УДК 004

МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ

Гренева К.В.,
Студентка
Магнитогорский государственный технический университет им. Г.И. Носова,
г. Магнитогорск, Россия

Мухина О.О.,
Студентка
Магнитогорский государственный технический университет им. Г.И. Носова,
г. Магнитогорск, Россия

Аннотация
В этой статье мы рассмотрели различные способы мошенничества в сети Интернет. Основной целью нашего исследования стало выявление видов мошенничества и правил, которые помогут не попасться на уловки злоумышленников.
Ключевые слова: Мошенничество, Интернет, злоумышленники, обман, вымогательство.

FRAUD ON THE INTERNET

Greneva K.V.,
Student
Nosov Magnitogorsk State Technical University,
Magnitogorsk, Russia

Mukhina Olga Olegovna
Student
Nosov Magnitogorsk State Technical University,

Magnitogorsk, Russia

Annotation

In this article we have considered various ways of scams in the Internet. The main aim of our study was to identify the types of fraud and rules that will help you not to fall for the tricks of criminals.

Keywords: Fraud, Internet criminals, deception, extortion.

В современном мире большинство людей учатся, работают, развлекаются, знакомятся, а также совершают покупки в сети Интернет. Использование Интернета для человека стало гораздо удобней, так как оно занимает намного меньше времени, а выбор товаров и услуг намного больше. В нашей статье мы хотим рассказать, какие виды мошенничества существуют и как обезопасить себя от них.

Для начала разберем, что такое мошенничество. Мошенничество – это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием [5].

Основываясь на человеческих стереотипах и психологии злоумышленники точно знают, как воздействовать на человека и какие предложения будут пользоваться спросом. На желании человека приобрести что-либо или получить ту или иную услугу за наименьшую стоимость совершается большинство обманов в сети Интернет. Также, чтобы нанести урон по затратам людей, мошенники пользуются их доверчивостью и добродушием, создавая сайты со сбором денег на операции детям и взрослым, на помощь бездомным животным и прочее. Со стороны закона все аферы являются уголовно-наказуемым деянием, и подходят под статью 159 УК РФ. Мошенники наказываются штрафом, обязательными работами, исправительными работами, ограничением свободы, принудительными работами, арестом, либо лишением свободы.

Рассмотрим основные виды Интернет-мошенничества:

1) Фишинг. Данный вид мошенничества направлен на получение у пользователя секретных личных данных. Пользователь получает электронное письмо от «известной» компании, в котором ему предлагается осуществить то или иное действие:

a) предоставить данные для входа на сайт, ввиду проблем на сервере или сбоем системы;

b) активировать свою учетную запись путем отправки SMS на короткий номер, за которое пользователь заплатит крупную сумму;

c) стать участником конкурса, заполнив анкету со всеми своими данными (паспорт, кредитка и пр.);

d) ввести на предоставленном по ссылке сайте свои данные, которые мошенники легко могут скопировать.

2) Кликфрод — один из видов сетевого мошенничества, представляющий собой умышленные клики на рекламную ссылку, как ручным, так и автоматическим способом. Кликнув на рекламу, человек переходит на вредоносный сайт, где для его закрытия необходимо заплатить определенную сумму.

3) Интернет-магазины. Большинство людей предпочитают совершать различные покупки в режиме онлайн, так как стоимость товара намного ниже, чем в магазине. Злоумышленники просят внести предоплату путем перечисления средств на электронный кошелек и осуществить заказ, который будет обработан в течение нескольких дней. Но спустя некоторое время этот интернет-магазин может исчезнуть, и клиент не получит товара, и не вернет своих денег.

4) Обманы и попрошайки в Интернет-чатах. В Интернете существует множество различных сайтов-знакомств, на которых люди ищут свою любовь. Знакомясь и переписываясь с человеком, злоумышленник узнает максимум информации и постепенно ненавязчиво просит помочь с деньгами, а затем прекращает общение и удаляет аккаунт.

5) Волшебные кошельки. Мошенники просят отправить на электронный кошелек или банковскую карту определённую сумму денег, с условием, что вы получите сумму больше той, которую отправляли (например, в два раза). После

этого деньги уходят навсегда или взамен приходит «приманка», то есть увеличенная сумма, с расчётом на то, что человек решится повторить перевод с наибольшим количеством денег, которые уже точно не вернутся.

