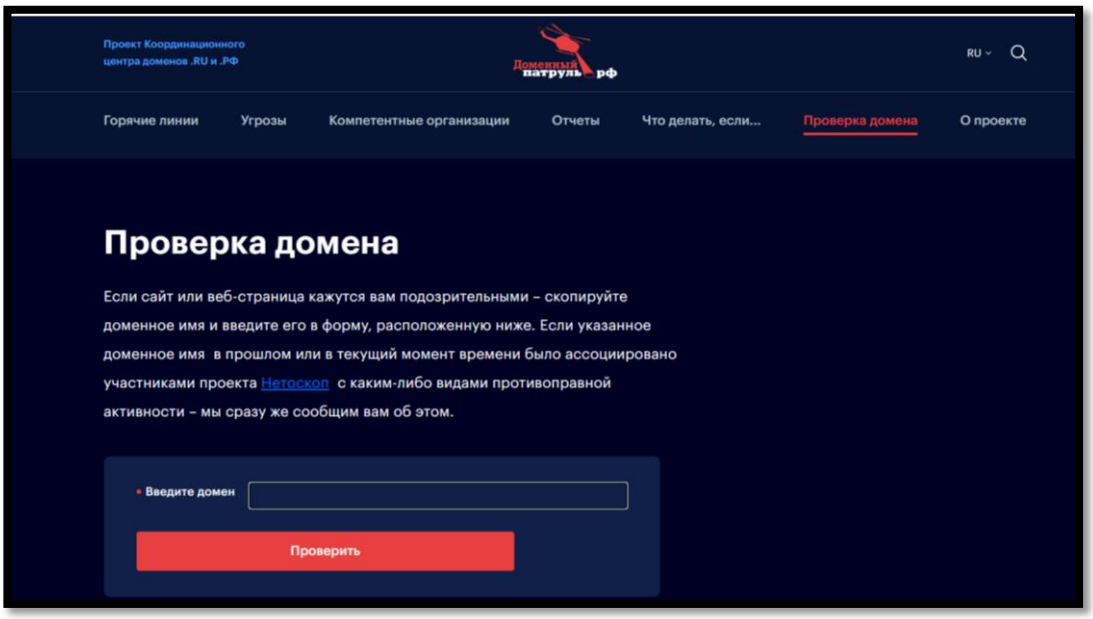
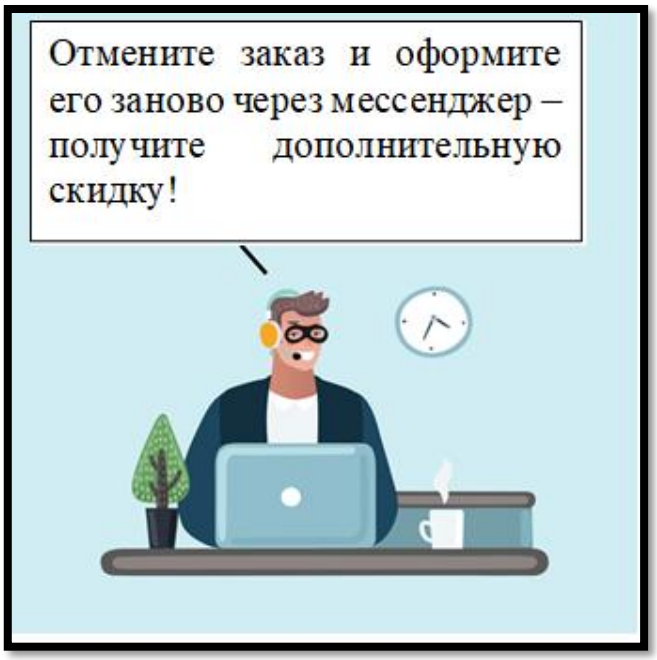
ОБ АКТУАЛЬНЫХ РИСКАХ ПРИ ПОКУПКАХ В СЕТИ ИНТЕРНЕТ

