Мошенничества в интернете

Кадакин Богдан Игоревич

Россия, Забайкальский край, город Чита, МБОУ «СОШ № 45», 6 класс Б

Аннотация

Цели работы:

Рассмотреть понятие интернет-мошенничества и его особенности; изучить основные виды мошенничества в Интернете; подготовить основные рекомендации «Как не попасть в ловушку мошенников»

Методы и приёмы. Для реализации цели и задач данного исследования использовались следующие методы: теоретические (структурно-функциональный, методы логической интерпретации, моделирования); эмпирические (наблюдение, эксперимент, сравнение, анкетирование, анализ)

Полученные данные. Рассмотрено понятие мошенничества и интернет-мошенничества; прояснена история появления этого феномена; приведены примеры основных видов мошенничества в Интернете; подготовлены основные рекомендации «Как не попасть в ловушку мошенников»

Выводы.

Интернет-мошенничество – это явление, проникшее из реального мира в мир виртуальный. Интернет-мошенничество подчиняется законам виртуального пространства: режиму «Интернет-времени», физической удаленности пользователей друг от друга, анонимности пользователей в Сети. Благодаря данным свойствам, привлечь к ответственности мошенников оказывается весьма затруднительно.

В нашей работе мы рассматривали Интернет-мошенничество как обман, выманивание денег т.п. Интернет-мошенники используют все возможные каналы обмана в Интернете, чтобы найти потенциальные жертвы.

По результатам эмпирического исследования мы выяснили, что большинство пользователей Рунета осведомлены об основных техниках мошенничества, а также встречались с ними во время работы в Интернете, но защититься часто не могут.

Типовыми мошенническими техниками, с которыми встречалось большинство пользователей, являются: спам, взлом в социальных сетях, кража аккаунтов, интернет-кошельки, интернет-магазины и др.

Наше исследование показало, что наибольшую опасность несут в себе:

1) загрузка подозрительных файлов;

2) посещения сайтов, которые не внушают доверия: содержат различные баннеры и

модальные окна. При работе в Интернете следует очень внимательно относиться к загрузке файлов на сайтах, которые не внушают доверия и выглядят подозрительно.

3) Необходимо обеспечить безопасность вашего устройства при помощи антивирусов.

Видов мошенничества много, бороться с ними очень тяжело и почти бесполезно. Побороть мошенников можно давлением со стороны обманутых и с привлечением полиции. Но опять же, собрать всех обманутых очень сложно, а полиции не за что “уцепиться” в уголовном деле. Отчасти это связано и с недостаточной профессиональной подготовкой лиц, осуществляющих выявление и расследование данного вида мошенничества. Помните, что Интернет – это мощный инструмент, с помощью которого злоумышленники выманивают огромные суммы денег у беспечных обывателей.

Мошенничества в интернете

Кадакин Богдан Игоревич

Россия, Забайкальский край, город Чита, МБОУ «СОШ № 45», 6 класс Б

План исследования

Проблема исследования: что такое интернет-мошенничество и как не попасть в ловушку мошенников.

Теоретическая значимость исследования заключается в том, что данная работа может явиться небольшим вкладом в изучение мошенничества в сети Интернет.

Практическая значимость исследования заключается в том, что мною предоставлено мини-пособие по интернет-мошенничеству для учащихся, и они могут им воспользоваться, если подозревают мошенничество. Если знать, с чем имеешь дело, можно и найти способ избежать этого или побороть это.

Новизна работы.

Изучив данную тему, проанализировав результаты анкетирования, мы пришли к выводам, что большая часть учащихся не знает об опасностях интернет-мошенничества. Возникла необходимость устранить этот пробел в знаниях подростков.

Описание **методов**.

Нами использовались аналитические методы и эмпирическое исследование. Обобщение и описание (обобщение полученных статистических и иных данных, описание их влияния на человека, визуальный анализ информационной базы, посвященной мошенничеству и Интернет-мошенничеству в Интернете).

