



ИБ-памятка для отпускника

Одна из крупнейших компаний в области кибербезопасности недавно провела исследование поведения людей в путешествиях с точки зрения информационной безопасности. Было опрошено почти 12 тысяч путешественников из 23 стран (включая Россию), которые путешествовали хотя бы раз за последний год.

Основные итоги опроса:

- Путешествуя люди чаще становятся жертвами кражи данных, нежели кражи денег;
- Половина путешествующих подключались к первой же попавшейся беспроводной точке выхода в интернет (как правило, в аэропортах и гостиницах), не обращая внимания на её безопасность;
- Трое из пяти подключались в путешествии хотя бы раз к публичным беспроводным сетям, при этом треть подключались, используя рабочие устройства (среди руководителей таких была половина);
- Почти половина путешественников, будучи за границей, совершали покупки или банковские операции, подключаясь с помощью личных устройств к публичным беспроводным сетям, а треть передавала по ним конфиденциальные рабочие документы с помощью рабочих устройств;
- Как правило, путешественники полагают, что рабочие устройства более безопасны нежели личные из-за встроенных средств обеспечения безопасности.

Общий вывод исследования: желая быть «на связи» любой ценой, большинство путешественников не принимают во внимание необходимость выполнения даже простых правил обеспечения безопасности, чем регулярно ставят под угрозу как личные, так и рабочие конфиденциальные данные. Желание «запостить» новое оригинальное фото, написать твит или пост во «ВКонтакте», обычно, берёт верх над рассудительностью и оценкой рисков.

Половина опрошенных признались, что, собираясь в отпуск, вообще забыли о том, что их устройства содержат конфиденциальные данные, так как сегодня мобильные телефоны и планшеты настолько многофункциональны, что используются буквально «для всего». При этом 18% сообщили, что хотя бы раз становились жертвой киберпреступников. Из них 9% пострадали, когда совершали онлайн-покупки, а 6% - при осуществлении банковских онлайн-операций. Устройства 7% были заражены вредоносным ПО.

Сегодня мы хотели бы дать простые советы, следование которым существенно снизит для вас вероятность стать жертвой злоумышленников в путешествии:

1. Выключайте wi-fi-модуль, если не пользуетесь им – тем самым вы и снизите риск кражи данных, и сэкономите заряд батареи устройства.
2. С подозрением относитесь к незапароленным беспроводным сетям – такие сети часто используются злоумышленниками для сбора данных.
3. Не пользуйтесь онлайн-банком и другими критически важными сервисами если не уверены в безопасности подключения. Если использование онлайн-банка действительно необходимо, менее рискованно использовать мобильный интернет.
4. Там, где возможно, используйте подключение по защищённому протоколу HTTPS. Например, его можно использовать для поиска в Google, Wikipedia и для Facebook. Для использования этого протокола в социальной сети «ВКонтакте» необходимо в настройках проставить галочку «Всегда использовать безопасное соединение».
5. Для интернет-сёрфинга с помощью браузеров Chrome, FireFox и Opera установите специальное расширение браузера HTTPS Everywhere (<https://www.eff.org/HTTPS-EVERYWHERE>), обеспечивающее более безопасную передачу данных.
6. Если возможно, используйте VPN-соединения. Это обычно платная услуга, но она обеспечивает эффективную защиту от перехвата трафика и взлома устройств.
7. Включите функцию шифрования данных вашего устройства.
8. Ну и, конечно, установите современное антивирусное и антивредоносное ПО и не забывайте обновлять его вирусную базу.

Безопасных вам путешествий!