Приднестровский республиканский банк

Как уберечь себя и близких от финансового мошенничества. Часть 2

Мошенничество с банковскими картами онлайн

В настоящее время легче стать жертвой мошенника в виртуальном пространстве, чем на улице.

Мошенники освоили схемы обмана через:

- сервисы объявлений
- социальные сети
- мессенджеры
- смартфоны
- электронную почту

! *Каждый раз мошенники применяют различные методы манипулирования людьми и постоянно совершенствуют их.*

Место действия: смартфон

Зловредные программы умеют маскироваться под мобильные банки и таиться в разных приложениях, которые вы скачиваете на телефон.

Как предотвратить?

- Скачивайте приложения на телефон только в официальном магазине.
- Обращайте внимание на разработчика приложения - в официальных приложениях указан сам банк.
- Внимательно читайте описание приложения.
- Не скачивайте приложения сторонних разработчиков!

Место действия: сервис объявлений

Если вы решили купить товар с рук или продать, будьте бдительны - мошенники нередко играют роль покупателей или продавцов!

На ваш товар находится покупатель, который готов перевести аванс и просит у вас номер карты и три цифры на обратной стороне карты

(CVC). Такой подход должен насторожить - для перевода денег достаточно знать только номер карты (или телефона) и ФИО владельца!
Если вы покупаете товар, у вас могут попросить предоплату и ВСЕ данные карты. Если перед вами мошенник, то в лучшем случае вы останетесь без вашего аванса. В худшем - рискуете остаться и без средств на счете!

Как предотвратить?

- Всегда старайтесь проверить потенциального покупателя или продавца по отзывам: в сообществах и на сервисах обычно есть админы и «черный список» покупателей и продавцов.
- Проверьте профиль продавца - часто мошенники создают страницы с минимумом информации.

! *С осторожностью предоставляйте данные своей карты, не передавайте CVC, коды авторизации, логин и пароль от Интернет-банка.*

Место действия: сайт-двойник

Мошенники копируют известные сайты, используя похожее название компании и оформление. Например, вы хотите продать товар через Маклер, а попадаете на фишинговый сайт, то есть сайт-клон.
Если вы введете на таких сайтах свои данные, они попадут в руки злоумышленников.

Как предотвратить?

Всегда обращайте внимание на адресную строку браузера: на сайте-клоне будет допущена ошибка. Внимательно изучите и содержание сайта - мошенники часто невнимательно относятся к наполнению сайта.

! *Добавьте в закладки сайты, которыми часто пользуетесь, чтобы не набирать адрес вручную!*

Место действия: социальные сети и мессенджеры

Друг пишет личное сообщение с просьбой одолжить денег или странной ссылкой - значит его аккаунт взломали!
Незнакомец присылает личное сообщение с предложением высокого дохода за несложную работу и ссылкой, по которой вы якобы найдете подробности - по такой ссылке есть лишь компьютерный вирус!

Сотрудник известной компании звонит и обещает: кредиты под низкий %, большие скидки, выигрыш в конкурсе, для получения требуется сообщить данные карты - такие предложения почти всегда обман!

Как предотвратить?

- Если сообщения через социальные сети шлет друг, позвоните ему и выясните, действительно ли нужна помощь.
- Ссылки из сообщений незнакомцев - не лучший способ искать заработок в интернете.
- Если вам пишут от лица компании, лучше уточнить информацию на ее официальном сайте.

Место действия: электронная почта

На почту присылают письма с обещанием подарков, денег и кредитов. Мошенники пытаются заманить чем угодно: предлагают работу с большой зарплатой, присылают ответ на якобы ваше письмо, хотят «познакомиться поближе».

Отправителем может быть как неизвестный человек, так и известный сайт, онлайн-сервис или банк.

Если вы переходите по ссылкам из письма или скачиваете вложения из него - рискуете заразить компьютер вирусом, который позволит мошенникам его контролировать.

Как предотвратить?

В почте есть встроенный спам-фильтр - часть подозрительных писем попадает в специальную папку. Но обращайте внимание на заголовок письма, его отправителя и содержание. Компании делают почтовые рассылки с одних и

тех же адресов и не допускают ошибки в письмах - а вот мошенники часто пишут с ошибками и искажают название компании в адресе.

! *Не переходите по ссылкам из таких писем и не скачивайте вложения из них.*

Не стоит забывать, что повышение финансовой грамотности – один из главных способов противостояния мошенникам!

При подготовке статьи были использованы материалы сайта Финансовая культура.