Метод анкетирования и интервьюирования (получение по разработанным анкетам необходимых для анализа и обобщения сведений). Моделирование (создание условной модели деятельности отдельных категорий лиц, участвующих в совершении преступления, а также их поведения в этом процессе). Статистический (при изучении официальной статистки, исторических фактов и т.п.). Сравнение (влияние особенностей деятельности лиц, совершающих мошенничество в сфере компьютерной информации и лиц, попавших в «сети» преступников).

Мошенничества в интернете

Кадакин Богдан Игоревич

Россия, Забайкальский край, город Чита, МБОУ «СОШ № 45», 6 класс Б

Научная статья (описание работы)

Проблема: что такое интернет-мошенничество и как не попасть в ловушку мошенников

Задачи исследования:

1. Рассмотреть суть интернет-мошенничества.
2. Изучить основные виды мошенничества в интернете.
3. Провести анкетирование обучающихся и проанализировать результаты.
4. Подготовить основные рекомендации «Как не попасть в ловушку мошенников».
5. Оформить и презентовать исследование.

Актуальность. Тема интернет-мошенничества актуальна как никогда, так как интернет все больше и больше проникает в нашу с вами жизнь, а “где есть рыба, там есть и рыбаки”. Если еще каких-то пять лет назад больше половины населения России с интернетом и не особо часто сталкивались, то теперь приток людей в сеть огромен.

С этой проблемой пыталось разобраться МВД Российской Федерации, однако продвижения в этом деле нет. Полиция не может найти достаточно фактов, чтобы возбудить уголовное дело. Интернет-преступники разрабатывают новые схемы и способы совершения мошенничества, активно используют достижения научно-технического прогресса в области высоких компьютерных технологий. Поэтому сегодня и возникла необходимость принятия соответствующих адекватных мер, позволяющих эффективно противодействовать фактам мошенничества в интернете.

1. Современное состояние понятия «Интернет-мошенничество»

Для того чтобы изучить явление Интернет-мошенничества, нужно сначала разобраться, что означает это понятие. Определения Интернет-мошенничества в научной литературе (словарях), к сожалению, найти не удалось. Существующее понятие и его признаки появились в рамках виртуального пространства и исходят от понятия «мошенничество».

На одном из Интернет-ресурсов приводится следующее определение: «Термин «мошенничество в Интернете» применим в целом к мошенническим махинациям любого вида, где используются один или несколько элементов Интернета – такие как комнаты в чатах, электронная почта, доски объявлений или веб-сайты – для привлечения потенциальных жертв, проведения мошеннических сделок или для передачи поступлений

от мошенничества в финансовые учреждения или иным лицам, участвующим в таких махинациях» [1].

Таким образом, определение этого термина по смыслу мало чем отличается от юридического определения мошенничества, которое подразумевает «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием» [2].

То есть преступник «втирается» в доверие к лицу, в последующем – пострадавшему, и под «весомым» предлогом выманивает деньги или прочие ценности. Подобная деятельность преследуется законом. Федеральным законом от 29.11.2012 г. №207-ФЗ мошенничество в сфере компьютерной информации определено как норма. В Уголовном кодексе Российской Федерации есть статьи № 158-159, которые предусматривает «ответственность за хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации, или информационно-телекоммуникационных сетей» [3].

2. История Интернет-мошенничества

Первое упоминание о мошенничестве на Руси в законодательстве относится к 1550 году. Судебник Ивана Грозного впервые в ст. 58 упомянул о понятии мошенничества, способом совершения которого и поныне остается обман: «А мошеннику та ж казнь, что и тятю. А кто на обманщике взыщет и доведут на него, ино у ищеи иск пропал. А обманщика, как его ни приведут, ино его бити кнутьем» [4]. За многие века статьи за мошенничество только принимали более строгую юридическую конструкцию.

Современные мошенники совершенствуют старые и изобретают новые приемы обмана.

В условиях стремительного роста информационных технологий и охвата всего населения планеты возможностью выхода в глобальную сеть появился новый вид обмана — мошенничество в интернете. Сегодня он является одним из самых популярных, поскольку существует огромное количество его схем, анонимность и множество способов скрыться, избежать наказания.

