попасть в даркнет

Подключиться к скрытой сети проще, чем вы могли подумать. Для входа чаще всего используют TOR-браузер. Его можно скачать бесплатно с официального сайта организации TOR Project.

После запуска программа отобразит подсказки, которые помогут вам её настроить. Как только откроется меню браузера, можно приступать к сёрфингу.

Сайты этой скрытой сети имеют специальные адреса в зоне .onion. Если вы не знаете, с чего начать знакомство с даркнетом, можете посетить через TOR эти безопасные ресурсы:

Каталог ссылок на популярные сайты даркнета

- The Hidden Wik
- Facebook
- Международная версия BBC
- Поисковик DuckDuckGo используйте только официальные версии

TOR-браузера и регулярно обновляйте его, чтобы программа была максимально стабильной и безопасной. Обратите внимание: из-за особенностей iOS официального приложения TOR для этой операционной системы не существует.

Чем опасен даркнет

В даркнете хватает тех, кто не только предлагает нелегальные товары и услуги, но также пытается обокрасть или эксплуатировать других пользователей. Конечно, такие люди присутствуют и в обычном интернете. Но анонимность скрытых сетей позволяет им действовать более эффективно.

Если же вы сами намерены нарушить закон и считаете, что даркнет обеспечит вам безнаказанность, подумайте ещё раз. Хоть скрытые сети приватны, по неосторожности или в силу технической неграмотности вы всё равно можете раскрыть свою личность. К примеру, достаточно случайно скачать из даркнета троян или оставить в неподходящем месте контакты.

2.2. Хакеры – гении преступного мира или профессиональные IT специалисты?

Термин происходит от английского слова «to hack», что на русский переводится как «**обтесывать**, делать зарубы».

В современном понимании хакер — это человек, занимающийся разными видами компьютерного мошенничества: цифровым взломом, выводом из строя оборудования, кражей, подменой, удалением данных.

Термин «хакер» появился вместе с первыми компьютерами. В то время **так называли гиков**, которые могли улучшить работу операционной системы путем создания кода для части ядра.

Виды хакеров

Как и большинство IT-специалистов, каждый хакер имеет **узкую специализацию** и не способен взламывать защиту программного обеспечения всеми возможными способами.

Вот несколько наиболее распространенных разновидностей хакеров:

1. **Фишеры**. Собирают пользовательские данные, в том числе вводимые данные банковских карт на формах фальшивых сайтов и в поддельных приложениях. Определить фишинговый сайт можно, обратив внимание на его URL.

   Например, вместо vkontakte.ru мошенники могут использовать схожее по написанию, но отличающееся на одну букву название —vkontahte.ru.

2. **Разработчики вирусов**. Это самый известный вид хакеров. Они создают вредоносные программы, с помощью которых получают доступ к данным на «инфицированном» компьютере.
   Некоторые вирусы выводят из строя аппаратную часть ПК (это что?), другие — помогают злоумышленникам получить интересующую их информацию, а с помощью третьих у владельцев зараженных устройств вымогаются деньги.
3. **Брутсофтеры**. Это специалисты, которые создают ботнеты и специализируются на брутсофте — перебирании паролей. Владельцы зараженных компьютеров даже не подозревают, что их устройства взломаны вирусом и используются им в своих целях.

4. **Взломщики игр**. Хакеры постепенно переходят в мир онлайн-игр: там они крадут у игроков ценные игровые предметы и ресурсы, чтобы перепродать их за реальные деньги другим.
5. **Охотники за криптовалютой**. С появлением биткоина и других видов криптовалюты участились случаи взлома криптовалютных кошельков. Хакеры также не стесняются взламывать смартфоны и ПК, чтобы установить туда программы для добычи новых денежных знаков.

Чем опасны хакеры

По большому счету, хакеры — **это умные мошенники**, которые используют свои знания с целью обмана доверчивых людей.

Они взламывают:

1. личные страницы пользователей в социальных сетях;
2. компьютеры и смартфоны;
3. аккаунты в платежных системах;
4. аккаунты в онлайн-играх;
5. электронную почту и мессенджеры;
6. облачные хранилища;
7. и многое другое.

Кроме огромного ущерба физическим лицам и организациям, хакеры способны стать **причиной настоящей катастрофы**. Проникнув в систему энергоснабжения, можно оставить весь город без света.

Но если замахнуться на более серьезные вещи вроде получения доступа на управление атомной электростанции, то плачевных последствий не избежать.

Самое интересное в том, что хакеры за свои деяния хотят получать оплату в криптовалюте, так как такие транзакции крайне сложно отследить.

