КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКА

В настоящее время участились случаи хищения денежных средств с карт-счетов банковских карточек.

На мобильный телефон потерпевших в мессенджере «Viber» звонят злоумышленники, которые представляются сотрудниками банка, после чего сообщают, что с карт-счёта потерпевшего производится несанкционированный перевод денежных средств. Злоумышленники поясняют, что для отмены операции необходимо сообщить реквизиты платёжной системы (номер карты, срок её действия, фамилию и имя владельца карты, CVC/CVV-код). Потерпевшие, будучи введёнными в заблуждение, предоставляют злоумышленнику всю запрашиваемую информацию, которая приводит к хищению денежных средств с карт-счёта потерпевших путём денежного перевода. Необходимо отметить, что имеются основания полагать, что злоумышленники обладают базовой информацией о потерпевших, а именно: анкетными данными (ФИО), номером их мобильного телефона. В действительности в базе клиентов банков имеется вся необходимая информация о клиентах (номер банковской карточки, личный номер паспорта и т.д.), в связи с чем сотрудникам банков нет необходимости запрашивать у клиентов номер банковской карточки, личный номер паспорта и иную информацию, особенно CVC/CVV-код.

При получении подозрительного вида сообщений в различных мессенджерах или звонков необходимо проявлять бдительность и не поддаваться на предложение сообщить информацию о реквизитах карточки, несмотря на то, что Вам могут писать или звонить родственники, знакомые, сотрудники служб банков и иные лица.

Указанный выше способ совершения хищения денежных средств с карт-счетов не является единственным. Помимо вышеуказанного способа хищения денежных средств с карт-счетов потерпевших распространены следующие способы:

- злоумышленником осуществляется взлом страниц пользователей различных социальных сетей, после чего от имени пользователей рассылаются сообщения их знакомым с безобидным содержанием, а именно: с просьбой о якобы переводе денежных средств с банковской платёжной карточки злоумышленника на банковскую карточку пользователя. При этом злоумышленник просит предоставить номер платежной карточки пользователя, срок действия, защитный код и иную информацию. После получения указанных данных злоумышленник совершает хищение денежных средств с карт-счетов пользователей социальных сетей;

- создание злоумышленником страницы-«двойника» одного из пользователей социальной сети «Одноклассники», с целью введения в

заблуждения знакомых пользователей и получения от них необходимой ему информации. Злоумышленник со страницы-«двойника» осуществляет переписку со знакомыми пользователей социальных сетей. В ходе переписки злоумышленник получает реквизиты банковской платежной карточки, идентификационного номера паспорта и иных личных сведений, которые позволяют злоумышленнику совершать хищения денежных средств с карт-счетов;

- фишинг, представляющий собой вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям (реквизитов банковских платежных карточек и др.). Это достигается путем направления потерпевшему прямой ссылки на сайт, внешне не отличимый от настоящего, либо на сайт с редиректом. После того, как пользователь попадает на поддельную страницу, вводит в соответствующей форме реквизиты банковской платежной карточки, злоумышленник завладевает ими и похищает денежные средства, Злоумышленники, располагая абонентскими номерами, указанными гражданами на торговых площадках, в том числе на площадке «kufar.by», связываются с ними посредством Интернет-мессенджеров (к примеру, посредством мессенджера «Viber»). В данном случае администрация торговой площадки не может каким-либо образом повлиять на законность сделки и предупредить совершение преступления. При последующем общении в мессенджере, используя социальную инженерию (метод получения необходимого доступа к информации, основанный на особенностях психологии людей), злоумышленники побуждают граждан перейти па якобы легальный (настоящий) ресурс, например kufar, cdek и другие, заполнить на них специальную форму для перевода денежных средств в качестве оплаты (предоплаты) за приобретаемый товар, в результате чего впоследствии совершается хищения денежных средств с карт-счетов.

Современные методы оплаты в сети интернет позволяют совершать платежи без знания пин-кода карты, путем введения в компьютерную систему сведений о номере карты, сроке ее действия, владельце, а также CVC-коде (как правило, трехзначный код, находящийся на оборотной стороне карты). Указанные обстоятельства позволяют злоумышленникам, завладевшим реквизитами банковской карточки совершать платежи, переводы в сети интернет без ведома владельца, обладая всей необходимой для этого информацией.

