"Мошенничество в сети Интернет"

Мошенничество (или в простонародье – лохотрон) – это обманный способ добычи денежных средств или других ценностей, основанный на доверчивости граждан.

Основные виды интернет-мошенничества

- Удаленная работа
- Фишинг
- Фейковые розыгрыши
- Онлайн-лотереи
- Фарминг
- Интернет-попрошайничество
- Нигерийские письма
- “Волшебные кошелек”
- Бесполезные Курсы
- Продажа Товара, Которого Нет

Удаленная работа

- Схема быстрого обогащения, в которой мошенник предлагает отличную работу с неплохим доходом, идеальные условия работы,бесплатное обучение, работать можно не выходя из дома,как действуют мошенники сначало вам приходит письмо с предложением “хорошей работы например (набор текста, поиск информации, оставление отзывов на какой либо информационный продукт),потом работодатель просит внести некую сумму так сказать в залог работодатель обещает ее вернуть когда вы приступите, но заплатив деньги вы не получите ни работу ни деньги. Есть еще одна вариация этого мошенничества это когда вы выполните какую-либо работу вам просто не выплатят деньги тем самым вы потеряете время и сделаете бесплатную работу мошенника,так же проделав работу могут потребовать внести некую сумму комиссию что бы осуществить вывод ну и в этом случае вы только потеряете деньги.

Фишинг

- Фишинг или выуживание персональной информаци
  следующей схеме. На Вашу электронную почту приходит сообщение о том, что Вам срочно необходимо обновить или передать Ваши персональные данные, в какой-либо системе.

- Например, Вам приходит письмо о том, что произошел какой-то сбой, и данные по Вашей банковской карте повреждены или утеряны и просят прислать их им заново. Сообщение Вам приходит, как правило, с угрозой блокировки счета или аккаунта.

- Еще существует,вишинг (англ. vishing) — это сплав слов «voice» и «phishing», проще говоря, «голосовой фишинг», то есть попытка мошенников обманом выведать у жертвы какие-то конфиденциальные сведения по телефону. Чаще всего это код подтверждения.

Фейковые розыгрыши

Один из видов интернет мошенничества при котором вам приходит смс,письмо на почту,либо сообщение в соц-сетях якобы вы выйграли какой либо приз при том что вы негде не участвовали, чтобы его заполучить нужно либо внести залог либо оплатить доставку, но как тут можно понять внесся этот залог вы просто отдадите деньги и все никто вам не будет ничего высылать да и возможно что вообще розыгрыша не было.

Онлайн-лотереи

- **Онлайн-лотереи** на сегодняшний день также пользуются большим спросом. Вероятность потратить незначительную сумму ради большого выигрыша манит многих пользователей. Каждый из них мечтает о легких деньгах. Мошенники же, в свою очередь, создают сайты с объявлениями о лотерее на выгодных условиях. В объявлениях пишут о том, что выиграть может каждый. Пользователи поддаются обману, потому что затраты предполагаются незначительные, а подарки обещают хорошие.После нескольких розыгрышей появляются проблемы с выводом средств. Сайт успешно закрывается, и мошенники исчезают вместе с деньгами. Для того чтобы испытать фортуну, нужно использовать бесплатные и проверенные сайты. Шансы будут низкими, однако хоты бы будет вероятность победы.

Фарминг

- Процедура скрытного перенаправления жертвы на ложный IP-адрес. Мошенники на компьютеры пользователей распространяют вредоносные программы, направленные на манипулирование файлом HOSTS или смену информации DNS. Пользователь способен получить данные вирусы на собственный компьютер, к примеру, открыв сторонний файл или письмо, посетив неправильный сайт. После того как пользователь переходит на поддельный сайт, ему предлагается ввести свою персональную информацию, которая затем будет использоваться против него. Основными целями для фарминга являются пользователи онлайн-банков или других финансовых систем и валютно-обменных сервисов.

Интернет попрошайки

- Попрошайничество в интернете или развод на деньги это особый вид мошенничества, который происходит в интернет пространстве, идея которого основана на рассылки жалостливых и душещипательных писем большому количеству пользователей, и которое основано на сострадании людей. Чем больше писем будет разослано мошенником, тем больше денег он заработает.Примером этого мошенничества Просьба денег в формате «кто сколько даст» на лечение якобы больного ребёнка. (К письму даже прикладывают фотографии детей) либо помощь больному животному примеров немало, чтобы отличить обманщика от нуждающегося в деньгах человека нужно спросить какие либо документы или что то подтверждающее что реально у ребенка болезнь.

