ГУ «Минский научно-
практический центр хирургии,
трансплантологии и гемаологии»

О содействиив устранении условий, способствующих совершению преступлений.

В Советском (г. Минска) районном отделе Следственного комитета Республики Беларусь в производстве находится уголовное дело №25121070476 о преступлении, предусмотренном ч. 4 ст. 209 УК, возбужденное 01.06.2025, по факту мошенничества.

Проведенное предварительное расследование показало, что в возглавляемом Вами коллективе остаются актуальными для обсуждения вопросы обеспечения безопасности граждан от противоправных действий, а также доведение до работников правил защиты от хищения имущества путем модификации компьютерной информации в целях исключения условий, способствующих совершению в отношении них указанного вида преступлений.

Полагаем необходимым проинформировать коллектив о следующих наиболее распространенных способах хищения имущества путем модификации компьютерной информации и типичных последствиях их применения.

1. Обман потерпевшего под предлогом продажи вещей на интернет-площадке. На торговых интернет-площадках правонарушитель находит объявление, размещенное пользователем о продаже какого-либо имущества, после чего в различных мессенджерах пишет данному пользователю о том, что хочет приобрести его имущество, указанное в объявлении, однако по различным причинам не имеет возможности лично за ним приехать. Он предлагает произвести оплату путем перевода денежных средств на банковскую платежную карточку (далее - БПК) пользователя и после того, как он соглашается, высылает в его адрес ссылку с фишинговой (поддельной) страницей сайта определенного банковского или иного 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 на поддельной странице интернет-банкинга. В открывшемся окне на указанном сайте пользователю, как правило, предлагается ввести свои реквизиты БПК, логин и пароль от интернет-банкинга либо паспортные данные, а также код из смс-сообщения. После ввода указанной информации пользователю сообщается об

ошибке либо невозможности совершить платеж. В это время всю введенную информацию видит злоумышленник и вводит на действительном сайте банка или ином ресурсе, получая тем самым доступ к денежным средствам жертвы и совершая их хищение. Проведя несанкционированную операцию по переводу денежных средств, правонарушитель нередко сообщает пользователю, что по техническим причинам не может ее осуществить, и просит повторить действия с какой-то другой карточкой (родственников или знакомых).

2. Обман поперевшего под предлогом покупки вещей на интернет-площадке. На торговых интернет-площадках злоумышленник размещает объявление о продаже какого-либо имущества, пользующегося спросом, и преднамеренно устанавливает цену ниже рыночной. Пользователи, увидевшие указанное объявление, пишут лицу, его разместившему, и в ходе переписки злоумышленник сообщает, что не имеет возможности лично встретиться для передачи имущества, предлагает воспользоваться курьерскими услугами (например, «Доставка Куфар», «Белпочта (EMC)», «Курьерская служба (СДЭК)»). При согласии покупателя правонарушитель высылает в адрес пользователя ссылку с фишинговой страницей сайта какого-либо вида доставки, где предлагается ввести реквизиты БПК для оплаты товара, услуг курьера, паспортные данные, номер мобильного телефона, а также код из смс-сообщения. После ввода данной 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, он сообщает пользователю, что по техническим причинам не может ее осуществить, и просит повторить указанные действия с какой-то другой карточкой (родственников или знакомых).

3. Обман потерпевшего под предлогом оказания помощи от имени банковских работников. На мобильный телефон потерпевшего поступает входящий звонок от злоумышленника. Как правило, при этом последний пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним, либо использует для осуществления звонка мессенджер (например, Viber), где у вызывающего абонента имеется ярлык с логотипом банковского учреждения. Далее он представляется сотрудником банка (может назвать пользователя по имени и отчеству, а также сообщить часть номера БПК либо информацию о недавно совершенных оплатах). Злоумышленник сообщает о подозрительных

операциях по переводу денежных средств в крупных суммах на карт-счета иностранных банков или оформлении кредитов на имя потерпевшего. Когда потерпевший отвечает, что никаких операций он не производил, злоумышленник сообщает, что указанные операции необходимо заблокировать, в связи с чем просит пользователя назвать отдельные реквизиты БПК либо паспортные данные и сообщает, что высылает в адрес пользователя смс-сообщение с кодом, который необходимо назвать после звукового сигнала. В это время все полученные сведения злоумышленник вводит на сайте банка, получает доступ к денежным средствам пользователя и совершает их хищение. Следует помнить, что запрашиваемая преступником информация сотрудникам банка не требуется ни при каких обстоятельствах и они не будут узнавать о ней у клиента.

4. Обман потерпевшего под предлогом покупки билетов в кино, театр, бронирования кальянных, саун и пр. (так называемая схема «Антикино»). Киберпреступники с фейковых аккаунтов на различных сайтах, представляясь девушками, знакомятся с мужчинами и предлагают продолжить общение в мессенджерах. Для убедительности они направляют собеседникам фотографии и голосовые сообщения, ведут беседы по телефону. Затем мошенники присылают фишинговую ссылку на сайт, например, несуществующего кинотеатра, в котором предлагают провести время. Мужчинам необходимо забронировать места и все оплатить. Потерпевшие вводят реквизиты своих БПК, тем самым предоставляя мошенникам полный контроль над карт-счетами. Таким образом злоумышленники завладевают деньгами. При попытке обратиться в службу поддержки сайта обманутые граждане снова попадают на киберпреступников, что препятствует своевременному обращению в правоохранительные органы.

