В современном мире человек использует в повседневной жизни множество высокотехнологичных устройств – мобильные телефоны, компьютеры, пластиковые карты. Постоянно появляются новые устройства, программы и сервисы. Все это делает нашу жизнь удобнее, но требует определенных навыков безопасности.

Одновременно с развитием новых технологий появляются новые виды мошенничества, позволяющие обмануть и похитить денежные средства граждан. Чтобы не поддаться на уловки злоумышленников необходимо соблюдать простые правила безопасности, а также иметь хотя бы минимальное представление о том, как действуют мошенники.

ВИРУС

Вирусы могут открыть удаленный доступ к вашему устройству, украсть логины и пароли от онлайн - и мобильного банка, а также перехватывают секретные коды из сообщений. Заполучив эти данные, киберпреступники могут похитить все деньги с ваших счетов.

Как правило, это происходит следующим образом: на телефон абонента приходит СМС следующего содержания: «Вам пришло ММС-сообщение. Для получения пройдите по ссылке …». При переходе по предложенной ссылке на телефон скачивается вирус и происходит списание денежных средств с вашего счета.

Не следует звонить на телефон, с которого пришло подобное сообщение. Возможно, в этом случае также с вашего счета будут списаны денежные средства.

НЕЛЕГАЛЫ

Прежде чем обращаться в банк, микрофинансовую организацию, страховую компанию или другую финансовую организацию, нужно убедиться, что они работают легально. Легальные организации имеют действующую лицензию Банка России или состоят в реестре компаний, которые могут работать на финансовом рынке. Это можно проверить с помощью онлайн-справочника на официальном сайте Банка России.

ОНЛАЙН-МОШЕННИКИ

Стать жертвой мошенников можно не только на улице. С развитием технологий преступники быстро освоили и виртуальное пространство. Аферисты могут подстерегать своих жертв на самых разных онлайн-площадках: они нередко играют роль покупателей или продавцов на интернет-сервисах для размещения объявлений о товарах и услугах, копируют известные сайты, присылают подозрительные ссылки через социальные сети, мессенджеры или на электронную почту.

К примеру, при продаже товара, который вы предлагаете на открытых онлайн-площадках, таких как «Авито», предполагаемый покупатель в качестве оплаты товара может настаивать на перечислении денежных средств на вашу банковскую карту. При этом они настойчиво предлагают продавцу сообщить номер карты, якобы, с целью перевода денежных средств. Называя номер своей банковской карты, вы можете стать жертвой мошенничества. В таких случаях рекомендуется лично встречаться с потенциальным покупателем, очно продавать товар и получать за него плату.

ПОДМЕННЫЕ НОМЕРА

Киберпреступники научились маскировать свой телефонный номер под официальные номера банков. Помните, что даже если у вас на телефоне отразился знакомый номер банка, ни в коем случае не делайте на него обратный звонок. Наберите номер «горячей линии» банка вручную. Телефон «горячей линии» можно найти на обратной стороне банковской карты или на официальном сайте банка.

С КАРТЫ УКРАЛИ ДЕНЬГИ

Пришло СМС, что с карты списали деньги, но вы ничего не покупали, переводы не делали и наличные не снимали. Вероятно, ваша карта или ее данные попали к мошенникам. В такой ситуации нужно немедленно заблокировать карту, сообщить в банк по «горячей линии» о краже денег и написать в отделении банка заявление о несогласии с операцией. Сделать все это необходимо не позднее следующего дня после того, как банк уведомил вас об операции, которую вы не совершали.

ТЕЛЕФОННЫЕ МОШЕННИКИ

Если Вам позвонили на мобильный телефон с незнакомого номера, представившись сотрудником службы безопасности банка, и сообщили о том, что неизвестные лица пытаются получить доступ к вашему личному кабинету, предлагают срочно перевести все деньги на безопасный счет, в такой ситуации нужно немедленно положить трубку. Это звонят мошенники! Они постоянно придумывают новые способы выманить у людей деньги или конфиденциальные данные для доступа к банковским счетам.

ФИНАНСОВЫЕ ПИРАМИДЫ

Вам предлагают вложить деньги под высокие проценты, обещают гарантированный доход и просят активно привлекать друзей в проект? Будьте осторожны, успешная инвестиционная компания может оказаться финансовой пирамидой. Количество финансовых пирамид год от года меняется, но совсем они не исчезают: закрывают одни, открываются новые. И, по данным Банка России и правоохранительных органов, ежегодно люди теряют в них миллиарды рублей.

ФИШИНГ

Фишинг — главное оружие киберпреступников. Другими словами — это выуживание конфиденциальных данных граждан: паролей, реквизитов карты или счета для кражи денег с карты или из интернет-кошелька. Воры играют на психологии: рассылают СМС, электронные письма и сообщения в чатах с просьбой, например, «подтвердить аккаунт» или «восстановить доступ к банковскому счету». При этом сообщения содержат ссылку на специальный фишинговый сайт — сайт-двойник банка, государственного органа или другой организации. Если вы не заметили подмены, то после ввода своего логина, пароля интернет-банка или реквизитов карты переведете деньги мошенникам.