Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- **Предварительная проверка**
- **Утеря / Кража устройства**
- **Wi-Fi доступ**
- **Общественные компьютеры**

# Безопасность в путешествии

## Обзор

В этом выпуске речь пойдёт о правилах безопасного использования Интернета в путешествии.


## Об авторе

Стив Армстронг - Технический директор CyberCPR компании Logically Secure, сертифицированный инструктор Института SANS. Стив ведет блоги в Twitter **@Nebulator** и Google+: **+SteveArmstrongSecurity**.


## Предварительная проверка

Ваша сеть дома или на работе, скорее всего, безопасна, но в путешествии вам приходится соединяться с потенциально опасной сетью. Неизвестно, какие опасности она в себе таит. Есть некоторые простые меры, которые помогут защитить данные в дороге.

- Определите, какие данные с устройства вам не понадобятся и удалите их. Это значительно снизит вред, в случае утере устройства, кражи или конфискации сотрудниками таможни или службы безопасности. Если это командировка, уточните у менеджера, выдают ли в вашей компании специальные устройства для работы в поездке.
- При поездках за границу уточните, какой тип разъёмов питания используется в стране - возможно, вам понадобится адаптер для зарядки мобильных устройств.
- Не забудьте проверить свой сервисный план у мобильного оператора.
- Зачастую, международный роуминг довольно дорог, так что стоит отключить телефон на время поездки или временно изменить сервисный план.
- Установите программу, позволяющую определять местонахождение устройства, а также удалять дистанционно данные в случае утери или кражи устройства.
- В большинстве мобильных устройств данная функция есть, вам нужно только подключить её (помните, что для этого понадобится Интернет).

За пару дней до поездки:

# Безопасность в путешествии

- Обновите устройство, приложения и антивирус, убедитесь, что используете последнюю версию.
- Подключите все настройки безопасности, например, фаерволлы.
- Защитите все ваши мобильные устройства надёжными паролями или кодами. Никто не сможет воспользоваться вашей информацией в случае утери или кражи устройства.
- Шифрование тоже поможет защитить данные от несанкционированного доступа. Некоторые устройства, например, iPhone, делают это автоматически при установки пароля или кода.
- Сделайте резервные копии всех ваших устройств. В случае чего, вся информация по-прежнему будет в безопасности и доступна вам.

*самое важное в поездке – подготовиться к ней заранее, обеспечить физическую безопасность устройства, контролировать все онлайн активности и использовать шифрование.*

## Утеря/кража устройства

В поездке, в первую очередь, необходимо обеспечить физическую безопасность устройств. Никогда не оставляйте устройства в автомобиле на видном месте, преступники могут разбить окно и украсть всё ценное. Ещё один вариант – использование троса с замком для фиксации устройства, например, ноутбука, когда вы отлучаетесь. От преступления, конечно, никто не застрахован, но вероятность потерять устройство намного выше, чем вероятность его кражи.

Согласно статистике Verizon за 10-летний период, риск потерять устройство в 15 раз выше, чем риск его кражи. Поэтому следует неоднократно проверять, забрали ли вы устройство после проверки безопасности в аэропорту, выписки из гостиницы, при выходе из такси или самолета.

## Wi-Fi доступ

В поездке доступ к Интернету возможен через общественный Wi-Fi, который есть в аэропорту, гостинице или кафе. Проблема заключается в том, что неизвестно не только, кто настраивал сеть Wi-Fi, но и кто ещё ей пользуется. Учитывая это, безопасность у них сомнительная; поэтому вы и предпринимаете ряд мер безопасности, описанных ранее. Помните, что Wi-Fi – это радиоволны, которые соединяют компьютер с точкой доступа в Интернет. Это означает, что любой может перехватить эту волну и наблюдать ваши действия.

# Безопасность в путешествии

Для безопасного использования публичного Интернета следует применять шифрование. Например, при подключении браузера убедитесь, что посещаете сайты, которые используют шифрование (их URL адрес начинается с «https://» и содержит символ замочка). Еще можно использовать аккаунт в VPN (Virtual Private Network – виртуальная частная сеть) – это позволит шифровать все ваши действия в Интернете. VPN аккаунт может быть служебным или для личного пользования. Если нет соединения, которому можно доверять, воспользуйтесь возможностями смартфона для соединения. (Внимание: как мы уже говорили, это может быть очень дорого в роуминге; сначала уточните стоимость услуги у провайдера).

## Общественные ресурсы

Не пользуйтесь общественными компьютерами, например, в лобби отелей, библиотеках или интернет-кафе. Вы же не знаете, кто пользовался этим компьютером до вас, компьютеры могут быть заражены вирусами случайно или специально. По возможности, используйте только свое устройство для соединения с Интернетом. Если возникнет необходимость воспользоваться публичным компьютером, то постарайтесь не пользоваться сервисами, требующими вводить логин и пароль.

## 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

| | |
|---|---|
| Менеджер паролей: | http://www.securingthehuman.org/ouch/2013#may2013 |
| Двухступенчатая Верификация: | http://www.securingthehuman.org/ouch/2013#august2013 |
| Шифрование: | http://www.securingthehuman.org/ouch/2014#august2014 |
| Как защитить новый планшет: | http://www.securingthehuman.org/ouch/2013#december2013 |
| Verizon 2014 Data Breach Investigations Report (DBIR): | http://www.verizonenterprise.com/DBIR/2014/ |



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



 