8 August 2017

TEISS Cracking cyber security

Visitors at the ongoing Edinburgh Festival Fringe are especially vulnerable to cyber criminals who are looking to obtain money and data from visitors.

Shared Wi-Fi hotspots and limited IT security at the Edinburgh Festival Fringe are leaving visitors vulnerable to cyber criminals.

According to Paul Motion, a partner at BTO Solicitors and a data-protection specialist, the ongoing Edinburgh Festival Fringe as well as other festivals offer 'cyber crooks an abundance of opportunities to obtain data and money from both vendors and customers'.

"Due to the nature of the festival, vendors are usually set up in temporary bars, stalls, box offices and venues with limited IT security, which can compromise the safety of transactions," he says.

Vendors at the festival are also making active use of public Wi-Fi hotspots to perform transactions and running apps for visitors. Security vulnerabilities in public Wi-Fi hotspots, as demonstrated countless times by researchers, can be easily exploited by hackers to obtain device information and financial details and to steal identities.

Last year, the Edinburgh Festival Fringe ran for 25 days, featured 50,266 performances and saw over 2.5 million ticket sales. The number of visitors attending the annual festival reached 2 million in 2013 and has been growing ever since. With millions of people thronging the venues, the opportunities for cyber criminals are massive.

At the festival, Paul Motion and his law firm will address a session on 'Cyber Risk and the Entertainment Industry', describing how visitors at the festival are exposed to cyber crimes and financial fraud.

'The ramifications can be twofold for vendors – not only do they face financial loss themselves, but reputational damage if customers are targeted. The convenience of free but unsecured Wi-Fi is another factor, with many people accessing personal, financial and sensitive information which can be easily intercepted by experienced hackers,' he says.