OUCH!

В ЭТОМ ВЫПУСКЕ…

- Фальшивые интернет магазины
- Безопасность компьютера/мобильного устройства
- Безопасность кредитных карт

Безопасность онлайн покупок

Обзор

В сезон праздников миллионы людей по всему миру ищут подарки для родных и близких. Многие предпочитают совершать покупки онлайн, чтобы получить скидки, избежать длинных очередей и нетерпеливой толпы. К сожалению, в это же время мошенники активно создают множество фальшивых интернет магазинов, чтобы обмануть и обокрасть людей.

В этом выпуске мы расскажем о рисках при онлайн покупках и о способах получить самое выгодное предложение безопасно.

Об авторе

Ленни Зельцер создаёт продукты защиты информационной безопасности в компании Minerva Labs и преподает курс лекций по борьбе с вредоносными программами в Институте SANS. Ленни ведёт блоги в Twitter **@lennyzeltser** и на сайте **zeltser.com**.

Фальшивые интернет магазины

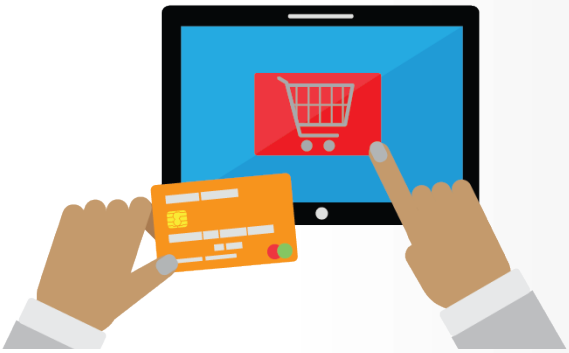
Среди множества интернет магазинов встречаются и фальшивые, созданные преступниками. Мошенники создают копии известных сайтов или используют названия известных магазинов и брендов. С помощью поддельных сайтов они охотятся на людей, которые ищут наиболее выгодные предложения. Поиск самых низких цен в интернете может привести вас на один из таких фальшивых сайтов. Следует остерегаться сайтов, которые предлагают цены, в разы ниже, чем у других поставщиков или предлагающие товар, который распродан у остальных поставщиков по всей стране. Причины, по которой цена может быть такой низкой или недоступный товар становится доступен: товар поддельный, получен нелегально, украден или вы вообще никогда не получите свой заказ. Несколько советов, которые помогут вам защитить себя:

- Старайтесь совершать покупки только в хорошо известных, надёжных интернет магазинах или в магазинах, с которыми вы уже имели дело.
- Проверьте подлинность адреса электронной почты и номера телефона, указанных для обратной связи на сайте. Если у вас есть подозрения, попробуйте пообщаться с представителем компании. Если у вас не получается связаться с кем-то из сотрудников, то это первый признак того, что сайт фальшивый.
- Обратите внимание на содержание текста на сайте: нереально заманчивые предложения, примитивный текст или грамматические ошибки – верный признак обмана.

© SANS Institute 2017

Безопасность онлайн покупок

- Многие фальшивые сайты очень похожи на настоящие, но имя домена может слегка отличаться от оригинала. Например, всем известный сайт Амазон имеет домен https://www.amazon.com. Но следует остерегаться сайта, который на него похож, с адресом http://store-amazoncom.com.
- Ознакомьтесь с отзывами других людей о сайте, введя его название или URL в поисковик. Обращайте внимание на негативные отзывы со словами «обман», «фальшивка», «никогда больше» или «подделка». Отсутствие или небольшое количество отзывов также может говорить о том, что интернет сайт очень новый и может быть подозрителен.
- Перед тем, как оплатить понравившийся товар, убедитесь, что соединение с сайтом зашифровано. Большинство браузеров показывают значок «замочек» и/или буквы HTTPS зеленым шрифтом перед именем сайта.



Безопаснее всего совершать онлайн покупки на известных и проверенных сайтах с хорошей репутацией.

Запомните, только то что сайт выглядит профессионально, не означает что он настоящий. Если вы не уверены в подлинности сайта, не используйте его. Вместо этого, найдите хорошо известный сайт, которому вы можете доверять или который вы использовали в прошлом. Вы можете не найти такого же нереально хорошего предложения, но вы скорее всего получите подлинный продукт и избежите кражи ваших персональных и финансовых данных.

Безопасность компьютера/мобильного устройства

Помимо совершения покупок на легальных сайтах, нужно обратить внимание и на безопасность вашего компьютера или мобильного устройства. Кибер преступники пытаются заразить их вирусами, чтобы получить доступ к вашим банковским счетам, кредитным картам или паролям. Поэтому следует соблюдать следующие правила:

- Если в доме есть дети, то следует выделить им отдельный компьютер. Дети необычайно любопытны и быстро осваивают технологии, в результате чего шансы получить вирус очень велики. Поэтому использование отдельного устройства для оплаты счетов, перевода денег и онлайн покупок снижает в разы вероятность получить вирус.

© SANS Institute 2017

Безопасность онлайн покупок

- Всегда используйте последнюю версию программного обеспечения, устанавливайте новейшие обновления и регулярно обновляйте антивирус. Это поможет предотвратить инфицирование компьютера вирусами.

Безопасность кредитных карт

Регулярно просматривайте ваши траты по кредитным картам в поисках подозрительных счетов, особенно если вы совершаете много покупок онлайн или сделали покупку в новом интернет магазине. Большинство провайдеров предоставляет услугу отправки письма по электронной почте или смс сообщения при каждой покупке или когда по карте превышен определённый лимит. Другой вариант – завести отдельную кредитную карту для онлайн покупок, в случае кражи данных другие платежи по-прежнему будут в безопасности. Если у вас есть подозрение, что вашей картой кто-то воспользовался, немедленно сообщите об этом в банк. По возможности, всегда используйте для онлайн покупок только кредитную карту, не стоит использовать дебетовую. Деньги по дебетовой карте идут непосредственно с вашего счета, поэтому в случае несанкционированного использования деньги сложно будет вернуть на счёт. Также рекомендуем применять для онлайн покупок кредитные карты, которые генерируют уникальный номер для каждой онлайн покупки, подарочные карты или известные платёжные сервисы, как PayPal, которые не передают номер кредитной карты продавцу.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте securingthehuman.sans.org/ouch/archives.

Ресурсы

Социальная инженерия:	https://securingthehuman.sans.org/ouch/2017#january2017
Четыре ступени безопасности:	https://securingthehuman.sans.org/ouch/2016#october2016
Безопасность домашней сети:	https://securingthehuman.sans.org/ouch/2016#february2016
Ежедневные рекомендации Института SANS:	https://www.sans.org/tip_of_the_day.php

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется Creative Commons BY-NC-ND 4.0 license. Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: ouch@securingthehuman.org

Редакция: Уолт Скривенс, Фил Хоффман, Кэти Клик, Шерил Конли
Русский перевод: Александр Котков, Ирина Коткова