А. Г. Кротов,
студент I курса Института бизнеса БГУ
Научный руководитель:
старший преподаватель
Д. Б. Урганова

СОВРЕМЕННЫЕ СПОСОБЫ МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

Сегодня любой пользователь интернета может стать жертвой мошенников. Их методы с каждым днем становятся совершеннее, и даже установленная антивирусная программа не всегда может защитить вас от действий мошенников. Если учесть, что многие пользователи считают ненужным покупать последнюю версию антивируса, то шанс оказаться жертвой мошенников, многократно возрастает.

Цель: рассмотреть новые способы мошенничества в интернете. Определить методы защиты от мошенников в интернете.

Методы: анализ современных способов мошенничества в интернете. Изучение реальных способов мошенничества, предоставленных пользователями интернета. Способом индукции получение советов для избегания мошенничества в интернете.

Согласно *отчету The Nilson Report* (*это один из самых* авторитетных источников новостей и аналитических материалов в мировой индустрии карточных и мобильных платежей), в 2018 г. мошенничество с картами привело к убыткам в размере около 24 млн долл. США, и в этом году оно должно значительно возрасти. Но, если технологии по защите пользователей совершенствуются с каждым годом; если банки внедряют новые системы безопасности, то почему эта цифра по прогнозам экспертов будет расти?

На этот вопрос можно ответить одним словом – «кардинг» – вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Но на сегодня существует много видов «кардинга», которые могут быть связаны как со взломами в интернете, так и с физической утерей карты или отправкой данных третьим лицам.

Одним из новых видом «кардинга» является получение данных карт с помощью применения цифровых масок. В даркнете есть рынок под названием «Genesis», который используется для продажи цифровых масок пользователей. Цифровая маска состоит из цифрового отпечатка пальца пользователя – истории веб-поиска, информации об ОС и браузере, установленных плагинах и т. д., и информации о поведении пользователя: что он делает в интернете и как он это делает. Злоумышленники, которые продают цифровые маски в даркнете, обычно получают их с помощью вредоносных программ, которые при попадании на устройство не выдают себя путем шифрования информации, не требуя заплатить выкуп, просто собирают информацию.

Цифровые маски используются системами защиты от мошенничества для проверки пользователей. Если цифровая маска, которую видит антифрод-система, совпадает с той, которую она ранее видела для того же пользователя, она пометит транзакцию как легитимную. Для многих банков это означает, что им даже не потребуется код 3D Secure, отправляемый по SMS или push-уведомление пользователю для подтверждения транзакции.

Таким образом, если преступник украдет вашу цифровую маску и учетные данные онлайн-банкинга, антифрод-система сочтет, что это вы и не будет предпринимать каких-либо действий. Это значит что, преступник сможет снять все деньги с вашего счета, не будучи замеченным.

Так же мошенники не обходят стороной и социальные сети. Одним из новых способов мошенничества с помощью социальных сетей стала кража относительно популярных аккаунтов (с количеством подписчиков от 1000 чел.), и дальнейшее вымогательство денежных средств за возвращение этого аккаунта. Все начинается с письма на электронную почту, которое сообщает владельцу аккаунта примерно следующее «Ваша учетная запись будет окончательно удалена за нарушение авторских прав. У вас есть 24 ч., чтобы подать апелляцию». В этих случаях в графе отправитель будет указан электронный адрес очень похожий на официальную электронную почту. В данном письме будет иметься кнопка «Рассмотреть жалобу». Если вы нажмете на нее, вы попадете на убедительную фишинговую страницу, где мошенники размещают сообщение, в котором говорится, что они очень заботятся о защите авторских прав, и предлагают вам ссылку на «Обжалование». Чтобы мошенничество выглядело еще более законным, они предлагают длинный список вариантов выбора языка, хотя он не работает – что бы вы ни нажимали, фишинговая страница всегда остается на английском языке. Как только вы нажмете ссылку «Апелляция», вам будет предложено ввести учетные данные Instagram. И это еще не конец. Сразу же появляется другое сообщение: «Нам нужно проверить ваши данные и проверить, соответствует ли ваша учетная запись электронной почты учетной записи Instagram». После того, как вы нажмете «Подтвердить мой адрес электронной почты», и вы увидите список поставщиков услуг электронной почты. Если вы выберете свой, вам будет предложено указать как ваш адрес электронной почты, так и пароль для вашей учетной записи электронной почты.

Соответственно, после всех этих действий аккаунт вместе с электронной почтой переходит во владение злоумышленников, и затем злоумышленники требуют выкуп.