"Нигерийские письма"

Электронное письмо с просьбой о помощи в переводе крупной денежной суммы, из которой 20-30% должно получить лицо, предоставляющее счет. При этом получателю необходимо срочно 6-10 тысяч долларов США отправить по системе электронных платежей по требованию адвоката. Как разновидность используется рассылка о выгодном капиталовложении или устройстве на высокооплачиваемую работу, получении наследства или иных способах быстрого обогащения при условии совершения предварительных платежей.

“Волшебные кошелек”

- Одна из самых старых схем мошенничества. В течении многих лет способ обмана несколько изменялся и усовершенствовался, кроме волшебных кошельков WebMoney и Яндекс.Деньги, в настоящее время активно используются счета в платежной системе Qiwi и даже счета настоящих банковских карт! Однако, сути развода это практически не меняет. Суть мошенничества: жертву развода убеждают в том, что существует некий «волшебный» электронный кошелек в платежной системе Qiwi, WebMoney, Яндекс.Деньги или счет в каком-либо банке, пополнение которого с нужным примечанием к платежу приводит к тому, что через некоторое время кошелек возвращает обратно большую сумму (иногда в разы).Но как можно понять никто не будет вам возвращать деньги.

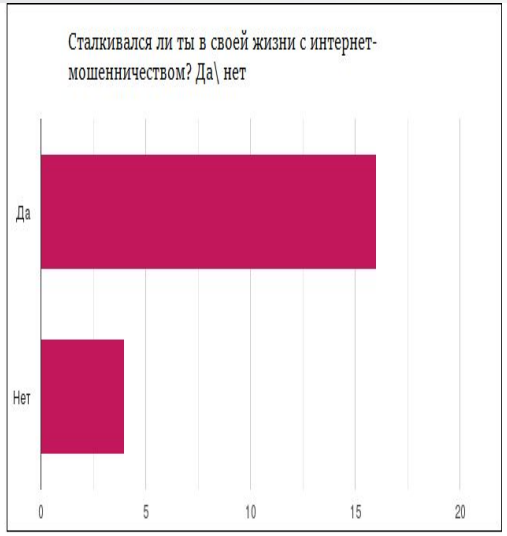
Бесполезные Курсы

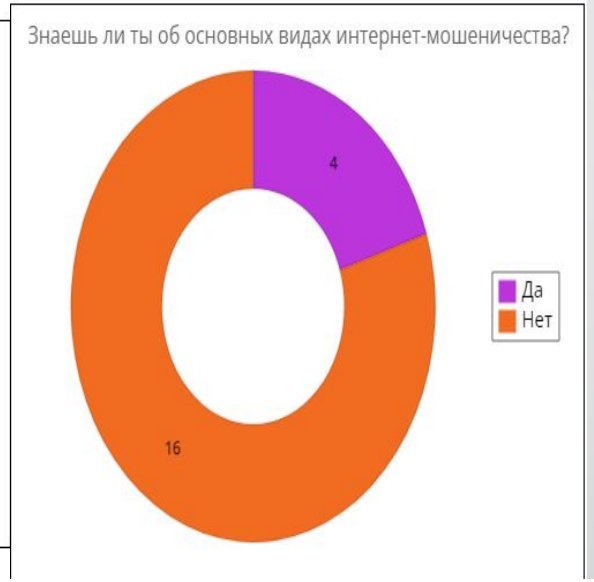
- **Бесполезные Курсы**-Различные бесполезные курсы якобы “как разбогатеть за месяц” чаще всего эти курсы нацелены на выкачку денег на доверчивых пользователях, вы платите за курс, в итоге получаете электронную книгу и рассылку из материалов абсолютно бесполезных или настолько очевидных, какие вы могли бы сами найти бесплатно в блогах, видео роликах книгах,такие курсы можно встретить в соц сетях либо просто в рекламе в браузере так же там могут фигурировать популярные медийные личности.

