

УДК 338.48:519.86

Богуславська А.М.¹

Домашенко Д.Г.²

¹канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»

²студ. гр. 6.1269 ЗНУ

КІБЕР-РИЗИКИ У СФЕРІ ТУРИСТИЧНИХ ПОДОРОЖЕЙ

У сучасному світі стрімкий технічний прогрес призводить до більшої частоти кібератак. Сьогодні великі технологічні цикли – електронна комерція, мобільні платежі, хмарні обчислення, великі дані, IoT, AI та соціальні медіа – все збільшує кібер-ризик для користувачів та бізнесу.

Кібербезпеку важко застрахувати саме тому, що існує багато різновидів кіберзлочинності, мотивація цих злочинів різна, цільові активи та засоби захисту також відрізняються. Більшість видів злочинної діяльності мають єдину ціль (наприклад, крадіжку грошей) та єдиний мотив (наприклад, розбагатіти). Кіберзлочинність має безліч мотивів, може мати різну форму і може здійснюватись різними типами зловмисників.

Більшість експертів з кібербезпеки сходяться на думці, що близько 20 відсотків туристів піддаються кіберзлочинам, перебуваючи за кордоном. Усі вони сходяться на думці, що подорожі ставлять туристів та їх організації під додатковий ризик інформаційної безпеки. Цей ризик виходить далеко за межі витрат на заміну експлуатованого обладнання. Злочинці можуть отримати доступ до персональних та конфіденційних даних через загальнодоступний Wi-Fi та встановити шпигунські програми. Хоча масштаби ризику, пов'язаного з подорожами, різняться залежно від країни, ризик, пов'язаний з даними, перевищує національні кордони. Тим не менше, туристи, які в'їжджають до країн, що мають досвід кібер-бандитизму, стають легкими мішенями для "spoofing" атак. За допомогою відповідного програмного забезпечення кіберзлочинці можуть приховано активувати камеру, контролювати електронні листи, читати збережені файли та викрадати ідентифікатори користувачів.

Під час ділових подорожей туристи часто стають важливими цілями, особливо ті, що працюють у корпораціях, ЗМІ, наукових та державних органах. Якщо відвідувана країна переживає громадянські заворушення або має високий рівень злочинності, турист стає головною мішенню для кібератак, кіберзлочинів, моніторингу та нагляду.

Спосіб доступу туристів до Інтернету також може зробити їх більш вразливими. Підроблені місця Wi-Fi у готелях, аеропортах, кафе та ресторанах можуть читати та зберігати такі важливі дані, як паролі. Не можна довіряти навіть діловим центрам готелів та кабельному доступу до Інтернету в готельних номерах, особливо за кордоном. Ноутбуки, смартфони та планшети також сприйнятливі до віддалених з'єднань Bluetooth. Зарядка та зберігання пристроїв також пов'язані з цим ризиками. Залишення ноутбука в порожньому готельному номері може зробити туриста відкритим для експлуатації в країнах, які практикують кіберзлочинність, що фінансується державою, тоді як станції USB в аеропортах можуть завантажувати збережені дані.

Лише у 2016 році щомісяця відбувалося 1000 кібератак на авіаційні системи, повідомляє Європейське агентство з авіаційної безпеки. У 2017 році авіакомпанія «Латам» та український аеропорт «Бориспіль» постраждали від програм-вимагачів. У січні 2018 року аеропорт Мюнхена відкрив центр інформаційної безпеки, який об'єднав ІТ-спеціалістів власника аеропорту та

європейських авіаційних експертів для розробки стратегій та підходів до захисту від кібератак. У сучасному бізнесі кібер-ризик зростає в геометричній прогресії, оскільки життя стає більш взаємопов'язаним.

Як туристи можуть зменшити кібер-ризик?

1. Вимкніть або заблокуйте телефон або планшет в аеропорту.
2. Уникайте доступу до конфіденційних даних та мереж під час подорожей.
3. Обмежте віддалений доступ до свого пристрою, вимкніть Bluetooth та Wi-Fi.
4. Створіть точку доступу Wi-Fi через свій смартфон і використовуйте віртуальну приватну мережу для шифрування даних, навіть якщо це робить ваше з'єднання повільнішим.
5. Візьміть із собою якомога менше пристроїв, коли ви подорожуєте, і ніколи не залишайте їх поза увагою.
6. Заряджайте пристрої, під'єднавши шнур живлення, що постачається, до звичайної електричної розетки або використовуючи власний мобільний зарядний пристрій, що працює від акумулятора.
7. Якщо вам потрібно зарядитись через USB на станції, вимкніть пристрій перед підключенням до мережі.
8. Не використовуйте будь-який пристрій, запропонований вам третьою стороною, і ніколи не дозволяйте іншим користуватися вашими пристроями.
9. Не завантажуйте будь-яке програмне забезпечення на свої пристрої під час вашого візиту, і попросіть IT-команду перевірити ваші пристрої після поїздки.