

OUCH!

В ЭТОМ ВЫПУСКЕ...

- Онлайн магазины
- Ваш компьютер
- Ваши кредитные карты

Онлайн шоппинг: техника безопасности

Сезон праздников – повышенная опасность

Начинается сезон праздников и скоро миллионы людей во всем мире начнут выбирать подарки. Многие будут покупать онлайн, чтобы сэкономить или избежать очередей и толпы людей. К сожалению, в это же время активизируются недобросовестные сайты, которые попытаются сбыть вам контрафактную продукцию, украсть данные кредитной карты или просто не привезут приобретённый товар. В этом выпуске мы поговорим об опасностях интернет магазинов и способах защиты от мошенничества.

Об авторе

Автор нашего выпуска – Ленни Зельцер. Ленни специализируется на защите клиентов компании NCR Corp. Он также преподаёт курс «Анализ вирусов» в Институте SANS. В Twitter Ленни ведёт записи как [@lennyzeltser](https://twitter.com/lennyzeltser) и у него есть блог, посвященный компьютерной безопасности: blog.zeltser.com.

Онлайн магазины

Проще всего мошенникам создать фальшивые веб сайты, которые являются копиями сайтов известных магазинов. После размещения таких сайтов в Интернет, мошенники начинают охоту на людей, ищущих низкие цены. Покупатели чаще всего ищут товары, которые хотят приобрести, через поисковики, например, Google или Bing, добавляя к названию товара слова «дешёвый» или «самая низкая цена». В свою очередь, на такие запросы поисковая система выдаст сотни сайтов, которые продают этот товар. Некоторые из этих сайтов могут оказаться фальшивыми.

Следует опасаться сайтов, которые предлагают слишком низкие цены на товар по сравнению с остальными. Объяснением столь низкой цены может быть то, что товар контрафактный, ворованный или вам просто ничего не привезут. Признаки мошеннических сайтов:

- На сайте не указаны телефоны отдела продаж или обратной связи
- Домен сайта отличается от имени домена, который используется в адресе электронной почты или указан в контактах
- Текст сайта примитивный или встречаются ошибки

Онлайн шоппинг: техника безопасности

- Сайт является точной копией того, которым вы пользовались ранее, но слегка отличается имя домена или название магазина

Помните, даже если сайт выглядит официальным, это не значит, что он таким и является. Если что-то на сайте кажется вам подозрительным, не пожалейте времени, чтобы это проверить. Например, позвоните по телефону, указанному в разделе «Контакты», чтобы убедиться в правильности номера. Или введите название магазина или URL в поисковую систему и почитайте отзывы людей, которые им пользовались. Если сомнения все ещё остались, не пользуйтесь этим сайтом. Лучше пользоваться проверенным и известным сайтом, которым вы или ваши друзья, члены семьи уже успешно пользовались. Возможно, цены будут и не самые низкие, зато получите качественный товар и вас не обманут.



*лучший способ защиты
при онлайн покупках –
использование проверенных
сайтов с хорошей репутацией*

Ваш компьютер

Остерегаясь фальшивых сайтов, помните и о безопасности вашего компьютера, с которого совершаете покупки. Если ваш компьютер заражён вирусами, даже находясь в любой точке мира, мошенники могут контролировать ваши файлы и нажатия клавиш. Это дает возможность злоумышленниками украсть ваш логин и пароль онлайн магазинов, данные кредитных карт, информацию о банковском счёте и другие конфиденциальные данные. Прежде всего, убедитесь, что ваш компьютер не заражён и подключён к надёжной сети. Подразумевается и использование последних обновлений программ безопасности и антивируса.

Если у вас есть дети, то следует приобрести два компьютера: один для детей, второй для взрослых. Дети очень любопытны и легко осваивают новые технологии, в результате чего легко могут заразить компьютер вирусами. Пользуясь отдельным компьютером для онлайн транзакций, например, онлайн банкинга или онлайн покупок, вы минимизируете риск заражения вирусами. Если нет возможности приобрести второй компьютер, то следует хотя бы разделить пользователей на одном и не наделять детей правами администратора.

Онлайн шоппинг: техника безопасности

Ваши кредитные карты

Пользуйтесь кредитными картами с умом. Имеется в виду регулярный контроль покупок по кредитной карте для выявления подозрительных операций. Необходимо просматривать платежи по карте не реже, чем раз в месяц. Некоторые банки предоставляют услугу уведомления об операциях по карте с помощью смс или по электронной почте или ограничение по сумме расходов. Если вы считаете, что было совершено мошенничество, например, видите неоднократные попытки платежей, которые отклонил банк или странные суммы платежей, нужно немедленно связаться с банком и объяснить ситуацию. Именно поэтому для покупок в Интернет лучше использовать кредитные, а не дебетовые карты. Деньги с дебетовой карты списываются непосредственно с вашего счета, и если совершится обман, деньги будет вернуть гораздо сложнее. Наконец, некоторые провайдеры предоставляют возможность генерировать уникальный номер карты для каждой покупки или воспользуйтесь услугами платежных систем, например, PayPal, чтобы не вводить данные карты для каждой покупки. Узнайте в своём банке о дополнительных услугах для онлайн покупок.

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 <http://www.securingthehuman.org>.

Дополнительная информация

- Stay Safe Online: <http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/online-shopping>
- Правила безопасности покупок в интернете: <http://lifehacker.ru/2013/03/12/infographics-online-shopping-security/>
- Покупки в Интернете: http://www.visa.com.ru/ms/smartbuy_internet.jsp
- Как делать покупки в Интернете более безопасно: <http://www.microsoft.com/ru-ru/security/online-privacy/online-shopping.aspx>
- Термины информационной безопасности: <http://www.securingthehuman.org/resources/security-terms>
- Институт SANS: Ежедневные советы по информационной безопасности: 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 3.0 license](http://creativecommons.org/licenses/by-nc-nd/3.0/). 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: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова