О наиболее распространенных способах совершения IT-преступлений, рисках хищений с применением цифровых технологий и методах защиты от них

Полиция всегда готова прийти на помощь пострадавшим от действий преступников, но самый лучший способ борьбы с правонарушениями-Ваша правовая грамотность и бдительность. С каждым годом мошенники придумывают все более изощренные схемы отъема денежных средств. Вот простые рекомендации, соблюдение которых поможет Вам сохранить деньги и ценности».

- **Заканчивается срок обслуживания СИМ-карты.** Лжепредставители операторов связи звонят абонентам и утверждают, что скоро ваша SIM-карта перестанет действовать и ее надо заменить или продлить. Для этого надо сообщить код из SMS, дающий доступ к личному кабинету, а далее — и к вашему банкингу. Никакого «продления обслуживания номера» не существует. Номер действует бессрочно, как и СИМ-карта. Последняя может устареть, но ее замена – ваше право, которое реализуется только очно в точке продаж оператора.
- **Деньги за опрос. Деньги за отметку аккаунта в сторис.** Фейковые аккаунты брендов предлагают пройти короткий опрос о степени удовлетворенности услугами или просят отметить сообщества в ваших сторис. А за это обещают начислить деньги на вашу карту. Изучите название аккаунта и его публикации. Как правило, весь контент на таких страницах загружен в один день и не имеет описания.Не переходить по входящим сомнительным ссылкам. Заблокируйте сомнительный аккаунт.
- **СМС-сообщение о неожиданном выигрыше.** Задумайтесь! Настоящий розыгрыш призов не должен подразумевать денежные выплаты с Вашей стороны! Не торопитесь расставаться со своими деньгами!
- **Близкие попали в беду.** Вам звонят с незнакомого номера и тревожным голосом сообщают, что Ваши близкие попали в беду. А для того, чтобы решить проблему, нужна крупная сумма денег – по такой схеме работают мошенники! Самостоятельно прекратите разговор и позвоните родственникам, чтобы проверить полученную информацию.

- **В интернет-магазине просят предоплату.** Нередки случаи мошенничеств, связанных с деятельностью Интернет-магазинов и сайтов по продаже авиабилетов. Чем привлекают потенциальных жертв мошенники? Прежде всего - необоснованно низкими ценами. При заказе товаров вас попросят внести предоплату, зачастую путем внесения денежных средств на некий виртуальный кошелек посредством терминала экспресс-оплаты. Далее магазин в течение нескольких дней будет придумывать отговорки и обещать вам скорую доставку товара, а потом бесследно исчезнет либо пришлет некачественный товар.

  Если вы хотите купить товар по предоплате помните, что серьезные Интернет-магазины не будут просить вас перечислить деньги на виртуальный кошелек или счет мобильного телефона. Поищите информацию о магазине в сети Интернет, посмотрите, как долго он находится на рынке. Если вы имеете дело с сайтом крупной или известной вам компании, убедитесь в правильности написания адреса ресурса в адресной строке вашего браузера. При необходимости потребуйте от администраторов магазина предоставить вам информацию о юридическом лице, проверьте ее, используя общедоступные базы данных налоговых органов и реестр юридических лиц. Убедитесь в том, что вы знаете адрес, по которому вы сможете направить претензию в случае, если вы будете недовольны покупкой.

- **Банковская карта абонента заблокирована.** Заметно участились случаи рассылки смс-сообщений, содержащих информацию о том, что банковская карта абонента заблокирована в силу ряда причин. Иногда подобные сообщения содержат призыв перевести деньги для разблокировки карты, иногда абонента просят позвонить или отправить смс на короткий номер.

  Необходимо помнить о том, что единственная организация, которая сможет проинформировать вас о состоянии вашей карты – это банк, обслуживающий ее. Если у вас есть подозрения о том, что с вашей картой что –то не в порядке, если вы получили смс-уведомление о ее блокировке, немедленно обратитесь в банк. Телефон клиентской службы банка обычно указан на обороте карты. Не звоните и не отправляйте сообщения на номера, указанные в смс-уведомлении, за это может взиматься дополнительная плата.

- **Крик о помощи.** Один из самых отвратительных способов хищения денежных средств. В интернете появляется душераздирающая история о борьбе маленького человека за жизнь. Время идёт на часы. Срочно необходимы дорогие лекарства, операция за границей и т.д. Просят оказать помощь всех неравнодушных и перевести деньги на указанные реквизиты.

  Прежде чем переводить свои деньги, проверьте - имеются ли контактные данные для связи с родителями (родственниками, опекунами) ребёнка. Позвоните им, найдите их в соцсетях, пообщайтесь и убедитесь в честности намерений.

- **Фишинг.** Является наиболее опасным и самым распространённым способом мошенничества в интернете. Суть заключается в выманивании у жертвы паролей, пин-кодов, номеров и CVV-кодов. Схем, которые помогают мошенникам получить нужные сведения, очень много.

  Так, с помощью спам-рассылок потенциальным жертвам отправляются подложные письма, якобы, от имени легальных организаций, в которых даны указания зайти на «сайт-двойник» такого учреждения и подтвердить пароли, пин-коды и другую информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы. Достаточно распространенным является предложение о работе за границей, уведомление о выигрыше в лотереи, а также сообщения о получении наследства.

- **Ошибочный перевод средств.** Абоненту поступает SMS-сообщение о поступлении средств на его счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги на его счет, при этом просит вернуть их обратно тем же «Мобильным переводом». В действительности деньги не поступают на телефон, а человек переводит свои собственные средства. Если позвонить по указанному номеру, он может быть вне зоны доступа. Кроме того, существуют такие номера, при осуществлении вызова на которые с телефона снимаются все средства.

  Чтобы не стать жертвой злоумышленников, необходимо соблюдать простые правила безопасного поведения и обязательно довести их до сведения родных и близких:

- не следует доверять звонкам и сообщениям, о том, что родственник или знакомый попал в аварию, задержан сотрудниками полиции за совершение преступления, особенно, если за этим следует просьба о перечислении денежных средств. Как показывает практика, обычный звонок близкому человеку позволяет развеять сомнения и понять, что это мошенники пытаются завладеть вашими средствами или имуществом;
- не следует отвечать на звонки или SMS-сообщения с неизвестных номеров с просьбой положить на счет деньги;
- не следует сообщать по телефону кому бы то ни было сведения личного характера.

Противостоять мошенникам возможно лишь повышенной внимательностью, здравомыслием и бдительностью.

Если Вы или Ваши близкие стали жертвами мошенников, или Вы подозреваете, что в отношении Вас планируются противоправные действия – незамедлительно обратитесь в полицию!