Приложение к письму
от «____» июня 2024 №_____

С какими мошенническими схемами можно столкнуться в 2024 году (данные МВД России)

Как не потерять деньги, продавая вещи в Интернете.

Не раскрывать свои персональные данные.

Составляя объявление в Интернете, ограничьтесь описанием товара. Не указывайте реквизиты карты и личные данные: точный адрес, номер паспорта и другую конфиденциальную информацию. Никогда не выкладывайте фотографии банковской карты и документов.

Номер своего мобильного телефона тоже лучше скрыть, если портал или приложение для объявлений позволяют это сделать. Покупатели смогут позвонить на тот номер, который вам предоставит онлайн-площадка, или связаться в чате сервиса объявлений.

Не обсуждать детали в сторонних мессенджерах.

Мошенники создают специальные фишинговые страницы, которые помогают им узнать данные карты пользователя. Эти страницы они маскируют под сайты служб доставки, платежные страницы сервисов объявлений, системы денежных переводов.

Не отказывайтесь от услуги «безопасная сделка», которую часто предлагают крупные сервисы объявлений. В таком случае покупатель оплачивает товар банковской картой, деньги резервируются на счете онлайн-площадки и поступают на карту продавца, как только покупатель получит посылку.

Известные российские и международные курьерские компании тоже позволяют провести оплату по такой схеме.

Если нет возможности рассчитаться с покупателем лично, можно отправить посылку наложенным платежом. Получатель оплатит ее в почтовом отделении, заберет товар, а почта переведет деньги вам.

Не сообщать покупателю конфиденциальную информацию о банковской карте.

В некоторых онлайн-магазинах для покупки не нужно вводить трехзначный код с обратной стороны карты и коды подтверждения от банка.

Мошенники этим пользуются. Они оплачивают счет чужой картой, зная только ее номер, срок действия и имя владельца.

Для перевода денег достаточно номера карты или счета. Никакую другую информацию сообщать нельзя.

Не отдавать товар раньше, чем покупатель его оплатил.

Иногда аферисты используют демоверсии банковских приложений. Там можно сымитировать перевод — экран просто показывает, как перечисление денег будет выглядеть в приложении, но на самом деле суммы со счета на счет не переходят. В некоторых случаях мошенники создают сайты-дубликаты, которые похожи на настоящие онлайн-банки.

Сначала покупатель должен оплатить товар и только потом его забрать. С карты на карту перевод проходит буквально за минуту. Обязательно дождитесь, когда банк пришлет вам сообщение о зачислении денег.

Когда вам дают наличные, убедитесь, что деньги настоящие. Или попросите при вас снять сумму в банкомате.

Опять же, может выручить услуга «безопасная сделка» сервиса объявлений или проверенной курьерской службы.

Не переходить по ссылкам от незнакомцев.

Нужно установить антивирусные программы на все свои гаджеты и регулярно их обновлять.

Никогда нельзя переходить по ссылкам из писем и сообщений незнакомых пользователей. Когда заходите на сайт известного вам онлайн-сервиса, магазина, банка или другой организации, крайне внимательно проверяйте адресную строку.

Поддельные сайты бывают очень похожи на настоящие, а их адреса могут различаться всего одним-двумя символами.

Часто в сети можно встретить заманчивые объявления с вакансиями. Делать на такой работе нужно мало, график удобный, деньги платят — что еще нужно для счастливой жизни на удаленке.

Однако не всем подобным предложениям стоит доверять.

Что нужно знать, чтобы не попасться на уловки мошенников, которые специализируются на обмане людей, находящихся в поиске работы? Вот несколько «красных флагов» от «Лапша Медиа».

Потенциальный работодатель просит что-то оплатить.

Как бы ни назывался платеж — предоплата за оборудование, плата за обучение или депозит безопасности — требование вложиться во что-то является серьезным признаком того, что вас пытаются обмануть.

«Рекрутера» не интересуют ваши стаж и опыт.

Если вас наняли на сложную и высокооплачиваемую работу после первого собеседования — это повод задуматься. Особенно, если у хорошей вакансии нет существенных требований к стажу и опыту соискателя.

Мошенники пытаются мимикрировать под известные бренды.

Возможно, рекрутинговая компания нанимает вас для работы в крупной компании или в госструктуру. Такое бывает, но важно проверить, что рекрутеры действительно сотрудничают с обсуждаемой на собеседовании фирмой.

Аферисты могут использовать фишинговые сайты.

Анкеты или объявления о работе могут быть размещены на мошеннических сайтах, имитирующих площадки известных брендов. Часто такие ресурсы используются для сбора персональных данных или для финансовых махинаций.

Как обезопасить себя во время поиска работы?

Не передавайте малознакомым людям личные данные заранее, с сомнением относитесь к слишком «выгодным» предложениям, обсудите вакансию с близкими, проверьте будущего работодателя, а также адрес сайта компании, не оплачивайте сомнительные услуги.

Мошенническая схема в отношении продавцов на досках объявлений.

Основное отличие этой мошеннической схемы от традиционной заключается в том, что злоумышленник играет роль покупателя, а не продавца.

На первом этапе обмана мошенники пишут продавцу сообщение с предложением приобрести предложенный товар, но с одним нюансом: сделка должна быть проведена с помощью «безопасного платежа» на псевдо «защищённом сайте».

Псевдопокупатели рассказывают, что там они уже якобы внесли свои денежные средства в систему, поэтому потенциальной жертве-продавцу необходимо просто перейти по указанной ссылке, ввести данные своей банковской карточки и нажать на кнопку «получить деньги».

Мошенник присылает продавцу ссылку, ведущую на фишинговый сайт. В том случае, если человек перейдёт на этот ресурс и введёт там свои платёжные данные, то они мгновенно будут отправлены киберпреступникам, которые всеми способами постараются опустошить банковский счёт потенциальной жертвы.

Отдел по вопросам общественной безопасности и профилактики правонарушений Администрации города Ханты-Мансийска