5. Зачастую мошенники делают рассылки в социальных сетях, мессенджерах, на электронную почту с информацией об акциях/скидках от лица маркетплейса. Для оплаты товара присылают ссылку на фишинговый сайт (поддельный сайт, который может полностью копировать оригинальный ресурс). Рекомендуем потребителям не переходить по ссылкам, полученным в личных сообщениях в мессенджерах и на сторонних сайтах в репутации которых вы не уверены на 100%. ***Все оплаты рекомендуется осуществлять только на сайте маркетплейса или продавца, использующего эквайринг.***

Фишинг

Фишинг – вид интернет-мошенничества, направленного на получение доступа к конфиденциальным данным пользователей — логинам и паролям.

Как правило, для этого осуществляются рассылки электронной почты или личных сообщений якобы от имени популярных сервисов, брендов или компаний (например, банков). В письме пользователя убеждают выполнить какое-то действие, зайдя на сайт по указанной ссылке. Сайт, на который переходит пользователь, как правило, визуально неотличим от сайта организации или сервиса. Как правило, фишинг можно отличить по доменному имени от подделываемого сервиса – так, подделка под PayPal может быть размещена на сайте с именем наподобие PayPal-Notifications. В одном из самых известных в Рунете случаев фишинга пользователям предлагалось совершить действия на доменном имени yanclex.ru – злоумышленники рассчитывали на визуальное сходство латинской буквы d и буквосочетания cl.

Фишинг использует для распространения технологии «социальной инженерии», поэтому технологические способы противодействия ему могут быть неэффективны.