ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕПРАВОМЕРНЫМ ЗАВЛАДЕНИЕМ РЕКВИЗИТАМИ ПЛАСТИКОВЫХ БАНКОВСКИХ КАРТ И ХИЩЕНИЕМ СРЕДСТВ С КАРТ-СЧЕТОВ ГРАЖДАН, А ТАКЖЕ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Материал подготовлен
управлением Следственного комитета Республики Беларусь
по Гродненской области

На сегодняшний день борьба с киберпреступностью – одно из приоритетных направлений в деятельности всей правоохранительной системы Республики Беларусь и Следственного комитета в частности.

Актуальность этого обусловлена значительным числом преступлений, совершаемых с использованием информационно-коммуникационных технологий (далее – ИКТ), доля которых составляет треть от общего числа всех зарегистрированных уголовно-наказуемых деяний.

Подавляющую часть преступлений, совершенных с использованием ИКТ, составляют хищения денежных средств с карт-счетов граждан путем завладения реквизитами банковских пластиковых карт.

В Гродненской области такие деяния фиксируются ежедневно, нередко за сутки более 10 таких хищений.

Потерпевшими от них являются все слои населения – преподаватели, студенты, медицинские работники, пенсионеры, безработные, лица, находящиеся в отпуске по уходу за ребенком в возрасте до 3-х лет, а также работники различных организаций и предприятий.

Все чаще имеют место случаи завладения крупными суммами.

Причины и условия, способствующие совершению преступлений, как правило беспечность самих пользователей, а именно держателей банковских карт, их излишняя доверчивость, неосмотрительность, неосведомленность о способах защиты и компрометации платежных реквизитов.

Уголовно-наказуемые деяния названной категории характеризуются высокой степенью латентности, и, как следствие, крайне низкой раскрываемостью.

Практика расследования уголовных дел о таких преступлениях показывает, что их легче предотвратить, чем раскрыть и найти виновного.

На текущий момент на территории Республики Беларусь и Гродненской области в частности можно выделить следующие наиболее распространенные способы и схемы хищений с использованием ИКТ:

1. Завладение денежными средствами **под предлогом продажи товаров** в социальных сетях и через мессенджеры. Наиболее часто в последнее время – в социальной сети «Инстаграм». Злоумышленники создают фейковые аккаунты по продаже одежды, обуви, предметов мебели и интерьера, наполняют их тематических контентом из свободных источников сети Интернет с фотографиями якобы реализуемого товара, рядом положительных отзывов, и с доступными ценами ниже рыночных, вступают в переписку в различных мессенджерах, предлагая внести за товар предоплату либо аванс путем перечисления на банковский счет. Для получения денежных средств при этом, как правило, используются банковские карт-счета подставных лиц («дропов», как осведомленных, так и нет), согласившихся оформить на свое имя банковскую карту, передав ее либо аутентификационные данные (логин и пароль системы дистанционного банковского обслуживания (далее – СДБО)) для доступа к счету. Далее происходят переводы денежных средств на иные счета, нередко обналичивание «дропами», иными нанятыми злоумышленниками лицами, обмен на криптовалюту посредством онлайн-сервисов либо ИП – граждан, предоставляющих указанные услуги путем размещений объявлений в сети Интернет.

Аналогичные объявления о продаже товара могут размещаться на веб-сайтах, в сообществах или путем рассылки в мессенджерах, а также на сайтах аренды надвижимости под предлогом внесения предоплаты за аренду квартиры.

2. **Фишинг** (от англ. fishing - рыбная ловля, выуживание) – один из видов мошенничества, целью которого является получение доступа к конфиденциальной информации пользователей (реквизитам банковских платежных карт, логинам и паролям СДБО, мобильного банкинга, паспортным данным и иным личным сведениям) в целях последующего хищения денежных средств посредством использования данных реквизитов. Наиболее часто данная преступная схема реализовывается в отношении клиентов торговых интернет-площадок (например, kufar.by). Выступая в роли покупателя, злоумышленник находит продавца товара и вступает с ним в переписку в мессенджерах («Viber», «Telegram», «WhatsApp»). Он сообщает, что товар его заинтересовал и уже якобы совершил предоплату (зачастую высылается скриншот электронного чека о перечислении средств). Для того, чтобы получить данные средства, продавцу якобы необходимо пройти по

гиперссылке и ввести данные. Невнимательный интернет-пользователь может и не заметить подмены, так как подобные страницы визуально схожи с оформлением сайтов известных сервисов (Куфар, ЕРИП, CDEK, Белпочта, сайты различных банков и др.). Адрес поддельной веб-страницы также может напоминать реальный (kufardostavka.by, erip-online.cot, belarusbank24.xyz, cdek-zakaz.info и др.). Если жертва «попадется на удочку» и заполнит форму, соответствующие реквизиты доступа к банковскому счету окажутся у преступника. Через считанные минуты злоумышленник осуществляет доступ к банковскому счету и переводит денежные средства на контролируемые им банковские счета посредством сервисов перевода («МТБанк», иные), зарегистрированные на подставных лиц.

Имели место случаи создания и использования злоумышленниками фишинговых сайтов, ориентированных под запросы пользователей в поисковых системах. Граждане попадают на них прямо из Google и Yandex после запросов типа «Беларусбанк личный кабинет», «Белагропромбанк интернет банкинг» и т.д. Увидев знакомый заголовок и логотип сайта в выдаче результатов поиска и не удостоверившись в соответствии адреса сайта действительному доменному имени банковского учреждения, потерпевший заполняет открывшуюся форму авторизации. В результате введенные данные отправляются преступнику, а не банку. Далее хищение денег происходит аналогично с выводом денежных средств на иные счета, обналичивания либо обмена на криптовалюту.

Также приобрела популярность мошенническая схема, связанная с проведением якобы «рекламных акций» от имени известных в Беларуси торговых брэндов. После прохождения опроса на поддельном сайте (практически не отличимом от оригинального) пользователю для получения выигрыша предлагалось скачать и установить мобильное приложение, привязав к нему бонусную и банковскую карту. Если жертва выполняла это условие - мошенники получали реквизиты для хищения денежных средств.

3. **Вишинг** (англ. vishing, от voice phishing) – один из способов мошенничества с использованием социальной инженерии, который заключается в выведении злоумышленников жертвы на желаемую модель поведения с целью завладения конфиденциальной информации для последующего хищения средств. Как правило, преступники маскируются в мессенджерах под логотипом узнаваемых белорусских банков, вводя в заблуждение потенциальных жертв. От имени банковского сотрудника или представителя правоохранительных органов злоумышленники сообщают жертве, что необходимо

осуществить какие-либо действия с банковской платежной картой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо производит подозрительную оплату. Завладев реквизитами банковской платежной карты, преступники осуществляют хищение денежных средств с банковского счета потерпевшего. В последнее время наиболее актуальная схема – побуждение жертвы открыть кредит. Злоумышленники сообщают жертве о том, что якобы кто-то посторонний пытается открыть кредит на ее имя, и для его деактивации необходимо самостоятельно обратиться в банк и открыть кредит, переслав впоследствии реквизиты счета.

Аналогично актуальна схема завладения денежными средствами посредством инсценировки ДТП по вине близких или родственников, когда пожилых людей вынуждают передать крупные суммы денежных средств для возмещения ущерба, под предлогом освобождения от уголовной ответственности и т.п., при которой также в какой-то части используются ИКТ.

4. **Вымогательство** или шантаж. В ряде случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства. Социальные сети – это кладезь персональной информации о человеке. Получив несанкционированный доступ к страницам в социальных сетях, переписке электронных почтовых ящиков и облачным аккаунтам и завладев изображениями, не предназначенными для публичного просмотра, преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая в случае отказа распространить их в сети Интернет. Аналогично «на удочку» преступников попадаются лица, вступающие в переписку с различными пользователями на сайте знакомств (эротического и порноконтента), когда общение продолжается в формате видеосвязи и злоумышленник вынуждает «жертву» показать обнаженные части тела, в дальнейшем требуя перевода денежных средств под аналогичной угрозой распространения фотографий или видеозаписи, в том числе указывая потерпевшему контакты знакомых из социальной сети.

5. **Свободный доступ к банковской карте.** В ряде случаев причиной хищений с банковских счетов становятся не хитрые схемы мошенников, а банальная утеря карты, оставление ее в легкодоступном месте или передача иным лицам для осуществления разовых платежей. Разновидностью подобного легкомыслия является хранение фотоизображений банковских карт или платежных реквизитов в памяти мобильного телефона, в почтовом аккаунте или дистанционном облачном хранилище. При несанкционированном доступе к такому

хранилищу преступник получает беспрепятственный доступ к банковскому счету его владельца. Риск остаться без заработанных денежных средств также увеличивает хранение PIN-кода рядом с картой (например, записанным на бумажке в кошельке или на самой банковской карте).

6. **BEC-атаки (компрометация деловой электронной переписки) с целью хищения денежных средств предприятий с подменой реквизитов банковских счетов контрагента.**

Способ совершения рассматриваемого вида мошенничества заключается в подмене реквизитов банковских счетов зарубежных контрагентов (Польша, Италия, Литва и др.) при оплате за поставку товаров.

Так, после согласования существенных условий контракта с зарубежным партнером, а в отдельных случаях и его подписания на электронную почту организации (предприятия) преступниками направляется сообщение якобы от имени сотрудника иностранного контрагента об изменении реквизитов банка и необходимости перечисления денежных средств на новый счет (например, по причинам уплаты значительного налога в ранее обслуживающем банке, превышения лимита на счету, проведения в отношении предприятия государственного аудита).

При этом адрес электронной почты мошенников имеет значительное сходство с реальным, что часто остается незамеченным (например, sales.bianchi@gmail.com вместо sales@bianchi.com), а в отдельных случаях является идентичным. Особенностью также является то, что в содержании первоначально направляемых писем отсутствуют какие-либо вложения, гиперссылки, в связи с чем они не вызывают подозрения у сотрудников организации и не определяются антивирусным программным обеспечением в качестве угрозы безопасности. Последующая переписка уже осуществляется с киберпреступниками.

Реализация подобной схемы хищения возможна с помощью получения несанкционированного доступа к электронной почте одной из сторон сделки (посредством действия вредоносной программы, фишинга, подбора пароля). Получив доступ к электронной почте субъекта хозяйствования, преступники располагают информацией о предмете, условиях договора и могут вести переписку, не вызывая подозрения. Поэтому в случае необходимости ими направляются дополнительное соглашение, инвойс, однако с измененными реквизитами банковского счета и контактными данными представителей фирмы путем их наложения на подготовленные ранее и сохраненные в

сообщениях документы. При этом письма реального контрагента вследствие изменения настроек электронной почты автоматически помечаются как прочитанные и переадресовываются в папку «Спам» или «Корзина».

Чтобы не стать жертвой киберпреступников необходимо придерживаться следующих правил:

- никогда, никому и ни при каких обстоятельствах не сообщать реквизиты своих банковских счетов и банковских карт, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов;

- не следует сообщать в телефонных разговорах и при общении в соцсетях полный номер карточки, срок ее действия, код CVC/CVV (находящиеся на обратной стороне карты), логин и пароль к интернет-банкингу, паспортные данные, кодовое слово (цифровой код) из SMS-сообщений;

- в случае поступления звонка «от сотрудника банка» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить в банк или в круглосуточную службу сервиса, номер которой написан на оборотной стороне платежной карты, сообщить о случившемся. Скорее всего, никаких несанкционированных операций не было, и никто из банка не звонил;

- в том случае, если с использованием Вашего счета и правда кто-то будет пытаться совершить несанкционированные операции и банк это заметит, то его сотрудники сперва инициативно заблокируют банковскую платежную карту, затем сообщат Вам причину принятого решения (ничего не уточняя) и пригласят посетить банк с паспортом для получения наличных денежных средств и написания заявления на перевыпуск карты;

