СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ»
СТАТЬИ

УДК 004.056.5:34

АНАЛИЗ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Дорожкин И.В., ст. гр. 173602; Шарафанович Я.О., ст. гр. 173602

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Пулко Т.А. – канд. техн. наук

Аннотация. Использование компьютерных и информационных технологий в различных сферах жизни общества становится обязательным атрибутом для достижения максимальной эффективности данной сферы. В связи с этим сфера информационных технологий становится всё более популярной для различного рода мошенников и преступников. Через информационные технологии проходит значительный поток финансов и различной личной информации. Мошенники пользуются этим, пытаясь различными способами выкрасть деньги или же личную информацию пользователя, чтобы в дальнейшем использовать её в своих целях. В данной статье рассмотрены различные источники угроз и виды преступлений в сфере информационных технологий. Основными выводами являются меры предосторожности, способные уберечь пользователя от потенциальных опасностей деятельности правонарушителей.

Ключевые слова: информационные технологии, киберпреступность, фишинг, кардинг, информатизация, компьютерная информация, вирус, уголовный кодекс.

Одним из самых распространенных видов правонарушений в сфере информационных технологий являются разного рода мошеннические схемы. Разделить такие преступления на отдельные категории довольно сложно, так как встречается довольно много пересечений. Однако в целом можно выделить следующие виды киберпреступлений:

– финансово-ориентированные преступления;

– киберпреступления, связанные со вторжением в личную жизнь;

– социальные и политически мотивированные киберпреступления.

Существует множество способов и схем, с помощью которых мошенники получают доступ к персональным данным пользователя, такими как пароли, данные банковских карт и многое другое. Наиболее часто встречающимися являются:

– фишинг;

– кардинг;

– “нигерийские” письма;

– кибервымогательство;

– взлом аккаунтов социальных сетей.

Рассмотрим каждый вид мошенничества подробнее.

Фишинг — вид интернет-мошенничества, который заключается в “выуживании” конфиденциальных данных у пользователя. Спецификой данного метода является то, что жертва мошенничества предоставляет свои данные добровольно. Для этого преступники используют специальные фишинговые сайты, email-рассылку, нацеленную рекламу. Как правило, мошенники маскируются под известные компании, социальные сети или сервисы электронной почты.

Примерами фишинга могут быть:

– рассылка поддельных сообщений с просьбой подтвердить логин или пароль;

– фишинговые схемы при проведении интернет-аукционов, при этом товары выставляются на продажу на легальном сайте, однако средства перечисляются через поддельный web-узел;

– фиктивные благотворительные организации, обращающиеся с просьбой о пожертвовании денежных средств на спасение больного ребёнка или вымирающего вида животного;

– создание фишинговых интернет-магазинов, где товары продаются по очень низким ценам либо с большими скидками, что привлекает посетителей, и они предоставляют данные своих банковский карт не подозревая, что становятся жертвами мошенничества[3].

Самым известным случаем, когда знаменитый человек стал жертвой фишинга, стал взлом хаккерами почты главы избирательного штаба предвыборной компании Хилари Клинтон Джона Подесты. Злоумышленники прислали ему письмо, что его пароль от почтового ящика Google был взломан и его стоит сменить. Политик перешёл по указанной ссылке на поддельный сайт и сменил там пароль, и, таким образом, передал данные своей почты хаккерам. Как результат, в интернет попали сотни его личных писем, многие из которых оказались компрометирующими. Из-за данного инцидента рейтинг Клинтон упал, и она проиграла выборы Дональду Трампу.

Кардинг — сфера киберпреступности, которая напрямую взаимодействует с деньгами обычных законопослушных граждан. При данном виде мошенничества производится операция с использованием платёжной карты, не инициированная её держателем[4]. Кража денежных средств — одна из самых страшных опасностей для любого человека, но есть факторы, из-за которых на сферу кардинга стоит обращать особое внимание.

В основном “кардеры” осуществляют свою деятельность на территории США или Европы. Это обусловлено тем, что уголовные сроки за такие преступления в Америке или Европе находятся в пределах 2-5 лет тюремного заключения, в то время как в странах СНГ этот срок может доходить и до десяти лет заключения. Также работа с русскоязычными счетами сопряжена с множествами проблем, ведь данные системы защиты сильно опережают западные. Однако не стоит отметать эту угрозу, ведь хоть для большинства кардеров присуща работа не в нашей стране, некоторые всё таки продолжают работать в СНГ. А если речь идёт о более мелких преступниках, то и подавно, ведь внимания к своей персоне они привлекают куда меньше.

Кардеры используют ряд методов для кражи платёжных средств:

фишинг, как и описывалось ранее, создаётся поддельный сайт, на котором пользователь должен ввести свои платёжные данные;

взлом баз данных мелких предприятий, например магазинов, сервера которых плохо защищены, а иногда и самовольная продажа банковских данных самой компанией или её сотрудниками;

После получения данных карты, злоумышленники либо просто снимают с неё все сбережения, либо же продают карту на специальных магазинах, называемых “кардер-шопами”.

Но опасность кардинга состоит еще и в том, что обычный пользователь может быть привлечён к уголовной ответственности. Так от кардеров вам может прийти сообщение, где будет предлагаться с помощью некоторого сервиса оплачивать такси или заказывать еду по очень выгодной цене, нужно лишь сбросить дельцу указанную сумму и пользоваться услугами такси или доставки через данный сервис. Выполнив такие действия, вы вполне можете получить повестку в суд по уголовной статье в роли соучастника, ведь деньги, которые вы выслали мошенникам были положены на украденную карту и именно с неё оплачивались все счета данного сервиса. Подобные схемы возможны и при оплате перелётов, туров и других дорогостоящих услуг.

“Нигерийские” письма — вид мошенничества, основанный на массовой рассылке электронных писем. Своё название письма получили из-за того, что данный вид мошенничества получил наибольшее распространение в Нигерии, причём ещё до распространения интернета, когда письма распространялись по обычной почте. Однако такого рода письма могут приходить и из других стран, но всё же в основном из стран Африки, например, Анголы, Того, Гамбии, Сомали и других.

Схема подобного рода мошенничества заключается в следующем:

В сети рассылается тысячи электронных писем с разного рода предложениями и услугами.

В случае, если мошенники получают от адресата ответное письмо, выражающее некоторую заинтересованность, преступники вступают в диалог с адресатом, пытаясь получить от него необходимые данные: счета, пароли, непосредственно деньги и тому подобное.

Переписка продолжается до тех пор, пока жертва не будет сама готова перечислить деньги мошенникам.

После перечисления денег возможны два сценария развития событий: если мошенники понимают, что их “клиент” безусловно верит им, то под каким-либо предлогом сообщают ему, что перечисленных им средств недостаточно, и необходимо выслать ещё; либо же переписка мошенников с их жертвой резко обрывается, а счёт, на который были переведены нужные средства моментально закрывается.

В настоящее время наиболее распространенными являются следующие сценарии мошеннических схем:

Адресату посылается письмо будто бы от представителя погибшего очень дальнего родственника жертвы. По заверению адресанта, жертве полагается крупное наследство, а для его перевода просят у него либо рассказать всю информацию о его банковском счёте, либо отправить некоторую сумму, чтобы разморозить счёт с наследством.

Жертве сообщается о выигрыше в лотерею или каком-нибудь проводимом розыгрыше. Например, адресату может сообщаться о выигранном новом смартфоне, могут даже высылаться

фотографии выигранного товара, что ещё больше подогревает интерес жертвы. Но для пересылки выигрыша требуется либо заплатить налог, либо произвести оплату посылки в город жертвы.

Высылаются письма об очень выгодной вакансии где-нибудь за рубежом, но для трудоустройства первоначально необходимо оплатить счета за визу, разрешения на проживание и работу.

