**О профилактике преступлений**

**против информационной безопасности.**

Такая проблема, как хищение денежных средств с карт-счетов доверчивых граждан с использованием глобальной компьютерной сети Интернет, коснулась уже очень многих ивьевчан.

Способы, с помощью которых злоумышленники завладевают денежными средствами граждан, разнообразны и совершенствуются с каждым днем. В основном, эти лица пользуются доверчивостью граждан, создавая фишинговые страницы известных интернет-платформ или официальных сайтов банковских учреждений, осуществляя звонки и представляясь сотрудниками банков, которыми якобы были зафиксированы попытки проведения подозрительных операций по карт-счету владельца.

Граждане, находясь в условиях минимального времени для рациональной и трезвой оценки сложившейся обстановки, зачастую идут на поводу у злоумышленников, сами передавая все необходимые реквизиты для доступа к своему карт-счету. По прошествии небольшого количество времени после осознания неправдоподобности произошедшей ситуации люди начинают проверять баланс своего счета, звонить по контактным номерам банков-эмитентов своих банковских карт. Но оказывается уже слишком поздно—злоумышленникам достаточно нескольких долей секунд, чтобы деньги перешли на их счет и ушли в неизвестном направлении. И требовать отмены операции у банка-эмитента бесполезно, ведь держатель карты сам передал все необходимые данные, в том числе зачастую и такой нужной услуги «3D-Secure», чтобы попрощаться со своими накоплениями.

Так, ранее были популярны такие способы хищения денежных средств, когда злоумышленники в сети Интернет получали несанкционированный доступ к аккаунтам граждан в различных социальных сетях, а затем вели переписку с лицами из числа «друзей» и под различными предлогами выманивали деньги или реквизиты банковских карт. В этих ситуациях следует помнить, что перед тем, как отправить деньги или дать реквизиты своей банковской карты, следует найти иной способ связаться с человеком и убедиться, что ему действительно нужна Ваша помощь. А если нет способа связаться, то хоть в переписке надлежит убедиться, что это не злоумышленник, спросив у человека какую-то информацию, известную только Вам.

Но со временем пользователи социальных сетей стали не такими доверчивыми, стали появляться новые схемы.

Сейчас набирают популярность следующие способы завладения денежными средствами доверчивых граждан:

- поступает звонок на номер мобильного телефона гражданина, зачастую даже от мобильного оператора иностранного государства (и тут уже следовало бы задуматься, ведь банк расположен на территории нашего государства); в ходе беседы гражданину сообщают, что по его счету зафиксированы подозрительные операции по переводу денежных средств и во избежание хищения необходимо подтвердить свои паспортные данные и указать реквизиты банковской карты; гражданин указывает свой номер карты, CVV-код (три числа на оборотной стороне банковской карточки), передает текст смс-сообщений с паролями доступа от банка (хотя в данных смс-сообщениях прямо указано, что данные пароли никому нельзя указывать), после чего злоумышленник, продолжая с гражданином беседы и не давая ему возможность критически оценивать ситуацию, тянет время, может в течение маленького промежутка времени перезвонить с иных номеров с указанием на то, что идет работа по сохранению денежных средств владельца, а в это время карт-счет гражданина опустошается. Здесь надо быть бдительным и ни под каким предлогом никому не передавать указанные выше сведения, а сразу завершить подобный звонок и самостоятельно перезвонить в свой обслуживающий банк, рассказать о ситуации, проверить свой баланс и проведенные операции, а при необходимости заблокировать свой карт-счет самостоятельно при помощи услуг «Интернет-банкинга» или «М-банкинга»;

- на популярной площадке торговых объявлений «Kufar» с продавцом вступает в переписку якобы потенциальный покупатель, который проявляет активный интерес к товару, изъявляет намерение его приобрести, интересуется характеристиками, но при этом переписку ведет только посредством мессенджера «Viber» (зачастую также с номеров мобильных операторов иностранных государств), под всякими благовидными предлогами избегая прямых контактов и не указывая своих каких-то иных контактных данных; в ходе переписки покупатель изъявляет желание приобрести товар с использованием доставки от «Kufar» или «Evropochta», передает гражданину в сообщении ссылку на сайт, который отличается от официального несколькими символами; далее злоумышленник зачастую убеждает продавца пополнить свой карт-счет на сумму, не меньшую сумме предстоящей покупки; гражданин, переходя по сомнительной ссылке, оставляет все реквизиты доступа к своему карт-счету на предложенном ему сайте, после чего расстается во своими сбережениями. В этой ситуации надо помнить, что покупки и переписку при использовании торговой площадки «Kufar» надо производить исключительно на самом сайте «Kufar» и внимательно следить, чтобы в адресной строке был прописан именно адрес «Kufar.**BY**», а также изучить условия и правила доставки и оплаты товара, указанные именно на данном официальном сайте. К тому же, следует всегда не забывать, что если сомневаетесь в добросовестности покупателя, то есть много иных безопасных способов оплаты при покупке- продаже, которые Вам знакомы и в которых Вы уверены;

