Муниципальное бюджетное общеобразовательное учреждение
«Магистральнинская средняя общеобразовательная школа №22»

Проект

на тему: «Виды мошенничества в сети»

Ученика 8Б класса
Ерусланова Матвея Алексеевича
Руководитель проекта:
Курчинская Анна Анатольевна

2019 год

Содержание

Цели и задачи……...3

Что такое мошенничество……...…4

Значение сети интернета в современном мире ……5

Актуальные виды мошенничеств в сети интернет……...6

Вирус-вымогатель……...9

Итог…….11

Литература……..12

Цели и задачи

1. Определить, что такое мошенничество
2. Определить основные методы мошенничеств в сети интернет
3. Научится распознавать и защититься

Что такое мошенничество

Из статьи 159 Уголовного кодекса Российской Федерации, Мошенничество – это, хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

То есть, если у вас просят данные, через которые возможно совершить какие-то действия от вашего лица, и совершают их без вашего согласия, это мошенничество. Если вы заключили договор и передали деньги другому лицу за услуги или товары, и не получили их, это акт мошенничества.

Значение Интернета в современном мире

Сегодня мы мало задумываемся о том, где найти ответ на тот или иной вопрос. Когда под руками есть Интернет, все сводится лишь к набору необходимого поискового запроса в Яндексе или Гугл. Интернет представляет собой один из самых мощных источников получения той или иной информации, данных, а также дает возможность постоянно оставаться на связи.

Возможность общения без границ - один из самых огромных подарков человечеству от Всемирной паутины. Конечно, никакие печатные буквы, ни изображение, передаваемое веб-камерой не способны заменить реального живого человека, однако приходится признавать, что последнее не всегда доступно и осуществимо в то время, как использование Интернета, социальных сетей, например, сайт вконтакте или Facebook, многочисленных Интернет-пейджеров и электронной почты позволяют наладить контакт с человеком, где бы он не находился.

В свое время Марк Цукерберг нашел очень правильную "кнопку" среди потребностей человека - это потребность быть в контакте с другими людьми, общаться, находить новые знакомства или восстанавливать старые контакты. Именно по этой причине его проект Facebook в кратчайшие сроки обрел всемирную популярность, а сам Марк Цукерберг снискал не только славу, но и неплохой доход.

Интернет - это возможность развивать собственное дело, не взирая на границы. Вряд ли кто-то станет отрицать, что Бизнес в сети открывает большое количество возможностей даже для тех компаний, которые функционируют в оффлайн режиме. Всемирная паутина - не только источник информации, но и источник возможности эту информацию безгранично распространять.

Ввиду постоянной нехватки времени, многие люди постепенно привыкают к тому, что большое количество действий они могут выполнить, не отрываясь от монитора: сходить в магазин, "побывать" на пресс-конференции, сделать телефонный звонок, почитать газеты и мн. др. Конечно, скептики тут же бросятся осуждать такой способ организации жизни: мол, скоро люди вообще перестанут выходить из дома. Однако нельзя отрицать тот факт, что возможность экономить собственное время таким способом позволяет выделить его для чего-то более важного: общения с семьей, походу в парк, отдыху с друзьями.

Актуальные виды мошенничеств в сети интернет

1. Честный заработок

Попасть в ловушку можно и на сайте объявлений. Вам предложат работу, которая в итоге не будет оплачена, а в ряде случаев, вы еще и оплатите необходимые вам материалы или внесете сумму «для проверки серьезности ваших намерений». Основные виды предложений:

- набор текста;
- сортировка бумаг, файлов, писем;
- изготовление мыла;
- вышивка картин.

Список можно перечислять бесконечно. Основная отличительная черта таких предложений – высокая оплата работы за простые действия.