В социальных сетях могут приходить письма, где якобы африканская девушка или парень, в зависимости от пола жертвы, которая представляется принцессой небольшого государства или наследницей крупного состояния. Она сообщает, что находится в лагере беженцев в другой африканской стране, из-за того, что на её родине произошел переворот. Девушка предлагает на ней жениться и унаследовать всё её состояние, но для этого ей нужны деньги, чтобы вернуться на родину, когда обстановка в стране стабилизируется.

Стоит отметить, что некоторые пользователи, понимая, что их хотят обмануть, отвечают мошенникам из любопытства, интересуясь, что им могут предложить и как будут пытаться обманывать. Однако, этого делать не стоит. Причиной этого является то, что когда адресат отвечает на такое сообщение, то автоматически заносит себя в базу данных мошенников. Это может обернуться, как минимум, засоренной почтой, а, как максимум, на компьютер жертвы может выслаться опасный вирус, после чего не составит труда получить доступ к личным данным пользователя[5].

Кибервымогательство — вымогательство с использованием интернета. Как правило, при таком способе вымогательства пользователь получает сообщение, в котором говорится, что злоумышленники получили личную информацию и угрожают выложить её в открытый доступ.

Хаккеры могут проводить кибератаки на различные серверы и компании, при этом условием неразглашения украденной ими информации является перевод денежных средств на указанный счёт.

Кибервымогательство связано с наличием прямых или косвенных угроз вторжения в личную жизнь, кражи личных данных, которые могут содержать информацию о переписке в социальных сетях, голосовых сообщений, данных используемых приложений, историю браузера и поисковых запросов, а также удалённый доступ к рабочему столу персонального компьютера и многое другое. Все эти действия способны нанести существенный моральный вред потенциальной жертве.

В случае с несогласием выдвинутых требований, злоумышленники угрожают распространением личных фотографий дискредитирующего характера и других данных, относящихся к частной жизни, что может привести к разрушению прав человека, нарушению деловой репутации, а также привести к эмоциональному стрессу и другим видам морального вреда.

Преступники используют ряд различных схем и программ с целью вымогательства. Также злоумышленники могут использовать шифрование данных с целью вымогательства денег за выдачу ключей расшифровки. Вирусы, запущенные вымогателем, шифруют данные на компьютере пользователя, из-за чего эти данные перестают быть доступными для пользователя, и требуют выкуп за возможность восстановить доступ к ним. Проникнув в корпоративную сеть, вымогатели способны блокировать сразу большое количество компьютеров пользователей данной компании. При отказе от уплаты выкупа, зашифрованные данные могут остаться недоступными для пострадавшего навсегда[6].

Взлом социальных сетей и дальнейшее вымогательство денег — один из самых распространенных и часто встречающихся способов мошенничества. Такая популярность данного метода вытекает из ненадёжности большинства социальных сетей — их очень легко взломать. При этом, необязательно быть специалистом в области информационных технологий. На просторах интернета есть куча информации, как взломать ту или иную социальную сеть, поэтому справиться с этой задачей может даже абсолютно неподготовленный человек, никак не связанный с хакерством.

Войдя в чужой аккаунт, злоумышленник для разных целей, например, кража личной информации, переписок и дальнейший шантаж жертвы. Однако наиболее популярным преступлением является рассылка “друзьям” пользователя сообщений с просьбой о долге.

Злоумышленник, зайдя в чужой профиль, пишет друзьям жертвы, якобы у него закончились деньги, и просит одолжить некоторою сумму денежных средств до определенного срока. Если жертва соглашается помочь, то мошенник либо просит предоставить данные банковских реквизитов, либо присылает номер счёта, на который нужно перевести необходимую денежную сумму.

При пользовании новейшими информационными технологиями необходимо осознавать риски, которые могут возникать при их эксплуатации. Прежде всего это угроза утечки конфиденциальных данных, а также заражение устройства вредоносными программами. Чаще всего это происходит из-за установки на устройство вредоносного программного обеспечения,

целенаправленных действий злоумышленника или неосторожности и несоблюдении правил безопасности личных данных.

