

Кибермошенники активизировались в преддверии майских праздников.

Аферисты активно рассылают фишинговые электронные письма от имени крупных российских продавцов бытовой техники с предложением о приобретении различных видов товаров по «горячей акции».

Оформление этих писем осуществляется в строгом корпоративном стиле, который характерен для многих российских ритейлеров.

Для удобства потенциальных жертв в мошенническом письме есть кнопка «использовать промокод», при нажатии на которую происходит автоматический переход на поддельный сайт, принадлежащий, якобы, одному из крупных российских ритейлеров бытовой техники.

Эту веб-страницу будет достаточно сложно отличить от оригинального ресурса из-за того, что мошенники применяют технику тайпосквоттинга (домены фейковых сайтов схожи с оригиналами).

Внимательно проверяйте электронные письма

Получив любое письмо, не спешите отвечать или выполнять инструкции из него: сначала обратите внимание на важные детали. Что должно насторожить?

1. Броская тема. Крупные переводы, денежные компенсации, взлом или блокировка учетной записи, мошеннические операции... Злоумышленники стараются завладеть вниманием, играя на чувствах жертвы, особенно часто — на жадности или страхе.
2. Нагнетание обстановки. Фразы вроде «срочно!» и «у вас осталось всего 3 часа», обилие восклицательных знаков — тоже уловки из арсенала мошенников, которые только и мечтают заставить вас торопиться, паниковать и от этого потерять бдительность.
3. Ошибки, опечатки и странные символы в тексте. Некоторые преступники и правда безграмотны, но иногда злоумышленники специально пишут слова с ошибками, например «розыгрышь призов», или меняют часть букв на похожие латинские. Так они пытаются обойти спам-фильтры.
4. Странный адрес отправителя. Нагромождение случайных букв и цифр или «левый» домен в адресе отправителя письма, якобы пришедшего от крупной организации, — верный признак подделки.

5. Ссылка в письме, если она там есть. Точнее, адрес сайта, на который она ведет. Чтобы увидеть его, нужно навести мышку на ссылку и внимательно проверить адрес. Часто в расчете на невнимательность жертв преступники вставляют в сообщения ссылки на сайты с именами известных компаний или брендов с небольшим изменением. Поэтому проверять ссылку надо очень внимательно.

[#МВДРоссии](#) [#МВД](#) [#МВД74](#) [#Полиция74](#) [#Челябинскаяобласть](#) [#ПолицияЮжногоУрала](#) [#ПолицияКатавИвановскийрайон](#) [#Профилактика](#) [#Мошенничество](#)