История интернет-мошенничества - это новейшая история, которая относится ко всем нам. Сегодня проблема интернет-мошенничеств переросла в масштабы мирового сообщества.

Появление мошенников в интернете можно отсчитывать с 1990 года, когда интернет начал распространяться по миру с огромной скоростью. Хакерство же ведет отсчет с 1960-х годов.

По последним данным, в России ежегодно регистрируют около 15 тысяч различных киберпреступлений и мошенничеств, но всё ещё нет чётких законов, по которым можно судить злоумышленников.

3. Виды интернет-мошенничеств

Давайте проведем краткий экскурс по некоторым видам интернет-мошенничеств.

Фишинг - способ кражи данных, паролей, текстов и всего прочего. Злоумышленники создают сайты-подделки, которые имеют похожие названия и дизайн. Чаще всего подделывают сайты социальных сетей и банковских сайтов, например, вместо sberbank.ru создается сайт с названием srbebank.ru. Скорее всего, вы даже не заметите разницы и попадетесь на обман.

Схема элементарна: вам на e-mail приходит сообщение якобы от вашей платёжной системы, в котором, по какой-либо причине (замораживание счёта, обновление системы) просят зайти в аккаунт по размещённой в письме ссылке. Вам даже могут написать, что потеряли ваш пароль и вам нужно ввести его заново, хотя в реальности такой ситуации просто не может произойти. Итак, письмо – фальшивка. Ссылка, по которой вас просят перейти – тоже. Она ведёт на поддельный сайт мошенников, точь-в-точь похожий на сайт платёжной системы, только у него, во-первых, другой адрес (это первое, что вы должны заметить), а во-вторых, вся вводимая вами на поддельном сайте информация передаётся в руки мошенников, в результате чего они завладеют вашими данными, паролем, после чего могут зайти в ваш настоящий аккаунт и снять с вашего счёта деньги, ограбить вас [5].

“Волшебные” кошельки и Киви-ваучеры.

Есть миф, в котором говорится, что существуют некие волшебные кошельки, “на который отправишь 100,01 рублей, а придет 200,02”. А Киви-ваучеры - способ передачи этих самых денег в платежной системе Visa Qiwi. Запомните! Не существует и не может существовать никаких волшебных кошельков. Это никому не выгодно.

“Вы выиграли айфон, отправьте 500 рублей на номер 8-924-356-72-35 за доставку и телефон ваш!” Именно в таком стиле к вам могут приходить SMS, электронные письма, “выскакивать” реклама на сайтах и т.п. На такие письма не стоит даже обращать внимание, кроме тех случаев, в которых в лотерее или конкурсе вы реально участвовали по собственной инициативе.

Мошенники могут под видом «честных» людей рассказывать о кошельках, которые якобы принадлежат каким-то мошенникам. Вам предлагается разорить их «умножением денег», отомстить за то, что они кого-то обманывают.

Бессмыслица, но и подобным историям кто-то верит, а в результате сам оказывается обманутым. На самом деле никогда не существовало каких-либо секретных счетов, возвращающих вам средства в увеличенном виде. А владельцы кошельков – это сами авторы подобных историй. Они просто стараются привлечь внимание и заставить людей перевести на свои счета деньги.

Почти все «волшебные» кошельки располагаются в системе Яндекс [6].

Суперпрограммы, суперзадачки для быстрого заработка.

Один из самых известных видов мошенничества. Вы покупаете какую-то программку, доступ на сайт или что-то подобное, решаете простые примеры или что-то подобное и зарабатываете деньги. Якобы зарабатываете. Думаете, вы получите заработанные деньги? Нет! Вы не получите ничего.

Продажа несуществующего товара.

В Сети есть очень много различных магазинов, и купить можно все что угодно. Но некоторые магазины размещают товар, как правило, по низкой цене, посетитель видит привлекательные условия, оплачивает, но товар до него не доходит. Он пишет в техническую поддержку сайта, звонит на телефон, но никто ему не отвечает. Сайт, скорее всего, через некоторое время исчезнет из интернета, кошелек на который вы отправили деньги, также будет удален [7].

Попрошайки в Сети.

Вам, наверное, много раз приходили в социальных сетях сообщения, что нужны срочно деньги на операцию, умирает ребенок или что-то в этом роде. Да, не спорю, есть люди, которым действительно нужна помощь, но в большинстве случаев такое объявление создает мошенник и пишет там номер своей банковской карточки. Вы, думаете, что помогаете ребенку вылечить рак, а на самом деле кормите мошенника. В общем, если у вас и возникло желание пожертвовать деньги, то это, конечно, нужно сделать, но не через социальные сети и даже не через волонтеров, а лучше отправлять деньги напрямую на карточку больному. Если номер карточки сказали по телевизору в какой-нибудь телепередаче, то естественно, она правильная [7].

А теперь - самое интересное - псевдоинвестиции. Псевдоинвестиции - это проекты, созданные для заработка мошенников на доверчивости людей. Также псевдоинвестиции называют Хайпами (1. Аббревиатура от High Yield Investment Program — высокодоходный и высокорискованный якобы инвестиционный проект. 2. Шумиха, ажиотаж, крикливая реклама и в том числе обман). Основные признаки хайпа - высокий процент. Многие хайпы предлагают огромный процент, от 3,5% в день, что больше, чем 100% в месяц.

Думаю, многие понимают, что такой заработок нереален. Второй признак - отсутствие реальных контактных данных. Они либо ненастоящие, либо их попросту нет.

Теперь поговорим о механике работы хайпа. На главной странице сайта написано, чем проект якобы занимается и якобы почему проект приносит такие доходы. Это могут быть продажи нефти, поиск звезд или вообще что угодно. Мы платим, к нам должен приходить процент. На самом деле эти проекты ничего не производят, так откуда у них деньги? Все просто. В проект приходят новые люди, вносят свой депозит. Вам дают процент. Если проект больше не платит или сайт вообще исчез, это называется скам (от англ. scam — мошенничество).

Список можно продолжить, но надо знать, что в интернете мошенничество происходит чаще всего под такими предлогами:

1. Заработок.
2. Помощь страждущим.
3. Разблокировка опций программ, приложений.
4. Выгодное приобретение товаров.
5. Розыгрыш ценных призов.

4. Результаты анкетирования обучающихся

Среди учащихся 6-11 классов было проведено анкетирование. Участие приняло 143 человека. В анкете были следующие вопросы:

1. Знаете ли вы, что такое интернет-мошенничество?
2. Сталкивались ли вы с интернет-мошенничеством?
3. Если сталкивались, то с каким видом? В какой форме?
4. Как обезопасить себя от интернет-мошенников?

Из 100 % опрошенных 63 % не сталкивались с интернет-мошенничеством. 37 % сталкивались с разными видами мошенничества. 7 % не знают, что такое интернет-мошенничество. Виды интернет-мошенничеств, с которыми сталкивались школьники:

Кража денег	Взлом в соцсетях	Кража аккаунтов	DoS атаки	Интернет-магазины	Интернет-рулетка	Неясные ответы
8 %	17 %	4 %	2 %	1 %	1 %	12 %

Таким образом, каждый второй учащийся в нашей школе сталкивался с интернет-мошенничеством.

Как избежать мошенничества и обмана в Интернете, как не стать жертвой мошенников, как обезопасить свои виртуальные деньги и личные конфиденциальные данные, как совершать финансовые операции в Сети, не боясь быть обманутым?

Отдельные ученики дали дельные советы по этому поводу. Один из них такой: все сайты вообще изначально считать подозрительными и сомнительными, а потом ищем доказательства и факты их искренности и честности.

5. Основные рекомендации «Как не попасть в ловушку мошенников»

Не стать жертвой финансовых махинаций можно, для этого нужно просто выполнять определённые правила и применять меры безопасности.

