Are you a 'cyberloafer?' Why internet procrastination is making life easier for hackers

December 22 2017, by Lee Hadlington

Credit: AI-generated image (disclaimer)

The biggest threat to an organisation's cyber-security comes from within, according to a growing body of evidence. Employees are frequently putting their companies at risk of hacking by sharing their passwords, using public WiFi networks to send sensitive information, or

not protecting the privacy of social media accounts.

But there's another threat that at first seems innocuous and that we're all probably guilty of, something that researchers have dubbed "cyberloafing". My research group's new study shows this practice of using work computers for personal internet browsing can become a serious security threat to a company when it goes too far.

Most companies accept that their employees will occasionally check social media or send personal emails from work computers. But in some cases things can get more serious, with people people spending significant amounts of time updating their own websites, watching videos or even pornography. Early estimates suggested that 45% of employees questioned cited surfing the internet at work for personal purposes as the number one distraction at work.

This can have a big impact on a company's productivity, with research suggesting that employees each waste an average of 2.09 hours a day while cyberloafing. But our new study also shows that the more employees engage in serious cyberloafing, the less likely they are to follow the rules and protocols designed to protect the company's IT systems, and the bigger threat they become to cyber-security.

We asked 338 part-time and full-time workers aged 26-65 about their cyberloafing habits, their knowledge of information security, and behaviour that could indicate internet addiction. Those who cyberloafed more often knew less about information security. And those who engaged in more serious cyberloafing (such as updating personal websites, visiting dating websites or downloading illegal files) had significantly poorer cyber-security awareness.

Typically, people undertaking more serious cyberloafing were less aware of how to stay safe online and how to protect sensitive information. One

reason for this could be that they are so determined to get online they don't want to pay attention to information about online safety and ignore the risks. On they other hand, they may believe their companies can protect themselves from anything that might happen as a result of risky behaviour.

Those in our survey who scored higher for internet addiction behaviour were also much more likely to have poorer awareness of and follow safety protocols. And those who were serious cyberloafers and potential internet addicts were the greatest risk of all.

As I explain in my recent book Cybercognition, internet addiction is a compulsion to get online, sometimes with the aim of fuelling other addictions to digital activities such as online gambling or shopping. Critically, the drive to get online can be the same as any physical addiction, so the internet acts like a drug for some people.

This means people who show aspects of internet addiction may be more determined to get online at any costs and more likely to try to get around security protocols or ignore advice about online safety. They may think they know better because they spend so much time online. Or they may not fully understand the risks because they are so absorbed in the online world.

How to tackle cyberloafing

All of this doesn't mean we should cut off all internet access for employees. Being able to surf the internet is an important part of some people's work. But excessive use of internet services and work IT systems can put companies at risk, particularly when people are accessing risky websites or downloading programmes from unknown sources.

There are a number of things companies can do to help mitigate the risks from excessive cyberloafing. As we suggest in our study's conclusion, some organisations may apply very strict penalties for serious rule breaking. But providing effective training that empowers employees to identify aspects of internet abuse and seek help could be a more effective management tool. Helping workers understand the risks of their actions might be more beneficial, particularly where these are communicated through focus groups and talks.

But one thing companies should avoid (and all too often don't) is simply sending out an email reminder. Research shows that messages about the potential risks to information security sent via email are the least effective. And if you're deep into a cyberloafing session, an email will be just another corporate message lost in an overloaded inbox.

More information: Lee Hadlington et al. Can Cyberloafing and Internet Addiction Affect Organizational Information Security?, *Cyberpsychology, Behavior, and Social Networking* (2017). DOI: 10.1089/cyber.2017.0239

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation