Ежемесячный журнал по вопросам компьютерной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Обзор
- Примеры сайтов-фальшивок
- Способы защиты

# Сайты-фальшивки

## ОБ АВТОРЕ

Автор данной статьи - Арриго Триулзи. Арриго работает в Женеве (Швейцария) консультантом по информационной безопасности. Он также является сертифицированным инструктором Института SANS.

## ОБЗОР

Одним из достоинств покупок через интернет является возможность найти товар или услугу по более низкой цене. Преступники знают об этом и будут использовать в своих интересах ваше желание найти выгодные предложения в интернет магазинах. Злоумышленники создают поддельные сайты, которые выглядят, как настоящие, но продают фальшивые товары. В худшем случае, вам вообще не доставят ничего из приобретённых вещей. В этом выпуске мы рассмотрим примеры такого обмана и способы защиты от подобного мошенничества.

## ПРИМЕРЫ САЙТОВ-ФАЛЬШИВОК

Допустим, Вы решили купить детскую коляску для новорожденного в качестве подарка друзьям или родственникам. Вы решаете посмотреть предложения производителя колясок марки *X* в Интернете, так как эту марку детских колясок предпочитают ваши друзья. Набрав в поисковике «Марка X», Вы находите несколько сайтов, продающих детские коляски данной фирмы. Цены на разных сайтах сильно отличаются. Вы выбираете сайт с самыми низкими ценами и покупаете товар через Интернет. Через несколько недель вам присылают покупку, и вы обнаруживаете, что качество не соответствует ожиданиям: части соединены криво, имеются дефекты или изделие устаревшее. Вы пытаетесь связаться с интернет-магазином, чтобы вернуть вещь, но не находите на их сайте номера телефона. Ваши письма по электронной почте интернет-магазина остаются без ответа. На сайте указано, что жалобы по поводу приобретённого товара не принимаются. Вы купили подделку или украденную вещь с фальшивого сайта.

Что же произошло? Преступники просто скопировали настоящий сайт производителя (в данном случае, производителя детских колясок Марки X) на сайт с новым доменным именем. Преступники указали очень низкие цены для привлечения покупателей. При покупке вам доставят поддельный, украденный или бывший в употреблении товар или вообще ничего не доставят. Таким образом, чистая прибыль преступников равна стоимости Вашего заказа.

## СПОСОБЫ ЗАЩИТЫ

Не секрет, что покупки в интернет-магазинах являются довольно выгодными.

Следующие советы помогут Вам защититься от мошенников:

© The SANS Institute 2012

# Сайты-фальшивки

- Если цены слишком низкие, то это подозрительно;
- Свяжитесь со Службой поддержки продавца. Стоп…нет телефона Службы поддержки, впрочем, других номеров телефона тоже нет? Ещё один тревожный сигнал;
- В большинстве случаев, преступники, создающие фальшивые сайты, не являются носителями языка этих сайтов. Используются примитивные фразы с грамматическими и даже орфографическими ошибками. Например, текст одного из таких сайтов по продаже детских колясок: «Мы хотеть приветствовать Вас на сайт Марка Х коляска, на распродажа. Бесплатный доставка». Солидные компании тщательно следят за содержанием и качеством информации на своих сайтах. Если грамматика бедная и текст написан с ошибками, то это очень подозрительно;
- Преступники часто используют марку товара в URL имени домена, чтобы всё выглядело правдоподобно. Но они также часто меняют URL адреса своих фальшивых сайтов, чтобы их было сложней закрыть. В результате этого, в процессе покупки вы видите различные домены и адреса электронной почты. Например, фальшивый сайт по продаже детских колясок может использовать одно имя домена для сайта www.brandxbabycarriers.com, другой домен для электронной почты sales@brandxcarrierstogo.com и третий домен для адреса электронной почты Службы поддержки support@babycarriersbrandx.com. Такое использование разных доменов является отчетливым сигналом опасности;
- Реальные, серьёзные компании всегда используют шифрование в процессе оформления и оплаты интернет покупок. Если шифрование не используется, не стоит совершать покупки на этом сайте. Вы легко можете определить, используется шифрование или нет: если в URL есть *HTTPS* и ваш браузер показывает замок;
- Сделайте поиск по имени или URL адресу интернет-магазина. Узнайте, есть ли жалобы других пользователей на данный магазин. Например, если вы собираетесь покупать вещи на www.brandxbabycarrier.com, и сделаете поиск по URL адресу, то увидите жалобы покупателей на некачественные или поддельные товары этого магазина;


***Если сайт продает товары или услуги по нереально низкой цене, будьте осторожны - скорее всего, это сайт-фальшивка.***

© The SANS Institute 2012

# Сайты-фальшивки

- Используйте PayPal, Яндекс-Деньги или другие способы оплаты без предоставления продавцу данных вашей карты. Например, некоторые банки предоставляют одноразовый пароль на совершение покупки по кредитной карте. Другой вариант – использование подарочных карт.
- Используйте специальные программы, позволяющие определить степень надёжности и безопасности сайтов, которые Вы посещаете;
- Если вы не уверены в безопасности сайта, не совершайте покупки на этом сайте. Используйте сайт, которому Вы доверяете: Вы можете купить не по самой низкой цене, но зато можете быть уверены в качестве продукта. В случае необходимости, вы сможете обменять или вернуть товар.
- Если вы стали жертвой интернет-мошенников, то сообщите об этом в Федеральную службу защиты прав потребителей (РОСПОТРЕБНАДЗОР). www.rospotrebnadzor.ru Кроме того, обязательно свяжитесь с Вашим банком и заблокируйте текущую кредитную карту; чтобы избежать новых мошенничеств, лучше заказать новую карту.

## ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Некоторые ссылки были сокращены для удобства чтения с помощью сервиса TinyURL. Для повышения безопасности OUCH! всегда использует функцию предварительного просмотра TinyURL, которая показывает вам настоящий адрес, на который будет переадресована ссылка и запрашивает ваше разрешение для перехода по ней.

Паутина Доверия (проверка сайта на степень надёжности): http://www.mywot.com/

Программа McAfee SiteAdvisor (проверяет сайты на вероятность мошенничества, загрузки вредоносных программ): https://www.siteadvisor.com/

Жалобы в Федеральную Торговую Комиссию FTC (США): https://www.ftccomplaintassistant.gov/

Термины по информационной безопасности: http://preview.tinyurl.com/6wkpae5

Институт SANS: Ежедневные советы по информационной безопасности: http://preview.tinyurl.com/6s2wrkp

Покупки онлайн: как уберечься от интернет-мошенников: http://www.vesti.ru/doc.html?id=604517

## УЗНАЙ БОЛЬШЕ

Подпишись на ежемесячную рассылку OUCH! по вопросам компьютерной безопасности для пользователей, просмотри архивы OUCH! и узнай больше о решениях в области компьютерной безопасности SANS, посетив наш сайт: http://www.securingthehuman.org.

*OUCH! издается в рамках программы SANS «Защита Человека» и распространяется по лицензии Creative Commons BY-NC-ND 3.0. Распространение данного журнала разрешено при следующих условиях: наличие ссылки на источник, содержание не может быть изменено и не может использоваться в коммерческих целях. Для перевода и получения дополнительной информации, пожалуйста, свяжитесь с нами: ouch@securingthehuman.org*

*Наши авторы: Билл Уайман, Уолт Скривенс, Фил Хоффман, Ланс Спицнер, Кармен Рael Харди.*
*Перевод: Александр Котков*