

Основные виды интернет-мошенничеств

Осведомленность об интернет-мошенничествах помогают предотвратить многие преступные посягательства и защитить не только себя, но и близких.

Хотелось бы выделить основные схемы мошенников:

1) звонки от имени сотрудников службы безопасности банков либо правоохранительных органов
- в ходе беседы злоумышленники оповещают о якобы проводимых несанкционированных, мошеннических операциях с использованием банковских счетов либо оформлении займов на имя потенциальных жертв, то есть на лицо, которому позвонили.

В таком случае необходимо прервать разговор и сообщить об этом в полицию. Ни в коем случае не поддаваться панике, так как в первую очередь мошенники попытаются навести страх и дезориентировать собеседника, получить все возможные сведения по банковским счетам и поступившим СМС-сообщениям. Не устанавливать какие-либо приложения, тем более для дистанционного управления Вашими устройствами (AnyDesk, RustDesk, TeamViewer и т.п.);

2) продажа товаров и услуг в социальных сетях и торговых площадках – данный вид предусматривает мнимую реализацию различного рода товаров и услуг. Как правило, это автомашины, бытовая техника, мебель, носимые вещи, аксессуары, товары народного потребления, продукты питания и т.д. Целью злоумышленников является получение выгоды. Они всяческим образом будут подводить и просить перевести денежные средства в качестве предоплаты. Лучше отказаться от таких сделок, до тех пор пока не увидите товар своими глазами, в противном случае Вы можете остаться без своих сбережений;

3) использование фишинговых сайтов – данный вид мошенничества нацелен на сбор персональных данных и банковских сведений. Такие сайты один в один идентичны с реальными сайтами.

К примеру, Вы выложили объявление на одном из сайтов, и к Вам обращается ранее незнакомый человек и просит оформить доставку. После чего он направляет ссылку для оформления. Перейдя по ссылке, будет предложено ввести Ваши данные, то есть ФИО, год рождения, номер банковской карты, срок действия и CVV-код. После заполнения начинается списывание денежных средств с банковской карты;

4) инвестирование в криптовалюту, ценные бумаги и т.п. – с приходом новых возможностей и технологий активно развивается движение криптовалют. Многие понимающие люди имеют хорошие доходы на этом. Но есть и недоброжелатели, которые зарабатывают обманным путем, пользуясь неграмотностью в данном направлении.

К примеру, в социальных сетях Вы увидели рекламу, где предлагается заработать на покупке и продаже акций или криптовалют. С Вами созванивается злоумышленник, представляется сотрудником Национальной компании либо другой организации, якобы предоставляющей услуги брокеров. Заманивают выгодными предложениями, уговаривают внести денежные средства, для начала небольшие суммы. Через несколько дней возвращают вложенные денежные средства с якобы заработанной выгодой. После чего просят внести уже суммы по значительней. Многие из тех, кто попался на уловки мошенников, говорят, что злоумышленники ведут себя уверенно, убедительно и в своем арсенале имеют хорошо разработанные интернет-сайты, в которых проходишь регистрацию, и в личном кабинете наблюдаешь за приумножением своих сбережений, но это все фейк;

5) звонки пожилым гражданам: злоумышленники представляются сотрудниками правоохранительных органов и сообщают, что их близкие люди оказались фигурантами уголовного дела – мошенники в ходе диалога убеждают своих собеседников в том, что произошел инцидент, за который их близкие (дети, родственники, друзья) могут оказаться в орбите уголовного преследования. В этой связи с целью освобождения от уголовной ответственности необходимы денежные

средства, которые должен будет забрать якобы их сотрудник. В свою очередь они направляют так называемых «дропов» либо курьеров, осуществляющих частную трудовую деятельность на различных интернет-платформах. А те уже, направляясь по заданному маршруту, получают денежные средства от пострадавших и передают злоумышленникам либо переводят на подставные банковские счета.

Также хотелось бы заострить свое внимание на этих «дропах» - лиц, оказывающих содействие преступникам, путем передачи своих банковских карт и личных данных для проведения незаконных финансовых операций или отмывания денег, добытых преступным путем.

Наиболее часто «дропами» являются молодые граждане, студенты, безработные и лица, ищащие легкого заработка.

Мы обращаемся к лицам, которые участвуют в деятельности, связанной с обналичиванием денежных средств, добытых преступным путем, с использованием банковских карт от третьих лиц. Подобное поведение предусматривает уголовно-наказуемую ответственность (не так давно привлечен к уголовной ответственности и осужден сроком на 6 лет гражданин РФ, который обналичивал денежные средства, добытые преступным путем, с использованием банковских карт третьих лиц, также проводится следственные действия в отношении 79 дропперов, которые обналичивали денежные средства).