- Прежде чем выходить в Интернет, установите на компьютер хорошую антивирусную программу. Следите за тем, чтобы антивирусные базы все время были актуальными, и помните, что в мире ежечасно появляется несколько новых вирусов.
- Будьте максимально бдительны и осторожны при посещении неизвестных страниц в Интернете. Сегодня широко распространены шпионы и вирусы, для заражения которыми достаточно просто зайти на определенную веб-страницу.
- После скачивания из Интернета файлов, архивов и т. п. надо сразу же проверить их антивирусной программой, и только после этого запускать на выполнение, распаковывать и т. д. Помните, что многие вредоносные программы распространяются в виде исполняемых файлов либо архивов.
- Старайтесь не открывать сайты платежных систем по ссылке (например, в письмах). Обязательно проверяйте, какой url (адрес, указывающий путь к интернет ресурсу, на котором размещены различные виды файлов) стоит в адресной строке или посмотрите в свойствах ссылки, куда она ведет. Вы можете попасть на сайт-обманку, внешне очень похожий, практически неотличимый от сайта платежной системы. Расчет в этом случае на то, что вы введете на таком сайте свои данные, и они станут известны мошенникам.
- Никогда никому не сообщайте ваши пароли. Вводить пароли можно и нужно только на сайтах самих платежных систем, но никак не на других ресурсах. Избегай стандартных паролей! Многие пользователи часто совершают одну и ту же ошибку, пользуясь стандартными, шаблонными паролями. Один из самых характерных примеров – когда пароль совпадает с логином. Подобрать такой пароль элементарно, а дальше злоумышленник будет действовать в зависимости от того, к чему относится данный пароль. Если это кредитная карта или банковский счет, управлять которым можно через Интернет – все деньги с этого счета исчезнут моментально.

- Если при посещении различных ресурсов в Интернете (форумы, страницы регистрации, и т. д.) требуется оставить о себе некоторые данные, то они должны содержать минимум сведений. В частности, никогда и никому не сообщайте свои паспортные данные, домашний адрес, различные пароли и т. п. Несмотря на то, что владельцы и руководители многих Интернет-ресурсов гарантируют полную конфиденциальность, не будьте наивными: если кому-то надо получить эту информацию, он ее получит, и вполне может использовать для шантажа, вымогательства и т. п.
- Не храните файлы с секретной информацией на доступных или недостаточно надежных носителях информации. Всегда делайте несколько копий таких файлов на разных носителях.
- Если вам предлагают удаленную работу и при этом просят оплатить регистрационный взнос, в качестве гарантии, за пересылку данных и тому подобное — не попадайтесь на эту ловушку. Настоящие работодатели никогда не просят денег с соискателей - они сами платят за работу.
- Предложения в духе «вышлите туда-то небольшую сумму и вскоре вы будете завалены деньгами» - это предложения от участников финансовых пирамид. Не верьте таким предложениям, в пирамидах выигрывают только их создатели. В любом случае, обоснование платежа значения не имеет – важно помнить одно: если в любом поступившем из Интернета предложении, рекламе и т. п. содержится требование или просьба перевести деньги – это однозначно мошенничество.
- Письма о проблемах с вашим счетом в какой-либо платежной системе, требующие перехода на сайт и каких-либо действий от вас, отправляйте в корзину, не глядя. Техническая поддержка платежных систем никогда не рассылает таких писем.
- Не давайте деньги в кредит неизвестным вам лицам - в интернете не существует гарантий возврата кредитов.
- В 99% случаев платежи, которые вы делаете онлайн, отменить нельзя. Поэтому семь раз подумайте, прежде чем один раз оплатить товар или услугу [8].

Помимо перечисленных правил безопасности, при работе в Интернете руководствуйтесь нормами и принципами, которые диктуется здравым смыслом и элементарной осторожностью.

Заключение.

Интернет-мошенничество – это явление, проникшее из реального мира в мир виртуальный. Интернет-мошенничество подчиняется законам виртуального пространства:

режиму «Интернет-времени», физической удаленности пользователей друг от друга, анонимности пользователей в Сети. Благодаря данным свойствам, привлечь к ответственности мошенников оказывается весьма затруднительно.

В нашей работе мы рассматривали Интернет-мошенничество как обман, выманивание денег т.п. Интернет-мошенники используют все возможные каналы обмана в Интернете, чтобы найти потенциальные жертвы.

