

В преддверии традиционной осенней распродажи, которая в 2020 году стартует в ночь на 27 ноября, аферисты начали массовые атаки на покупателей. Люди получают ссылки якобы для предзаказа товаров со скидкой, а после того как они вводят данные карт, мошенники опустошают их счета.

Чаще всего преступники действуют от имени крупных торговых сетей. Они звонят, присылают СМС-сообщения и электронные письма с описанием больших скидок на электронику и бытовую технику, одежду и обувь, товары для дома и здоровья.

Чтобы «зарезервировать товар» или «получить дополнительный дисконт», людям предлагают «сделать предзаказ» по ссылке. Такая ссылка ведет на фишинговую страницу, с помощью которой мошенники узнают реквизиты карт покупателей и получают доступ к их счетам.

На самом деле крупные торговые сети не присылают отдельные «ссылки на оплату». Все операции проходят через их официальные сайты. Но мошенники часто создают сайты-клоны, адреса которых отличаются от настоящих всего одним-двумя символами, поэтому всегда проверяйте, не оказались ли вы случайно на поддельном сайте.

Прежде чем вводить реквизиты карты на странице оплаты, удостоверьтесь, что сайт использует защищенное соединение: адрес должен начинаться с <https://>, а в адресной строке стоять значок закрытого замка. Не переходите по ссылкам от неизвестных отправителей. Если предложение приходит от популярного магазина, лучше самостоятельно зайти на его официальный сайт и перепроверить информацию.

Пресс-служба ГУ МВД России по Волгоградской области