Как обезопасить себя от мошенников при использовании социальных сетей

В настоящее время столкнуться с мошенниками в интернете, к сожалению, стало довольно привычным делом. Существует множество способов обмана людей через интернет и постоянно появляются все новые методики, направленные на выманивание денег у пользователей Сети.

Самые популярные схемы мошенничества:

Сообщения о чрезвычайных ситуациях. Угроза безопасности. Эта уловка задействована на эмоциональное состояние человека. Вас уведомляют о попытке взлома банковского счета. Мошенники от имени службы безопасности банка рекомендуют перевести сбережения на определенные реквизиты, якобы для защиты денег, в результате чего жертва теряет свои накопления.

Онлайн-знакомства или «кэт-фишинг». Аферисты в соцсетях с аккаунта привлекаемого мужчины или женщины знакомятся с противоположным полом. И когда контакт с жертвой уже налажен, начинают выманивать деньги.

Лжеблаготворительные акции. Мошенники создают аккаунты благотворительных проектов и фондов и начинают от их имени сборы на лечение детей, помощь животным и т. д. Зачастую они используют фото реальных людей, которым необходима помощь, однако собранные средства до нуждающихся не доходят.

Онлайн-магазины. Продажа несуществующего товара или товара, не обладающего заявленными характеристиками. Покупатель, видя привлекательную цену, стремится воспользоваться предложением и переводит деньги в адрес интернет-магазина или частного продавца. В лучшем случае он получит продукцию, не соответствующую заказу, а в худшем — останется и без денег, и без посылки.

Взлом аккаунта. Многие соцсети предлагают своим пользователям привязать банковскую карту для осуществления платежей внутри платформы. Мошенники взламывают такие аккаунты и выводят деньги с банковской карты.

Ложные предложения о работе. Предложения об удаленной работе под видом корпоративных рассылок. Такие сообщения могут иметь вид приглашения принять участие в Zoom-конференции. Так мошенники заставляют перейти по небезопасным ссылкам или заполнить платную анкету, оплатить взнос или приобрести некие продукты за свой счет, чтобы стать сотрудником проекта.

Как не стать жертвой мошенников в социальных сетях?

✓ Никому не сообщайте данные паспорта, банковской карты, коды и другие персональные данные

✓ Никогда не переходите по подозрительным ссылкам, особенно если их прислали незнакомые люди

✓ Не соглашайтесь обсуждать детали покупки или продажи в сторонних мессенджерах

✓ Настаивайте на оплату товара после его прибытия, не соглашайтесь на предоплату, особенно — переводом на карту

✓ Остерегайтесь слишком выгодных предложений

✓ Обращайте внимание на дату регистрации профиля: если аккаунт создан 1—2 месяца назад, это могут быть мошенники

✓ С подозрением относитесь к аккаунтам, у которых мало или совсем нет отзывов и которые ничего еще не продавали

✓ Чтобы обезопасить себя от взлома аккаунта создавайте сложные пароли, используя цифры, символы, а также прописные и заглавные буквы

✓ При входе на свою страницу, где необходимо ввести данные, всегда смотрите на адрес сайта в поисковой строке браузера. Если он отличается от оригинального знаком или одной буквой, он является фальшивым

✓ Не доверяйте всем письмам и сообщениям в чатах. Обращайте внимание на то, как написан текст, а также смотрите на адрес, с которого пришло письмо

✓ Устанавливайте приложения только из официальных источников

Если вы стали жертвой интернет-мошенников необходимо обратиться в следующие инстанции:

✓ в Банк (блокировка, перевыпуск карты);
✓ в Роскомнадзор (киберпреступления, сбор персональных данных);
✓ в Роспотребнадзор (ассортимент, качество товара);
✓ в полицию (мошеннические действия в сети, угрозы);
✓ в суд (с требованием возмещении ущерба).

Подготовлено Консультационным центром ФБУЗ «Центр гигиены и эпидемиологии в Красноярском крае» по материалам, опубликованным на сайте: https://rg.ru/