***Семь советов для защиты от виртуальных мошенников***

**Сотрудники Банка России и полиции постоянно предостерегают курян от общения с потенциальными мошенниками, призывают к бдительности и напоминают о том, что нельзя ни под какими предлогами передавать конфиденциальные данные своей банковской карты и информацию с секретными кодами из СМС. Но есть и такие мошенники, которые могут заполучить чужие деньги, ничего не спрашивая и не требуя подтверждения операции по переводу средств.**

На самом деле за нашими электронными финансами охотятся постоянно. Это очень «удобный» вид мошенничества – в нем не нужно использовать дар убеждения, что-то объяснять, узнавать, манипулировать. Иногда даже уметь программировать не обязательно. «Кража» денег со счета происходит незаметно – при оплате покупок онлайн и использовании интернет-банкинга.

**Как они это делают и как защититься от таких «умельцев»? Управляющий Курским Отделением Банка России Евгений Овсянников дает семь советов.**

Многие понимают, что самый простой способ добраться до пароля пользователя – выманить заветную комбинацию обманом. «Даже если вам не звонят, вы можете получить письмо или СМС, где вас довольно убедительно попросят предоставить PIN-код, код с обратной стороны карты или логин и пароль от интернет-банка. Понятно, что делать этого нельзя ни в коем случае», - напоминает Евгений Викторович.

Прежде чем вводить данные банковской карты, например, при онлайн-покупке, убедитесь, что вы не попали на фальшивый сайт с незащищенным подключением. Евгений Овсянников объясняет: «В адресе поддельного сайта могут быть перепутаны буквы или добавлен лишний символ. Есть два признака, по которым можно распознать защищенное или зашифрованное подключение – это значок в виде замочка в начале адресной строки вашего браузера и префикс https:// (именно с буквой «s» на конце, а не просто http) перед адресом сайта. Если такие идентификаторы защиты отсутствуют, лучше не иметь никаких финансовых дел с этим сайтом».

Всегда выходите из всех платежных сервисов перед тем, как закроете вкладку браузера или нажмете кнопку «Назад».

Постарайтесь не проводить никаких финансовых операций с общественных сетей Wi-Fi в кафе, отелях, аэропортах.

«Для оплаты товаров в Интернете лучше завести отдельную карту с небольшим балансом, а для безопасности основные сбережения хранить на другой карте или депозите. Для этих целей подойдет еще одна пластиковая карта, но можно завести и виртуальную, - советует Евгений Овсянников. - Доступ к приложениям и сайтам, позволяющим использовать ваши деньги, следует защитить надежным и уникальным паролем. Используйте метод двухфакторной аутентификации, когда в подтверждение к паролю нужно вводить, например, код из СМС или отпечаток пальца. На самом деле запомнить несколько хороших паролей не так сложно».

Кроме того, существуют хитрые вирусы-трояны, которые маскируются под мобильные приложения и перехватывают сообщения от банков. «От них не защищены даже те, кто пользуется только официальными магазинами Google и Apple, - предупреждает Евгений Викторович. – Именно поэтому очень важно ставить качественные антивирусные программы не только на ПК и ноутбуки, но и на телефоны и планшеты».

«Вредоносные программы бывают разные: одни следят за клавиатурой, а другие научились делать снимки экранов. Из-за этого любители функции «Показать пароль» рискуют лишиться своих банковских данных. Лучший способ защиты и в этих случаях – хороший антивирус», ‒ напоминает Евгений Овсянников.

Запомните эти семь простых советов, следуйте им при работе с онлайн-финансами — и сбережете свои деньги от кибермошенников. А поскольку преступники, как правило, слишком ленивы, обнаружив достойную защиту, они быстро потеряют к вам интерес и отправятся на поиск более беспечных «клиентов».