КИБЕРУГРОЗЫ В СЕТИ ИНТЕРНЕТ

Интернет – это множество компьютеров и устройств, связанных между собой в огромную сеть. У каждого устройства в сети Интернет есть свой сетевой адрес.

Информация и приложения хранятся на специальных компьютерах, которые называются веб-серверами.

Веб-сервера также соединены друг с другом через коммуникационные сети, поэтому другие компьютеры могут соединиться с ними и получить информацию.

Когда компьютер, или сервер, или другое устройство соединены с интернетом, они могут взаимодействовать с другими компьютерами, тогда мы говорим, что они «онлайн».

Как компьютеры общаются друг с другом?

Мы можем понять, что говорит человек, только когда знаем язык, на котором он разговаривает. Точно также и с компьютерами.

В интернете компьютеры общаются друг с другом на специальном языке, который называется **«TCP/IP»**. Это универсальный язык, который понимают компьютеры в любой стране мира. Даже если они находятся в Беларуси, Китае или США.

В настоящее время наиболее широко распространен набор протоколов под общим названием TCP/IP. (Следует помнить, что во многих странах Европы применяется протокол X.25).

Основные функции семейства протоколов TCP/IP: электронная почта, передача файлов между компьютерами и удаленный вход в систему.

Пользовательская команда mail, пользовательские команды обработки сообщений (MH) и команда сервера sendmail могут применять TCP/IP для

передачи сообщений между системами, а основные сетевые утилиты (BNU) могут применять TCP/IP для передачи файлов и команд между системами.

TCP/IP – это набор протоколов, который задает стандарты связи между компьютерами и содержит подробные соглашения о маршрутизации и межсетевом взаимодействии. TCP/IP широко применяется в Internet, поэтому с его помощью могут общаться пользователи из исследовательских институтов, школ, университетов, правительственных учреждений и промышленных предприятий.

TCP/IP обеспечивает связь подключенных к сети компьютеров, обычно называемых хостами. Любую сеть можно подключить к другой сети и организовать связь с ее хостами. Несмотря на то, что существуют различные сетевые технологии, многие из которых основаны на коммутации пакетов и потоковом режиме передачи, набор протоколов TCP/IP обладает одним важным преимуществом – он обеспечивает аппаратную независимость.

Что такое беспроводные сети?

Вы наверняка пользуетесь смартфонами, чтобы зайти в интернет. Как же они соединяются с интернетом, если нет проводной сети? Все такие устройства, например: планшет, смартфон, ридер, игровая приставка, Smart TV – соединяются с интернетом через беспроводные сети.

Пространство вокруг нас заполнено радиоволнами. Беспроводные сети используют радиоволны, чтобы помочь устройствам «общаться» друг с другом. Есть очень много разных видов беспроводных технологий, например, GSM (мобильная связь), Bluetooth и Wi-Fi. Объединяет их то, что все они беспроводные.

В интернете очень много разных форм обмана. Чтобы не быть обманутыми, нам необходимо знать, какие наиболее популярные методы используются злоумышленниками для получения несанкционированного доступа к нашей частной информации и финансовым данным.

Scam – что это такое?

Скам (**scam** – с англ. яз. афера, мошенничество) – это мошенничество в сети Интернет.

Фишинг-мошенничество происходит при общении по электронной почте или в социальных сетях. Киберпреступники отправляют пользователям сообщения / электронные письма, пытаясь обмануть их, чтобы получить ценные и конфиденциальные данные (учетные данные для входа – из банковского счета, социальной сети, рабочего аккаунта, облачного хранилища).

Кажется, что такие электронные письма приходят из официального источника (например, банковских учреждений или любых других финансовых органов, законных компаний или представителей социальных сетей для пользователей).

Нажав ссылку в письме, вы перейдете на поддельную страницу сайта, который похож на настоящий, но на самом деле он контролируется мошенниками. В таких случаях нельзя указывать свои учетные данные и другую личную информацию.

Нигерийские письма

Письма названы так потому, что особое распространение этот вид мошенничества получил в Нигерии, причем еще до распространения интернета. Это эмоциональные электронные письма, текстовые сообщения или сообщения в социальной сети от мошенников («официальных членов правительства, бизнесменов или членов очень богатого члена семьи, нигерийского принца, к примеру» – обычно женщины), которые просят вас оказать помощь в получении крупной суммы денег в банке, заплатив изначально небольшую плату за документы и юридические вопросы. За помощь вам обещают очень большую сумму денег.

Они будут настойчивыми и попросят вас платить все больше и больше денег за дополнительные услуги, такие как транзакции или расходы на перевод. Вы даже получите документы, которые должны заставить вас поверить, что все по-настоящему. В конце концов вы останетесь без денег и без обещанных денег.