В наши дни люди часто хранят всю свою личную информацию на компьютерах и телефонах. Если пользователь устанавливает на своё устройство вредоносное ПО, это может привести к обширной утечке данных и многим другим последствиям, например, краже персональных данных.

Кража персональных данных зачастую происходит с целью дальнейшей подмены личности или же кражи финансовой личности. При данном виде кражи преступник выдаёт чужую личность за свою в финансовых целях. Это может быть взятие кредита на чужое имя, осуществление покупок в интернет-магазинах или же получение информации о медицинском и финансовом положении жертвы.

Другой формой вторжения в личную жизнь с помощью информационных технологий может стать шпионаж. Шпионаж может проявляться по-разному: от взлома устройств пользователя и прочтению его личных данных и переписок, вплоть до полноценной слежки и нелегального отслеживания всей жизни жертвы.

Преступники используют различные методы хищения данных, наиболее популярные методы представлены ниже:

Отслеживание нажатия клавиш. За отслеживание отвечают специальные программы, которые определяют, какие комбинации клавиш пользователь использует чаще всего. Данный способ обычно используется для выявления паролей от банковских счетов и других сервисов.

Подбор паролей. Если преступникам известна некоторая личная информация о пользователе, например имя, фамилия, год рождения и тому подобное, то они могут попытаться подобрать пароль исходя из этих знаний, используя разные комбинации таких данных в качестве пароля. Данный способ является наиболее простым и лёгким, но при этом срабатывает крайне редко, так как очень малое количество людей используют личную информацию в качестве пароля от чего-либо. Тем не менее, такие люди встречаются, и мошенники могут использовать этот факт.

Backdoor программы — программы, позволяющие преступникам входить в систему компьютера пользователя или выходить из нее. Такие программы помогают злоумышленникам удаленно контролировать деятельность пользователя, а также просматривать личную информацию, в том числе пароли.

Обман сети. Злоумышленники могут создавать ложные сети, например Wi-Fi. Правонарушитель может ждать свою жертву в общественном месте, где создаст сеть с названием этого места. Когда пользователь подключится к такой сети, то преступник сможет отслеживать его действия в интернете, а также просматривать файлы вашего устройства или даже установить на него вирус или другую зловредную программу.

Сейчас абсолютно любой человек может стать жертвой киберпреступников, хотя многим до сих пор сложно представить, что кто-то может всерьёз интересоваться их личными данными, кому-то может быть интересно и важно всё знать об их личности и даже шпионить за ними. Из-за этого многие люди могут не использовать все меры предосторожности при использовании современных информационных технологий[7].

Некоторые типы киберпреступлений направлены на изменения настроений в политической среде или нанесение намеренного вреда или снижения влияния отдельных личностей или группы людей. Преступления на почве ненависти по отношению к личности или группе людей обычно совершаются на основе гендерной, расовой, религиозной, национальной принадлежности сексуальной ориентации и других признаков.

Примерами таких киберпреступлений являются домогательства и рассылка оскорбительных сообщений, и распространение ложных новостей, касающихся определенной группы лиц. Анонимность и легкодоступность интернета серьезно затрудняют борьбу с преступлениями на почве ненависти.

Группировки экстремистской и террористической направленности все чаще используют киберпространство для запугивания, распространения пропаганды и иногда нанесенияя вреда IT-инфраструктурам.

Зачастую объектами таких киберпреступлений могут стать крупные корпорации или даже целые государства.

Примером атаки на крупную корпорацию может стать взлом одной из самой популярной социальной сети мира Facebook в 2020 году. В результате хакерской атаки, в сеть утекли данные более чем 260 миллионов пользователей. После таких утечек суд обязал компании выплатить штраф в размере 5 миллиардов долларов, что является крупнейшим штрафом за утечки данных в истории.

