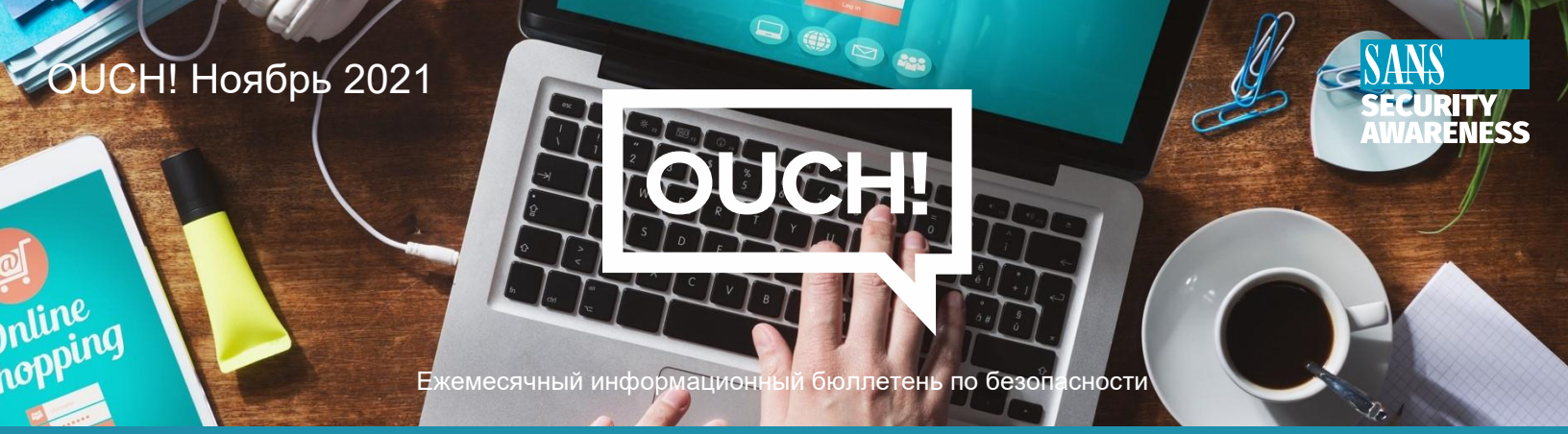

Безопасные покупки в Интернете

Приближается праздничные дни. Скоро миллионы людей будут покупать подарки, и многие из нас будут делать покупки в Интернете. К сожалению, киберпреступники также будут активны, создавая поддельные веб-сайты и другие мошеннические операции с покупками в Интернете, чтобы украсть вашу информацию или деньги. Узнайте, как можно найти выгодные предложения, не становясь жертвой.

Поддельные интернет-магазины

Преступники создают поддельные интернет-магазины, которые имитируют внешний вид реальных сайтов или используют названия известных магазинов или брендов. Когда вы ищете лучшие онлайн-предложения, вы можете оказаться на одном из этих поддельных сайтов. Покупая на таких веб-сайтах, вы можете получить поддельные или украденные товары, или ваши покупки могут никогда не быть доставлены. Примите следующие меры, чтобы защитить себя:

- По возможности покупайте в интернет-магазинах, которые вы уже знаете, которым доверяете и с которыми ранее работали. Добавьте эти интернет-магазины в закладки.
- С подозрением относитесь к рекламе или продвижению в поисковых системах или социальных сетях, в которых цены значительно ниже, чем те, которые вы видите в известных интернет-магазинах. Если сделка звучит слишком хорошо, чтобы быть правдой, это может быть мошенничество.
- Будьте осторожны с веб-сайтами, с которыми нет возможности связаться, с неработающими контактными формами или с личными адресами электронной почты.
- Относитесь с подозрением, если веб-сайт выглядит так же, как тот, который вы использовали в прошлом, но доменное имя веб-сайта или название магазина отличаются. Например, вы могли совершать покупки на Amazon, адрес веб-сайта которого - www.amazon.com, но в итоге оказались на поддельном веб-сайте, который выглядит похожим, но с адресом www.amazonshoppers.com.
- 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».
- Защитите свои учетные записи в Интернете, используя надежный пароль для каждой из ваших учетных записей. Не можете запомнить все свои пароли? Подумайте об использовании менеджера паролей.

Мошенники на законных сайтах

Будьте бдительны даже при совершении покупок на проверенных веб-сайтах. Интернет-магазины часто предлагают товары, продаваемые третьими сторонами - разными лицами или компаниями, - которые могут иметь мошеннические намерения. Такие онлайн-направления похожи на реальные рынки, где одни продавцы заслуживают большего доверия, чем другие.

- Перед размещением заказа проверьте репутацию каждого продавца, прочитав отзывы о них.
- Остерегайтесь продавцов, у которых новый интернет-магазин, не имеют отзывов или продают товары по необычно низким ценам.
- Ознакомьтесь с политикой интернет-магазина в отношении покупок у третьих лиц.
- В случае сомнений покупайте товары, продаваемые непосредственно в интернет-магазине, а не у сторонних продавцов, которые участвуют в его онлайн-рынке.
- Даже с законными поставщиками, прежде чем совершать покупку убедитесь, что вы понимаете правила гарантии и возврата.

Онлайн-платежи за покупки

Регулярно просматривайте выписки по кредитной карте, чтобы выявить подозрительные платежи. Если возможно, включите уведомление по электронной почте, в текстовом сообщении или в приложении о списании средств. Если вы обнаружите какую-либо подозрительную активность, немедленно сообщите об этом в компанию, обслуживающую вашу кредитную карту. Используйте кредитные карты вместо дебетовых для онлайн-платежей. Дебетовые карты принимают деньги прямо с вашего банковского счета; если будет совершено мошенничество, вам будет намного сложнее вернуть их. Электронные платежные сервисы или электронные кошельки, такие как PayPal, также являются более безопасным вариантом для покупок в Интернете, поскольку они не требуют, чтобы вы сообщали поставщику номер кредитной карты. Избегайте веб-сайтов, которые принимают оплату только в криптовалюте или требуют малоизвестных способов оплаты.

Тот факт, что интернет-магазин имеет профессиональный вид, не означает, что он законный. Если веб-сайт вызывает у вас недоверие, не используйте его. Вместо этого перейдите на известный сайт, которому вы можете доверять или которым вы безопасно пользовались в прошлом. Возможно, вы не найдете самое лучшее предложение, но у вас гораздо больше шансов избежать мошенничества.

Приглашенный редактор

Марк Орландо - руководитель службы безопасности, защищавший сети в Пентагоне, Белом доме и многочисленных клиентов из частного сектора. Сегодня он является генеральным директором и соучредителем фирмы Bionic, занимающейся кибербезопасностью, а также инструктором и автором курсов в Институте SANS. [Twitter: @markaorlando]

Ресурсы

Создание простых паролей: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Социальный инжиниринг: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Текстовые сообщения /SMS фишинг: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks/
Обман через социальные сети: https://www.sans.org/newsletters/ouch/scamming-you-through-social-media/

Роман Полаков

OUCH! публикуется SANS Security Awareness и распространяется под лицензией Creative Commons BY-NC-ND 4.0. Вы можете свободно делиться или распространять этот информационный бюллетень, если вы не продаете или не изменяете его. Редакционная коллегия: Уолтер Скривенс, Фил Хоффман, Алан Ваггонер, Лесли Ридаут, Принцесса Янг.