Как не стать жертвой Интернет-мошенников: основные схемы хищений денежных средств с банковских платежных карточек

Уважаемые граждане,

С каждым годом количество мошеннических схем, связанных с хищением денежных средств с банковских платежных карточек, только увеличивается. Развитие технологий упрощает нашу жизнь, однако благодаря этому мошенники также совершенствуют свои методы. В настоящей статье я бы хотел проинформировать Вас о наиболее распространенных схемах хищений и дать рекомендации, которые помогут защитить себя.

Основные схемы мошенничества:

1. Фишинг (от англ. «Fishing» – рыбачить выуживать) – это обман пользователя с целью получения его личных данных, таких как логин, пароль, номер телефона или сведения об идентификационных данных банковских платежных карточек. Фишинг был и остается одним из самых распространенных способов Интернет-мошенничества. Злоумышленники под различными предлогами рассылают пользователям электронные письма, сообщения в социальных сетях или СМС, в которых от имени различных организаций, в том числе банковских учреждений, просят перейти по ссылкам на заведомо фальшивые сайты. На данных сайтах пользователей, под различными предлогами, убеждают ввести данные о своей банковской платежной карточке, а также иную информацию, необходимую для совершения хищения денежных средств. Чтобы избежать этого, всегда проверяйте адрес сайта и никогда не переходите по ссылкам, которые Вы получили из непроверенных источников.
2. Вишинг (от англ. «Vishing» («**V**oice» (голос) и «Fishing») – это, по своей сути телефонный фишинг, когда мошенники звонят Вам, выдавая себя за представителей банковских учреждений, правоохранительных органов и иных организаций. Они могут говорить о «необходимости подтверждения транзакций», «обнаружение проблемы с Вашей картой» или придумать ряд других причин для того, чтобы получить Ваши личные данные или номера банковских платежных карточек. Для совершения подобных звонков мошенники зачастую используют приложения мессенджеров «Viber», «Telegram» и «WhatsApp». Если Вы получите такой звонок, то лучше всего сразу же повесить трубку и обратиться в организацию, от имени которой Вам звонили злоумышленники, по официальному номеру телефона. Кроме этого также прошу обратить внимание на то, что сотрудники правоохранительных органов и банковских учреждений Республики Беларусь для осуществления звонков гражданам мессенджеры «Viber», «Telegram» и «WhatsApp» не используют.
3. Мошеннические Интернет-магазины – это также весьма распространенный вид Интернет-мошенничества, для осуществления которого злоумышленники создают специальный Интернет-сайт, группу или аккаунт в социальной сети, где предлагают приобрести различные товары с обязательным внесением предоплаты на предоставляемые реквизиты банковских платежных карточек. Все может выглядеть очень правдоподобно, однако сразу же после того, как злоумышленники завладеют Ваши денежными средствами, они перестанут выходить с Вами на связь и никакого товара Вы не получите. Чтобы избежать подобного исхода обязательно проверяйте репутацию магазина, читайте отзывы и ищите дополнительную информацию в сети Интернет.
4. Лотереи и выигрыши: Вам может прийти уведомление о выигрыше, но для получения приза необходимо внести предоплату или сообщить данные карты. Помните: если вы не участвовали в лотерее, то выиграть в ней невозможно.
5. Романтические мошенничества: Злоумышленники создают фальшивые профили на сайтах знакомств, в социальных сетях. После установления доверительных отношений они просят деньги для «решения проблем». Если Вы начнете замечать такие просьбы, будьте осторожны и лучше прекратите общение.

Рекомендации по защите:

1. Создавайте сложные и уникальные пароли для Ваших онлайн аккаунтов. Лучше всего использовать комбинации букв, цифр и символов.
2. Следите за движением средств на своих банковских счетах и карточках. Если заметите подозрительные транзакции, немедленно сообщите в банк.
3. Никогда не сообщайте номера своей банковской платежной карточки, срок ее действия и CVV-код (три цифры с оборотной стороны) кому-либо по телефону или через Интернет.
4. Остерегайтесь сомнительных предложений. Если кто-то предлагает Вам «тут же» увеличить доход или приобрести товар с «огромной» скидкой, это может быть ловушка. Подобные предложения зачастую скрывают истинные намерения мошенников.

Наша основная задача – защитить Вас от мошенничества в Интернете. Будьте бдительны и проявляйте осторожность в своих онлайн-действиях. Если Вы стали жертвой мошенничества, незамедлительно сообщите об этом в правоохранительные органы и в службу поддержки Вашего банка.