Но самым распространенным видом мошенничества в социальных сетях является вымогательство денег с помощью различных психологических приемов. Обычно у мошенников имеется план, как обмануть жертву:

1. Давить на жалость, заставить поверить жертву в то, что вы случайно попали в плохую ситуацию.

2. Если жертва поверила, что вы действительно попали в плохую ситуацию, но хочет увидеть доказательства, надо ее/его поторапливать, для того, чтобы было меньше вопросов.

3. Если вам так и не поверили, начинать агрессивно себя вести, для того, чтобы жертва себя почувствовала неловко из-за того, что он/она никак не может помочь.

В качестве примера применения этого приема можно рассказать ситуацию, связанную с сервисом v-banking, который привязан к вашему номеру телефона если вы владелец сим-карты «velcom» («A1»).

Мошенник первым делом напишет, вам номер телефона уточнит, не ваш ли это номер, сказав, что произошла ошибка, и вам на счет v-banking случайно пришло 100 BYN. Затем вас попросят скачать это приложение и активировать кошелек, и вы там действительно увидите 100 BYN. Но т. к. мошенник будет торопить вас, вы не будете углубляться в подробности, откуда появилась эта сумма и, скорее всего, поверите, что эти деньги действительно пришли вам по ошибке (вы конечно можете попросить чек о транзакции, но его можно сделать средствами программы Adobe Photoshop). После чего мошенник отправит номер счета

или телефона, на который попросит вас отправить эти деньги. Если это действительно произойдет, то эти 100 р. просто снимутся с баланса вашего номера телефона. Но в данном случае мошенник не сможет полностью замаскировать себя. Если вы сразу поймете, что это мошенник, то можно отправить ему фишинговое изображение, с помощью которого, можно будет определить IP-адрес злоумышленника, что существенно поможет правоохранительным органам.

В современном мире, когда технологии становятся с каждым днем все лучше и лучше, мошенники также не стоят на месте и их методы становятся все более изощренными, причем в самых различных сферах. Жертвой мошенников может оказаться любой пользователь интернета, но можно предпринять определенные меры для того, чтобы уменьшить вероятность стать жертвой мошенников:

1. Использовать самые последние версии антивирусных программ (как минимум они смогут предостеречь вас от фишинговых ссылок).

2. Использовать сложные пароли никак не связанные с именем, фамилией, датой рождения, номером телефона (это помогает злоумышленникам взломать вашу страницу с помощью программ, которые подбирают пароль на основе данных о пользователе).

3. Размещать минимальное количество информации о себе в социальных сетях (никогда не оставляйте на странице адрес электронной почты, к которой привязан аккаунт, и номер телефона, т. к. это помогает злоумышленникам взломать вашу страницу, а также вы можете стать жертвой мошенничества связанного с балансом номера вашего телефона).

4. Обращать внимание на страницу неизвестного собеседника: дата создания страницы, количество друзей (подписчиков), количество фото, активность под фото и т. д. Если страница создана недавно и активность на странице маленькая, то, скорее всего перед вами страница ненастоящего человека, следовательно, такому собеседнику доверять не стоит.

5. Никому и ни при каких обстоятельствах не отправлять полностью все данные карты (оплачивать товары или услуги только в магазинах, в которых вы на 100 % уверены).

6. Для банков можно рекомендовать ввести защиту, которая требует введения обязательной двухфакторной аутентификации, возможно, даже с использованием некоторых биометрических показателей, таких как считывание отпечатков пальцев (реальное, а не цифровое), сканирование радужной оболочки глаза или распознавание лица в качестве второго фактора.

7. Самое главное – всегда обращаться в правоохранительные органы. Согласно Уголовному кодексу Республики Беларусь злоумышленники могут быть осуждены по ст. 209 (мошенничество – Завладение имуществом либо приобретение права на имущество путем обмана или злоупотребления доверием). Либо по ст. 212 (Хищение путем использования компьютерной техники – Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации).

Список использованных источников

1. How crooks use your doppelgangers to pay with your card [Electronic resource]. – Mode of access: https://www.kaspersky.com/blog/digital-masks-card-fraud/26357/. – Date of access: 04.03.2019.

2. Instagram accounts hijacked with fake copyright infringement notifications [Electronic resource]. – Mode of access: https://www.kaspersky.com/blog/instagram-hijack-new-wave/25997/. – Date of access: 05.03.2019.

3. Антифрод [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Антифрод. – Дата доступа: 05.03.2019.