ОСТОРОЖНО!!!! МОШЕННИЧЕСТВО С БАНКОВСКИХ КАРТ!

БУДЬ БДИТЕЛЬНЫМ, МОШЕННИК РЯДОМ!!!

В настоящее время участились случаи хищения денежных средств с банковских счетов, доступ к которым **обеспечивается** при использовании банковских платежных карт, после ***передачи*** информации о реквизитах банковских платежных карт злоумышленникам, ***либо завладения*** такой информацией.

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 и владельце, введения кода безопасности - СУС (как правило, трехзначный код, находящийся па оборотной стороне карты), а также кодов (паролей, сеансовых ключей) подтверждения совершения операций, присылаемых банком на мобильный телефон владельца карты. Указанные обстоятельства позволяют злоумышленникам, завладевшим указанными реквизитами банковских платежных карт, совершать платежи в сети интернет без ведома владельца, обладая всей необходимой для этого информацией.

Вместе с тем, система дистанционного банковского обслуживания (интернет-банкинга и мобильного банкинга) постепенно завоевывает статус основной платформы для заказа банковских услуг, осуществления денежных переводов и управления открытыми расчетными счетами. Для доступа к системе виртуального банкинга клиент должен установить мобильное приложение или зарегистрироваться на официальном сайте финансового учреждения. Авторизация производится с привязкой к мобильному номеру телефона. Часто пользователи интернет-банкинга при регистрации указывают пароль доступа, который совпадает с логином пользователя в учетной записи, то есть номером телефона клиента, что позволяет методом подбора осуществлять вход в личные кабинеты пользователей.

В последнее время участились случаи противоправных действий в сфере информационных технологий, а именно хищений с банковских платежных карт и счетов физических и юридических лиц. Примеры подобных фактов приведены далее:

1) Злоумышленник после несанкционированного доступа к страницам пользователей в **социальных сетях** рассылает пользователям, находящимся в разделе **«Друзья»,** сообщения, носящие, в себе просьбы в оказании помощи в переводе денежных средств под различными предлогами: «Привет, не мог ли ты одолжить мне денег, отдам через пару дней», «Привет, положи пожалуйста 10 рублей на телефон, я отдам», «Привет, можно я переведу тебе на карту свои деньги, а то у меня закончился срок действия карты (или не получается перевести на свою)». Далее неравнодушным пользователям он входит в доверие

и якобы для перевода им денежных средств просит сообщить реквизиты банковских платежных карт и коды из смс-сообщений банка, после чего пользователь, будучи введенным в заблуждение относительно лица, осуществившего указанную рассылку, и не догадываясь о преступности его намерений, сообщает ему указанные сведения, ввиду чего злоумышленник получает доступ к денежным средствам пользователя и совершает их хищение. Проведя несанкционированную операцию по переводу денежных средств, злоумышленник зачастую сообщает пользователю, что у него что-то не получается и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

2) На торговой площадке «Куфар», «Барахолка», «Онлайнер» и т.д. злоумышленник находит объявление, размещенное пользователем о продаже какого-либо имущества, после чего в различных мессенджерах пишет указанному пользователю о том, что хотел бы приобрести его имущество, указанное в объявлении, однако по различным причинам не имеет возможности за ним приехать. Он предлагает произвести оплату путем перевода денежных средств на банковскую платежную карту продавца, и после того, как пользователь соглашается, высылает в его адрес ссылку с фишинговой (поддельной) страницей сайта какого-либо банковского учреждения либо службы доставки, например «Доставка Куфар», «Белпочта (EMC)», «курьерская служба (СДЭК)», «Европочта» и т.д. (страница может быть визуально схожа со страницей интернет- банкинга либо службы доставки, как правило, и отличается только символом в адресной строке доменного имени сайта). Переходя по указанной ссылке, пользователь не замечает, что находится не на действующей странице интернет-банкинга определенного банка либо службы доставки. В открывшемся окне на указанном сайте пользователю, как правило, предлагается ввести реквизиты банковской платежной карты, свой логин и пароль от интернет-банкинга, паспортные данные, СУУ-код, а также коды из смс-сообщений банка. Введя указанную информацию, пользователю сообщается об ошибке либо отсутствии платежа. В это время, получив всю указанную информацию, злоумышленник вводит на действительном сайте банка, после чего получает доступ к денежным средствам пользователя и совершает их хищение. Проведя несанкционированную операцию по переводу денежных средств, злоумышленник зачастую сообщает пользователю, что у него что-то не получается и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

3) На торговых площадках «Куфар», «Барахолка», «Онлайнер» и т.д. злоумышленник размещает объявление о продаже какого-либо имущества, пользующегося спросом, и выставляет цену зачастую ниже рыночной. Пользователи, увидевшие указанное объявление, пишут лицу, его разместившему, и в ходе переписки злоумышленник сообщает, что не имеет возможности встретиться для передачи указанного в объявлении имущества и

