Ежемесячник по информационной безопасности для всех

OUCH!

В ЭТОМ ВЫПУСКЕ…

- **Подготовка**
- **Потерянные / украденные устройства**
- **Подключение к сети Wi-Fi**
- **Компьютеры общего доступа**

Безопасность в пути

Обзор

Мы хотим максимально использовать современные технологии, даже во время путешествий. В этом выпуске мы расскажем, как вы можете безопасно подключаться к интернету и использовать свои мобильные устройства в пути.

Об авторе

Марк Уильямс – ведущий архитектор корпоративных систем информационной безопасности компании BlueCross BlueShield штата Теннесси (США). Он также является инструктором Института SANS и президентом отделения Ассоциации Безопасности Информационных Систем (ISSA) города Чаттануга. Марк много путешествует, и он прекрасно знаком с проблемами, которые могут появиться, когда вы берете любимые технические игрушки с собой в путь.

Подготовка

Ваша сеть дома или на работе может быть хорошо защищена, но, когда вы путешествуете, вы должны считать небезопасной любую сеть, к которой вы подключаетесь. Вы никогда не знаете, кто ещё подключен к этой сети и что они там делают. Несколько простых советов, которые помогут вам надёжно обезопасить себя и свои данные перед поездкой.

- Самая безопасная информация – та, которой у вас нет. Подумайте, какая информация вам не понадобится в пути и удалите эту информацию со всех устройств, которые возьмете с собой. Это значительно сократит ущерб в случае потери или кражи вашего устройства или его конфискации таможенными или пограничными службами. Если вы едете в деловую поездку, узнайте у своего руководителя, предоставляет ли ваша организация устройства, специально предназначенные для работы в пути.
- Защитите ваши мобильные устройства и/или лэптоп сильным паролем или кодом. В этом случае, если устройство украдено или утеряно, посторонние не смогут получить доступ к данным на нём. Дополнительно к этому, включите или установите программу/функцию шифрования дисков ваших мобильных устройств и лэптопов. В большинстве мобильных устройств эта функция включается автоматически, когда вы используете блокировку экрана.
- Установите на вашем устройстве приложение или включите функцию, позволяющую вам удаленно отслеживать местонахождение устройства и даже удаленно стирать информацию с него в случае кражи или потери.
- Обновите операционную систему, приложения и антивирусные программы на ваших устройствах перед поездкой - чтобы они использовали новейшие версии. Многие атаки направлены на системы с устаревшими программами.

Безопасность в пути

- Сделайте резервные копии всех ваших устройств. В этом случае, если с ними что-то случится в пути, у вас останется ваша информация, сохранённая в безопасном месте.
- Перед зарубежной поездкой, проверьте у своего мобильного оператора, какой план услуг доступен для вашего телефона. Зачастую мобильные операторы имеют очень высокие тарифы на международный интернет роуминг. Вы можете либо отключить функции мобильного интернета, либо купить местную SIM карту на время путешествия.

Для безопасного путешествия: защитите ваши устройства перед тем, как покинуть дом; обеспечьте их физическую безопасность и шифруйте все интернет коммуникации.

Потерянные / украденные устройства

Отправившись в путь, позаботьтесь о физической безопасности ваших устройств. Например, никогда не оставляйте ваши устройства в машине, на виду у посторонних: преступники могут просто разбить стекло вашей машины и схватить все ценные предметы, попавшиеся им на глаза. Хотя риск преступлений существует, согласно результатам исследований, проведённых недавно компанией Verizon, вероятность потерять мобильное устройство в 100 раз выше вероятности его кражи. Всегда внимательно проверяйте, чтобы ваше мобильное устройство было при вас сразу после прохождения осмотра службой безопасности аэропорта, при выходе из такси или ресторана, сдачи гостиничного номера или перед выходом из самолета. Всегда проверяйте кармашки самолетного кресла!

Подключение к сети Wi-Fi

Для доступа к интернету в поездке часто используются общественные точки доступа к сетям Wi-Fi, такие как те, что предоставляются в гостинице, кофейне или аэропорту. Две проблемы общественных сетей Wi-Fi: вы никогда не можете быть уверенны, кто установил их, и вы никогда не знаете, кто подключен к ним. Поэтому, они должны рассматриваться, как небезопасные сети. Именно поэтому вы предприняли перед поездкой все эти шаги по обеспечению безопасности ваших устройств. Кроме того, Wi-Fi использует радиоволны; это означает, что любой, находящийся вблизи от вас, может перехватывать ваши коммуникации. Поэтому, если вы используете общественные сети Wi-Fi, позаботьтесь о шифровании всех ваших интернет коммуникаций. Например, при использовании браузера, убедитесь, что интернет сайты, которые вы посещаете, используют шифрование. Вы можете проверить это, поискав приставку «HTTPS://» и/или значок закрытого замочка в поле адреса браузера.

Безопасность в пути

Дополнительно, вы можете использовать VPN (Virtual Private Network), которая будет шифровать все ваши интернет коммуникации. Функционал VPN может быть предоставлен вашей организацией; вы также можете подписаться на эту услугу самостоятельно. Если вы не нашли внушающей доверие сети Wi-Fi, вы можете использовать мобильный интернет, предоставленный вашим смартфоном (функция Tethering).

Предупреждение: как упоминалось ранее, это может быть очень дорогая услуга при поездках за границу – ознакомьтесь с тарифами вашего мобильного оператора.

Компьютеры общего доступа

Не используйте для доступа к учетным записям или конфиденциальной информации компьютеры общего доступа, такие как установлены в лобби отелей или в интернет кафе.

Вы не знаете, кто пользовался этим компьютером до вас; они могли случайно или умышленно заразить этот компьютер. Когда возможно, пользуйтесь только устройствами, которым вы можете доверять. Компьютеры общего доступа пригодны для доступа к общедоступной информации, такой как прогноз погоды или выпуски новостей. Использование любой учетной записи, такой как Google, может оказаться приглашением для хакеров.

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

Парольные фразы:	https://securingthehuman.sans.org/ouch/2015#april2015
Резервное копирование и восстановление данных:	https://securingthehuman.sans.org/ouch/2015#august2015
Что такое вредоносные программы:	https://securingthehuman.sans.org/ouch/2016#march2016
Шифрование:	https://securingthehuman.sans.org/ouch/2016#june2016
Архивы OUCH:	https://securingthehuman.sans.org/ouch/archives

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

