Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Поддельные сайты онлайн магазинов
- Безопасность вашего компьютера/ мобильного устройства
- Безопасность ваших кредитных карт

Безопасность онлайн покупок

Повышенная опасность в сезон праздников

Приближается сезон праздников и миллионы людей по всему миру начнут покупать подарки родным и близким. Многие предпочитают делать покупки онлайн, так как это выгодно и позволяет избежать длинных очередей и нервной толпы. К сожалению, для мошенников это самое любимое время для финансовых афер. В этом выпуске мы поговорим об опасностях, подстерегающих при онлайн покупках и способах их избежать.

Об авторе

Джонатан Хомер (**@JonathanLHomer**) – известный специалист в сфере обучения Информационной безопасности. Он работает в государственном и коммерческом секторе. Джон использует прогрессивные методики обучения и вовлечения аудитории.

Поддельные онлайн магазины

Наряду с официальными онлайн магазинами существует большое количество фальшивых, созданных мошенниками. Преступники копируют сайты известных брендов или используют их названия. Затем заманивают на эти сайты людей очень выгодными предложениями. Если вы ищете товар по очень низкой цене, то есть риск попасть на такой сайт.

Когда вы выбираете сайты для покупки товара или услуги, остерегайтесь сайтов с нереально низкими ценами, которые в разы ниже подобных по стране. Низкая цена или доступность товара может быть обусловлена тем, что он поддельный, нелегальный или ворованный, есть еще риск при заказе вообще ничего не получить. Защитить себя можно с помощью следующих правил:

- Проверить легальность сайта можно через контакты: написать на электронную почту или позвонить по указанному телефону. Если сайт выглядит подозрительным, пообщайтесь с их сотрудниками.
- Обратите внимание на такие явные признаки, как грамматические ошибки или примитивная лексика.
- Проявляйте особую осторожность с сайтами, которые выглядят в точности, как известные, но название или имя домена немного отличается от привычного. Например, вы всегда пользовались сайтом Амазона https://amazon.com для онлайн покупок. Но остерегайтесь сайтов, притворяющихся Амазоном, например, с адресом http://store-amazon.com

Безопасность онлайн покупок

- Наберите название сайта или URL адрес в поисковике и почитайте отзывы о нем. Особенно стоит обратить внимание на негативные, со словами «афера», «никогда», «фальшивый». Отсутствие отзывов тоже нехороший признак того, что сайт слишком новый.

Помните, если сайт выглядит профессионально, это не значит, что так оно и есть. Если что-то вас настораживает, не спешите, внимательно его изучите. Если что-то кажется подозрительным, просто не пользуйтесь этим сайтом. Вместо этого найдите хорошо известный сайт, или тот, которым вы уже успешно пользовались. Даже если вы не получите огромную скидку или специальное предложение, то приобретете подлинный товар и ваши деньги на карте будут в сохранности.

совершайте онлайн покупки только на проверенных сайтах с хорошей репутацией.

Безопасность Вашего компьютера/ мобильного устройства

Для полной безопасности вам не только нужно пользоваться проверенными веб сайтами, но и соблюдать правила безопасности использования компьютера/мобильного устройства. Кибер преступники могут попытаться инфицировать ваше устройство для получения доступа к банковским счетам, кредитным картам и паролям. Придерживайтесь следующих правил:

- Если у вас есть дети, то настоятельно рекомендуем завести им отдельное устройство: у детей свое устройство, а у взрослых свое. Дети любознательны и активны, в результате чего вероятность заражения устройства вирусами очень высокая. Но используя разные устройства, вы обеспечите безопасность онлайн операциям, таким, как банковские переводы и покупки. Если нет возможности обеспечить детей отдельным устройством, используйте различные аккаунты и не давайте детям прав администратора.
- При проведении финансовых операций подключайтесь только к надежным WiFi сетям, например, домашней или другой проверенной сети. Использование публичных WiFi сетей, например, в кофейне, подходит для чтения новостей, но не для входа в банковский аккаунт.
- Всегда устанавливайте последние обновления и используйте обновлённую версию антивируса. Злоумышленникам будет намного сложней заразить ваше устройство.

Безопасность онлайн покупок

Безопасность Ваших кредитных карт

Регулярно просматривайте ваши расходы по кредитной карте для выявления подозрительных трат. Вы должны делать это регулярно, не реже, чем раз в месяц. Некоторые провайдеры кредитных карт предлагают услугу отправки письма по электронной почте или смс сообщения после каждой покупки или при превышении лимита карты. Как вариант, можно завести отдельную карту для онлайн покупок, в случае взлома карты вы можете её заблокировать без ущерба для других платежей. Если вы обнаружите подозрительные расходы, немедленно позвоните в банк и объясните ситуацию. Вот почему кредитные карты являются более безопасными, чем дебетовые. По дебетовой карте деньги снимаются непосредственно с вашего счета, в случае взлома карты деньги вернуть намного сложнее.

Наконец, современные технологии позволяют проводить платежи без использования номера карты. Существуют такие карты, которые генерируют уникальный номер для каждой онлайн покупки, или можно использовать специализированные платежные сервисы, например PayPal, которые позволяют не использовать номер карты при покупках.

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.

Ресурсы

Пять шагов к безопасности:	https://www.securingthehuman.org/ouch/2014#october2014
Безопасность домашней сети:	https://www.securingthehuman.org/ouch/2014#january2014
Безопасность планшета:	https://www.securingthehuman.org/ouch/2013#december2013
Ежедневные советы Института SANS:	https://www.sans.org/tip_of_the_day.php

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова