Одним из самых распространенных киберпреступлений остается хищение денежных средств при помощи модификации компьютерной информации. Причем в большинстве случаев эти преступления становятся возможны из-за беспечности самих потерпевших, предоставивших реквизиты доступа к своим банковским счетам.

Преступники завладевают реквизитами, необходимыми для осуществления преступных транзакций, посредством следующих основных способов:

«Звонок из банка»

Вишинг (англ. vishing, от voicephishing) 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, для совершения звонка преступники используют один из распространенных мессенджеров, используя функцию подмены номера, Как следствие, у потерпевшего на экране мобильного телефона может отображаться совершенно любой номер телефона, заданный злоумышленником, Также преступники маскируются 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.

«Фишинг»

Фишинг (от англ. 3shing -- 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 роди 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 прлучить данные средства, продавцу якобы необходимо пройти по 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. сот, 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.

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.

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 хранилище преступник получает беспрепятственный доступ к банковскому счету его владельца.

Риск остаться без заработанных денежных средств также увеличивает хранение РИН-кода рядом с картой (например, записанным на бумажке в кошельке или на самой банковской карте).

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) тр4ется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту, электронный кошелек. Обычно после перечисления ожидаемый товар так и не поступает, а «продавец» не выходит на связь.

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.

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 тутпредставляют 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.

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.

Также 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).

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.

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!

Ни в коем случае не предоставляйте доступ к мобильному устройству посторонним лицам!

Никогда не устанавливайте по просьбам незнакомых лиц дрограммы 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,

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 могут 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

В целях правильной квалификации хищений денежных средств из банкоматов с использованием банковских платежных карточек необходимо четкое представление способа совершения данного преступления:

- банковская платежная карточка (далее-карточка) – платежный инструмент, обеспечивающий доступ к банковскому счету и проведение безналичных платежей за товары и услуги, получение наличных денежных средств и осуществление иных операций;

- система расчетов с использованием карточек (далее - система) -совокупность банковских и иных организаций, обеспечивающих эмиссию, использование карточек, процессинг, эквайринг, осуществление расчетов по операциям, совершаемым при использовании карточек;

- владелец системы - юридическое лицо, определяющее правила и процедуры проведения участниками системы операций с карточками;

- банк-эмитент банк, осуществляющий эмиссию карточек и определяющий правила совершения операций с карточками (собственник карточек);

- банкомат электронный программно-технический комплекс, обеспечивающий выдачу наличных денежных средств и совершение других операций при использовании карточек, а также регистрацию этих операций;

- процессинг деятельность по сбору и обработке информации, поступающей от предприятий торговли (сервиса), банкоматов, пунктов выдачи наличных денежных средств либо в электронном виде из иных источников (оборудование и программные средства, обеспечивающие процессинг, подпадают под понятие компьютерной системы, содержащееся в ГОСТ ИСО/МЭК 2382-1-99 «Информационная технология. Словарь. Часть 1. Основные термины.»); - держатель - физическое лицо, правомерно использующее карточку;

- авторизация - разрешение, предоставляемое банком-эмитентом или

владельцем системы на проведение операции, совершаемой при использовании карточки, в результате которого возникает обязательство банка-эмитента или владельца системы по оплате документов, составленных при использовании карточки.

Как следует из приведенных понятий, правила осуществления операций с использованием карточек определяются владельцем конкретной системы расчетов. Банки Республики Беларусь на сегодняшний день являются участниками двух международных систем (Visa International и MasterCard International) и одной внутренней системы (Белкарт). Согласно правилам, определенным международными системами, для совершения операции с карточкой, в частности для получения наличных денежных средств в

банкомате, необходимо: пластиковая карточка с магнитной полосой, на которой в форме, определенной системой расчетов, хранится часть информации, необходимой для авторизации;

1) ПИН-код (персональный идентификационный номер) идентификатор держателя карточки;

