МИХАИЛ ГУБИН

Преступления в сети Интернет

УЧЕБНОЕ ПОСОБИЕ

Михаил Губин

Преступления в сети Интернет. Учебное пособие

«Издательские решения»

Губин М. С.

Преступления в сети Интернет. Учебное пособие / М. С. Губин — «Издательские решения»,

ISBN 978-5-44-987368-2

В наше время преступления совершаются повсюду. Интернет также не стал исключением из правил. В этом пособии показаны основные моменты преступлений в сети Интернет, показаны их примеры, а также рассмотрены преступления, касающиеся детей.

ISBN 978-5-44-987368-2

Содержание

Преступления в сети Интернет
Учебное пособие

Михаил Сергеевич Губин

ISBN 978-5-4498-7368-2
Создано в интеллектуальной издательской системе Ridero

1. ВМЕСТО ВСТУПЛЕНИЯ

Сеть Интернет является развивающейся и меняющейся структурой. Она объединяет разрозненные сайты, сервера, проекты пользователей в одну большую группу. История Интернета начинается в далеких 1950х годах двадцатого века, когда была создана сеть, связывающие оборонные точки США под названием ARPANET. После возникновения ARPANET сети пошли дробиться, сперва на сеть для военных MILNET и сеть для вузов NFSNET, после этого через некоторое время MILNET закрылась, а NFSNET дала непосредственное начало современному Интернету, породив большое количество различных сетей. Даже P2P, который мы используем в торрентах и DC++, был рожден в то далекое время. Та же самая ARPANET представляет раннюю версию P2P.

Возникают новые технологии – появляются люди, которые хотят с помощью этих технологий получить прибыль тем или иным способом. Возьмем ту же Hormel Foods Corporation и ее торговую марку SPAM для мясных консервов. В 1936 году была зарегистрирована сама марка «SPAM» (SPiced Ham – ветчина со специями), а во время Второй мировой войны Hormel Foods Corporation занималась поставками этого самого SPAM'а на фронт американцам.

Но в 1945 году гитлеровская Германия была побеждена, Вторая мировая закончилась, и тут проявился несколько смешной факт. Hormel Foods Corporation на своих складах накопила огромное количество этой самой тушенки, а девать ее было некуда. И срок некоторых консервов давно истек. Что делает компания? Правильно, рекламирует по газетам, телевидению, просто развешивает рекламу на улице. Причем массово. Эту рекламу продрали в скетчах и, таким образом, первый раз слово SPAM было употреблено применимо к массовой рекламе.

Позже, администратор группы news.admin. policy, входящей в сеть USENET, придумал программу ARMM, которая должна была удалять посты пользователей группы после их публикации. Программа оказалась не доделанной, и произошел баг, во время которого 200 сообщений прилетели в группу от имени администратора. Вот тогда один из пользователей со своей легкой руки и применил слово SPAM относительно к рассылке.

Федеральный закон Российской Федерации от 13 марта 2006 г. №38-ФЗ «О рекламе» говорит по поводу спама следующее: «Распространение рекламы по сетям электросвязи, в том числе посредством использования телефонной, факсимильной, подвижной радиотелефонной связи, допускается только при условии предварительного согласия абонента или адресата на получение рекламы. При этом реклама признается распространенной без предварительного согласия абонента или адресата, если рекламораспространитель не докажет, что такое согласие было получено.».

Давайте же посмотрим, какие преступления существуют в современной сети Интернет, и как с ними обычно борются.

2. МОШЕННИЧЕСТВО

Интернет-это палка о двух концах. С одной стороны, это делает большую часть нашей жизнь легче, позволяя нам общаться с близкими и деловыми партнерами независимо от того, где они находятся на земном шаре. С другой стороны, это позволяет интернет-мошенничеству проникать прямо в наши офисы, наши дома и в нашу повседневную жизнь.

Существуют всевозможные стратегии нападения. От вредоносного программного обеспечения, которое использует уязвимости в компьютерных системах и законном программном обеспечении, до хитроумных фишинговых мошенничеств, которые происходят в наименее ожидаемых частях мира, где трудно добиться справедливости для преступников, которые провоцируют эти мошенничества.

Чтобы защитить себя, вам нужно знать, какие типы интернет-мошенников нужно искать и как их избежать. Их много, но некоторые встречаются чаще, чем другие.

1.1. Мошенничество с помощью электронной почты. Фишинговая афера

Более трети событий кибербезопасности начинаются с фишингового сообщения электронной почты или какого-либо вредоносного вложения в сообщении электронной почты, которое отправляется сотрудникам компании. Эти мошенничества варьируются от простых до сложных; они меняются каждый день, часто превращаясь в более хитрые или более сложные мошенничества.. В настоящее время они представляют собой одну из наиболее серьезных угроз для организаций и отдельных лиц.

