ПРОКУРАТУРА
г. Донецка

ОСТОРОЖНО: ФИШИНГОВЫЕ САЙТЫ!



НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

Фишинговые сайты — это поддельные страницы, которые внешне копируют известные ресурсы: банков, госуслуг, интернет-магазинов и других сервисов. Их цель — получить ваши логины, пароли, данные карт и другую конфиденциальную информацию.

КАК РАСПОЗНАТЬ ФИШИНГОВЫЙ САЙТ

АДРЕС САЙТА
Отсутствие https или странный адрес (ошибки, лишние символы, замена букв).

НЕТ ЗАЩИЩЁННОГО СОЕДИНЕНИЯ
Нет значка замка в адресной строке или браузер выдает предупреждение.

ССЫЛКИ ИЗ ПИСЕМ И СООБЩЕНИЙ
Переход по ссылкам из писем, SMS и мессенджеров может вести на поддельный сайт.

НЕОБЫЧНЫЙ ДИЗАЙН И ОШИБКИ
Ошибки в тексте, некачественный дизайн, отличия от официального сайта.

ЗАПРОС ЛИЧНЫХ ДАННЫХ
Сайт требует ввести логин, пароль, номер карты или код из СМС — это повод насторожиться.

СЛИШКОМ ВЫГОДНЫЕ ПРЕДЛОЖЕНИЯ
Обещания лёгких денег, большие скидки и призы — часто уловка мошенников.

ЗАПОМНИТЕ!

- Не переходите по подозрительным ссылкам и не открывайте вложения от неизвестных отправителей.
- Не вводите данные на сайтах, в подлинности которых вы не уверены.
- Банки и госорганы никогда не запрашивают пароли, коды из СМС и данные карт через интернет.
- Всегда проверяйте адрес сайта и наличие защищённого соединения (https и значок замка).
- При сомнениях — закройте сайт и зайдите на официальный ресурс самостоятельно.

КАК ЗАЩИТИТЬ СЕБЯ

- Вводите адрес сайта вручную или пользуйтесь официальными закладками.
- Используйте антивирус и регулярно обновляйте его.
- Включите двухфакторную аутентификацию в сервисах.
- Проверяйте актуальные уведомления на официальных сайтах организаций.
- Будьте внимательны и не торопитесь! Мошенники рассчитывают на вашу спешку и невнимательность.

БУДЬТЕ БДИТЕЛЬНЫ!

ВАША ВНИМАТЕЛЬНОСТЬ — ЛУЧШАЯ ЗАЩИТА ОТ МОШЕННИКОВ!