Если говорить о преступлениях в отношении целого государства, то примером является взлом и получение доступа к 269 Гб секретных данных правоохранительных органов и спецслужб Соединенных Штатов Америки группировкой хакеров Anonymous. Среди этих данных содержались

видеоролики, электронные письма, документы по планированию и разведке за последние 5 лет. Из-за произошедшего в стране разразился громкий скандал. Репутация власти США и, в частности, американских спецслужб сильно пошатнулась[8].

Стоит отметить, что любая размещённая пользователем информация в интернете является публичным высказыванием, даже если информация, размещённая пользователем, не является популярной и её почти никто не просматривает. И при пользовании интернетом обязательно стоит знать и руководствоваться правилами и законами страны, в которой пользователь проживает.

Наиболее часто встречаемым правонарушением в интернате является популяризирование запрещенной информации. При этом не обязательно размещать информацию о чём-то наиболее радикальном. Человека могут привлечь к административной ответственности и за банальные “смешные картинки”. Важно, что пользователь может и не быть автором данной статьи в интернете, достаточно просто “оценить” данную статью или оставить свой комментарий под запрещенным материалом. Также необходимо учитывать, что существует понятие как длящееся правонарушение, то есть если пользователь распространял любой запрещённый материал много лет назад, но он до сих пор доступен в сети, то такой пользователь всё равно считается правонарушителем. При этом удаление ранее размещенного контента не всегда помогает, ведь при дальнейшем разбирательстве правоохранители могут руководствоваться обычными скриншотами. Так что единственным способом быть защищённым от данного правонарушения — это хорошо знать, какие темы находятся под запретом и по возможности их избегать.

Далее перечислены темы, за распространение которых предусмотрена уголовная и административная ответственность, согласно уголовному кодексу Республики Беларусь:

– умышленные действия, направленные на возбуждение расовой, национальной, религиозной либо иной социальной вражды или розни по признаку расовой, национальной, религиозной, языковой или иной социальной принадлежности;

– публичные призывы к организации или проведению незаконных собрания, митинга, уличного шествия, демонстрации либо пикетирования, либо привлечение лиц к участию в таких массовых мероприятиях;

– публичные призывы к захвату государственной власти, или насильственному изменению конституционного строя Республики Беларусь, или измене государству, или совершению акта терроризма или диверсии, или осуществлению действий, направленных на нарушение территориальной целостности Республики Беларусь, или совершению иных действий, направленных на причинение вреда национальной безопасности Республики Беларусь, в том числе на применение мер ограничительного характера (санкций) в отношении Республики Беларусь, физических и юридических лиц Республики Беларусь, либо распространение материалов, содержащих такие призывы, при отсутствии признаков более тяжкого преступления;

– умышленное унижение чести и достоинства личности, выраженное в неприличной форме (оскорбление), в публичном выступлении, либо в печатном или публично демонстрирующемся произведении, либо в средствах массовой информации, либо в информации, распространенной в глобальной компьютерной сети Интернет, иной сети электросвязи общего пользования;

– пропаганда или публичное демонстрирование, в том числе с использованием глобальной компьютерной сети Интернет либо иной информационной сети, изготовление, распространение нацистской символики или атрибутики, а равно хранение или приобретение такой символики или атрибутики[9].

Другим правонарушением со стороны обычного пользователя может стать спам — рассылка писем без согласия получателя. Конечно, чаще всего спам — это дело мошенников, которые могут предлагать обычным пользователям различные махинационные схемы или предложения выгодной покупки или заработка, однако спам могут распространять и обычные люди, не видящие ничего противозаконного в своих действиях. Например, если человек устроился работником в какую-нибудь организацию, и посредством массовой рассылки рекламы своим друзьям и знакомым о данной организации пытается повысить её узнаваемость на рынке, то его действия также будут считаться нелегитимными и могут быть осуждены в соответствии с законодотельством путём наложения денежного штрафа.

Очень частым правонарушением с использованием информационных технологий является нарушение авторских прав. В наше время любой человек ежедневно сталкивается с объектами авторского права. Это может быть прослушивание музыки, просмотр фильмов и фотографий, поиск и скачивание файлов в интернете. В таких условиях очень сложно не пересечь ту грань, где использование чужих объектов собственности становится преступлением.