Фишинговая афера основана на электронной почте, хотя иногда она может быть совершена в социальных сетях. Преступник отправит пользователю электронное письмо или сообщение с целью обмана, чтобы заставить его предоставить ценные данные, такие как учетные данные для входа, которые впоследствии могут быть использованы для кражи дополнительных данных или денег.

Электронные письма должны выглядеть так, как будто они приходят из официального источника, например, финансового органа. Преступник потребует социальной инженерии, чтобы убедить вас нажать на ссылку, которая якобы приведет вас на законный сайт. Затем вас направят на страницу входа, которая выглядит устрашающе похожей на реальную сделку, и попросят ввести ваши учетные данные.

Чтобы увеличить свои шансы на успех, мошенники создают ощущение интенсивной срочности. Они будут использовать тактику запугивания, например, сообщат вам, что ваш счет в банке или в другом месте находится под угрозой, и вам нужно немедленно войти в систему, чтобы подтвердить свою личность. После того, как вы заполните учетные данные, мошенники будут использовать их для доступа к вашей реальной учетной записи или связывать их с учетными данными других пользователей и продавать их в темной сети.

1.2. «Нигерийский принц»

Это один из старейших трюков в книге онлайн-мошенничества, и он по-прежнему является одним из самых распространенных. Он также известен как нигерийская афера 419, названная в честь раздела в Уголовном кодексе Нигерии, который запрещает эту практику.

Предположение состоит в том, что член богатой нигерийской семьи, хотя это может быть любая другая национальность, нуждается в вашей помощи, чтобы получить доступ к своему наследству и даст вам часть этого богатства взамен. Он начинается с очень эмоционального сообщения или письма от мошенника, который утверждает, что является членом богатой семьи, бизнесменом или членом правительства. Статистически это скорее всего будет женщина, потому что женщины более убедительны.

Они попросят вас помочь получить значительную сумму денег из какого-нибудь банка и попросят вас заплатить небольшую плату, в начале, чтобы помочь с юридической и бумажной работой. За вашу помощь, часть этой большой суммы денег будет вашей.

Они будут раздвигать границы, насколько это возможно, и пытаться заставить вас платить все больше и больше за импровизированные административные задачи, включая расходы на перевод и транзакции. Вы даже получите законные документы, которые убедят вас поверить, что все это реально. В конце концов, у вас закончатся деньги, и вы не получите ни одной из обещанных вам денег.

1.3. Мошенничество с поздравительными открытками

Праздничные открытки – обычное явление, будь то Пасха или Рождество. Одно из мест, где мы получаем много поздравительных открыток – это наши электронные письма. К сожалению, даже этот, казалось бы, безобидный жест может быть использован в злонамеренных целях интернет-мошенниками.

Если вы откроете письмо с поздравительной открыткой и нажмете на нее, вы можете загрузить и установить вредоносное программное обеспечение на свой компьютер без вашего ведома. Если Вам повезет, это будет не более чем раздражающая программа, которая запускает всплывающие окна на вашем экране. Если нет, то это может быть еще более зловещим. Он может даже превратить ваш компьютер в бота в большой сети зараженных компьютеров. Ваша финансовая и другая личная информация может в конечном итоге быть отправлена на серверы преступников.

Чтобы защитить себя, имейте специализированную программу компьютерной безопасности или антивирус, который защищает вас от этого и других типов онлайн-угроз.

1.4. Мошенничество с кредитными картами или банковскими кредитами

Если это звучит слишком хорошо, чтобы быть правдой то вероятно, что так оно и есть. Такие аферы обманывают людей немного больше, чем ожидалось, даже в век, когда информация настолько доступна, что мы должны быть мудрее. Вы можете получить сообщение из банка о том, что большая сумма денег была предварительно одобрена и предложена вам в качестве кредита. Если вы видите такую аферу, вы должны спросить себя, как банк может легко предварительно одобрить такие большие суммы денег, не оценив предварительно ваше финансовое положение.

Когда дело доходит до кредитных карт, этот вид мошенничества становится все более популярным из года в год и приводит к потере миллиардов невинных жертв. Чтобы не стать жертвой, внимательно следите за своими онлайн-транзакциями и счетами, воспользуйтесь услугами по защите прав потребителей и подпишитесь на бесплатный кредитный мониторинг.

