Профилактика мошеннических действий

Как Вы все знаете, количество пользователей сети Интернет во всём мире, в том числе в Республике Беларусь постоянно растёт. Количество интернет-пользователей в нашей стране ежегодно увеличивается и в настоящее время составляет порядка 80 % всего населения.

Согласно исследованиям, 46% белорусов делают покупки или оплачивают счета через интернет.

Указанные темпы проникновения информационных технологий и безналичных платежей во все сферы жизнедеятельности человека наряду с имеющей место неквалифицированностью и неосмотрительностью определенной части пользователей являются предпосылкой возрастающего количества преступлений в сфере информационной безопасности.

В структуре преступности большую часть (89,3 %) составляют хищения с использованием компьютерной техники, все они совершены в большей степени с использованием реквизитов банковских платёжных карточек, полученных путём обмана в сети Интернет и незначительно – с использованием подлинных карточек, неправомерно вышедших из законного обладания потерпевших.

Наиболее частым способом совершения преступлений с использованием компьютерной техники являлось хищение денежных средств с использованием реквизитов, полученных в результате вишинга (осуществления звонков держателям карт от имени сотрудников банковских учреждений) и на торговых интернет-площадках, наиболее распространённой – «Kufar.by»

При этом имеющиеся правовые механизмы получения информации с использованием возможностей правоохранительных органов иных государств не позволяют своевременно и в полном объёме получать необходимые сведения, что вызывает объективные трудности по установлению личности преступника и привлечению его к ответственности в соответствии с законодательством Республики Беларусь.

Среди актуальных на сегодняшний день видов преступлений, совершаемых в отношении граждан в сети Интернет, необходимо выделить:

- завладение денежными средствами с карт-счета с использованием соцсетей;
- хищение с карт-счета с использованием **вишинга** по телефону;
- завладение денежными средствами с карт-счета с использованием **фишинга**;
- несанкционированный доступ к учетной записи в соцсети, электронной почте.

Остановимся подробнее на двух относительно новых формах способах хищения денежных средств в сети Интернет «вишинг» и «фишинг».

Суть **«вишинга»** заключается в том, что преступники завладевают личными данными и реквизитами банковских карточек путем осуществления звонков от имени сотрудников банков. Благовидным предлогом для передачи данных может стать, например, мнимый факт совершаемого хищения с Вашей карты и необходимость ее срочной блокировки. В данном случае важно понимать, что вся конфиденциальная информация о клиентах, равно как и возможность блокировки подозрительных транзакций, у уполномоченных сотрудников банков имеется. Любая просьба о передаче CVV-кодов, pin-кодов, содержания SMS-уведомлений, данных о личном номере должна восприниматься как попытка совершения мошеннических действий.

В данной ситуации правильным решением будет следующее: не передавать никакой информации собеседнику, уточнить его фамилию, перезвонить в банк (номер можно найти на официальном сайте банка либо на Вашей банковской карточке) для уточнения имевших место обстоятельств.

Хочется отметить, что совсем недавно Viber представил инструмент, который призван обезопасить пользователей мессенджера в Беларуси от звонков мошенников. В мессенджере появилась функция «Защита от лишних звонков», при активации которой пользователь не будет получать уведомления о звонках с номеров, не входящих в его список контактов.

Новая функция доступна в последней версии Viber для всех пользователей с белорусскими номерами мобильных телефонов. После этого пользователь не будет получать входящие видео- и аудиозвонки от неизвестных контактов. Информация об этих звонках будет сохранена только в списке чатов как «Пропущенный вызов», а также в разделе «Недавние вызовы». Так, пользователи не пропустят ничего важного и смогут перезвонить при необходимости.

На фоне участившихся случаев мошенничества через мессенджеры в Беларуси Viber даёт возможность пользователям оградить себя от общения с неизвестными контактами. При этом функция не включена по умолчанию, и пользователь сам решает, хочет ли он полностью запретить звонки от незнакомых ему людей в Viber или оставить такую возможность.

Беларусь стала одной из первых стран, в которых запущена эта опция. На данный момент функция «Защита от лишних звонков» доступна на устройствах на базе Android и iOS, а также на компьютерной версии приложения.

В настоящее время наблюдается бум фактов «фишинга», совершаемых с использованием крупных интернет-площадок для

размещения объявлений. Потенциальным потерпевшим от рук мошенников может стать каждый продавец, оставивший сведения о товаре и свой контактный номер. Как правило, с использованием популярных мессенджеров, зачастую с подложного номера, с продавцом связывается мошенник и заверяет о намерении приобрести товар с использованием службы доставки. После обсуждения цены продавцу приходит ссылка на ресурс одного из сервисов доставки (злоумышленники используют известные наименования, например «Белпочта», «Европочта», «Куфар доставка» и другие). Перейдя по ссылке, продавец увидит страницу, внешне напоминающую сайт соответствующей компании и форму для получения долгожданной суммы в качестве оплаты.

Для получения денег необходимо всего лишь ввести 16 цифр номера карты, имя ее владельца, срок действия, CVV-код (указан на обратной стороне карты), при необходимости код подтверждения из SMS-уведомления, либо в других случаях реквизиты доступа к интернет-банкингу (логин и пароль либо временный код). Следующим шагом после введения и отправки указанных данных станет их получение злоумышленником и последующее хищение с карты определенной суммы денежных средств.

В таком случае всегда нужно обращать внимание на наименование и внешний вид страницы. Ее имя может отличаться от настоящего всего на несколько букв, например kufar.be вместо kufar.by, или belpost.bz, а не belpost.by.

В новой для некоторых граждан тенденции цифровизации всех сфер жизнедеятельности необходимо проявлять бдительность и стремиться к повышению уровня своих познаний, что поможет адекватно реагировать на возможные современные угрозы.

Во избежание хищений с банковских карточек на уровне пользователя можно дать следующие рекомендации:

- внимательно ознакомиться с правилами пользования банковскими платежными карточками Вашего банка;
- не передавать карту и ее реквизиты третьим лицам;
- использовать отдельную карту для Интернет-покупок и не хранить на ней деньги («Нереальная карта» Белагропромбанк);
- подключить услуги 3D-Secure, SMS-информирование, установить необходимые лимиты;
- осуществлять оплату в сети Интернет на проверенных ресурсах, работающих по безопасному протоколу https.

В любой ситуации необходимо проявлять бдительность и помнить, что абсолютное большинство киберпреступлений становятся возможными ввиду неосмотрительности со стороны самого слабого звена информационной системы – человека.

Телефонные аферисты продолжают «кошмарить» пожилую часть нашего населения. В день пенсионерам поступают десятки звонков, некоторые из них, к сожалению, идут на поводу у злоумышленников и расстаются со своими сбережениями. Во всех случаях денежные средства требуются для разрешения тех либо иных вопросов, связанных с дорожно-транспортными происшествиями.

Помните: Ваша беспечность - в Ваших руках. Будьте бдительными!