«Мошенничество в интернете. Виды и способы защиты»

• Фишинг. Похищение личных данных.

У каждого из нас есть конфиденциальные данные. Пин-коды банковских карт, пароли и прочее. В некоторых случаях мошенники, обладающие вашими данными, смогут украсть ваши деньги. Например, совершить покупку с вашей карты без вашего ведома.

Часто жулики рассылают смс-сообщения или письма на e-mail о какой-либо ошибке/блокировке, и для решения проблемы нужно указать личные данные или позвонить по указанному номеру телефона, а в ходе разговора уже будут пытаться обмануть. Но конфиденциальных данных не спрашивают даже сотрудники банков или сервисов электронных денег.

Как защититься: не сообщать личных данных никому, установить двухфакторную аутентификацию (подтверждение операций через смс на мобильный телефон) везде, где это возможно.

• Покупки в интернете.

Нередко можно увидеть какой-либо товар по потрясающе низкой цене. Человек верит – отправляет деньги, а взамен не получает ничего.

Например, продают iPhone 11 за 7990 рублей, когда как реальная цена начинается от 60 тысяч.

Так же бывает и с предоплатами. Продавец просит выслать предоплату, после чего якобы вышлет товар. Но после перевода денег, продавец и товар просто исчезают.

Как защититься: покупать товары только в официальных и известных интернет-магазинах. Проверять реквизиты продавца. Не верить в сказочно низкие цены.

• Финансовые пирамиды, инвестиционные проекты.

Еще одно очень распространенное мошенничество в интернете - финансовые пирамиды и инвестиционные проекты. Людям рассказывают о пассивном доходе, будто каждый день, ничего не делая, приходят деньги. Нужно лишь только вложить сначала свои финансы и/или привести еще 10 человек, которые вложат свои деньги. При этом какого-либо дохода никто не получит и не сможет вернуть свои денежные средства.

Как защититься: никогда не вкладывать деньги в сомнительные проекты.

• Взлом аккаунтов в социальных сетях.

Нередко бывает, что мошенники взламывают профили в социальных сетях. После чего могут разослать спам по всем вашим контактам или попросить срочно перевести деньги. Ваши друзья думают, что это просите Вы, верят и переводят деньги мошенникам.

Как защититься: не переходить по сомнительным ссылкам в социальных сетях, использовать сложные пароли и использовать двухфакторную аутентификацию.

Белоярская межрайонная прокуратура