6) Удалённая работа. Злоумышленник отправляет письмо с предложением работы на дому, где подробно описывает суть работы, указывает контактные данные и просит перейти на определенный сайт. Перейдя на этот сайт, человека просят ввести свои личные данные (паспорт, номер банковской карты и т.д.) и перевести небольшую сумму в виде залога. После того, как злоумышленник получит деньги, на связь он больше не выходит. Вы не получаете ни работы, ни своих денег [4].

Для того, чтобы обезопасить себя от мошенничества в Интернете, необходимо следовать некоторым правилам:

1. Регулярно проверяйте выписки с банковского счета.
2. Открывайте вложения электронной почты с осторожностью. Тщательно проверьте имя отправителя, особенно если оно вам неизвестно, прежде чем открыть вложение электронной почты.
3. Используйте надежные пароли. Чем надежнее ваш пароль доступа к услугам (для каждой услуги рекомендуется создавать разные пароли), тем труднее злоумышленнику получить ваши данные. Наилучшие пароли — это комбинации букв и чисел разного регистра длиной не менее восьми символов.
4. Ознакомьтесь с политикой конфиденциальности сайта. Если веб-сайт запрашивает какую-либо конфиденциальную или личную информацию, внимательно ознакомьтесь с текстом политики конфиденциальности. Если вы не доверяете веб-сайту, воздержитесь от ввода данных.
5. Никому не сообщайте PIN-коды
6. Запишите сведения о поставщиках устройств и программ. Если вы приобрели продукт в интернет-магазине, запишите адрес и номер телефона продавца, особенно если это небольшая компания или индивидуальный розничный продавец. Электронного адреса может оказаться недостаточно; если

компания окажется ненастоящей, эта информация может вам вернуть свои деньги.

7. По возможности выбирайте сайты, передающие данные в зашифрованном виде. Если адрес веб-сайта начинается с «https», это свидетельствует о том, что он прошел независимую проверку подлинности. Символ замка в адресной строке означает, что все операции входа в систему и оплаты на данном веб-сайте являются безопасными.

8. Не принимайте и не осуществляйте денежные переводы от имени другого лица. Если вы получили несанкционированное письмо с просьбой зачислить деньги на ваш счет, существует большая вероятность того, что эти деньги были украдены с других банковских счетов. Соглашаясь, вы не только становитесь участником преступления, но и предоставляете злоумышленникам доступ к своему банковскому счету.

9. Существенно заниженная цена на товар должна вас насторожить. Постарайтесь найти в сети аналогичную продукцию и сравните стоимость.

10. При перечисление денег на лечение человека уточните данные организации и расчетные счета, по которым предлагается внести пожертвование. Обычно, сбором занимаются группы активистов, которые по первому требованию предоставляют полную информацию о больном, стоимости и месте его лечения, и о том, сколько средств уже собрано.

Если вы стали жертвой мошенников и подверглись их аферам, вам необходимо немедленно обратиться в правоохранительные органы. В каждом регионе есть специальный отдел МВД, который расследует преступления в сети Интернет. Постарайтесь запомнить и рассказать максимум информации о мошенничестве – адрес сайта, расчетный счет, адрес электронной почты, номер электронного кошелька и т.д., тогда шанс на нахождение злоумышленника и возвращение ваших денежных средств будет гораздо выше.

Будьте внимательны и осторожны при использовании сети Интернет! Не отправляйте денежные средства незнакомым лицам, тщательно проверяйте информацию и остерегайтесь нежелательных сайтов.

Библиографический список:

1. Chernova E. V., Bobrova I. I., Movchan I. N., Trofimov E. G., Zerkina N. N., Chusavitina G. N. Teachers training for prevention of pupils deviant behavior in ICT/ В сборнике: Proceedings of the 2016 Conference on Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSSM 2016) 2016. С. 294-297

2. Karmanova E. V., EfimovaI Yu., Guseva E. N., Kostina N. N., Saveleva L. A., Bobrova I. I. modeling of students' competency development in the higher education distant learning system/ в сборнике: Proceedings of the 2016 Conference on Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSSM 2016) 2016.С. 308-315

3. Макашова В. Н., Чернова Е. В., Боброва И. И. Современные аспекты распространения киберэкстремистской идеологии в молодежной ИТ-среде/Фундаментальные исследования. 2014. № 12-6. С. 1294-1297

4. Мошенничество в Интернете [Электронный ресурс]. URL: https://ru.wikibooks.org/wiki/%D0%9C%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE_%D0%B2_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5

5. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 26.08.2017): принят Гос. Думой 24 мая 1996 г. : одобр. Советом Федерации 5июня 1996 г., ст. 159