МАТЕРИАЛЫ

для информационно-пропагандистских групп
(сентябрь 2022 г.)

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

Борьба с киберпреступностью – одно из актуальных направлений в деятельности правоохранительных органов, о чем свидетельствуют ежедневные факты возбуждения следственными подразделениями области уголовных дел данной категории. Подавляющую их часть составляют хищения денежных средств с карт-счетов граждан путем завладения реквизитами банковских пластиковых карт.

Указанные общественно опасные деяния в Гродненской области фиксируются ежедневно, нередко за сутки более чем по 10 таких хищений.

Потерпевшими от названных уголовно-наказуемых деяний 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 – беспечность самих пользователей, а именно держателей банковских карт, их излишняя доверчивость, неосмотрительность, неосведомленность о способах защиты и компрометации платежных реквизитов.

Преступления названной категории характеризуются высокой степенью латентности, и, как следствие, крайне низкой раскрываемостью. Ввиду чего преступления названной категории легче предотвратить, чем раскрыть и найти виновного.

В настоящее время наиболее распространенными способами завладения реквизитами доступа к банковским счетам являются:

1. Вишинг (англ. vishing, от voice phishing) - один из методов 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.

2. Фишинг (от англ. fishing - рыбная ловля, выуживание) - один из видов мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам и паролям) и последующего хищения денежных средств. Наиболее часто данная преступная схема реализовывает в отношении клиентов торговых интернет-площадок. 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 или электронные кошельки, зарегистрированные на подставных лиц.

3. 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).

4. Покупка с предоплатой. Наиболее простой, но от этого не менее работающей формой интернет мошенничества, является размещение преступниками объявлений о продаже каких-либо товаров по бросовым ценам. Но для его получения (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту, электронный кошелек. Обычно после перечисления ожидаемый товар так и не поступает, а «продавец» перестает выходить на связь.

5. Шантаж. В некоторых 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.

6. Онлайн-игры. Индустрия производства игр для персональных компьютеров и мобильных гаджетов давно стало высокодоходным бизнесом. Не удивительно, что повышенным вниманием она пользуется и у мошенников. Ценность тут представляют и аккаунты пользователей, к которым нередко привязаны реквизиты банковских платежных карт для покупки игровых преимуществ, и коллекционные предметы, которые игроки также нередко приобретают за реальные деньги.

В последнее время участились случаи создания 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.

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.

Чтобы не стать жертвой киберпреступников необходимо придерживаться следующих правил:

- никогда, никому и ни при каких обстоятельствах не сообщайте 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. Сообщите 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 предоставляйте доступ к мобильному устройству посторонним лицам! Никогда не устанавливайте по просьбам незнакомых лиц программы удаленного доступа, такие, например, как «AnyDesk», «TeamViewer» и др. Не сообщайте незнакомым лицам сеансовые коды! Через эти приложения мошенники могут получить доступ к мобильному приложению интернет банкинга на Вашем устройстве и совершить хищение денежных средств. Учтите: 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 рассчитывайтесь 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 пополните ее необходимой суммой с основной карты - и никаких проблем!;

- 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 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). Создавайте 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 менеджерам 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;

- 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.