Обманные поздравительные открытки

Когда вы открываете такое электронное письмо и нажимаете на открытку, вы обычно получаете вредоносное программное обеспечение, которое загружается и устанавливается в вашей операционной системе. Вредоносная программа может быть раздражающей программой, которая будет запускать всплывающие окна с рекламой, неожиданными окнами по всему экрану.

Если ваша система заражена таким опасным вредоносным ПО, вы станете одним из ботов, которые являются частью большой сети зараженных компьютеров. Когда это произойдет, ваш компьютер начнет отправку личных данных и финансовой информации на мошеннический сервер, контролируемый IT-преступниками.

Лотерея – Lottery scam

Мошенничество в виде лотереи – это электронное сообщение, информирующее вас о том, что вы выиграли огромную сумму денег, и для того, чтобы получить свой приз или выигрыш, вам нужно заплатить небольшую плату.

Повезло вам, да?! Даже не имеет значения, что вы никогда не покупали лотерейных билетов!

Вымогательство

Киберпреступники отправляют вам письма с угрозами и вымогают деньги. Этот вид онлайн-мошенничества может иметь различные формы, например, угроза похищения члена семьи, если выкуп не будет выплачен в срок.

Чтобы создать видимость реальной опасности, сообщение заполняется подробностями из жизни жертвы, полученными из онлайн-аккаунта, личного блога или из учетной записи социальной сети.

Вот почему небезопасно предоставлять какую-либо конфиденциальную или личную информацию о вас в социальных сетях. Это может показаться безопасным и уединенным местом, где вас окружают только друзья, но в действительности вы никогда не сможете точно знать, кто за вами следит.

Опасные онлайн-знакомства

Онлайн-мошенничество в социальных сетях очень распространенное явление. Романтическая афера обычно происходит на сайтах знакомств или путем отправки простого электронного письма потенциальной цели и затрагивает тысячи жертв со всего мира. Зачастую такие знакомства заканчиваются вымогательством или совершением противоправных действий против жертвы.

Поддельные антивирусные программы

Мы все хотя бы раз видели это сообщение на наших экранах: *«Вы заразились! Скачайте антивирус X прямо сейчас, чтобы защитить свой компьютер!»*

В таких случаях ваша система может заразиться вредоносным ПО, таким как троянец или кейлоггер. Такого рода сообщения могут также исходить от одной из самых опасных угроз-вымогателей, таких как CryptoLocker, которая способна блокировать и шифровать вашу операционную систему и запрашивать у вас денежную сумму в обмен на ключ дешифрования.

Не забывайте всегда применять существующие обновления для ваших программных продуктов и устанавливать только законные программы с проверенных веб-сайтов.

Кража учетной записи в социальных сетях или игровых аккаунтов и ценностей

Если ваш аккаунт взломан – преступник получает все ваши персональные данные.

Следующие советы могут помочь вам избежать этих мошеннических действий в интернете:

1. Не принимайте запросы на дружбу от людей, которых вы не знаете;
2. Не делитесь своим паролем с другими;
3. При входе в систему используйте двухфакторную аутентификацию;
4. Избегайте подключения к публичным и бесплатным сетям Wi-Fi;
5. Держите ваш браузер и приложения обновленным;
6. Добавьте дополнительный уровень безопасности и используйте программное обеспечение кибербезопасности.

Мошенничества с заработком денег

Киберпреступники заставят вас поверить, что вы можете легко и быстро заработать деньги в интернете. Они пообещают вам несуществующую работу, включая планы и методы быстрого обогащения. Например, это онлайн игра Rich Birds. Интернет пестрит постами и отзывами о том, как выводить деньги, как легко заработать, но система игры построена по принципу пирамиды, и без определенного количества донатов и рефератов, которые тоже донатят игру,

вы не можете потребовать вывода денег, а при их наличии требования постоянно увеличиваются – и фактически вывод невозможен.

Поддельные новости мошенников

Распространение поддельных новостей в интернете представляет опасность для всех нас, поскольку оно влияет на то, как мы фильтруем всю информацию, которую нашли и прочитали в социальных сетях. Это серьезная проблема, которая должна беспокоить наше общество, главным образом из-за вводящих в заблуждение ресурсов и контента, найденных в интернете, что делает невозможным для людей различать, что реально, а что нет.

Мы рекомендуем получать доступ только к надежным источникам информации, поступающей от друзей или знакомых (блоггеров, отраслевых экспертов), которые читают регулярные каналы из надежных источников, чтобы избежать поддельных новостей.

SMS Scaming (Smshing) – поддельные смс

Smishing (использование текстовых сообщений SMS) – это метод, похожий на фишинг, но вместо отправки электронных писем злоумышленники отправляют текстовые сообщения своим потенциальным жертвам.