2. Мошенничества Интернет-магазинов

Опасаться стоит и Интернет-магазинов. Сегодня довольно легко открыть небольшой интернет-магазин с заманчивыми ценами. Заказ в таком магазине обычно предполагает только предоплату – отправку денег на электронный кошелек. При этом после оплаты покупки товар вам так и не доставят. На ваши звонки тоже навряд ли ответят, а сам сайт магазина исчезнет с просторов сети в течение месяца – двух.

Основные признаки подставных Интернет-магазинов:

- низкая цена;
- отсутствие адреса или телефона продавца;
- использование исключительно электронных кошельков для оплаты.

3. Пополни кошелек

Еще один популярный вид мошенничества связан с пополнением кошельков или аккаунтов. Наиболее популярные схемы:

- Вам предлагают легкую схему заработка на сайте. К примеру, вы регистрируетесь на сайте и получаете в подарок курицу, несущую золотые яйца. Каждое из виртуальных яиц можно продать за реальные деньги. После того, как на вашем счету окажется определенная сумма, средства можно снять. Но для этого необходимо всего одна мелочь – пополнить свой аккаунт на некую сумму, зачастую, рублей в 100 как минимум. Естественно, ничего вы вывести затем не сможете.

- На ваш аккаунт в социальной сети или на почтовый ящик приходит уведомление, что вы победили в лотерее и выиграли подарок. Но опять-таки, вам необходимо перевести на кошелек организаторов некую сумму. В итоге вы не увидите ни денег, ни подарка.
- Волшебный кошелек. Вы переводите на счет средства и вам тут же возвращают на счет удвоенную сумму. Итог ясен.

4. Сбор средств

Как ни странно, в Интернете также процветает попрошайничество. Основных схем несколько:

- Сбор на лечение ребенка или тяжелобольного человека. Нет, сама информация и даже фотография принадлежат действительно больному человеку и, зачастую, взятые с официального сайта. Но вот номер карты, на которую необходимо перевести деньги – фальшивый.
- Человек якобы попал в неприятную ситуацию и ему требуется некоторая сумма для решения проблемы. К примеру, его незаконно осудили и для взятки необходимо собрать 10 000 или 100 000 рублей.
- Популярная в последнее время схема в социальных сетях и работает на взломанных страницах. Ваш друг может написать вам, что ему необходимо срочно занять денег до завтра и попросить перевести их на карту или кошелек. Ни в коем случае не отправляйте денег, пока лично не переговорите с ним хотя бы по телефону.

5. Интернет-фишинг

Одна из наиболее популярных схем – фишинг, то есть развод на деньги доверчивых пользователей. Представляет собой рассылку от имени банков или платежных систем. Зачастую, на почту приходит письмо, в котором просится зайти на сайт денежной системы. Предлог может быть любой. Наиболее частые – изменение пунктов в договоре-оферте, угроза закрытия счета. При этом вам дается липовая ссылка. Переходя по ней, вы попадаете на сайт, внешне похожий на оригинальный сайт компании. Вводите номер банковской карты или кошелька, пин-код и другие данные.

Другой вариант – это звонок из банка с просьбой погасить кредит. Как только вы начинаете возражать, вас просят предоставить данные для проверки – все те же номер, пин-код, проверочное слово и т.д.

Получив эту информацию, злоумышленники могут без труда обнулить ваш счет в несколько секунд.

6. И многие другие схемы мошенничеств.

Онлайн казино, Ставки на спорт, Финансовые пирамиды, Хайп проекты, и т.д. . .

Вирус-вымогатель

Вирус-вымогатель- тип зловредного программного обеспечения, предназначен для вымогательства, блокирует доступ к компьютерной системе или предотвращает считывание записанных в нём данных (часто с помощью методов шифрования), а затем требует от жертвы выкуп для восстановления исходного состояния.