предлагает воспользоваться услугами «Доставка Куфар», «Белпочта (ЕМС)», «курьерская служба (СДЭК)», «Европочта» и т.д. Получив согласие, злоумышленник высылает в адрес пользователя ссылку с фишинговой страницей сайта какого-либо вида доставки, где на указанном сайте пользователю, как правило, предлагается ввести реквизиты банковской карты для оплаты товара либо услуг курьера, либо паспортные данные, номер мобильного телефона, СУУ-код, а также коды из смс-сообщений. После введения указанной информации, пользователю, как правило, сообщается об ошибке либо сайт перестает загружаться (зависает). В это время, получив всю указанную информацию, злоумышленник вводит ее на действительном сайте банка, после чего получает доступ к денежным средствам пользователя и совершает их хищение. Проведя несанкционированную операцию по переводу денежных средств, злоумышленник зачастую сообщает пользователю, что у него что-то не получается и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

4) На мобильный телефон физического лица поступает входящий звонок от злоумышленника. Как правило, в указанном способе злоумышленник пользуется сервисом по подмене номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним. Далее злоумышленник представляется сотрудником банка (он может назвать пользователя по имени и отчеству, а также назвать часть номера банковской карты, либо информацию о недавно совершенных оплатах). Злоумышленник сообщает о подозрительных операциях по переводу денежных средств на крупные суммы на карт- счета иностранных банков либо иных лиц. Когда пользователь сообщает, что никаких операций он не производил, злоумышленник сообщает, что указанные операции необходимо заблокировать, в связи с чем просит пользователя сообщить отдельные реквизиты банковской платежной карты, либо паспортные данные, после чего сообщает, что в адрес пользователя он высылает смс-сообщения с кодами, которые ему необходимо будет назвать. В это время всю полученную информацию злоумышленник вводит на действительном сайте банка, после чего получает доступ к денежным средствам пользователя и совершает их хищение. (Вся запрашиваемая информация известна сотрудникам банка, и они не стали бы спрашивать ее в ходе телефонного разговора).

Для того, чтобы обезопасить себя и свои денежные средства от подобных способов хищения, необходимо:

1. Не разглашать логины, мобильные номера телефонов, пароли, ПИН-коды, реквизиты расчетных счетов и банковских платежных карт, секретные СУС/СХУ- коды, данные о последних платежах и сроке действия пластиковых карт третьим лицам.

2. В ходе использования карты подключить и использовать технологию «3D Secиге». На настоящий момент это самая современная технология

обеспечения безопасности платежей по карточкам в сети интернет. Позволяет 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 (кодом, сеансовым ключом), который он получает в виде SMS-сообщения на свой мобильный телефон.

3. Исключить передачу посторонним лицам полученные в SMS-сообщениях временные пароли (коды, сеансовые ключи) для подтверждения операций, а также своих банковских карт каким бы то ни было способом.

4. Вводить секретные данные только на сайтах, защищённых сертификатами безопасности и механизмами шифрования. Доменные имена этих ресурсов в адресной строке каждого браузера начинаются с https://.

5. Производить регулярный мониторинг выполненных операций, используя раздел с историей платежей.

6. Не отказываться от дополнительного уровня безопасности (системы многоуровневой аутентификации).

7. Подобрать сложный пароль, используя набор цифр, заглавных и строчных букв, который будет понятен лишь владельцу аккаунта. Менять пароль каждые 2-4 недели, если пользуетесь чужими компьютерами для входа в систему интернет-банкинга.

8. Не использовать автоматическое запоминание паролей в браузере, если к персональному компьютеру открыт доступ посторонним лицам или для входа на сайт пользуется общественный компьютер.

9. В ходе использования интернет-банкинга устанавливать антивирусную защиту, своевременно обновляя базы данных вирусов и шпионских утилит.

10. Вход в личный кабинет на сайте интернет-банкинга привязать к MAC или IP-адресу. Это действие обеспечит максимальный уровень безопасности.

Обращаю особое внимание на то, что в случае обнаружения утерянной кем-либо банковской платежной карты, не стоит выкладывать ее фотографию в сети интернет с целью поиска владельца. Информации, имеющейся на изображении карты, достаточно для совершения операций с использованием этих данных без ведома владельца банковской карты, чем и пользуются злоумышленники.

Таким образом, основной причиной совершения преступлений является недостаточная осведомленность потерпевших о правилах использования реквизитов банковской платежной карты при осуществлении операций в глобальной компьютерной сети Интернет.

Следователь отдела Следственного комитета Фрунзенского района г. Минска
Т.С. Войцеховская