Ежемесячный информационный бюллетень по безопасности

Три самых распространенных мошенничества в социальных сетях

Обзор

Хотя социальные сети — это фантастический способ общаться, делиться информацией и развлекаться с другими, для киберпреступников это также недорогой способ обмануть и использовать миллионы людей. Не становитесь жертвой трех самых распространенных видов мошенничества в социальных сетях.

Мошенничество с инвестициями

Вы когда-нибудь видели сообщение об инвестиционной возможности, которая обещает огромную отдачу от инвестиций в очень короткий промежуток времени с якобы минимальным риском или без него? Реальность такова, что эти гарантии на самом деле являются мошенничеством с инвестициями. Мошенники просто крадут ваши деньги после того, как вы им заплатите. Эти мошенничества часто включают рекламу или истории успеха от прошлых клиентов для продвижения инвестиций, но это всего лишь поддельные отзывы, чтобы повысить ваше доверие. Часто эти инвестиционные аферы связаны с инвестированием в криптовалюты или недвижимость, и оплата часто производится в криптовалютах или другими нестандартными способами оплаты. Если инвестиции кажутся слишком хорошими, чтобы быть правдой, скорее всего, это обман. Помните, что нет такой вещи, как гарантированные, высокодоходные инвестиции. Инвестируйте свои деньги только в проверенные, известные ресурсы, а не в незнакомцев, которых вы встречаете в Интернете, продвигающих схему быстрого обогащения.

Романтическое мошенничество

Когда преступники развивают онлайн-отношения с кем-то, кого они идентифицировали как одинокого или уязвимого, чтобы выманить у него деньги, это называется мошенничеством в романтических отношениях. Преступник будет использовать любую тактику, чтобы завоевать доверие, в том числе обмениваться поддельными фотографиями или отправлять подарки, а затем рассказывать трагическую историю о том, что ему нужны деньги для оплаты таких расходов, как больничные счета или дорожные расходы, чтобы лично посетить жертву. Чтобы избежать личной встречи, эти преступники могут говорить, что они работают в отрасли, которая не позволяет им этого делать, например, в строительстве, международной медицине или вооруженных силах. Они часто запрашивают деньги в виде банковского перевода или подарочных карт, чтобы быстро получить

наличные и остаться анонимными. Эти виды мошенничества распространены не только в социальных сетях, но и в приложениях для онлайн-знакомств. Будьте осторожны с людьми, с которыми вы встречаетесь в Интернете, не торопитесь и никогда не отправляйте деньги тому, с кем вы общались только в Интернете.

Кроме того, если вы считаете, что кто-то из ваших знакомых может быть уязвим для такой атаки или находится в онлайн-отношениях, предложите им помощь. Иногда тому, кто поглощен эмоциональной связью, может быть очень трудно понять, насколько опасной стала ситуация.

Мошенничество в интернет-магазинах

Мошенничество с онлайн-покупками происходит, когда вы покупаете товары в Интернете по невероятно низким ценам, но так и не получаете их. Заманчивая реклама в социальных сетях будет предлагать невероятные цены и содержать ссылки, ведущие на сайты, которые кажутся законными и продают известные бренды, но эти сайты часто являются поддельными. Остерегайтесь веб-сайтов, на которых нет контактной информации, неработающие контактные формы или используются личные адреса электронной почты. Введите название интернет-магазина или его веб-адрес в поисковую систему, чтобы узнать, что о нем говорят другие. Ищите такие термины, как «мошенничество», «никогда больше» и «фальшивка». Будьте очень осторожны с онлайн-акциями или предложениями, которые кажутся слишком хорошими, чтобы быть правдой. Гораздо безопаснее покупать товары, которые могут стоить немного дороже, но на проверенных сайтах, которыми вы или ваши друзья пользовались раньше.

Хорошая новость: вы лучшая защита для себя. Вы контролируете ситуацию. Просто будьте начеку, чтобы не допустить подобного мошенничества, и вы сможете безопасно и надежно пользоваться всеми социальными сетями.

Приглашенный редактор

Крис Элджи (@chriselgee) является тестировщиком и разработчиком задач для @CounterHackSec, командования кибербатальона Национальной гвардии и сертифицированный инструктор SANS. Ему нравится узнавать о мельчайших технических деталях, превращать их в более широкое организационное понимание и делиться им со студентами и клиентами.

Ресурсы

Мошеннический трекер Better Business Bureau: https://www.bbb.org/ScamTracker
Социальный инжиниринг: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Безопасные покупки в Интернете: https://www.sans.org/newsletters/ouch/shopping-online-securely-nov-21/
Вишинг - атаки на телефонные звонки и мошенничество: https://www.sans.org/newsletters/ouch/vishing/

Переведено для сообщества: Роман Поляков