2) наличие денежных средств на карт-счете (если карточка дебетовая) либо наличие возможности распоряжения определенными средствами (если карточка кредитная). Процесс получения наличных денежных средств заключается в следующем. Карточка вставляется в банкомат (аналог помещения дискеты в дисковод компьютера), который считывает информацию с магнитной полосы карточки и передает ее по компьютерной сети (компьютерная сеть - сеть из узлов обработки данных, взаимосвязанных с целью обмена данными в компьютерную систему процессингового центра. В целях удостоверения факта использования карточки ее держателем компьютерная система процессингового центра запрашивает ПИН-код, который держатель карточки вводит с использованием имеющейся в банкомате клавиатуры. Здесь следует отличать характер вводимой информации в зависимости от того, кем она вводится, держателем карточки и злоумышленником. Несмотря на то, что по содержанию информация одинаковая, в противном случае не будет получено разрешение на выдачу денежных средств, для злоумышленника указанная информация является заведомо ложной, т.е. на предложение ввести свой идентификационный номер (сообщить свое имя) злоумышленник заведомо вводит номер, который ему не присваивался (сообщает не свое имя, а имя держателя карточки). Следовательно, такая информация об использовании карточки именно держателем для процессингового центра будет являться ложной. После проведения проверки введенной информации лицу, использующему карточку, предоставляется доступ к банковскому счету и, соответственно, возможность распоряжаться денежными средствами по нему. Такой доступ является несанкционированным (несанкционированный доступ - доступ к компьютерной информации лица, не имеющего права на доступ к этой информации либо имеющего такое право, но осуществляющего его помимо установленного порядка). Затем осуществившее несанкционированный доступ лицо, воспринимаемое компьютерной системой как правомерный держатель банковской платежной карточки, вводит в компьютерную систему информацию, посредством которой дает команду на совершение определенной операции по банковскому счету (выдача наличных, проведение платежа либо др.). Такая информация является ложной, поскольку она не отражает волю владельца счета, вводится не им и не уполномоченным им лицом. После этого в результате введения указанной ложной информации происходит выдача

банкоматом запрошенной суммы наличных денежных средств либо оформление предусмотренных платежей. При этом совершается завладение денежными средствами банка, обслуживающего используемый банкомат (банк-эквайер). Впоследствии вопрос о возмещении суммы, выданной через банкомат в результате несанкционированного доступа, между банком-эмитентом, банком-эквайером и держателем пластиковой карточки решается в соответствии с условиями заключенных договоров и правилами платежной системы. Поэтому при решении вопроса о том, кто должен признаваться потерпевшим и гражданским истцом по делу, следует исходить из положений договора, заключенного между гражданином-владельцем карт-счета и банком-эмитснтом, в котором, как правило, определены условия, при соблюдении которых банк возмещает либо не возмещает гражданину суммы денежных средств, полученных с использованием банковской карточки в результате несанкционированного доступа.

Таким образом, хищения денежных средств банков Республики Беларусь из обслуживаемых ими банкоматов при помощи банковских пластиковых карточек лицами, не являющимися их держателями, сопряжены с несанкционированным доступом к компьютерной информации о карт- счетах держателей банковских пластиковых карточек и совершаются путем введения в компьютерную систему процессингового центра (которым являются сами банки либо ОАО «Банковский процессинговый центр») заведомо ложной информации об использовании банковских пластиковых карточек их держателями, что подлежит квалификации по ч. 2 ст. 212 УК Республики Беларусь, а при наличии соответствующих квалифицирующих признаков по частям 3 или 4 указанной статьи.

Статья 222. Незаконный оборот средств платежа и (или) инструментов

1. Изготовление в целях сбыта либо сбыт поддельных банковских платежных карточек, иных платежных инструментов и средств платежа, а равно совершенное из корыстных побуждений незаконное распространение реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам, -

наказываются штрафом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок от двух до шести лет.

2. Те же действия, совершенные повторно, либо организованной группой, либо в особо крупном размере, -

наказываются ограничением свободы на срок от трех до пяти лет или лишением свободы на срок от трех до десяти лет со штрафом или без штрафа.

Статья 212. Хищение имущества путем модификации компьютерной информации

1. Хищение имущества путем модификации компьютерной информации -

наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. То же деяние, совершенное повторно либо группой лиц по предварительному сговору, -

наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, совершенные в крупном размере, -

наказываются ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от двух до семи лет со штрафом или без штрафа и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

4. Деяния, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок от пяти до двенадцати лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 209. Мошенничество

1. Завладение имуществом либо приобретение права на имущество путем обмана или злоупотребления доверием (мошенничество) -

наказываются общественными работами, или штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. Мошенничество, совершенное повторно либо группой лиц, -

наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок до четырех лет, или лишением свободы на тот же срок.

3. Мошенничество, совершенное в крупном размере, -

наказывается ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от двух до семи лет со штрафом или без штрафа.

4. Мошенничество, совершенное организованной группой либо в особо крупном размере, -

наказывается лишением свободы на срок от трех до десяти лет со штрафом.