Remote workers vulnerable to cyber crime attacks

Almost a third of Ireland’s office workers feel vulnerable to cybersecurity risks when working from home, new research from DataSolutions reveals.

One in 10 Irish office workers say they have been targeted by cybercriminals since they began working from home when the pandemic began.

That’s according to a study by Censuswide on behalf of IT firm DataSolutions which revealed almost a third of workers feel vulnerable to cybercrime attacks and aren’t adequately protected.

57pc said their company didn’t provide additional security training to prepare them for working from home, as 56pc said they were using their own personal devices to work from home. Furthermore, a fifth said they have shared or stored work documents on personal devices - which obviously has a multitude of issues, including GDPR compliance and cybersecurity.

Cybersecurity needs to be part of plans for future

“At the moment, the only decision that businesses can make with any confidence is that homeworking will be a part of their strategy for the foreseeable future,” said David Keating, Group Security Sales director at DataSolutions.

“Therefore, they need to have the right infrastructure and technologies in place to enable employees to work from home effectively and, more importantly, securely.

“This is going to be a long-term need and while Irish organisations have certainly managed their response well so far, more work is needed to support and safeguard the new normal. Not only are systems and data at risk, but there are also potentially huge implications in terms of cost and reputation for companies who become exposed to cyberattacks – which are much greater at the moment as hackers are well aware that people are working by themselves, potentially using unprotected devices and possibly not as alert as they would be in the office.

“As well as security, the current situation is also putting GDPR compliance at risk with workers

using more personal devices. It is extremely worrying that just half of organisations changed their security strategy in light of what has happened and considering that entire workforces are accessing systems across locations, potentially on unprotected devices and networks. Furthermore, even those that did adapt early would now need to review, evolve and ensure that their approach remains fit for emerging more sophisticated and targeted home worker attacks."

Pandemic panic

The research reveals glaring holes in Irish businesses' preparedness in the wake of Covid-19.

Just 39pc of those new to homeworking received additional cybersecurity training.

31pc of office workers said they noticed an increase in cybersecurity threats when home working.

"With the widespread shift to remote working as a result of the pandemic, security should really be the top priority for Irish businesses," said Hugh McGauran, country manager for Ireland at Check Point Software.

"However, this research shows that this hasn't necessarily been the case – not only are workers lacking the additional safeguards that their employers should be putting in place, they haven't received the training required to sufficiently protect themselves and the devices they are using when working from home.

"Furthermore, this will be putting the organisations themselves at heightened risk and the truth is the makeshift solutions that were put in place quickly at the beginning of the pandemic are simply insufficient. Cyber criminals have evolved very sophisticated new techniques to attack vulnerable home workers and gain access to company systems. Therefore, organisations also need to evolve by updating their strategies and technologies," McGauran said.

By John Kennedy *(john.kennedy3@boi.com)*

Published: 10 December 2020