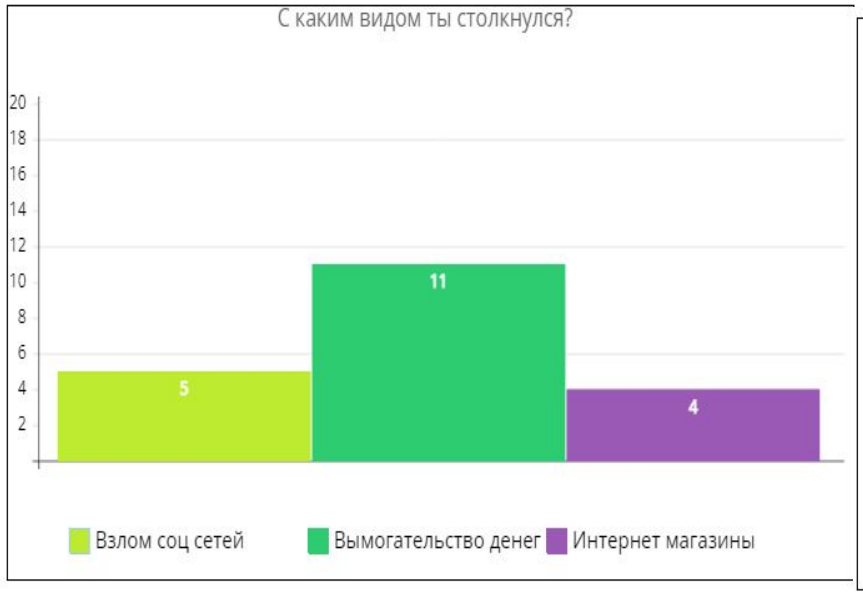
Продажа Товара, Которого Нет

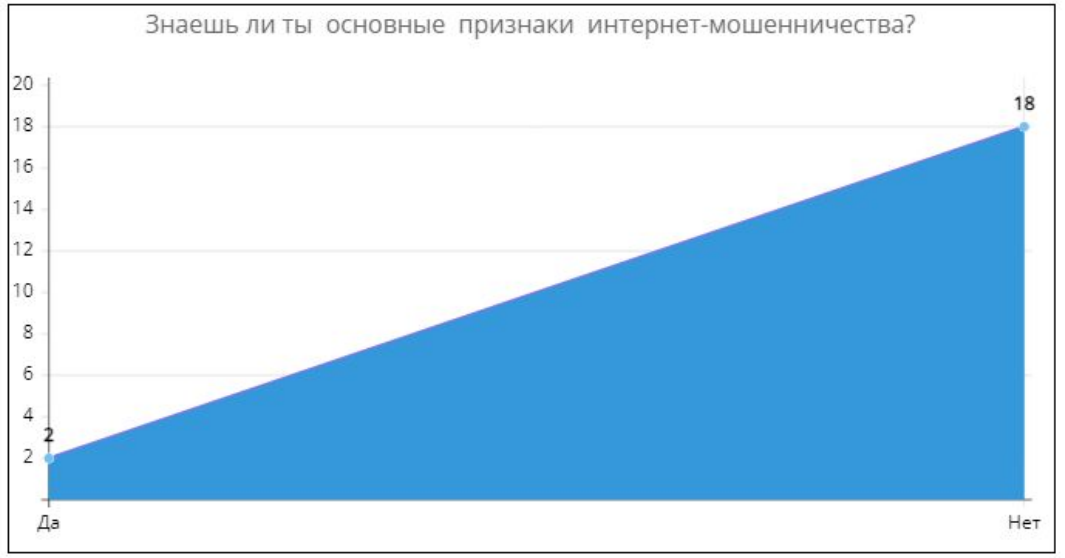
- **Продажа Товара, Которого Нет-**мошенники продают товары в интернет-магазинах по заниженным ценам. вы платите, но никогда не получаете товар, сайт-однодневка через какое-то время пропадает.либо просто оплатите а вам ничего не вышлют. Также мошенники могут потребовать предоплату.

Результат анкетирования









Основные признаки мошенничества в Интернете

- Слишком сладкие обещания, например, вам предлагают получать нереально высокий доход за какую-то ерундовую работу.
- Отсутствие контактных данных на сайте для обратной связи, иногда они есть, но не действуют.
- Сайт, предлагающий Вам высокий дополнительный доход, сам расположен на бесплатном хостинге.
- Заманчивое предложение пришло к Вам на почтовый ящик в виде СПАМа.
- Просьба выслать или перевести на электронный кошелёк деньги за регистрацию, за инструкции, за почтовые расходы и т. п.
- SMS-оплата на короткий номер. В результате с баланса Вашего телефона снимут сумму в несколько сотен.

