Фишинг — это вид интернет-мошенничества, направленный на получение доступа к конфиденциальной информации пользователей, например, таким как логины и пароли.

Мошенники отправляют электронные письма или личные сообщения от имени популярных брендов, банков или государственных органов, в которых содержатся ссылки на поддельные сайты, внешне неотличимые от настоящих (официальных).

После перехода на поддельный ресурс аферисты пытаются побудить пользователей ввести свои логин, пароль или иную конфиденциальную информацию, которые затем используют в противоправных целях.

Чтобы распознать фишинг, обратите внимание на следующие признаки:

Упоминание в записи сообщества: мошенники могут фальсифицировать группу известной радиостанции или использовать другие популярные темы.

SMS-рассылка: злоумышленники могут включить ваш номер в SMS с предложением обмена и ссылкой на страницу якобы товара.

Электронная почта: письма могут содержать информацию о взломе почты, банковском счёте, социальных сетях, уведомления от органов власти или благотворительных организаций.

Сайты: мошенники подделывают доменные имена, используют HTML-вёрстку и маскируют адрес фишингового сайта под знакомый пользователям домен.

Отсутствие SSL-сертификата: популярные сайты используют шифрование SSL для передачи данных пользователей, адрес сайта начинается на «https://».

Грамматические, орфографические и дизайнерские ошибки: крупные компании имеют профессиональных дизайнеров и корректоров, ошибки могут указывать на мошенничество.

Подозрительные платёжные формы: проверьте структуру страниц и дизайн форм, они могут отличаться от оригинального сайта.

Отсутствие пользовательских соглашений и странные контакты: убедитесь, что текст соглашений не указывает на сторонние компании и проверьте адрес контактов.

Для противодействия фишингу соблюдайте правила интернет-гигиены, используйте антивирус и инструменты защиты.