1.5. Афера с лотерейным сбором

Это еще одна классика, которая сегодня так же популярна, как и всегда. В основном вы получаете электронное письмо, которое сообщает вам, что вы выиграли в лотерею и можете претендовать на огромную сумму денег, сразу после того, как заплатите небольшую плату. И возможно, Вам так повезет, что вы даже не вспомните, что никогда в жизни не покупали лотерейный билет.

Сила этой аферы в том, что она нацелена на ваши самые смелые мечты и использует их против вас, позволяя вашему воображению играть главную роль в том, чтобы обмануть вас. Как только вы платите деньги, вы понимаете, что вы просто еще одна жертва онлайн-мошенничества. Ни при каких обстоятельствах не позволяйте себе поддаться на эту удочку.

1.6. Мошенничество на сайте знакомств

Мы используем Интернет для общения, поэтому вполне естественно, что мы также используем его, чтобы найти любовь. Существует множество приложений для знакомств, которые помогают людям найти свою вторую половинку. Однако не все из них имеют счастливый конец.

Методы, используемые любовными мошенниками, такие же, как и те, которые используются типичными домашними насильниками, и являются очень манипулятивными по своей природе. Тысячи мужчин и женщин со всего мира становятся жертвами таких мошенников, и вы должны стремиться не поддаваться их тактике. Никогда, ни при каких обстоятельствах, не отправляйте деньги кому-то, кого вы только что встретили через Интернет, независимо от того, насколько вы верите, что это может быть тот самый человек.

3. ШАНТАЖ

В Интернете встречается и такое преступление, как шантаж. Если жертва особенно робка или восприимчива к конкретной угрозе, а лицо, угрожающее ей, делает это с таким знанием или намерением действовать в соответствии с этой конкретной робостью или восприимчивостью, то будет установлено, что они действовали с угрозами. И наоборот, если очевидная серьезная угроза не может запугать жертву, это не освобождает истца от ответственности, если обычное лицо, обладающее нормальной стабильностью и мужеством, могло бы подвергнуться влиянию или вызвать опасения, с тем чтобы удовлетворить это требование.

Чаще всего злоумышленник представляется неизвестным хакером и пишет или сообщает, что имеет доступ к каким-то конкретным данным либо списку ваших контактов. Он может писать ваш пароль доступа к конкретному сайту, ваш логин и требование к определенным действиям. На самом деле, большинство данных из таких писем – это сведения из опубликованных баз логинов и паролей, которые могут быть устаревшими.

Упор в интернет-шантаже идет именно на психику жертвы и не важно, старые это сведения или новые. Как говорится, в этом случае нельзя «кормить тролля» – то есть ни в коем случае не идите на поводу у злоумышленников. Если вы идете у них на поводу то это уже ваша собственная воля. Принудить вас совершить тот или иной поступок никто не может.

4. DDOS АТАКИ

Распределенная атака отказа в обслуживании (DDoS) – это попытка сделать онлайн-сервис недоступным, перегружая его трафиком из нескольких источников. Такие атаки нацелены на широкий спектр важных ресурсов, от банков до новостных сайтов, и представляют собой серьезную проблему для обеспечения того, чтобы люди могли публиковать информацию и получать доступ к важной информации.

DDoS-атака запускается с многочисленных скомпрометированных устройств, часто распределенных по всему миру, называемых ботнетом. Он отличается от других атак типа «отказ в обслуживании» (DoS) тем, что использует одно подключенное к Интернету устройство (одно сетевое соединение) для заполнения цели вредоносным трафиком. Этот нюанс является основной причиной существования этих двух, несколько отличающихся друг от друга определений.

Вообще говоря, DoS и DDoS атаки можно разделить на три типа:

3.1. Атаки на основе объема

Включает в себя UDP наводнения, ICMP наводнения и другие поддельные пакеты наводнения. Целью атаки является насыщение полосы пропускания атакуемого сайта, а ее величина измеряется в битах в секунду (бит/с).

3.2. Атаки по протоколу

Включает в себя флуд SYN, фрагментированные атаки пакетов, Ping of Death, Smurf DDoS и многое другое. Этот тип атаки потребляет фактические ресурсы сервера или промежуточного коммуникационного оборудования, такого как брандмауэры и балансировщики нагрузки, и измеряется в пакетах в секунду (Pps).

3.3. Атаки прикладного уровня

Включает в себя низко-и медленные атаки, наводнения GET/POST, атаки, нацеленные на уязвимости Apache, Windows или OpenBSD и многое другое. Такая атака состоит из, казалось бы, законных и невинных запросов. Целью этих атак является сбой веб-сервера, величина атаки измеряется в запросах в секунду (Rps).

3.4. Часто используемые типы DDoS атак

Некоторые из наиболее часто используемых типов DDoS-атак включают:

Конец ознакомительного фрагмента.