Вместе с тем, для того, чтобы обезопасить себя и свои денежные средства от подобного способа хищения, необходимо:

1) исключить передачу данных своей банковской карты третьим лицам, каким бы то ни было способом, в том числе посредством социальных сетей или мобильному телефону, так как имеют место случаи взломов страниц, создания страниц «двойников» в социальных сетях, а также не реагировать на

поступающие рассылки с просьбой о помощи переводов, оплаты либо снятии денежных средств при помощи вашей банковской карты, не реагировать на телефонные звонки от представляющихся сотрудников банков, когда последний банка запрашивает информацию о номере банковской платежной карточки, личном номере паспорта;

2) в случае обнаружения утери, либо передачи данных карты, немедленно связаться с банком-эмитентом карты, сообщить об этом и заблокировать доступ с помощью, указанной карты к банковскому счету (для возможности экстренной блокировки банковской карты необходимо всегда дополнительно иметь при себе контактные телефоны банка, которые для сведения указаны на оборотной стороне банковской карты);

3) в ходе использования карты подключить и использовать технологию «3D Secure». Данная технология позволяет однозначно идентифицировать подлинность держателя карты, осуществляющего операцию, и максимально снизить риск мошенничества по карте. При использовании этой технологии держатель банковской карты подтверждает каждую операцию по своей карте специальным одноразовым паролем, который он получает в виде SMS-сообщения на свой мобильный телефон.

6 ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

1 Надёжные пароли

Необходимо:

+ Создавать персональные (уникальные) пароли
+ Использовать сложные пароли: минимум 10 символов; одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы
+ Доверять только проверенным менеджерам паролей

Не рекомендуется:

- Использовать повторение символов
- Хранить пароли н а бумажных носителях
- Использовать в качестве пароля свой логин (имя пользователя, учётная запись, никнейм)
- Сохранять пароль автоматически в браузере
- Использовать биографическую информацию в пароле

2 Безопасный WI-FI

Необходимо:

+ Отключать общий доступ к своей WI-FI точке, даже если у Вас «безлимитный» интернет
+ Использовать надёжный (см. выше/) пароль для доступа к Вашей WI-FI точке
+ Деактивировать автоматическое подключение своих устройств к открытым WI-FI точкам

Не рекомендуется:

- Вводить свой логин и пароль доступа к учётной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам WI-FI в кафе, в транспорте, торговых центрах и т.д.

3 Проверенные браузеры и сайты

Необходимо:

+ Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещения сомнительных сайтов

Не рекомендуется:

- Переходить по непроверенным ссылкам
- Вводить информацию на сайтах, если соединение не защищено (нет https)

4 Безопасность электронной почты

Необходимо:

+ Подключать двухфакторную аутентификацию

+ Использовать минимум 2 типа e-mail адресов: закрытый (только для привязки устройств и средств их защиты) и открытый (для переписки, подписок и т.д.)

+ Использовать СПАМ-фильтры

Не рекомендуется:

- Реагировать на письма от неизвестного отправителя: скорее всего это спам или мошенники

- Открывать подозрительное вложение к письму: сначала позвоните отправителю и узнайте, что это за файл

5 Использование приложений, соцсетей и мессенджеров

Необходимо:

+ Устанавливать приложения только из PlayMarket, AppStore или из проверенных источников

+ Обращать внимание, к каким функциям гаджета приложение запрашивает доступ

+ Обмениваться сообщениями в соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения

Не рекомендуется:

- размещать персональную и контактную информацию о себе в открытом доступе

- Использовать указание геолокации на фото в постах

- отвечать на обидные выражения и агрессию в соцсетях – лучше напишите администратору ресурса

- Устанавливать приложения с низким рейтингом и отрицательными отзывами

6 Защита данных банковской карточки

Необходимо:

+ Хранить в тайне пин-код карты

+ Прикрывать ладонью клавиатуру при вводе пин-кода

+ оформить отдельную карту для онлайн-покупок и не держать на ней большие суммы

+ Использовать услугу «3-D Secure» и лимиты на максимальные суммы онлайн-операций

+ Скрыть CVV-код на карте (трёхзначный номер на обратной стороне), предварительно сохранив его

Не рекомендуется:

- Хранить пин-код вместе с карточкой/на карточке
- Сообщать CVV-код или отправлять его фото
- Распространять свои паспортные данные (информацию личного характера, номер мобильного телефона), «логин» и «пароль» доступа к системе «Интернет-банкинг»
- Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации, пароль 3-D Secure и т.д.