**Четыре признака кибермошенника: алгоритм от экспертов**



Вместе с ростом покупок подарков на Новый год активизируются и кибермошенники. Для них это самое прибыльное время: миллионы людей просматривают десятки миллионов страниц интернет-магазинов.

В предпраздничной лихорадке намного проще заманить покупателя на поддельный сайт и украсть деньги или данные карты.

Провайдер электронных платежей bePaid утверждает, что разработал специальный алгоритм действий, используя который любой покупатель в Сети сможет с максимальной вероятностью определить мошеннический сайт за 1 минуту и сохранить свои деньги.

“Мы рекомендуем использовать этот алгоритм абсолютно во всех случаях. Неважно, как вы зашли на этот сайт: через поисковик, получив письмо на почту или сообщение в Вайбере, кликнув на рекламное объявление или по ссылке от вашего налогового инспектора. У мошенников огромное количество способов заманить вас к себе. А ваши хорошие знакомые могут и не знать, что сайт поддельный – они просто увидели привлекательное предложение в чате или соцсетях”, – говорит сооснователь и директор eComCharge LLC (бренд – bePaid) Александр Шостак.

Прежде всего проверьте сайт с помощью сервиса “Безопасный просмотр” от Google. Оптимальный вариант – если вы внесете ссылку на этот сервис в закладки и будете проверять все новые сайты, на которые заходите.

****

**Признаки мошенничества**

* **У сайта отсутствует SSL-сертификат**

****

Речь идет о том самом “замочке” в браузерной строке в начале адреса сайта. Если его нет – лучше сразу закрыть этот ресурс. Ведь это означает, что сайт не использует безопасного шифрования, а это значит, что любая введенная информация может быть похищена.

* **Вам предлагают ввести реквизиты вашей карты прямо на сайте**

****

Если на сайте вас просят ввести номер карты и CVV/CVC код (те самые заветные 3 цифры с обратной стороны вашей карты) – не делайте этого. 99,9% интернет-магазинов во всем мире пользуются услугами специализированных платежных сервисов. Для приема платежей создается специальная защищенная страница, которая может открываться как на отдельной вкладке интернет-браузера, так и в айфрейме поверх сайта продавца. Именно на ней и следует вводить свои платежные данные. Интернет-магазин не может и не должен получить информацию, которую вы там введете.

* **На сайте работает таймер – до конца акции от 5 до 15 минут**

****

Начинайте опасаться: такой таймер – излюбленный прием мошенников. Сделано это для того, чтобы вы меньше обращали внимание на нестыковки на сайте, а побыстрее вводили свои данные.

* **У платежной страницы странный адрес**

У платежной страницы, как и у всех остальных, есть адрес. Внимательно проверьте: он должен содержать основной домен провайдера. Мошенники пытаются подделать ссылку – отличия могут быть в сдвоенных (или наоборот, пропущенных) символах, замене символов на похожие. Самый простой вариант – скопировать доменное имя и зайти на основной сайт провайдера. Если не получается или сайт провайдера выглядит странно и не вызывает доверия – немедленно закройте страницу. Точно так же можно проверить и достоверность платежной ссылки, которую вам прислали.

На все действия, указанные выше, уходит 1-2 минуты. Но это может сэкономить вам солидную сумму. Кроме того, для покупок в Сети проще всего завести бесплатную виртуальную карту и проводить расчеты через нее. И не переводить на нее больше денег, чем вы собираетесь потратить на покупку.

Вы можете сделать и доброе дело: заметив такой мошеннический ресурс, сообщите о нем в специальные службы Google и Яндекс или напрямую в компанию, за которую мошенники пытаются себя выдать. Помогите остальным не попасться на крючок.