Why security savvy Generation Z are a suspicious lot

Generation Z has never known a world without the internet or mobile devices and for this reason it appears they are much more street smart than their millennial colleagues when it comes to cybersecurity.

A study commissioned by specialist IT distributor DataSolutions and carried out by Censuswide in May 2019 found Gen Z to be the most suspicious generation when it comes to hackers targeting devices used on a daily basis. In fact, Gen Z office workers topped every category as the most concerned group in relation to the hacking of internet connected devices including game consoles, wearables, smart security cameras and smart TVs.

For example, 25pc of Gen Z office workers are worried about their wearables (such as smart watches) being hacked, compared to 15pc of millennials, 19pc of Gen Xs and 15pc of baby boomers.

The study found that 19pc of all Irish office workers have sent sensitive work-related information to the wrong email recipient. Furthermore, 14pc of Irish office workers have copied sensitive company data from previous or current employers for their own use.

The findings also reveal that 28pc of Gen Z employees admitted to having access to company information or private logins from a previous.

Datasolutions will host the seventh annual Secure Computing Forum at the RDS, Dublin, on Thursday, 12 September 2019.

David Keating, group security director at DataSolutions, explained why Gen Z could be the most suspicious generation yet.

Do younger workers pose a security risk when Gen Z actually are savvier when it comes to technology? What is the precise risk they pose?

While Gen Z are more aware of types of attacks they can be hit with – and our survey showed that

they are the most suspicious generation in terms of hackers – they also can't live without their devices. When it boils down to it, the younger generations are more likely to overlook security issues if they are going to impinge on their use of technology. This means that they are more likely to continue using devices, such as their work phone or laptop, even if they suspect they have been infected with a virus.

For example, when the WhatsApp breach was announced earlier this year, who actually updated or deleted the app? I would say it was fewer than you might expect. The messaging platform was seen as too valuable, from both a personal and business perspective, so people felt it was worth the risk to keep it on their phones.

Our research also found that 42pc of Gen Z office workers had lost a device that was linked to their business email account and that can create all kinds of security issues. If that device fell into the wrong hands, a person could potentially have access to all kinds of confidential information and company data.

It is generally the case that younger people hold more junior roles in the workplace, which means they maybe aren't as invested in the company as a business owner or manager would be. That's not to say they don't care – of course they do – but they might just feel that work-related security issues don't directly impact them. We actually did an experiment a few years ago where we approached young workers during their morning commute and offered chocolate bars for passwords, and we got loads!

Should employers be concerned that Gen Z aren't vigilant enough when it comes to protecting the company network and data assets, is it because they care more about their own personal data?

Managers need to be cognisant of the fact that Gen Z have a different relationship with technology, having grown up with the internet and social media. I don't think it's a case that they are more protective of their own personal data; I think they simply have a higher threshold for what they share and therefore discretion when it comes to company data isn't necessarily a priority. I think that perhaps they are also too reliant on technology in terms of having in-built protection.

Of course, owners and managers need to be concerned. Ultimately, everyone in an organisation is a link in the protection of the business and the company is a link in a larger supply chain. The last thing anyone wants is to be the link that gets compromised or hacked. Not only is it a threat to the organisation itself, but it also puts customers at risk. It's easily done as well: all it takes is one person responding to an email, which then gives access to the network and allows a customer's infrastructure to be infected. It doesn't matter whether your company has 10 people or 50,000; if you're the weakest link between you and your customers, you're in trouble. It's vital for everyone, not just Gen Z, to be vigilant.

What's your overall feeling about the threat landscape as it exists today when it comes to small and medium-sized businesses?

An awful lot of small- and medium-sized business are under-protected. I would estimate that the majority are four or five years behind where they should be. Many of them bury their heads in the sand and think that because they are small, they will fade into obscurity within the threat landscape. While this can work for a time, cybercriminals are utilising automation as much as everyone else. They have been developing artificial intelligence (AI) that delivers custom attacks. These systems don't care who you are or how small you are: if you can be used as a gateway to a major customer or client, you're a target.

For example, small solicitors have good connections with reputable clients which makes them a target. Hackers look for ways to target and access larger customers through smaller businesses. Owners of small- and medium-sized businesses need to think about everyone they have contact with and that's why they need greater protection. Training and education about cyber risks and threat detection is something that tends to be lacking but it is an effective first step. Just being able to identify simple warning signs, such as unusual phrasing within an email or a strange email address, could help to protect your organisation. These are human checks, but there are also tools that can analyse emails and attachments, and filter out suspicious ones.

What kind of threat do automation and IoT pose when it comes to protecting the businesses of tomorrow?

Cybercriminals are using automation in the same way as everyone else – to make processes faster and outcomes more effective. They are most definitely ahead of the curve and it also means that attacks are much more targeted. These systems automatically select vulnerable companies, or companies that have access to bigger organisations. Any and every business is at risk.

In terms of IoT devices, these are somewhat lacking in security and are often manipulated by cybercriminals to launch attacks. The most surprising thing is that there are solutions out there, that organisations aren't using, which enable IoT devices to be built into company security structures and managed by firewalls that protect them. There's no excuse not to be implementing such safeguards.

Written by John Kennedy

Published: 10 July 2019