- приходит рассылка на электронную почту или в личные сообщения в социальных сетях с информацией о том, что Вы стали победителем какого-то супер-розыгрыша или были выбраны среди множества иных пользователей (тут уже стоит задуматься, особенно, если в каких-либо розыгрышах Вы не участвовали, а про то, что «холявы» не бывает, как-то забыли), а для того, чтобы получить деньги, надо перейти по предложенной ссылке; перейдя по ссылке, гражданин может попасть на какую-то яркую страницу, где надо выбрать среди прочих какой-то сундучок или наподобие того и (о чудо!) он становится счастливым обладателем внушительной суммы денежных средств, зачастую, даже в иностранной валюте; и тут для того, чтобы получить эту неожиданно именно Вам доставшуюся сумму, надо всего лишь дать данные своей банковской карты, которые гражданин, уже мысленно продумывая, куда же он потратит свой клад, не задумываясь, вносит; но, конечно же, возникают какие-то «мелкие» трудности, для устранения которых надо дать еще свой номер телефона, паспортные данные, коды из смс-сообщений, чтобы не потерять выигрыш; а после передачи всех указанных сведений, выигрыш растворяется вместе с балансом банковской карты. В этих и подобных ситуациях просто надо помнить, что «холявы» не бывает и никакие деньги из воздуха именно Вам не придут (если, конечно, нет какого-то совершенно неожиданно почившего богатого родственника, у которого не было иных наследников). При этих случаях надо опять же ни под каким предлогом никому не передавать указанные выше сведения о своей банковской карте и свои данные, перезвонить в свой обслуживающий банк, проверить свой баланс и проведенные операции, а при необходимости заблокировать свой карт-счет самостоятельно при помощи услуг «Интернет-банкинга» или «М-банкинга»;

- следует избирательно относиться к предлагаемым легким способом заработка в сети Интернет, когда злоумышленники предлагают совершено «безопасно» и быстро приумножить свои сбережения путем вложения в какие-то проекты сомнительного содержания, о которых нет внятной официальной информации; как, например, для вывода якобы «замороженных» счетов различных интернет-казино, где, выбирая желаемую сумму, гражданин вносит процент от ее полного размера на предложенный злоумышленником счет; потом гражданин, которого продолжают уверять, что возникли какие-то трудности с переводом, переводит еще и еще деньги, не желая потерять уже внесенные суммы, а его возможно уже закрадывающиеся подозрения пытаются развеять, предоставляя ему переписки со «счастливыми обладателями» подобных выведенных денежных средств, которые просто в шоке от того, что они так просто заработали деньги и что и дальше будут так зарабатывать. Следовало бы задуматься в подобных случаях, какая от этого выгода якобы потенциальному «работодателю», который почему-то остро нуждается именно в Вашей помощи в выведении таких легкодоступных денежных средств;

- при оплате в сети Интернет следует внимательно относиться к тому, какие сайты используете, так как, например, при переходе по первой попавшейся ссылке по запросу в браузере, желая попасть на сайт ОАО «АСБ Беларусбанк» для дальнейшего перехода в личный кабинет Интернет-банкинга, можно легко попасть на фишинговый сайт, который внешним оформлением будет казалось бы абсолютно идентичным официальному сайту банка; отличием будет только то, что в адресной строке будет прописано не «belarusbank.by» и не «asb.by» (официальные сайты) и что после посещения этих фишинговых сайтов (на которых владельцы карт пытаются неоднократно провести операции, введя все свои установочные данные и запрашиваемые логины и пароли) баланс будет равен 0.

Учитывая, что при совершении преступлений злоумышленники активно используют анонимайзер (компьютерная программа, позволяющая изменить IP-адрес при выходе в сеть Интернет), то не следует тешить себя надеждами, что деньги все вернуться обратно, стоит только обратиться в банк и сказать, что все указанные операции провели не Вы сами. Большинство преступлений, как правило, ведут за пределы Республики Беларусь.

Ну и универсальный совет на все времена: не стоит хранить свои банковские карты вместе с пин-кодами к ним и не следует писать цифры пин-кода на самой банковской карте. Ведь никто не застрахован от того, что может просто случайно утерять свою банковскую карточку или иным образом ей может завладеть злоумышленник. Также не лишним было бы установить лимит на снятие наличных или на сумму проводимых безналичных операций по своей банковской карте.