1.2. ИНТЕРНЕТ-МОШЕННИЧЕСТВО:

- **Фейковые сайты банков, Госуслуг (фишинг):** Мошенники создают поддельные сайты и приложения, которые визуально очень похожи на настоящие. Таким образом мошенники пытаются выманить ваши логины, пароли и другую конфиденциальную информацию, которую вы вводите при входе в личные кабинеты приложений и сайтов. **Не скачивайте приложения с непроверенных ресурсов.**

- **Поддельные интернет-магазины:** Товар на сайте представлен, цена привлекательная, но после оплаты вы ничего не получаете. Магазин исчезает, а связаться с ним невозможно. **Совершайте покупки в интернете только на проверенных сайтах и в проверенных интернет-магазинах**

- **Обращение от лица руководства:** Через мессенджер с вами связывается якобы ваш руководитель *(начальник, директор, ректор и т.д.)*. В профиле мошенника, как правило, используется официальное фото и ФИО, чтобы вызвать доверие. Вас предупреждают о предстоящей проверке со стороны прокуратуры, налоговой или других контролирующих органов. Далее сообщается, что с вами свяжется сотрудник этой службы чтобы задать «важные вопросы». После этого обычно следует звонок, в котором мошенники, выдавая себя за представителей силовых или контрольных структур, пытаются выманить конфиденциальную информацию или деньги. **Блокируйте лженчальника и не отвечайте на незнакомые номера.**