Как это происходит? Вы получаете срочное текстовое сообщение на свой смартфон с прикрепленной ссылкой, в которой говорится, что оно принадлежит вашему банку и вам необходимо получить к нему доступ, чтобы обновить банковскую информацию или другую информацию онлайн-банкинга.

Мошенничество при покупках / продажах в сети Интернет

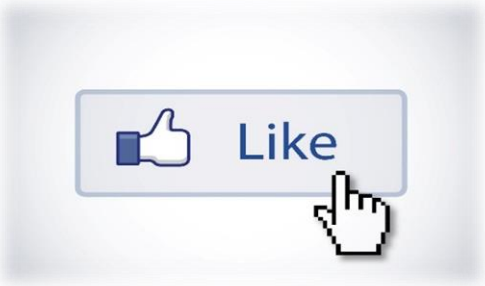
Следуйте этим советам по безопасности, чтобы защитить себя от переплаты онлайн-мошенников:

1. Если вы заметили подозрительное письмо от ненадежного источника или что-то необычное, сообщите в органы правопорядка об этом как можно скорее;
2. Если вы получили электронное письмо подобное тому, которое получил ваш знакомый, не переводите лишние деньги кому-то, кого не знаете, особенно если он / она хочет переплатить;
3. Кроме того, не переводите деньги поддельной транспортной компании или частному агенту по доставке, потому что это часть мошенничества;

4. Не предоставляйте личную информацию людям, которые не заинтересованы в покупке вашего товара;

5. Не отправляйте товар покупателю до тех пор, пока оплата не будет завершена и не поступит на ваш банковский счет.

Обман в социальных сетях – лайкомания



Зачастую мы встречаемся в социальных сетях с предложениями о накрутке лайков, голосов или иных способах продвижения страницы. Чтобы получить такую услугу, требуется перевести деньги на телефон или отправить смс на определенный номер. Правда, после этого лайки не появляются и не происходит никаких продвижений, а преступник требует еще больше денег.

Персональные данные

Персональные данные – это любая информация, которая относится к вам. Это имя, фамилия, дата рождения, номер школы, номер телефона, домашний адрес и многое другое.

Персональные данные могут использоваться в интернете для того, чтобы зарегистрироваться на сайте или в социальных сетях, делать покупки или играть в игры.

Кража данных и личности (Identity theft)

Кража личности. Для получения денежных средств. Преступники могут украсть базы с данными пользователей для их последующей перепродажи, использовать полученные сведения для изготовления фальшивых документов с целью получения кредитов и оформления покупок на чужое имя. Известны случаи взлома страниц в социальных сетях или создания клонов, затем от имени жертвы рассылались сообщения друзьям с просьбой отправить деньги на указанные мошенниками реквизиты.

Преступная кража личности. Связана с получением документов (например, при краже SSN в США, с его помощью можно получить медицинскую помощь, которая будет оплачена со страхового счета жертвы) по предоставленным мошенниками данным. Потом злоумышленники совершают различные противоправные действия, в результате чего жертвы могут получить судебные иски или штрафы для оплаты.

Кража данных. Кража данных с целью изменения личности. К такому способу прибегают лица, скрывающиеся от кредиторов или по другим причинам, незаконные иммигранты. Сюда также относятся те, кто желает сохранить анонимность по каким-либо причинам. Похищение медицинских данных используется преступниками в основном с целью приобретения отпускаемых только по рецепту врача средств, включая содержащие наркотические вещества препараты.

Создание клонов. Часто третьи лица создают в различных социальных сетях страницы актеров, музыкантов или спортсменов для получения славы или использования известного имени в собственных, исключающих материальную выгоду, целях. Не считается уголовным преступлением до тех пор, пока владелец аккаунта не станет использовать раскрученное имя для получения незаконной прибыли.

Нежелательный контент – вредоносные и потенциально опасные программы, запрещенная и нежелательная информация

Нежелательный контент – это не только материалы (картинки, видео, аудио, тексты), содержащие насилие, порнографию, пропаганду наркотических средств, азартных игр, но и различные вредоносные и шпионские программы, задача которых получить доступ к информации на компьютере владельца. Также к нежелательному контенту относятся сайты, запрещенные законодательством. В современном мире интернетом пользуются люди разных возрастов, будь то ребенок или пожилой человек, каждый имеет страницу в социальной сети, пользуется поисковыми системами для получения ответов на вопросы, смотрит видео, читает книги или слушает музыку. В связи с этим вероятность того, что пользователь встретит в сети нежелательный контент, очень велика, и от вида контента будет зависеть размер полученного ущерба.

Информация подготовлена педагогом социальным ОВРМ Слонимской В.В.