Осторожно, фишинг! Будьте внимательны, совершая покупки через Интернет

Проблема совершения хищений путем использования компьютерной техники в Беларуси остается актуальной.

Одним из распространенных способов хищения является фишинг, цель которого завладеть реквизитами банковской платежной карты. Злоумышленник под любым мошенническим предлогом вынуждает жертву пройти по ссылке на поддельный интернет-ресурс и ввести там номер карты, срок действия и CVV-код, чтобы похитить эти данные и «очистить» банковский счет. Киберпреступники умело подделывают различные популярные интернет-ресурсы, которые оказывают услуги населению и имеют сервис совершения онлайн-платежей: торговые интернет-площадки, службы доставки, сайты торговых сетей и так далее.

Чтобы не потерять все сбережения, надо соблюдать ряд простых, но очень важных правил.

Первое. Если вам кто-то пишет в мессенджере и предлагает оплатить товар, перейдя по ссылке, не спешите это делать! Внимательно проверьте электронный адрес сайта через поисковые системы. Фишинговый ресурс от оригинального может отличаться буквально одним или несколькими символами. К примеру, вместо официального адреса belpost.by вам пришлют ссылку bellpost.be, belpost.bj, belposta.bz, bellpochta.be, и т.д.

Второе. Если ссылку вам прислал незнакомый абонент, и вы твердо намерены совершить с ним сделку, тогда самостоятельно отыщите через «поисковик» официальный сайт компании или предприятия и воспользуйтесь платежным сервисом непосредственно на подлинном ресурсе.

Третье. Для осуществления онлайн-платежей заведите отдельную банковскую карту, без доступа к основному карт-счету. Пополняя ее по необходимости, вы тем самым убережете свой главный банковский счет: в случае компрометации этой карты добыча преступника будет весьма незначительной.