**ВНИМАНИЕ! ХИЩЕНИЕ ДЕНЕЖНЫХ СРЕДСТВ**

**С КАРТ-СЧЕТОВ БАНКОВСКИХ КАРТОЧЕК**

**

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

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.

*Ситуация:*

На мобильный телефон потерпевшего в мессенджере «Viber» позвонил злоумышленник, который представился сотрудником ОАО «АСБ Беларусбанк», после чего сообщил потерпевшему ложные сведения о том, что с его карт-счета производится несанкционированный перевод денежных средств. Злоумышленник пояснил, что для отмены операции необходимо сообщить реквизиты банковской платежной карты (номер карты, срок ее действия, фамилию и имя владельца карты, CVC/CVV-код). Потерпевший, будучи введенный в заблуждение, предоставил злоумышленнику всю запрашиваемую информацию. Предоставление данных сведений привело к тому, что злоумышленник совершил хищение денежных средств с карт-счета потерпевшего путем денежного перевода.

**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.

**СПОСОБЫ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ С КАРТ-СЧЕТОВ:**

- 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 платежной карточки злоумышленника на банковскую карточку пользователя. При этом злоумышленник просит предоставить номер банковской платежной карточки пользователя, срок действия, защитный код и иную информацию. После получения указанных данных злоумышленник совершает хищение денежных средств с карт-счетов пользователeй социальных сетей;

- создание злоумышленником страницы-«двойника» одного из пользователей социальной сети «Одноклассники», с целью введения в заблуждение знакомых пользователей и получения oт 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 на 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 хищение 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.

**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, которые запрашивают 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 на своей карте специальным одноразовым паролем, который он получает в виде SMS-сообщения на свой мобильный телефон.

**НЕЛЬЗЯ** сообщать кому-либо реквизиты банковской платежной карточки, пароли и коды доступа, паспортные данные и другую конфиденциальную информацию третьим лицам.

В базах данных банков имеется вся необходимая информация о клиентах банков, в связи с чем спрашивать дополнительно номер банковской платежной карточки, идентификационный номер паспорта и иные конфиденциальные сведения у них нет необходимости.