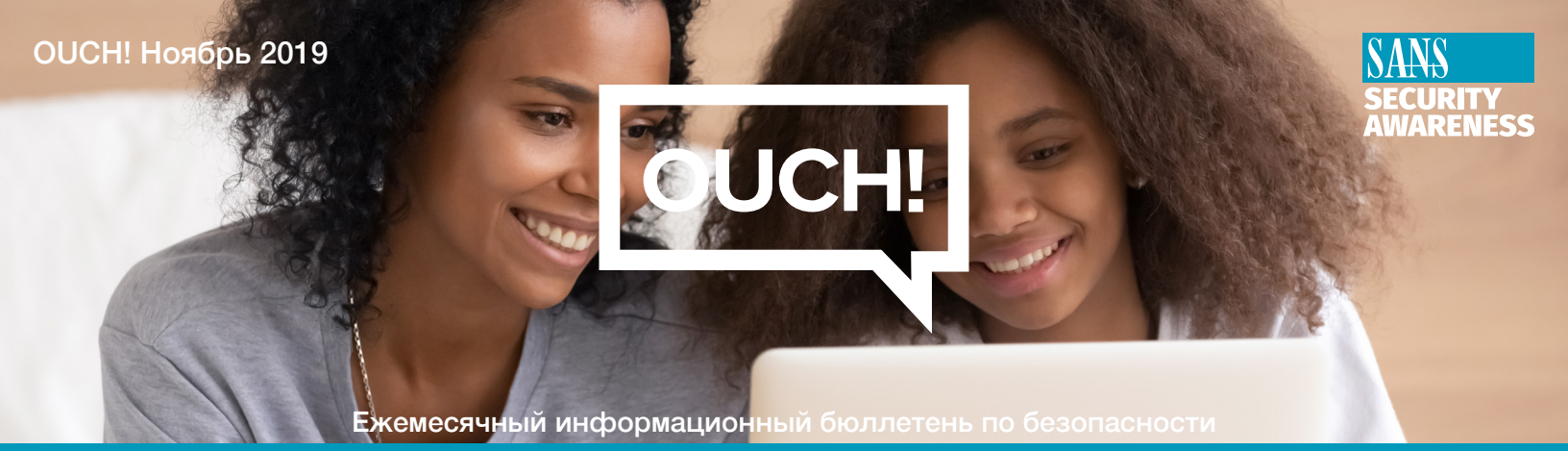

SANS SECURITY AWARENESS

OUCH!

Ежемесячный информационный бюллетень по безопасности

Безопасные покупки онлайн

Обзор

Для многих из нас приближается сезон отпусков, и скоро миллионы людей будут в поиске идеального подарка. Во избежание шумной толпы и в поисках выгодных предложений, многие будут совершать покупки онлайн. К сожалению, киберпреступники тоже будут активны, создавая поддельные веб-сайты и используя разную тактику для мошенничества. В этом бюллетене мы объясним, как можно делать покупки в Интернете безопасно и не стать жертвой.

Поддельные интернет-магазины

Киберпреступники создают поддельные интернет-магазины, которые имитируют внешний вид реальных сайтов или используют названия известных магазинов или брендов. Когда ищете лучшие онлайн предложения, вы можете оказаться на одном из таких поддельных сайтов. Покупая на таких веб-сайтах, вы можете получить поддельные или украденные вещи, а в некоторых случаях ваши покупки могут быть не доставлены. Сделайте следующие шаги, чтобы защитить себя от поддельных интернет-магазинов:

По возможности приобретайте товары в интернет-магазинах, которым доверяете и с которыми уже имели дело. Добавьте в закладки интернет-магазины, которые посещали ранее.

Обращайте внимание на цены, которые значительно ниже, чем те, которые вы видите в официальных интернет-магазинах. Если предложение звучит слишком заманчиво, чтобы быть правдой, это может быть подделкой.

Будьте бдительны, если веб-сайт который вы использовали в прошлом, но доменное имя веб-сайта или название магазина немного отличается. Например, вы можете делать покупки в Amazon, адрес веб-сайта которого - www.amazon.com, но в конечном итоге вы совершаете покупки на поддельном веб-сайте с аналогичным адресом, где буква «о» заменяется цифрой «0».

Введите название интернет-магазина или его веб-адрес в поисковой системе, чтобы увидеть другие отзывы об нём. Ищите такие термины, как «мошенничество», «никогда больше» и «фальшивка».

Используйте надежный пароль для каждой учетной записи. Не можете запомнить все свои пароли? Рассмотрите хранение их в менеджере паролей.

Мошенники на законных веб-сайтах

Будьте бдительны даже при совершении покупок на надежных веб-сайтах. Крупные интернет-магазины часто предлагают товары, продаваемые разными лицами или компаниями, которые могут иметь мошеннические намерения. Такие онлайн-направления похожи на рынки, где одни продавцы заслуживают большего доверия, чем другие. Проверьте репутацию каждого продавца перед размещением заказа. Будьте осторожны с новыми интернет-магазинами которые продают товары по необычно низким ценам. Ознакомьтесь с политикой интернет-магазина в отношении покупок у третьих лиц. В случае сомнений, приобретайте товары продаваемые напрямую интернет-магазином, а не сторонними продавцами, участвующими в онлайн-магазине.

Онлайн платежи за покупки

Регулярно просматривайте выписки по кредитной карте, чтобы выявить подозрительные расходы. Если возможно, включите опцию уведомления по электронной почте, СМС или приложению каждый раз, когда с вашей кредитной карты будет снята сумма. Если вы обнаружите какие-либо подозрительные действия, немедленно позвоните в компанию, обслуживающую кредитную карту, и сообщите об этом. По возможности старайтесь не использовать дебетовые карты. Дебетовые карты снимают деньги прямо с вашего банковского счета. Если было совершено мошенничество, вам будет гораздо сложнее вернуть деньги. Другим вариантом является использование известных платежных сервисов, таких как PayPal, для покупок в Интернете, которые не требуют, чтобы вы сообщали поставщику номер своей кредитной карты. Наконец, рассмотрите возможность использования подарочной карты для покупок в Интернете.

То, что интернет-магазин имеет хорошо продуманный и профессиональный дизайн, не означает, что он легитимен. Если веб-сайт кажется вам подозрительным, не используйте его. Вместо этого, перейдите на известный сайт, которому вы можете доверять или который безопасно использовали в прошлом. Возможно вы не найдете такое выгодное предложение, но у вас гораздо больше шансов получить легитимный продукт и избежать мошенничества.

Приглашенный

Ленни Зельцер *- директор по информационной безопасности в Axonius и старший преподаватель и автор в Институте SANS. Вы можете следить за ним в Twitter как@lennyzeltser и читать его блог назeltser.com.*

Ресурсы

Социальная инженерия:	http://www.sans.org/u/X7k
Мошенничество в социальных сетях:	http://www.sans.org/u/X7p
Создание простых паролей:	http://www.sans.org/u/Xu9