Кто такие белые хакеры

Но не все так плохо, как может казаться. Например, один программист обнаружил уязвимость в системе защиты платежной системы PayPal и… сообщил об этом напрямую в компанию. Понимая, какой ущерб смог предотвратить бдительный айтишник, в PayPal решили поощрить его чеком на 70 000$.

Это пример белого хакера — специалиста, который занимается ***взломом для повышения безопасности*** *систем защиты.*

Если им удается найти уязвимости, они передают эти данные разработчикам и предлагают рекомендации по их устранению. Такие хакеры не занимаются кражей денег, а работают либо на добровольной основе, либо по найму.

2.3. 10 крупнейших интернет-афер всех времен

1. "Русские хакеры". В августе 2014 г. группе хакеров удалось украсть 1,2 млрд паролей и аккаунтов у самых разных компаний. В общей сложности пострадало 420 тыс. сайтов. Некоторые из них были совсем небольшими, другие принадлежали участникам списка богатейших предприятий Fortune 500. Пострадавшие компании при помощи властей пришли к выводу, что нападение совершили "русские хакеры". Также стало известно, что они не пытались украсть важную информацию, хотя могли это сделать. Взломщики лишь заразили компьютеры спамом. Так что бизнес испугался не того, что было сделано, а того, что могло быть сделано. Появились слухи о том, что хакеры из России дали понять, что санкции со стороны Запада не останутся без ответа.

2. Нападение на Sumitomo Mitsui. В 2004 г. офисы японского банка Sumitomo Mitsui были атакованы хакерами. Злоумышленники использовали инструмент под названием keylogger, и с его помощью украли пароли от банковских счетов. Ограбление могло стать одним из самых масштабных в истории, так как хакерам удалось украсть $420 млн. Но злоумышленники не знали, как избавиться от опасных денег, и попытались распределить их по счетам в других банках. Во время одной из таких операций был пойман гражданин Израиля Йерон Белонди. Он попытался внести $27 млн на счет в израильском банке. Другие преступники также были арестованы.

3. Кража $45 млн с карт с хранимой стоимостью. Хакеры покупали карточки с хранимой стоимостью и изменяли сумму, которая зашифрована в них. Примером такого типа карты можно считать карту предоплаты, однако в данном случае речь шла именно о кредитках, для которых изменялся лимит на получение денег. В Нью-Йорке были арестованы люди, которые пытались в двух банках одновременно получить из банкомата $2,7 млн наличными. Позже выяснилось, что группа насчитывала восемь человек, а украсть им удалось $45 млн.

4. Нападение на Nordea Bank. Хакеры использовали метод фишинга. Они заражали компьютеры клиентов Nordea Bank специальным вредоносным ПО, которое считывало нажатия на клавиши и позволяло воссоздать пароль от аккаунта в интернет-подразделении банка. При вводе личных данных пользователь видел сообщение о том, что сайт временно не работает, а злоумышленники тем временем получали возможность делать все, что им заблагорассудится. В общей сложности хакеры украли таким образом $943 тыс.

5. Один хакер против трех банков США. Хакер, известный под ником Soldier, использовал специальный набор инструментов для виртуального взлома под названием SpyEye и с его помощью крал по $17 тыс. в день. Этот злоумышленник сумел взломать 3,5 тыс. банковских счетов в трех крупных американских банках - Chase, Wells Fargo и Bank of America. За шесть месяцев Soldier утащил из-под носа программистов, пытавшихся заткнуть дыры в безопасности, $3,2 млн. Затем хакер притворился компанией и через подставной аккаунт сумел обналичить деньги.

6. Похищение bitcoin. Криптовалюта bitcoin позволяет расплачиваться за товары и услуги платежным средством, которое выпускается без участия центробанков. Это чрезвычайно удобная для некоторых типов транзакций "валюта", которая, однако, привлекла внимание хакеров. Дело в том, что bitcoin надо где-то хранить, и существуют специальные онлайн-кошельки, где лежат виртуальные монетки. Один из таких кошельков, inputs.io, был взломан, в результате чего злоумышленник получил 4,1 тыс. bitcoin, что сегодня соответствует $1,3 млн. Едва ли хакера поймают, так как перемещения криптовалюты очень сложно отследить.

7. Подозрительно частые хакерские атаки в Аризоне. Сложно с уверенностью сказать, почему американский штат Аризона страдает от хакерских нападений чаще, чем любое другое место на Земле. Возможно, именно здесь действуют некие группы злоумышленников, которые создали особую сеть киберпреступности, а может быть, это просто совпадение. В любом случае статистика выглядит угрожающе: на 100 тыс. жителей в Аризоне приходится 149, пострадавших от кражи личных данных. Преступники зарабатывают во время заполнения налоговых деклараций своих жертв, так как успевают получить налоговые компенсации раньше, чем это делает настоящий владелец декларации.