Нарушение авторских прав — это использование, копирование, распространение чужого произведения, либо несоблюдения условий договора по использованию данного объекта. Причём даже такая мелочь, как играющая на фоне музыка в салоне красоты или ресторане может стать нарушением, в случае ее использования без согласия правообладателя. Пользователь может

использовать чужие материалы лишь после получения исключительного права на произведение — право использовать чужие произведения в любой форме. При этом необходимо чётко обговаривать с автором назначение использования. Например, если было получено разрешение публиковать фото в интернете, пользователь не может напечатать его на афише. Если пользователь хочет законно использовать чужие материалы, ему необходимо получить разрешение у автора и указать при этом его имя, так будут соблюдены и права на использование, и личные неимущественные права автора[10].

Как уже стало понятно из описания методов правонарушений в области информационных технологий, данные действия могут нести серьёзную опасность для финансов, конфиденциальности пользователя. Тем очевиднее факт, что необходимо знать способы защиты от киберпреступлений и их предостережения.

Защита от фишинга включает в себя соблюдение нескольких элементарных правил безопасности в интернете.

Необходимо помнить, что ни в коем случае нельзя передавать такие конфиденциальные данные как пин-код банковской карты, пароль электронной почты или аккаунтов в социальных сетях. Ни банк, ни соцсеть никогда не станут запрашивать такого рода данные используя электронную почту.

Если пользователь зашёл на зловредный сайт, на его компьютер может быть выслан опасный вирус. Вирус — это специальная программа, способная самопроизвольно присоединяться к другим программам при запуске последних и выполнять различные нежелательные действия.

Наличие вируса может проявляться следующими способами:

– некоторые программы перестают работать или начинают работать некорректно;

– на экран выводятся посторонние сообщения, сигналы и другие эффекты;

– работа компьютера существенно замедляется;

– структура некоторых файлов оказывается испорченной.

По способу заражения вирусы классифицируют на следующие виды:

– троянские программы, назначением которых, по аналогии с троянским конём, является имитация каких-либо полезных программ, после активации которых программа активируется и выполняет определенные нежелательные действия;

– утилиты скрытого администрирования по интерфейсу и функционалу во многом напоминают системы администрирования компьютера в сети, при инсталяции которых происходит установка на компьютер скрытой системы удаленного управления;

Intended-вирусы — вирусы, которые не могут размножаться или размножаются только один раз, то есть вирусы, которые заразив какой-либо файл, утрачивают способность к дальнейшему размножению.

По деструктивным возможностям выделяют такие виды вирусов:

– неопасные вирусы, влияние которых ограничивается уменьшением свободной памяти на диске, замедлением работы компьютера, графическими или звуковыми эффектами;

– опасные вирусы, которые потенциально могут привести к нарушениям в структуре файлов и сбоям работы компьютера;

– очень опасные вирусы, в алгоритм которого специально заложены процедуры уничтожения данных и возможности обеспечивать быстрый износ движущихся частей механизма компьютера.

Для защиты от вирусов рекомендуется установить на компьютер надёжный антивирус — программы, препятствующей распространению вируса на компьютере пользователя.

Антивирусы разделяют на пять основных групп:

1 Мониторы. Программы мониторы располагаются в оперативной памяти компьютера, перехватывают и сообщают пользователю об обращениях операционной системы, которые используются вирусами для размножения и нанесения ущерба. Пользователь имеет возможность разрешить и запретить такие обращения. Такие антивирусы могут выявлять даже неизвестные вирусы на ранней стадии заражения.

2 Детекторы — программы, которые проверяют, имеется ли в файлах и на дисках специфическая для данного вируса комбинация байтов. При её обнаружении выводится соответствующее сообщение.

