**«Черная пятница»: как не попасть в ловушку на маркетплейсах**

*В ноябре стартуют онлайн-распродажи. Многие владимирцы стали активно заказывать товары на маркетплейсах. Отделение Владимир Банка России предупреждает о ловушках, которые могут поджидать покупателей в сети.*

Маркетплейсы защищают свои мобильные приложения и онлайн-кабинеты от взлома. Но порой обойти все эти барьеры мошенникам помогают сами покупатели. Разберём несколько популярных схем обмана на маркетплейсах, с помощью которых мошенники пытаются завладеть паролями от аккаунтов, реквизитами банковских карт и кодами из уведомлений для хищения денег с карт.

**«Суперскидки» по ссылке**

Накануне «черной пятницы» многие владимирцы получают письма по электронной почте, через соцсети и мессенджеры от якобы известных маркетплейсов о распродаже со скидками более 50%. В этих сообщениях всегда есть ссылка, по которой можно выгодно купить товар. Но вместо сайта реального магазина она ведет на сайт-двойник. С его помощью преступники воруют деньги и данные карт доверчивых покупателей.

«Когда вы получаете сообщение от знакомой компании, внимательно проверьте отправителя. Аватарка с логотипом компании не гарантирует, что вам пишет представитель настоящего магазина. А если адрес хотя бы одним символом отличается от официальной почты организации, письмо лучше сразу удалить. Иначе вы рискуете попасть на фишинговый сайт — клон настоящего магазина. Лучше всего самому зайти в приложение или на официальный сайт магазина — персональные скидки вы увидите после авторизации. При этом ни по каким ссылкам переходить не придется», — рекомендует эксперт по кибербезопасности владимирского отделения Банка России Евгений Гаврилюк.

**Поддельная техподдержка**

В группах маркетплейсов в соцсетях мошенники выискивают людей, которые жалуются на проблемы с заказами, и точечно обрабатывают таких покупателей. Предлагают бонусы от компании или помощь в возврате товара. Форма возврата, которую присылают аферисты, на самом ведет на поддельную страницу банка. Поскольку они не просят денег, а наоборот — обещают возврат, люди теряют бдительность и выдают секретные реквизиты карты.

«Общайтесь со службой поддержки только в проверенных каналах — в чате приложения или сайта маркетплейса. Если решите использовать дополнительные каналы связи, используйте только те, что указаны на официальной странице магазина. Не передавайте никому полные данные карты — срок действия, три цифры с оборота — ни в каких соцсетях и мессенджерах», — подчеркнул Евгений Гаврилюк.

**Взлом аккаунта**

Мошенники взламывают электронную почту человека и с ее помощью входят в его аккаунт на маркетплейсе. Набирают заказов и оплачивают картой, которая привязана к аккаунту. Если покупка не превышает 1000 рублей, коды подтверждения операций от банка не требуются. Аферисты рассчитывают обмануть как можно больше покупателей и исчезнуть до разбирательства интернет-магазина

«Чтобы избежать подобных проблем, используйте для электронной почты сложный пароль. Для каждого аккаунта на сайтах магазинов, банков и других организаций создавайте свой пароль. Стоит завести отдельную карту для интернет-покупок и каждый раз переводить на нее нужную сумму прямо перед оплатой. Или вообще не сохранять данные карты для оплаты в разных сервисах и магазинах — просто вводить их перед каждой покупкой», — пояснил эксперт Отделения Владимир Банка России.

**Легкий заработок**

Мошенники часто завлекают людей в свои сети обещаниями дистанционной работы и высоким заработком. Задачи могут быть самыми разными, – к примеру, оформлять заказы на сайте маркетплейса, затем отменять их. Якобы это повышает рейтинги выбранных продавцов и самой торговой площадки. Называется эта должность обычно очень красиво — «трейдер маркетплейса», в обязанности которого входит «увеличение конверсии и объема транзакций».

Чтобы убедить человека, что работа настоящая, мошенники могут поначалу даже перечислить ему небольшую «зарплату». Для этого «новому работнику» нужно зарегистрироваться на маркетплейсе по специальной ссылке от куратора. Там же нужно внести депозит. Если отправить 500 рублей — вернется столько же плюс 30%. За 1000 рублей — уже 50%, а за 3000 рублей — все 70%. Но как только человек пополнит «депозит» на крупную сумму — эти деньги уже не вернутся, и работодатель исчезнет.

«Не верьте обещаниям высокого заработка за неквалифицированный труд без опыта работы. Обращайте внимание на список обязанностей: расплывчатые формулировки — явный признак обмана. И, главное, не связывайтесь с людьми и компаниями, которые просят внести плату за регистрацию в их сервисах, перечислить «страховой взнос» или купить что-то, чтобы начать работать. Почти наверняка это мошенники», — заключил эксперт по кибербезопасности.