5. Обман потерпевшего под предлогом продления срока действия SIM-карты. На телефон поступает звонок от неизвестного, представляющегося официальным лицом сотовой компании, которое сообщает об окончании срока действия SIM-карты. Для его продления мошенники просят назвать код из смс-сообщения, который приходит на телефон. Так они пытаются получить доступ в личный кабинет на сайте оператора связи, после чего устанавливают переадресацию на контролируемый преступниками номер. Иногда для вхождения к ним в доверие предлагают перейти потерпевшим по фейковой ссылке.

6. Обман потерпевшего под предлогом оказания содействия в получении посылки на «Белпочте». Потерпевшему направляются сообщения о пришедшей посылке, которую можно получить после заполнения недостающей информации, перейдя по ссылке. В реальности же

последняя является фишинговой, а ввод данных позволяет мошенникам получить доступ к карт-счету и похитить деньги.

7. Обман потерпевшего под предлогом оказания помощи его родственнику или близкому. На мобильный телефон потерпевшего поступает входящий звонок от злоумышленника, который сообщает, что родственник жертвы попал в неприятную историю (например, он участник ДТП, ему грозит тюрьма, он находиться в больнице). После этого трубку берет якобы врач (следователь, милиционер, прокурор) и говорит, что срочно нужны деньги, чтобы оплатить дорогостоящее лечение или дать взятку («откупиться»). В процессе диалога потерпевший беспрекословно выполняет требования мошенника: в некоторых случаях устанавливает на своем телефоне программу AnyDesk, RustDesk, с помощью которых мошенник отслеживает и контролирует все его действия, выведывает конфиденциальную информацию доступа к банковскому счету, вынуждает оформить и переоформить кредит, либо сообщает, что приедет курьер, которому следует передать наличные деньги. Таким образом, в результате мошеннических действий потерпевший лишается денежных средств.

8. Обман потерпевшего под предлогом временного заимствования денег. После несанкционированного доступа к страницам пользователя в социальных сетях злоумышленник рассылает от его имени лицам, находящимся в разделе «Друзья», сообщения с просьбой об оказании помощи, выражающейся в переводе денежных средств, для чего используются различные предлоги: «*Привет, не мог бы 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 преступник входит в доверие к неравнодушным пользователям и якобы для перевода денежных средств просит сообщить реквизиты БПК и коды из смс-сообщений. Пользователь, введенный в заблуждение относительно лица, осуществившего указанную рассылку, не догадавшийся о преступности его намерений, сообщает запрашиваемые сведения, ввиду чего злоумышленник получает доступ к денежным средствам жертвы и совершает их хищение. Проведя несанкционированную операцию по переводу денежных средств, то есть фактически уже похитив деньги с одной карты, злоумышленник часто сообщает, что по техническим причинам не может осуществить операцию и просит повторить указанные действия с какой-либо другой карточкой (родственников или знакомых), чтобы продолжить хищения с других банковских счетов.

Все приведенные примеры показывают, что мошенники используют фактор неожиданности и создают для жертвы максимально неудобные, ограниченные по времени условия для анализа происходящего. Обычно их интересует номер БПК, логин и пароль от кабинета пользователя, коды из смс-сообщения.

Для того чтобы обезопасить себя и свои денежные средства, необходимо соблюдать следующие правила:

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

подключить и использовать технологию «3D Secure», которая обеспечивает безопасность платежей в сети Интернет, позволяет однозначно идентифицировать подлинность держателя карты, осуществляющего операцию, и максимально снизить риск мошенничества. При использовании этой технологии держатель БПК подтверждает каждую операцию по своей карточке специальным сеансовым паролем, который он получает в виде смс-сообщения на свой мобильный телефон;

исключить передачу посторонним лицам полученных в смс-сообщениях сеансовых паролей для подтверждения операций, а также своих БПК, 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: //, а не http://;

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

использовать дополнительный уровень безопасности (системы многоуровневой аутентификации, смс-информирование о расходных операциях);

подобрать сложный пароль, используя набор цифр, заглавных и строчных букв, который будет понятен лишь владельцу аккаунта. Изменять 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 если для входа на сайт используется компьютер общего доступа;

устанавливать антивирусную защиту, своевременно обновляя базы данных вирусов и шпионских утилит;

привязать к MAC или IP-адресу вход в личный кабинет на сайте интернет-банкинга;

выкладывать фотографию БПК в сеть Интернет, поскольку имеющихся на изображении сведений может быть достаточно для совершения операций с использованием этих данных без ведома владельца.

В целях устранения причин и условий, способствовавших совершению преступления, руководствуясь ст, 4 Закона Республики Беларусь от 13.07.2012 г. № 403-З «О Следственном комитете Республики Беларусь», п. 11.5 Положения о Следственном комитете Республики Беларусь, утвержденного Указом Президента Республики Беларусь от 10.11.2011 № 518 «Вопросы Следственного комитета Республики Беларусь»,