3 Доктора — программы, восстанавливающие зараженные файлы путём удаления из них тела вируса. Обычно такие программы рассчитаны на конкретные виды вирусов. Такие программы необходимо часто обновлять для получения версий, способных обнаружить новые виды вирусов.

4 Ревизоры анализируют изменение состояния файлов, проверяют состояние загрузочного сектора, а также время атрибуты и время создания файлов. При обнаружении несоответствий, пользователю сообщается об этом.

5 Вакцины модифицируют программы так, что это не отражается на их работе, но вирусы, от которых происходит вакцинация, считаю такие программы уже зараженными.

Также для защиты от фишинга необходимо обращать внимание на дизайн сайтов, на которые переходит пользователь. Если он кажется странным, недоработанным, сделанным на скорую руку, то вполне возможно, что это фишинговый сайт.

Всегда нужно обращать внимание на адресную строку в ссылке перехода — незначительное изменение в электронном адресе может привести абсолютно на другой сайт. Существует возможность дешифровать ссылку с помощью специальных сервисов и посмотреть, на какой сайт она ведет.

При посещении сайтов нужно следить, чтобы было установлено защищенное соединение https://. В адресной строке должен отображаться специальный символ — замок.

Письма с незнакомых номеров, имеющие экстренный характер должны в первую очередь вызывать подозрение. Письма, в которых говориться, что аккаунт пользователя взломан или был получен крупный выигрыш, почти всегда является мошенническим.

Стоит остерегаться заходить в банковские аккаунты через точки доступа общественного интернета, ведь с помощью их преступники могут установить доступ к личным данным пользователя. Безопаснее пользоваться мобильным интернетом или защищенным соединением.

Не стоит игнорировать предупреждения от браузера или социальной сети о переходе на подозрительный сайт. Если браузер советует пользователю не переходить по данной ссылке, то стоит прислушаться.

Чтобы обезопасить себя от утечки платежных данных пользователь должен предпринять следующие действия:

1 Не вводить данные о банковской карте в непроверенных магазинах и вообще постараться предостеречься от любых онлайн-покупок. Оставлять данные о финансовой карте лучше либо на максимально проверенных сервисах, либо вообще нигде.

2 Не пытаться сэкономить деньги там, где это попросту невозможно. Конечно, ситуация, где пользователя могут привлечь как соучастника по делу об отмыве “скарженных” средств, хоть и с довольно малой вероятностью, но все же может стать реальностью. Поэтому лучше отказываться от быстрых и простых способов сэкономить.

3 Необходимо подключить услугу о снятии денежных средств с банковской карты от мобильных банков. Пользователь будет получать уведомления о снятии денежных после каждой проведенной транзакции в интернете. Чем быстрее обнаружится взлом и несанкционированное снятие денег, тем больше будет шансов их вернуть.

4 Всегда нужно оставаться бдительными и не позволять панике или эмоциям влиять на принятые решения. Кардеры, как и прочие киберпреступники, умело пользуются общественной паникой[11].

Чтобы обезопасить себя от того, чтобы быть обманутыми нигерийскими письмами можно порекомендовать следующее:

– не высылать персональные данные или копии каких-либо документов и номера банковских счетов по запросу организаций, в которые пользователь не обращался, или людям, которых до этого никогда не знал;

– если пользователь является участником интернет-форумов, то следует завести для этого отдельную почту с другим паролем;

– пользоваться программами-фильтрами, которые фильтруют информацию, поступающую на почту пользователя, и при получении нигерийских писем рекомендуют владельцу почты такие письма удалять.

Существует несколько способов, чтобы пользователь мог обезопасить себя от шифрования важных данных и дальнейшего шантажа.

В первую очередь, нужно быть осторожным с сообщениями, приходящими на почту или в социальные сети. Чаще всего троянские вирусы с шифровальными программами находятся во вложениях писем или на зараженных сайтах. Поэтому стоит относиться к каждому письму от незнакомого источника как к потенциально опасному.

