10 правил, как не стать жертвой одной из мошеннических схем при дистанционной покупке товаров.

1. Старайтесь не переходить по ссылкам из рекламных писем на сайты магазинов. Это может быть мошенническая копия, на которой получится только оплатить товар (перевести деньги мошеннику), но, конечно, не получить его. Вводите адрес известного магазина в строке браузера самостоятельно и проверяйте, действительно ли в нем есть акция, о которой идет речь в письме.

2. Всегда обращайте внимание на доменное имя сайта: мошеннические ресурсы имеют схожие с известными магазинами имена, но написанные с ошибками или замененными символами.

3. Проверьте дату создания сайта с помощью Whois-сервисов. Если странице пара недель или месяц, то она с высокой долей вероятности фейковая, созданная к праздничной дате в целях наживы.

4. Удостоверьтесь, что сайт использует протокол https и имеет действующий сертификат безопасности (символы https и изображение замочка в адресной строке). В противном случае никогда не вводите на сайте свои персональные и платежные данные.

5. Проверьте отзывы о товарах и магазине. Если их нет или они исключительно положительные и написанные примерно в одно и то же время - перед вами, скорее всего, фейк. Отзывы об интернет-магазине читайте не на сайте самого интернет-магазина, а на сторонних ресурсах.

6. Обратите внимание на косвенные индикаторы фейка: требование обязательной предоплаты, недоступность самовывоза и отсутствие возможности оплатить покупку при получении. Эти три фактора должны насторожить вас и предупредить о том, что перед вами, возможно, мошеннический сайт.

7. Сравнивайте цены. Перед покупкой обращайте внимание на цену на товар в сравнении с предложениями других магазинов. Если цена сильно ниже рыночной, особенно в период высокого спроса, то велика вероятность, что вы получите товар сомнительного качества или не получите его вовсе.

8. Проверяйте реквизиты интернет-магазина перед покупкой. На мошеннических сайтах чаще всего это реквизиты физического лица, номер карты или электронного кошелька. Таким сайтам доверять нельзя.

9. Не ведитесь на манипуляции, к которым относятся: всплывающие заманивающие баннеры, акции с таймерами оставшегося времени, надпись «этот товар вместе с вами смотрят N человек» и многое другое. Все эти приемы не должны подгонять вас совершить покупку - сначала убедитесь, что сайту можно доверять.

10. Всегда держите включенным антивирус на компьютере и телефоне - это поможет избежать заражения троянской программой, позволяющей злоумышленникам обчистить ваш банковский счет.