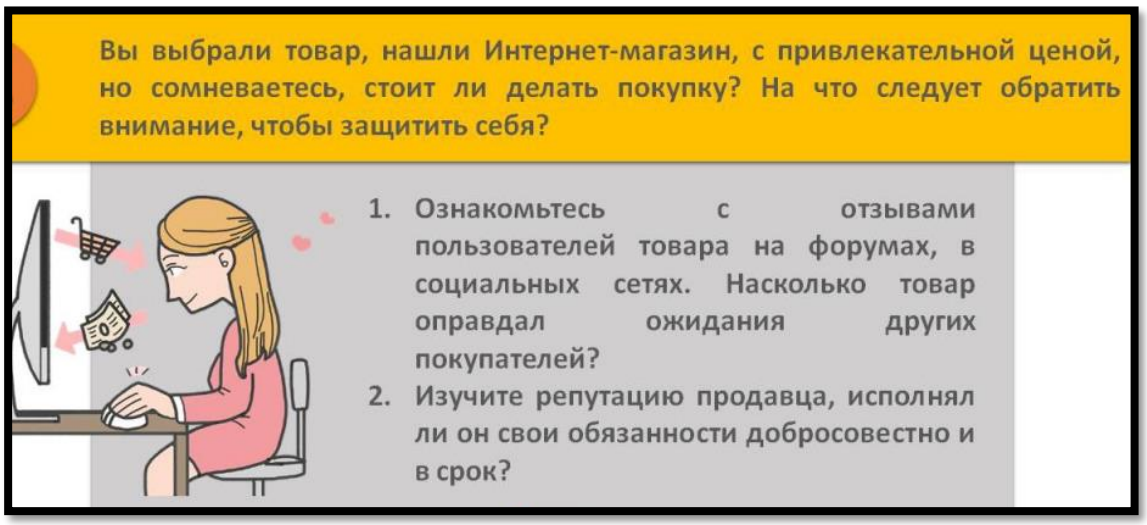
Если вы столкнулись с мошенниками, рекомендуем обратиться в «Доменный патруль», это специальный ресурс, объединяющий усилие специалистов, компаний и государственных органов, противостоящих киберугрозам.



1. При бронировании товара на сайте маркетплейса или продавца или после оплаты учтите, если вас просят отменить заказ и оформить его заново на другом сайте или через мессенджер под разными предлогами (дополнительные скидки, бесплатная доставка или иные бонусы) ***это могут быть мошенники.***



2. Совершая покупки на электронных площадках (маркетплейсы, доски объявлений) на большие суммы, обратите внимание ***на ассортимент продавца***, ***наличие положительных и отрицательных отзывов***, ***объемы его продаж***. На крупных маркетплейсах все продавцы, как правило, проходят проверку, предоставляя правоустанавливающие документы, они имеют свои службы безопасности и сотрудничают с правоохранительными органами. А вот право на использование доменного имени сайта в сети интернет может приобрести любое, даже физическое лицо. Выбирая незнакомый интернет-магазин, на специальном ресурсе можно сделать проверку доменного имени. Если домен зарегистрирован на частное лицо, оплату принимают переводом на карту, предлагают доставку наложенным платежом – воздержитесь на время от покупки, посмотрите отзывы в интернете, выясните, есть ли на сайте информация о месте нахождения продавца, спросите о безопасных способах покупки (оплата при получении товара, после его проверки).



3. Мошенники в последнее время применяют новые схемы, например, за вознаграждение покупают/берут в аренду личные кабинеты клиентов маркетплейсов и торговых площадок. ***Никогда не предоставляйте доступ к своему личному кабинету третьим лицам!***

4. Все чаще мошенники размещают на сторонних сайтах информацию о лотереях и выигрышах по случаю юбилея маркетплейса или иной крупной площадки от лица сотрудников службы поддержки. ***Рекомендуем не переходить по сторонним ссылкам, так как служба поддержки крупных организаций отвечает только в официальных каналах связи.***

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.