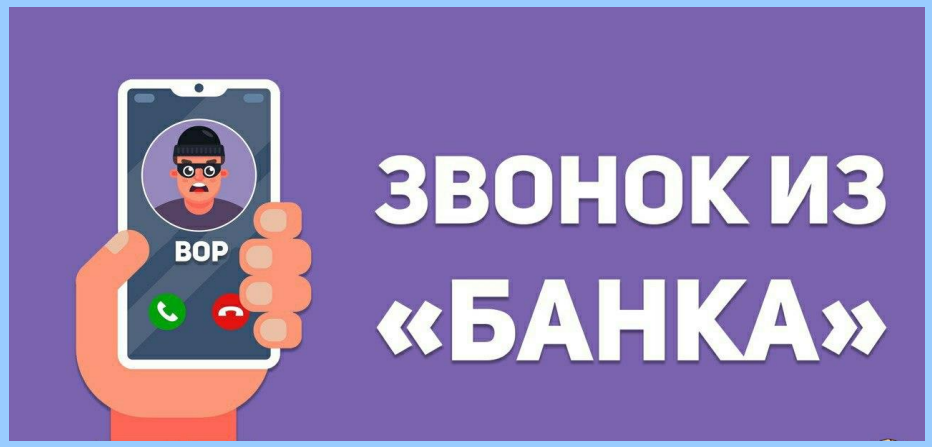
Прокуратура Ивановской области разъясняет как не стать жертвой киберпреступников

1. Научитесь распознавать мошенников. Мошенники чаще всего представляются кем-то, кто вызывает доверие, например, сотрудником государственного ведомства, благотворительной организацией или вашим родственником. Не переводите деньги и не предоставляйте личную информацию, если вас попросят об этом в текстовом сообщении, в мессенджерах, по телефону или по электронной почте. Не переходите по подозрительным ссылкам, полученным через смс и ммс – сообщения.



2. Распространение получила мошенническая схема с незаконным использованием подменных абонентских номеров. Звонок осуществляется якобы сотрудником банка, который информирует о попытке оформления неизвестным третьим лицом кредита в онлайн-банке. Далее злоумышленник убеждает гражданина в необходимости самостоятельно оформить онлайн-кредит на ту же сумму, обналичить поступившие на банковскую карту деньги и перечислить их на так называемый резервный счет для погашения кредита.

3. В некоторых случаях телефонные мошенники используют модернизацию голоса звонящего с целью введения потенциальной жертвы в заблуждение в отношении того, с кем он ведет телефонный разговор. Если кто-то звонит и голосом близкого человека просит срочно перевести деньги на новый номер или на банковскую карту, скорее всего у адресата не возникнет подозрений. Идеальным способом защиты выступает прекращение разговора с собеседником, личность которого вызывает подозрение. Если вы считаете, что звонящий, возможно, говорит правду, то просто проверьте полученную от него информацию, перезвонив обратно по подлинному номеру телефона.

4. Социальные сети — место для развлечений и общения с друзьями, удобный способ завести новые знакомства. Увы, кроме честных и добропорядочных пользователей в соцсетях есть множество наглых и бессовестных воришек, взламывающих чужие аккаунты. Злоумышленники действуют по уже знакомой всем схеме: взламывают аккаунт и рассылают сообщения с просьбой о помощи (на лечение или просто в долг, а также придумывая новые легенды) якобы от имени его владельца. Если ваш аккаунт взломан, то оперативно попросите несколько знакомых отправить жалобу на вашу страничку, чтобы ее оперативно заблокировали; свяжитесь с техподдержкой соцсети и сообщите, что вашу страницу взломали; игнорируйте любые предложения незнакомых лиц, готовых помочь за деньги.

5. Оплата покупки без товара в ложном (фейковом) интернет – магазине. Самый грубый и примитивный способ обмана. Человек хочет приобрести в интернет-магазине товар, оплачивает его, но покупка так и не приходит либо приходит совсем другой товар, намного дешевле заказанного. Подобными обманами занимаются магазины-однодневки; часто они предлагают товар в рамках короткой акции по цене значительно ниже обычной, а желающие сэкономить торопятся оплатить. Чтобы избежать подобной ситуации, стоит приобретать товары (особенно дорогие) в проверенных интернет-магазинах.

6. Никому не сообщайте пин-код от банковской карты, не пишите его на карте и храните отдельно. Набирая пин-код, всегда прикрывайте клавиатуру рукой. В том числе, при расчете в кафе и магазинах.

7. Если вам приходит СМС о зачислении средств (и сообщение похоже на привычное уведомление банка), а затем Вам звонит человек, который по ошибке зачислил вам деньги и просит вернуть, не спешите ничего возвращать. Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, СМС - не от вашего банка, а звонил вам злоумышленник. Проверьте состояние вашего счета, закажите выписку в онлайн-банке или позвоните в банк, прежде чем переводить кому-то деньги.

8. Если вы столкнулись с мошенничеством необходимо незамедлительно обращаться в органы полиции. Не стоит думать, что раз вы не знаете мошенника в лицо, то дело безнадежно.