«Введите реквизиты банковской карты»

Лариса, Электросталь

Мы с мужем решили подарить сыну смартфон на день рождения. Он выбрал дорогую модель, но 18 лет не каждый день исполняется — надо его порадовать. Посмотрели в интернете, где купить такой телефон, и наткнулись на московский интернет-магазин с доставкой в любую точку России. Цены там намного ниже, чем везде.

Насторожились — почему такая разница? Прочитали на сайте интернет-магазина, что он так продвигает безналичные платежи. Там же была фотография склада и подробная схема на карте, как проехать. Все выглядело убедительно. Тем более друзья уже давно заказывают через интернет то телевизор, то пылесос — дешевле выходит.

Отправили предоплату через сайт. Сделали все по инструкции: ввели данные карты и пин-код. Пришла смс о списании, а через несколько минут сообщения стали приходить одно за другим, и скоро на карте не осталось денег. Позвонили в полицию и банк, написали заявление и заблокировали счет, но что толку?

Муж ездил в Москву, благо недалеко живем, а на месте магазина ничего нет — вывеску просто пририсовали! Телефон, указанный на сайте, не работал, а сам сайт пропал через два дня. Сын остался без подарка, а мы месяц жили на мою зарплату — у мужа с карты утекло 50 000 рублей. Больше интернет-магазинам не доверяем.

Совет эксперта по противодействию мошенничеству:

Это типичный случай фишинга, от английского fishing, «рыбалка». «Рыбак» выманивает у пользователя персональные данные — чаще всего реквизиты банковской карты.

Для доступа к чужому банковскому счету мошенники создают сайт, который выглядит как интернет-магазин, платежный сервис или банк. Внешний вид подделки копирует реально существующий портал, а адрес на первый взгляд похож.

На фишинговый ресурс попадают по ссылке в электронном письме или через контекстную рекламу. Вас попросят ввести данные карточки,

в том числе пин- и трехзначный код с обратной стороны карты, и таким образом вы откроете доступ к любым мошенническим операциям.

Как отличить фишинговый сайт от настоящего?

- Длинное и сложное доменное имя или имя, похожее на название известного интернет-магазина, банка, социальной сети, бренда. Перед адресом сайта нет префикса https: буква s означает secure — безопасное соединение.

- Сайт зарегистрировать совсем недавно. Проверить дату создания домена можно здесь: whois-service.

- Встречаются опечатки, несоответствия, небрежности и ошибки: орфографические, пунктуационные, фактические.

- Цены ниже рыночных более чем на 20%. Даже если их объясняют таможенным конфискатом или ликвидацией товара, это настораживает. Ссылка пришла из неизвестного вам источника. Будьте осторожнее и со ссылками друзей в соцсетях: их могли ввести в заблуждение или взломать.

- Вы попали на сайт, вызвавший подозрения, когда использовать открытую сеть Wi-Fi без пароля.

- Похожие схемы мошенничества работают и вне интернета, поэтому никому не сообщайте данные карты. Звонок «от банка» с просьбой назвать пин-код и реквизиты, чтобы якобы разблокировать карту, — сигнал повесить трубку и позвонить на подлинную горячую линию банка.

- Обнаружив, что письмо или сообщение в соцсети — фишинговое, помечайте его как спам или нажимайте «Пожаловаться». Так вы поможете остановить злоумышленников. Если вы уже стали жертвой мошенников, сообщите об этом в банк, заблокируйте карту и не откладывая напишите заявление в полицию. Банк обязан вернуть деньги, если вы не говорили никому пин-код и обратились в службу поддержки сразу — но даже если вы не соблюли эти условия, полиция должна помочь.