Issued 7/31/17

Employees Working While on Holiday Open Organizations to Security Risks

Many workers will feel the need to check-up on work emails while they are away from the office and enjoying a well-earned vacation. Unfortunately, by doing that, they can open organizations to many security risks. T-Systems, the corporate IT and cyber-security arm of Deutsche Telekom, has asked 2,050 full-time workers UK about their cyber security practices while on holiday, and found that:

• Nearly a third of employees (31%) use free Wi-Fi hotspots, and nearly a quarter (24%) use them for work-related emails and documents. These are a big danger area as they are insecure and easy for hackers to clone (getting access to all email and web traffic, including any work documents and passwords)

• 28% of employees email work documents to and from their personal email, despite this creating numerous security problems

• 10% use free USB charging points at airports and stations. These ports can be used to transfer viruses and malware to unsuspecting users.

The blame, however, cannot solely be placed on the employees, as 28% of employees have never in their working career had any cyber security training to protect themselves and their employer, and 66% of respondents

had received no up-to-date education within the past twelve months. “Our message to businesses for the holiday season is ‘let your employees enjoy an uninterrupted break’. Strongly discourage them from taking work on holiday, and make sure employees do not feel pressured to work when they should be taking time out,” says Scott Cairns, the UK head of cyber security at T-Systems. “Where it is unavoidable, businesses should ensure there is training, and clear guidelines to be followed.

This training is particularly important, as our research shows many employees are not knowledgeable on the multitude of ways their devices can be infected with viruses and malware... and those who thought they were ‘very knowledgeable’ frequently gave the wrong answer when questioned!” “We’ve already begun to see the financial impact these malware attacks have had on multinationals in 2017, including Reckitt Benckiser and Mondelez (the maker of Cadbury chocolate). Reckitt disclosed to the Financial Times this month that it expected sales would be hit by an estimated £110m this year as a direct result,” he noted. “Training your employees regularly on effective cyber security practice is probably the single-most effective step organizations can undertake to dramatically reduce their risks of viruses, malware and other common forms of cybercrime.” Cyber security training for all employees is particularly important as the dangers continue when employees come home from holiday. T- Systems’ research found that:

•18% of employees admit to connecting their digital camera to their work computer to download photos.

•15% admit to connecting USB sticks and memory cards that they share with their family members to their work computer. This is a sure way for viruses to quickly spread from home to business.