- ни в коем случае не предоставлять доступ к мобильному устройству посторонним лицам. Никогда не устанавливать по просьбам незнакомых лиц программы удаленного доступа, такие, например, как «AnyDesk», «TeamViewer» и др. Не сообщать незнакомым лицам сеансовые коды. Через эти приложения мошенники могут получить доступ к мобильному приложению интернет банкинга на Вашем устройстве и совершить хищение денежных средств. Следует знать: сотрудники банков никогда не используют для связи с клиентами мессенджеры («Viber», «Telegram», «WhatsApp»);

- в настоящее время просто необходимо наличие второй банковской платежной карты, не привязанной к основному банковскому счету (например, зарплатному). Этой картой следует рассчитываться в сети Интернет, заранее пополняя ее на необходимую сумму. В таком

случае Вы сможете обезопасить свой основной банковский счет. Многие банки предлагают своим клиентам услугу выпуска «виртуальной карты». Процесс ее открытия не требует посещения клиентом банка и представляет собой достаточно быстрый процесс. В итоге Вы станете обладателем электронного аналога банковской карты, посредством которой сможете рассчитываться за услуги в сети Интернет без риска скомпрометировать основной банковский счет. Просто перед оплатой следует пополнить ее необходимой суммой с основной карты;

- каждый владелец банковских платежных карт может настроить собственный алгоритм безопасности при их использовании. Для обеспечения сохранности денежных средств, размещенных на банковских счетах, каждый держатель карточки посредством систем дистанционного банковского обслуживания может установить индивидуальные ограничения (лимиты/запреты). Среди основных – следующие: подключение технологии 3D-Secure (обязательное подтверждение операций, совершаемых держателями карточек с применением их реквизитов в сети Интернет); установление банком-эмитентом ограничение на проведение расходных операций (максимальная сумма и количество операций в определенный период времени); возможность самостоятельно устанавливать ограничения (на проведение операций в сети Интернет, на совершение операций в конкретной стране, на совершение отдельных видов операций);

- для доступа к системам дистанционного банковского обслуживания (СДБО) и личным аккаунтам необходимо использовать сложные пароли, исключающие возможность их подбора. Рекомендуется составлять комбинации паролей не менее чем из 12 знаков (цифры, буквы и символы в разном регистре). Следует создавать уникальные пароли для каждого сервиса в отдельности. Стоит воздержаться от паролей, составленных из дат рождения, имен, фамилий – то есть тех, которые легко вычислить из общедоступных источников информации (например, тех же социальных сетей). Также следует регулярно менять пароли, чем чаще – тем лучше. Пользуйтесь только проверенным менеджером паролей;

- при поступлении в социальных сетях сообщений от лиц, состоящих в категории «друзья», с просьбами о предоставлении реквизитов банковских платежных карточек – не следует сразу же отвечать на подобные сообщения. Нередко такие просьбы рассылаются от имени друзей преступниками, взломавшими аккаунт в социальной сети и получившими доступ к конфиденциальной переписке. Поэтому сначала необходимо связаться с этим человеком (по телефону, лично встретиться) и уточнить, действительно ли он нуждается в помощи;

- для того, чтобы не стать жертвой мошенника, позвонившего по телефону и сообщившего о попадании в беду родственника, необходимо немедленно прекратить телефонный разговор. Этим преступник лишится возможности использовать свои психологические приемы для воздействия. После этого следует перезвонить близкому человеку и лично уточнить у него, что произошло. Если звонивший уверяет, что родственник находится в милиции или с его участием проводятся следственные действия, необходимо позвонить в дежурную часть органа внутренних дел или по номеру 102, и выяснить правдивость его слов;

- в целях защиты устройств необходимо использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систем. Установить антивирусную программу следует не только на персональный компьютер, но и на смартфон, планшет и регулярно обновлять ее.