8. Тинейджеры-нацисты. ФБР потратила несколько лет на расследование, столкнувшись с масштабной хакерской атакой, результатом которой стало похищение информации о 411 тыс. владельцев кредитных карт и взлом серверов 47 компаний, образовательных учреждений и ведомств. Оказалось, что группа преступников состояла сплошь из тинейджеров, а самому старшему хакеру было всего 22 года. Деятельность группировки удалось пресечь, и 28 человек в результате были арестованы. Еще немного, и им бы удалось украсть $205 млн.

9. Ограбление ритейлера TJX 0 В 2006 г. была взломана защита серверов ритейлера TJX, который контролирует такие американские сети, как TJ Maxx, Marshall's и HomeGoods. Этот взлом поражает своими масштабами: была похищена информация о кредитных картах 94 млн человек. Позже был пойман хакер Альберт Гонзалес, осуществивший нападение в сговоре с еще 11 злоумышленниками. Главарь банды получил тюремный срок 40 лет. Также стало известно, что у TJX вообще не было нормальных файерволлов, способных защитить от подобной атаки.

10. Взлом Heartland Payment Systems. Heartland Payment Systems - система, которая проводит денежные транзакции между американскими компаниями. Это уже не раз приводило к попыткам использования системы для кражи ценной информации. И несмотря на то, что эксперты рекомендовали компании укрепить защиту, достаточно быстрой реакции не последовало, что позволило хакерам утащить из Heartland Payment Systems информацию о 134 млн кредитных карт. Если бы им удалось обналичить с каждой хотя бы по доллару, они могли бы жить безбедно. Однако известно, что управлял операцией Альберт Гонзалес, а он, как мы уже сказали, в итоге был пойман.

Глава 3. Практика

3.1. Практическая часть

Создание пароля стоит начать с места хранения для дальнейшего запоминания, ведь все мы люди и не можем всё запомнить.

В моей работе я упоминал следующие проекты: KeePass, LastPass, RoboForm, Protect (дополнение Яндекс. Браузера), но есть риск в виде неожиданной поломки накопителя информации.

Можно прибегнуть к старому способу - записывания пароля на листочек бумаги, но есть риск потерять бумажку.

По-моему мнению, стоит записать пароль в оба варианта из мною предложенных.

Осталось понять, что записать.

Обычный пароль из комбинации цифр (12345) мало эффективен, поэтому стоит усложнить его буквами (ЗАЧЁТ12345)

Теперь стоит заменить буквы на латинский аналог, а цифры можно заменить на значки, которые находятся вместе с этими цифрами на клавиатуре (ZaЧЁt1@34%)

Пользуясь сайтом для выяснения надёжности пароля: https://2ip.ru/passcheck/

Стоит сделать вывод, что мой пароль уже является не простым для злоумышленников и прост в запоминании.

В создании пароля можно использовать любой из шифров, что я приводил выше. Порой самое банальное является простым и гениальным решением.

3.2. Заключение

Подводя вывод всему выше сказанному, я хочу, чтобы вы запомнили самое главное:

Не стоит использовать свои инициалы и дату рождения в пароле.

Если у вас есть персональный компьютер, то стоит установить антивирус. Стоит упомянуть, что антивирус требует производительности от вашего компьютера, поэтому бессмысленно устанавливать его на «слабое железо».

В нынешнее время технологии развиваются очень быстрыми темпами, поэтому компьютеры научились считывать черты лица или отпечатки пальца людей. Отпечатки у каждого человека уникальны, что делает их великолепной электронной защитой от недоброжелателей.

Пользоваться безграничными возможностями всемирной паутины стоит в меру. Автор безобидного сайта, с картинками милых животных, может украсть, от части, всю вашу жизнь, зная всего лишь один единственный язык – двоичный код.

Роберт Чалдини рекомендует думать прежде, чем доверяться незнакомцу, показавшемуся вам доброжелательным. Незнакомцем может быть мастер уговоров. В своих уловка такие деятели, чаще всего, используют: принцип последовательности, принцип взаимного обмена, принцип социального доказательства, принцип авторитета, принцип благорасположения и принцип дефицита. Настоящие асы подобное могут провернуть и в сети.

Список литературы и других источников информации

Литература

1. Роберт Чалдини «Психология влияния»
2. Роберт Чалдини «Психология согласия»
3. Алан и Барбара Пиз «Новый язык телодвижений»
4. Даниил Туровский «Вторжение. Краткая история русских хакеров»

Интернет-ресурсы

1. https://www.kaspersky.ru
2. https://invlab.ru
3. https://club.dns-shop.ru
4. https://tv.rbc.ru/?utm_source=topline
5. https://ktonanovenkogo.ru/glavnaya-v-i-o
6. https://fishki.net
7. https://2ip.ru/passcheck/