Рекомендации по защите от интернет-мошенничества

- Не оставляйте незаблокированными смартфоны и компьютеры, не выбрасывайте бумаги и носители данных (жесткие и съемные диски, сим-карты, SD-карты), на которых хранятся пароли.
- Не храните в электронной почте и не выкладывайте в открытый доступ копии документов, удостоверяющих личность: если мошенники взломают вашу почту, они смогут воспользоваться личными данными.
- Перед работой на чужом компьютере перейдите в приватный режим. Если такой возможности нет, очистите кеш и cookie после завершения работы. Либо создайте отдельный профиль в браузере и после завершения работы удалите его.
- Не вводите личную информацию в подозрительные поля, особенно в электронных письмах.
- Не открывайте вложения и не переходите по ссылкам из электронной почты или мессенджеров (Telegram, WhatsApp и т. п.) от сомнительных адресатов. Если адресат кажется вам подозрительным, внесите его в черный список.
- Позвоните по официальному номеру банка или другой организации, от имени которой было отправлено подозрительное письмо, и проверьте информацию.
- Перед онлайн-покупками проверяйте отзывы и рейтинг магазинов, аккаунты продавцов и условия оплаты.
- Пользуйтесь только официальными сайтами торговых площадок, общайтесь с продавцами или покупателями во внутренних чатах, не переходите по ссылкам на другие сайты и мессенджеры.
- Оплачивайте покупки только через известные платежные сервисы и системы (например, VISA, WebMoney, QIWI, ЮMoney, Apple Pay, Google Pay, PayPal, Yandex Pay) — такие платежи надежно защищены.
- Перед вводом логина и пароля на сайте убедитесь, что в адресной строке браузера указан верный адрес. Фишинговые веб-страницы могут иметь адрес, очень похожий на настоящий (например, yanclex.ru вместо yandex.ru).
- Закройте страницу, если в браузере появится сообщение о переходе на подозрительный сайт.
- Подключите двухфакторную аутентификацию для всех своих аккаунтов. Например, в Яндексе это можно сделать с помощью Яндекс Ключа.
- Не отправляйте СМС на короткие номера, не узнав прежде их реальную стоимость! Не оставляйте номер своего мобильного на сомнительных сайтах!
- Всегда проверяйте контактные данные, представленные на сайте компании или частного лица, с которыми планируете иметь дело.
- Проверьте регистрационные данные самого сайта, на какую компанию или частное лицо было зарегистрировано доменное имя и как давно.
- Если вам предлагают работу, то платить должны вам, а не вы. Не отправляйте деньги за регистрацию, за почтовые расходы, как залог за комплектующие, с которыми вам предстоит работать и т. п.
- Почитайте отзывы других пользователей сети об этой компании, сайте или частном лице.

Заключение

Мошенничество, увы, неискоренимо. И на просторах Интернета оно подстерегает нас везде: в электронной почте, социальных сетях, на различных сайтах. С годами злоумышленники изобретают новые приемы, но основные механизмы обмана не меняются. Только сам пользователь может сделать свою жизнь в виртуальном пространстве безопасной. Мы надеемся, что предоставленная информация будет вам полезна.

В исследовательской работе я представил лишь мизерную долю того многообразия видов мошенничества, что есть в Интернете. Если описывать все варианты, то получится целая книга из нескольких томов!

У меня была цель не только перечислить и описать способы отъема денег при помощи Интернета, а донести до вас, что никто просто так в Интернете денег не дает. Не стоит верить в обещания об огромных заработках уже через неделю, реальная работа в Интернете – это действительно работа в полном смысле этого слова. Есть много честных способов заработка при помощи Интернета, они требуют усилий и времени.

Изучив результаты анкетирования, я пришел к выводам, что не каждый знает об опасностях, подстерегающих их на просторах сети Интернет. Моей задачей являлось выявить и устранить этот пробел в знаниях учеников. На мой взгляд, я с ней справился

Не стоит думать, что Интернет – это безопасное место, в котором можно чувствовать себя полностью защищенным. Чтобы максимально обезопасить себя и своих близких от опасностей сети Интернет, нужно постоянно совершенствовать свои знания и навыки в области информационной безопасности в сети Интернет.