Сегодня существует 3 основных типа:

- Вирусы-блокировки экрана (ScreenLockers). Эти вирусы появились на заре развития интернета. Основной принцип работы данных вирусов, поместить сообщение компрометирующего содержания с требованием выкупа на весь экран монитора и заблокировать управления компьютером. Расчет мошенников на то, что безграмотные пользователи компьютеров побоятся обратиться к специалистам, для удаления данных типа вирусов, и заплатят выкуп.

- Вирусы-шифровальщики (DataLockers). Содержат в себе алгоритм шифрования, который применяют к файлам на зараженном компьютере. После заражения пользователю предлагается отправить деньги для получения ключа для дешифрования. Примеры таких вирусов: CryptoLocker, Locky, CryptoWall.

- Вирусы-блокировщики (Computer Locker). Являются гибридами выше перечисленных вирусов. Принцип их работы заключается в том, что они блокируют операционную систему на устройстве и не позволяют получить доступ к программам и файлам, пока жертва взлома не переведёт определенную сумму денег. К этому типу относятся вирусы из семейств Petya и Satana.

Начнем с того, что вымогателей стало уж очень много и встречаются они уж очень часто. Они есть для всех операционных систем: для Windows, для Mac OS X, для Linux и для Android. То есть трояны-вымогатели встречаются не только для компьютеров, но и для смартфонов и планшетов. Больше всего их для Windows и Android.

К тому же заразиться довольно просто: трояны-вымогатели чаще всего попадают в компьютер, когда пользователи открывают нехорошие почтовые вложения, переходят по сомнительным ссылкам или устанавливают приложения из неофициальных источников. Но могут проникать и с абсолютно добропорядочных сайтов — например, злоумышленники навострились подсовывать их в рекламу.

Также преступники научились убеждать людей, что им предлагается скачать или открыть что-то полезное — письмо из банка, счет, какую-нибудь ценную программу

и так далее. При этом на самом деле на компьютер попадает блокировщик или шифровальщик.

Пожалуй, главная проблема шифровальщиков состоит в том, что просто вылечить их невозможно. То есть вылечить шифровальщика антивирусом или специальной утилитой, скорее всего, получится — вот только файлы это не вернет: они так и останутся зашифрованными.

Вирусы-шифровальщики нацелены на заражения компьютеров организация. Работник организации, чей компьютер был заражен, тем более если вирус попал в сеть организации, в страхе потерять работу, готов заплатить выкуп. Организации потерявшие базы данных, собранные годами, готовы заплатить выкуп.

Более того, заплатить выкуп — тоже не универсальное лекарство. Во-первых, это дорого. Во-вторых, это поощряет преступников делать новых и новых шифровальщиков. А в-третьих, это еще и не всегда помогает.

Итог

Пользуясь интернетом, нельзя забывать, что, как и в реальной жизни, есть люди, которые хотят наживаться за ваш счет. Бесплатный сыр есть только в мышеловке. Никто ничего не даст просто так. Секреты заработка, на то и секреты что бы о них знало, как можно меньше людей. Рекламы казино и подобных мошеннических проектов рекламируются на пиратских сайтах и фильмах. Надо уважать труды разработчиков, по возможности покупать интересующий продукт, а не искать сомнительные по содержанию взломанные программы и игры.

Надо всегда использовать Антивирус с хорошим сетевым экраном. Не нажимать на подозрительные ссылки. Не скачивать не известные файлы. Нельзя использовать одни и те же пароли при регистрации на сайте и почты. Надо проверяйте адресную строку в браузере перед тем, как вести личные данные или платежной карты. Создавать резервные копии важных данных. Не храните все яйца в одной корзине.

Литература

1. https://ru.wikipedia.org/wiki/ Вирус-вымогатель
2. https://sovetadvokatov.ru/238-moshennichestvo-v-internete.html
3. https://businessman.ru/new-kakim-byvaet-moshennichestvo-v-internete.html
4. http://deflab.ru/blog/vredonosnoe-po/Trojan-lockScreen1.html
5. https://www.kaspersky.ru/blog/
6. http://1ix.ru/