Профилактика киберпреступлений

Следует отметить, что в последнее время участились случаи противоправных действий в сфере информационных технологий, а именно хищений с БПК 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 с просьбой об 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 входит в доверие к неравнодушным пользователям и, якобы для перевода им денежных средств, просит сообщить реквизиты БПК и коды из смс-сообщений. Пользователь, введенный в заблуждение относительно лица, осуществившего указанную рассылку, и не догадываясь о преступности 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 часто сообщает пользователю, что по техническим причинам не может осуществить операцию и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

2. На торговых площадках «Куфар», «Барахолка» и других правонарушитель находит объявление, размещенное пользователем о продаже какого-либо имущества, после чего в различных мессенджерах пишет данному 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 БПК пользователя и, после того как пользователь соглашается, высылает в его адрес ссылку с фишинговой страницей сайта какого-либо банковского учреждения (страница может быть визуально схожа со страницей интернет-банкинга и отличаться 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.

В открывшемся окне на указанном сайте пользователю, как правило, предлагается ввести свой логин и пароль от интернет-банкинга либо паспортные данные, а также коды из смс-сообщений. Введя указанную

информацию пользователю, как правило, сообщается об ошибке либо отсутствии платежа. В это время всю введенную информацию видит злоумышленник и вводит на действительном сайте банка, получая тем самым доступ к денежным средствам пользователя и совершая их хищение. Проведя несанкционированную операцию по переводу денежных средств, правонарушитель нередко сообщает пользователю, что по техническим причинам не может осуществить операцию, и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

3. На торговых площадках «Куфар», «Барахолка» и других злоумышленник размещает объявление о продаже какого-либо имущества, пользующегося спросом, и выставляет цену, как правило, 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 (EMC)», «курьерская служба (СДЭК)» и т. д. При согласии покупателя злоумышленник высылает в адрес пользователя ссылку с фишинговой страницей сайта какого-либо вида доставки, где предлагается ввести реквизиты банковской карты для оплаты товара, услуг курьера, паспортные данные, номер мобильного телефона, а также коды из смс-сообщений. После ввода указанной информации пользователю обычно сообщается об ошибке либо сайт перестает загружаться (зависает). В это время всю введенную информацию видит злоумышленник и вводит ее на действительном сайте банка, получая доступ к денежным средствам пользователя и совершая их хищение. Проведя несанкционированную операцию по переводу денежных средств, злоумышленник сообщает пользователю, что по техническим причинам не может осуществить операцию 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, данным способом злоумышленник пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним. Далее он представляется сотрудником банка (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 крупных сумм денежных средств на карт-счета иностранных банков. 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 БПК либо паспортные данные, и сообщает, что в адрес

пользователя высылает смс-сообщения с кодами, которые необходимо назвать после звукового сигнала. В это время всю полученную информацию злоумышленник вводит на действительном сайте банка, получает доступ к денежным средствам пользователя и совершает их хищение.

5. На мобильный телефон физического лица поступает входящий звонок от злоумышленника. Как правило, при данном способе мошенничества злоумышленник пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним. Далее он представляется сотрудником правоохранительных органов (милиционером, следователем) (может назвать пользователя по имени и отчеству, а также назвать часть номера банковской карты либо информацию о недавно совершенных оплатах). Злоумышленник сообщает о том, что на имя потерпевшего от неустановленного сотрудника банка взят кредит, и с целью установления данного сотрудника банка, в настоящее время проводится спецоперация и потерпевшему необходимо принять в ней участие, а именно – взять кредит на своё имя (в одном или нескольких банках). После получения кредита просит предоставить сведения о карте, либо самостоятельно перечислить денежные средства на указанный им счёт с целью аннулирования кредита. В последующем предлагает направиться в другой банк, либо просто прекращает общение с потерпевшим. В дальнейшем потерпевший узнаёт, что на его имя оформлен кредит (либо кредиты), а денежные средства похищены неустановленным лицом.

6. На мобильный телефон физического лица (как правило пожилым родственникам) поступает входящий звонок от злоумышленника. Как правило, данным способом злоумышленник пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним. Далее он представляется сотрудником правоохранительных органов (милиционером, следователем) и сообщает, что родственник потерпевшего попал в ДТП и находится без сознания (либо иногда дают пообщаться по телефону якобы с дочерью, сыном, мужем и т.п., которые в ходе разговора просят помочь) и родственник виноват в данном ДТП и для «решения» вопроса просят передать через курьера конверт с денежными средствами. После чего приезжает курьер и забирает данные денежные средства.

Вся запрашиваемая преступником указанная в выше обозначенных ситуациях информация известна сотрудникам банка, которые не устанавливают ее в ходе телефонного разговора.

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

не разглашать логины, номера телефонов, пароли, ПИН-коды, реквизиты расчетных счетов, секретные CVC/CW-коды, данные касательно последних платежей и срока действия пластиковых карт третьим лицам;

в ходе использования карты подключить и использовать технологию «3D Secure». На настоящий момент – это самая современная технология обеспечения безопасности платежей по карточкам в сети Интернет. 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;

исключить передачу посторонним лицам полученные в SMS-сообщениях временные пароли для подтверждения операций, а также своих банковских карт, каким бы то ни было способом;

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

производить регулярный мониторинг выполненных операций, используя раздел с историей платежей;

не отказываться от дополнительного уровня безопасности (системы многоуровневой аутентификации);

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;

не применять автоматическое запоминание паролей в браузере, если к персональному компьютеру открыт доступ посторонним лицам или для входа на сайт используется компьютер общего доступа;

в ходе использования интернет-банкинга устанавливать антивирусную защиту, своевременно обновляя базы данных вирусов и шпионских утилит;

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

в случае просьб взять кредит, самостоятельно обратиться в банковское учреждение (либо лично, либо по абонентским номерам, указанным на официальном сайте с городского телефона) с целью уточнения имеется ли на его имя кредит. Не поддаваться на уговоры взять на себя какие-либо денежные обязательства;

не участвовать в «спецоперациях по телефону» (в случае проведения спецоперации, сотрудники милиции обращаются лично, с представлением служебного удостоверения и с обязательным представлением соответствующих документов лицу, с которыми он ознакамливается и подписывает). Сотрудники милиции никогда не проводят спецоперацию «по телефону» и не отправляют фотографию своего служебного удостоверения в мессенджерах;

не поддаваться на уговоры неизвестных лиц, представляющихся сотрудниками правоохранительных органов, на передачу им денежных средств. Сотрудники правоохранительных органов Республики Беларусь никогда «не решают» вопросы о невозбуждении уголовного дела путём передачи им денежных средств или иных услуг. Одним из приоритетных направлений деятельности правоохранительных органов Республики Беларусь является борьба с коррупцией, при поступлении аналогичных звонков, либо предложений от сотрудников о даче им взятки, незамедлительно прекращать диалог с данными лицами (независимо от того разговор был по телефону, либо лично) и сообщать в службу «102», либо по горячей анонимной линии в МВД.

В случае обнаружения утерянной кем-либо БПК не стоит выкладывать ее фотографию в сети Интернет с целью поиска владельца. Информации, имеющейся на изображении БПК, достаточно для совершения операций с использованием этих данных без ведома владельца банковской карты, чем и пользуются злоумышленники.