Телефонное и интернет-мошенничество – что это?

С ростом электронных расчетов и развитием технологий человек все больше сталкивается с киберпреступностью.

На территории Архангельской области участились случаи совершения мошеннических действий лицами, которые обманным путем с использованием мобильных операторов сотовой связи, под заранее хорошо спланированными и продуманными предлогами, склоняют граждан перечислять денежные средства на банковские лицевые счета подставных лиц. Кроме того, в настоящее время получило распространение приобретение товаров в интернет-магазинах и на интернет-сервисах для размещения объявлений о товарах.

Как не перевести деньги мошеннику? Как обезопасить себя при покупках в интернете? Что следует знать и как можно защитить себя во сети Интернет?

Следует отметить, что преступники постоянно придумывают новые мошеннические способы и схемы получения денежных средств у граждан. Как правило, они действуют по следующим схемам:

- **«доска объявлений»**, мошенники ищут в Интернете объявление о продаже вещей либо сдаче в наем жилья. Звонят, представившись покупателем, просят продиктовать номер карты, чтобы якобы перевести на нее деньги в качестве залога или всю сумму целиком. При этом просят все данные карты платежную систему, срок действия карты, код на обороте (CVV). Многие не сразу догадываются, что их просят сообщить гораздо больше сведений, чем требуется для перевода. Мошенники получают доступ к банковскому счету гражданина и могут делать покупки через Интернет.

- **«возврат потерянных вещей»:** мошенники ищут объявления об утрате имущества, после чего звонят и сообщают, что нашли вещь, и просят вознаграждение за возврат – перевести деньги на номер мобильного телефона или QIWI-кошелек, при этом могут даже назначить встречу с целью возврата вещи. Естественно, после получения денег они исчезают.

- **«проблемы у родственника»:** мошенник представляется родственником (сыном, братом, мужем и т. п.) и взволнованным голосом сообщает, что задержан полицией за совершение преступления или правонарушения (ДТП, хранение наркотиков, нанесение тяжких телесных повреждений). Далее в разговор может вступить якобы сотрудник полиции или сам звонивший говорит, что необходимо перевести деньги на номер телефона либо QIWI-кошелька. При этом главное для злоумышленника – не дать жертве опомниться, чтобы созвониться с настоящим родственниками.

- **«ошибочный перевод средств»:** гражданам поступает СМС-сообщение о поступлении средств на счет мобильного телефона, при этом в сообщении с целью усыпить бдительность может содержаться якобы рекламная информация от оператора связи (погода на сегодня, курс валюты и др.). Сразу после этого поступает СМС-сообщение об ошибочном переводе средств с просьбой вернуть деньги на определенный номер телефона.

- **«смс-просьба»**: например абонент получает на мобильный телефон сообщение «У меня проблемы, позвони по указанному номеру, если номер недоступен, положи на него определенную сумму и перезвони». Этот номер, естественно, оказывается выключенным. Доверяя СМС-просьбе, граждане могут перевести на указанный мошенниками номер телефона деньги.

- **«помоги другу»:** взломав страницу в социальных сетях (либо незаконно ее скопировав), преступники рассылают сообщения о помощи Вашим друзьям на странице с просьбами перевести деньги на номера телефонов, банковских карт или QIWI-кошельков. Причем перед сообщением с просьбой о переводе денег мошенники могут вести переписку на отвлеченные темы.

- **«платный код»**: гражданам поступает звонок якобы от службы техподдержки оператора мобильной связи с предложением подключить новую эксклюзивную услугу, или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи. Для этого предлагается набрать под диктовку код,

который является комбинацией для мобильного перевода средств со счета абонента на счет злоумышленников.

- **«ваша карта заблокирована»:** гражданам поступает сообщение или звонок, что банковская карта заблокирована, и предлагается бесплатно позвонить на определенный номер для получения подробной информации. При звонке на номер телефона сообщают, что на сервере произошел сбой, и просят сообщить номер карты и пин-код для ее перерегистрации. Получив реквизиты банковской карты, преступники переводят с нее деньги.

- **«покупка дорогого смартфона»** (иного дорогостоящего товара) со скидкой в 60-70% на сайтах интернет-магазинов скорее всего будет обманом: продается не оригинальный смартфон (товар), а его подделка: устройство будет только внешне напоминать дорогой аппарат, но внутри будет самая дешевая «начинка». Будьте осторожны - бесплатный сыр только в мышеловке.

- также наиболее распространенными являются случаи обмана под предлогами **покупки «чудодейственных» лекарственных средств**, выплаты компенсации за ранее приобретенные лекарства и иных предметов, в том числе под видом сертифицированного медицинского оборудования, излечивающего от всех болезней.

- **обман при покупке в интернет-магазине**. Тут может быть два варианта:- Вы переводите деньги, но не получаете товар; - вы переводите деньги, и магазин «ворует» данные Вашей банковской карты, денежные средства списываются на счета подставных лиц.

Как же обезопасить себя от такой покупки?

Покупайте только в проверенных местах. Каждый уважающий себя интернет-магазин будет зарегистрирован на Яндекс Маркете и содержать отзывы от постоянных покупателей. В любом случае - перед покупкой ознакомьтесь с информацией о магазине: отзывы, юридический адрес, телефоны. Если у магазина нет телефонного номера, или он не отвечает - лучше купить в другом месте.

Будьте аккуратнее с покупкой на одностраничных сайтах - где продается только один товар. Такой сайт создается за пару часов – возможно, это очередной сбор денег мошенниками. **Всю информацию нужно проверять.**

Будьте внимательны и воздержитесь от любого перечисления денежных средств на номера и лицевые счета банков неизвестных абонентов!

Помните! Никогда и никому не говорите срок действия карты и CVV код на обратной стороне!

Никому и никогда не говорите коды из ваших смс-сообщений! Даже сотруднику банка!

Уполномоченный по правам человека в Архангельской области

Как обезопасить себя от телефонных и интернет - мошенников?

Архангельск,
2020