По результатам эмпирического исследования мы выяснили, что большинство пользователей Рунета осведомлены об основных техниках мошенничества, а также встречались с ними во время работы в Интернете, но защититься часто не могут.

Типовыми мошенническими техниками, с которыми встречалось большинство пользователей, являются: спам, взлом в социальных сетях, кража аккаунтов, интернет-кошельки, интернет-магазины и др.

Полученная в результате исследования информация дает некоторое представление о феномене Интернет-мошенничества, которое учит пользователя быть внимательным во время работы в Интернете.

Советуем пользователям расширять знания касательно возможностей Интернета, а главное, особенностей виртуального пространства, в силу которых неосведомленный пользователь оказывается уязвимым перед мошенниками.

Главная причина широкого распространения мошенничества в Интернете – это безнаказанность мошенников. Правоохранительным органам необходимо законодательно урегулировать меры ответственности за виртуальное мошенничество, вводить больше органов по контролю за безопасностью в Интернете и практиковать наказания Интернет-мошенников.

Наше исследование показало, что наибольшую опасность несут в себе:

1) загрузка подозрительных файлов;

2) посещения сайтов, которые не внушают доверия: содержат различные баннеры и модальные окна. При работе в Интернете следует очень внимательно относиться к загрузке файлов на сайтах, которые не внушают доверия и выглядят подозрительно.

3) Необходимо обеспечить безопасность вашего устройства при помощи антивирусов.

Одной из популярных причин краж личных данных является, в первую очередь, взлом, совершенный вследствие неосторожного хранения паролей.

Также стоит ознакомиться с различными методами защиты, как они работают и на что влияют. Различные защиты от фишинга существуют во всех популярных браузерах.

Итак, хочется верить, что наше исследование поможет учащимся избежать попадания в

мошеннические сети, хитроумно расставленные по всему Интернету. Мы познакомили с материалами, из которых можно узнать, где и чего следует опасаться, как проверить заманчивое предложение о сотрудничестве, и почему ни в коем случае нельзя переводить деньги неизвестным лицам (если, конечно, вы не хотите оказать им благотворительную помощь). Помните, что Интернет – это мощный инструмент, с помощью которого злоумышленники выманивают огромные суммы денег у беспечных обывателей.

Литература

1. Мошенничество в Интернете/ Государственные Департамент США [Электронный ресурс]: На сайте содержится информация о текущей внешней политике и жизни в Соединенных Штатах Америки. – Режим доступа: http://www.infousa.ru/information/internet_fraud.htm

2. Мошенничество. Статья 159 Уголовного кодекса РФ/ Большой юридический словарь. 3-е изд., доп. и перераб. / Под ред. проф. А. Я. Сухарева. — М.: ИНФРА- М, 2007. [Электронный ресурс]: Яндекс. Словари. - Режим доступа: http://slovari.yandex.ru/dict/jurid

3. В редакции Федерального закона Российской Федерации от 8 декабря 2003 г. № 162-ФЗ с дополнениями, внесенными Федеральным законом Российской Федерации от 27.12.2009 N 377-ФЗ, Федеральным законом Российской Федерации от 7 марта 2011 г. N 26-ФЗ, Федеральным законом РФ от 7 декабря 2011 года № 420-ФЗ, Федеральным законом Российской Федерации от 29 ноября 2012 г. N 207-ФЗ.

4. Российское Законодательство X-XX вв. в 9 т.- М., 1985. - Т.2.- 270 с.

5. https://ru.wikipedia.org/wiki/Фишинг

6. http://oliaus.ru/prostoj-zarabotok/volshebnyj-koshelek-yandeks-dengi-otzyvy/

7. http://dyly.ru/moshennichestvo-v-internete-novye-vidy-i-sxemy/

8. Гладкий А.А. Мошенничество в Интернете. Методы удаленного выманивания денег, и как не стать жертвой злоумышленников. Электронный ресурс: http://e-libra.su/read/363830-moshennichestvo-v-internetemetodi-udalennogo-vimanivaniya-deneg-i-kak-ne-stat-jertvoy-zloumishlennik.html