В связи с тем, что опасность может находиться на каком-либо сайте, то стоит остерегаться незнакомых и подозрительных сайтов. Так, если после клика на баннер появляется совсем не тот ресурс, который ожидался, или сайт выдает предложение загрузить что-нибудь на устройство пользователя, то его с большой вероятностью пытаются заразить.

В процессе использовании какой-либо программы в ней часто находятся уязвимости, которыми пользуются мошенники. Но, как правило, разработчики со временем выпускают обновления, в которых существующие неполадки исправляются. Поэтому люди, которые не обновляют своё программное обеспечение или другие программы рискуют больше тех, кто эти программы регулярно обновляет.

Стоит использовать современные защитные программы, которые способны распознавать и оперативно блокировать программы-шифровальщики. Антивирус анализирует действия запущенных файлов и блокирует попытки шифра какой-либо программы.

Одним из самых действенных решений является резервное копирование данных. Стоит регулярно сохранять важные файлы и документы в облачное хранилище типа диска Google или на внешний жёсткий диск. Стоит отметить, что при копировании информации на резервный жёсткий диск стоит только тогда, когда пользователь что-то копирует или считывает с него. Если он окажется соединен с компьютером во время нападения, то его также зашифруют. Также, при хранении данных на жёстком диске нужно защитить его надёжным паролем, желательно с двухэтапной аутентификацией, это существенно снизит вероятность взлома облачного хранилища пользователя[12].

Список использованных источников:

[1] Информатизация - [Электронный ресурс]. – Режим доступа: http://multilang.pravo.by.

[2] Правонарушения в сфере информационных технологий - [Электронный ресурс]. – Режим доступа: https://www.elibrary. ru/download/elibrary_ 37130233_76877572.pdf.

[3] Фишинг - [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3.

[4] Кардинг - [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D1%80%D0%B4%D0%B8%D0%BD%D0%B3.

[5] Нигерийские письма - [Электронный ресурс]. – Режим доступа: https://nigeria.mfa.gov.by/ru/letters/.

[6] Кибервымогательство — это вымогательство в интрнете - [Электронный ресурс]. – Режим доступа: https://news.ykt.ru/.

[7] Виды киберпреступлений - [Электронный ресурс]. – Режим доступа: https://internetpolicy.kg/literacymodule/course_2/module1/glava1_2.html.

[8] Десять самых громких атак XXI века - [Электронный ресурс]. – Режим доступа: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e.

[9] Уголовный кодекс Республики Беларусь - [Электронный ресурс]. – Режим доступа: https://kodeksy-by.com/ugolovnyj_kodeks_rb.

[10] Инструкция: как не нарушить авторские права - [Электронный ресурс]. – Режим доступа: https://www.asi.org.ru/2020/04/23/instruktsiya-avtorskie-prava/.

[11] Что такое кардинг, и как защитишься от взлома, покупая в интернете - [Электронный ресурс]. – Режим доступа: https://trends.rbc. ru/trends/industry/60ae051f9a7947c4dc22101b.

[12] Как защититься от шифровальщиков-вымогателей: 5 советов - [Электронный ресурс]. – Режим доступа: https://www.kaspersky. ru/blog/ransomware-five-tips/31352/.

UDC 004.056.5:34

OFFENSES IN THE SPHERE OF INFORMATION TECHNOLOGIES

Dorozhkin I.V., Sharafanovich Ya.O.

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Pulko T.A. – PhD in Technical sciences

Annotation

The use of computer and information technologies in various spheres of society is becoming a mandatory attribute to achieve maximum efficiency in this area. In this regard, the field of information technology is becoming increasingly popular for various kinds of scammers and criminals. A significant flow of finance and various personal information passes through information technology. Fraudsters take advantage of this by trying to steal money or personal information of the user in various ways in order to further use it for their own purposes.

This article discusses various sources of threats and types of crimes in the field of information technology. The main conclusions are the precautions that can protect the user from the potential dangers of the activities of offenders.

Keywords

Information technologies, cybercrime, phishing, carding, informatization, computer information, virus, criminal code.