ПРОКУРАТУРА ИРКУТСКОГО РАЙОНА РАЗЪЯСНЯЕТ:

МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ: ПОКУПКИ, ОБЪЯВЛЕНИЯ, ФЕЙКОВЫЕ САЙТЫ

Чаще всего злоумышленники используют фишинг: создают сайты-двойники известных магазинов, маркетплейсов или сервисов, копируя дизайн, логотипы и даже часть контента. Цель — получить персональные данные. Встречаются и схемы с объявлениями: вам предлагают товар по очень выгодной цене, но требуют полную предоплату, после чего продавец исчезает.

Как распознать опасность? Обращайте внимание на несколько признаков:

- **Подозрительный адрес.** Мошенники часто вносят в домен едва заметные изменения: меняют одну букву («bakn.ru» вместо «bank.ru»), добавляют лишние слова или используют непривычные доменные зоны (например, .space вместо .ru). Перед вводом данных сверьте адрес с официальным сайтом компании.
- **Проблемы с соединением.** Наличие значка замка и https в адресной строке — хороший знак, но не гарантия: мошенники тоже могут получить такой сертификат. Если браузер явно предупреждает о небезопасном соединении — это тревожный сигнал.
- **Непрофессиональный вид.** Орфографические и пунктуационные ошибки, картинки низкого качества, «кривая» вёрстка, обилие навязчивой рекламы, незаполненные разделы (нет условий доставки, пользовательского соглашения, политики конфиденциальности) — всё это поводы насторожиться.
- **Слишком заманчивые предложения.** Обещания огромной скидки, «эксклюзивного товара по суперцене» или «беспроигрышной лотереи» — классический приём, чтобы заставить действовать быстро и не дать времени на проверку.
- **Давление и спешка.** Фразы вроде «акция заканчивается через 5 минут», «только сегодня», «осталось пару штук» — попытка отключить критическое мышление.
- **Запрос конфиденциальной информации.** Ни один надёжный сервис не попросит вас прислать пароль, CVC-код карты или код из СМС в ответ на сообщение или через форму на сайте.
- **Сомнительные контакты.** Если на сайте нет физического адреса, телефона или реквизитов компании (ИНН, ОГРН), а связаться можно только через форму или мессенджер — это тревожный знак. Можно проверить указанный адрес в картах: существует ли по нему реальная организация.
- **Возраст домена и отзывы.** Если сайту всего несколько месяцев, а он позиционирует себя как давно работающий — это подозрительно.

Проверяйте отзывы не на самом сайте (там они могут быть заказными), а на независимых площадках: в Яндекс Картах, на форумах, в тематических чатах. Если положительных отзывов слишком много и они однотипные — скорее всего, их накрутили.

Что делать, чтобы обезопасить себя?

- Перед покупкой самостоятельно найдите официальный сайт магазина или проверьте карточку продавца на проверенной площадке, а не переходите по ссылкам из писем, СМС или сообщений в соцсетях.
- Для оплаты используйте отдельную или виртуальную карту с лимитом, а не основную, где хранятся все сбережения.
- При покупках на маркетплейсах пользуйтесь встроенными сервисами площадки («безопасная сделка», оплата через платформу), а не переводите деньги напрямую продавцу «в обход» — так у вас будет защита сервиса.
- Подключите двухфакторную аутентификацию для важных аккаунтов.
- Регулярно просматривайте выписки по картам: так вы быстрее заметите подозрительные списания.

А если вы уже попали в ловушку? Если вы ввели данные карты или аккаунта на подозрительном сайте — немедленно смените пароль, заблокируйте карту и сообщите в поддержку сервиса, от имени которого действовал мошенник. В случае хищения денег обратитесь в полицию.