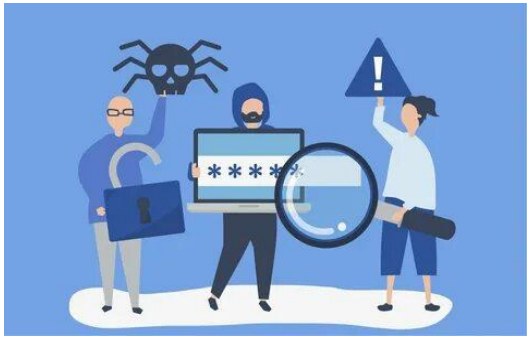
Прокуратура Ленинского района г. Красноярска разъясняет, как не стать жертвой киберпреступника.

1. «ТЕЛЕФОННЫЙ ЗВОНОК»

В ходе телефонного разговора злоумышленники представляются: сотрудниками банка, правоохранительных органов, социальных служб, специалистами портала «Госуслуги».

Способы защиты:

- Не отвечайте и не перезванивайте на незнакомые номера;
- Прервите разговор, если он касается финансовых вопросов;
- Обратитесь в полицию, банк или организацию;
- Не сообщайте сведения о картах (CW/CVC-коды);
- Не переводите денежные средства по просьбе (требованию) неизвестных лиц.



2. Мошенничества, совершаемые в сети интернет

Преступления, совершаемые в социальных сетях, мессенджерах, торговых площадках в сети Интернет (Авито, Дром и т.д.).

Способы защиты:

- Не осуществляйте предоплату;
- Называйте только абонентский номер для перевода денежных средств (достаточно для осуществления перевода);
- Оплачивайте покупки только после доставки.
- Проверяйте рейтинг продавца и отзывы.

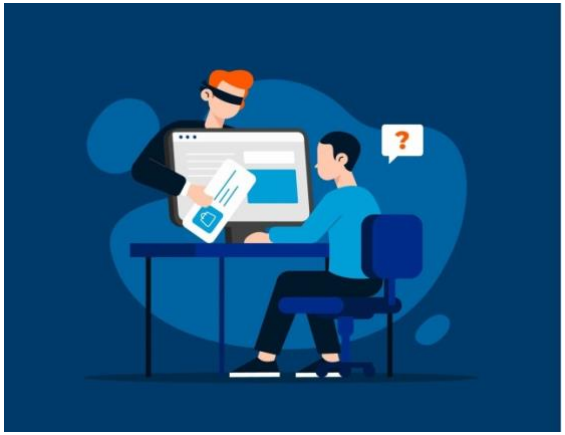
3. Фишинг – сайт двойник или зеркальный сайт

Преступником создается сайт «двойник», визуально схожий на какой-либо известный официальный сайт (в названии имеются отличия).

Способ защиты:

При проверке обратите внимание:

- Мошенники заменяют буквы символами – например, ЦИФРА 1 вместо БУКВЫ «l» (onL1ne вместо onLine);
- Имя сайта максимально приближено к оригиналу (onLLine.sberbank.ru вместо onLine.sberbank.ru);
- Фейковый сайт может располагаться в нестандартной зоне, например rzd.INFO или rzd.NET, когда оригинал: rzd.RU



Будьте осторожны!