Мошенничество в интернете существует примерно столько же , сколько и сама Всемирная сеть.Новые технологии рождают новые замыслы в головах злоумышленников . Основной целью интернет -мошенничества является обман пользователей глобальной паутины и кража конфиденциальной информации, которая , после используется в личных целях преступника. В результате такой деятельности , миллионы людей во всем мире несут значительные убытки каждый год .Существует большое количество различных видов интернет-мошенничества :фишинг , нигерийские письма и тд .

Фишинг -это вид интернет-мошенничества , целью которого является получение доступа к конфиденциальным данным пользователей -логинам и паролям .Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов , а также личных сообщений внутри различных сервисов , например, от банков или внутри социальных сетей . В письме часто содержится прямая ссылка на сайт , внешне неотличимый от настоящего, либо на сайт с редиктором .После того как пользователь попадает на поддельную страницу , мошенники пытаются различными психологическими приемами побудить пользователя ввести на поддельной странице свои логин и и пароль, который он использует для доступа к определенному сайту , что позволяет мошенникам получить доступ к аккаунтам и банковским счетам .

Нигерийские письма -это «Мошенничество с предоплатой» .Распространенный вид мошенничества , типа писем счастья , получивший наибольшее развитие с появления массовых рассылок по электронной почте.

Письма названы так потому , что особое распространение этот вид мошенничества получил в Нигерии, причем еще до распространения Интернета , когда такие письма распространялись по обычной почте.Однако нигерийские письма приходят и из других африканских стран , а также с городов с большой нигерийской диаспорой (Лондон, Амстердам, Мадрид , Дубай) Рассылка писем началась в середине 1980-х гг.

2

Как уберечь себя от компьютерных мошенников.

Для того чтобы не попасться на удочку интернет-мошенников ,необходимо выполнять несколько простых правил :

1 Не доверять всем непонятным сообщениям , в которых содержится просьба предоставить личные данные ;

2 Игнорировать спам ;

3 Никогда не сообщать ваши персональные данные личностям в чистоте намерений которых вы не уверены;

4 Быть аккуратными при совершении онлайн-покупок , выбирать для этого сайты , обеспечивающие безопасность сделок и конфиденциальность личных данных ;

5 Необходимо пользоваться многоуровневой системой безопасности ;

6 На все учетные записи нужно ставить пароль;

7 Не отвечайте на сообщения с просьбами о помощи больным людям или животным , и, уж тем более , не перечисляйте им денежные средства. Если вы действительно хотите помочь , то обратитесь к фондам помощи, которые зарегистрированы в РФ ;

8 Ни в коем случае не реагируете на странные сообщения от друзей , в которых они просят перевести им денежные средства . Если уж вы переживаете за своего друга либо близкого человека , то позвоните ему и спросите о том , что случилось по телефону ;

9 Смартфон-тоже под паролем . Обязательно ставьте пин-код на разблокировку , а лучше покупайте телефон со сканером отпечатков пальцев или заменяющей его технологией вроде Face ID;

3

10 Двухфакторная аутентификация . Наверняка вас уже почти все онлайн-сервисы достали принудиловкой на тему двухфакторной аутентификации , но, поверьте, это не пустое дело , Как минимум , есть смысл настроить подтверждение через номер телефона на вход в e-mail, который будет вашей спасательной палочкой для восстановления паролей и учетных записей в социальных сетях и других сайтах;

11 Отдельная или временная почта для сомнительных сайтов;

12 Контролируйте разрешения мобильных приложений

Когда устанавливаете приложения особенно на Android , всегда внимательно читайте , какие именно разрешения оно запрашивает ;

13 Избегайте публичных Wi-Fi сетей. Если все-таки приходится -желательно делать это через VPN-сервисы ;

14 Уникальные пароли для всего. Золотое правило-на каждом сайте у вас должен быть разный пароль. Даже если он будет отличаться на одну букву или цифру это уже значительно снизит возможность взлома ;

15 Никому не сообщайте секретные данные.

Никогда и никому не сообщайте свои пароли , ключевые слова и любые данные по кредитной карте , кроме ееномера . Никакая администрация любых сервисов не будет требовать эти данные . Пароль всегда можно сбросить , современные сайты не хранят его у себя в открытом виде , только в незашифрованном (и расшифровать его нельзя) , а карта -это ваши личные деньги .

Что делать , если вас все же обманули

Если же вдруг вы поняли , что стали жертвой преступления , незамедлительно сообщайте об этом в правоохранительные органы и добивайтесь того, чтобы было возбуждено уголовное дело.

Заключение

В заключении хотелось бы сказать . Остерегайтесь мошенничества . Не видитесь на их уловки . Всегда проверяйте сайты на которых вы совершаете покупки, вводите какие-либо личные данные , чтобы в лишний раз не попасться на уловки мошенников.

Список литературы

1) https://ru.m.wikipedia.org/wiki/