Doll Martin Associates
Management Consultants

How To Stay Cyber Secure While Working From Home

10 tips for your employees

How To Stay Cyber Secure While Working From Home: 10 tips for your employees Working from home may very well be here to stay. While COVID-19 has been extremely difficult for all of us, there are some beneficial outcomes that may change the way that we live, travel, think, and work. With ongoing work from home arrangements, remote employee cyber security awareness is essential for organisations.

Over the course of COVID-19, the Australian Bureau of Statistics reported that 46% of Australians switched to working from home, with 89% of those who were not working from home indicating that their job was incompatible with that type of arrangement.

For many organisations, this period has been an indication that much of their workforce can be comfortable and productive working outside of the office. What this means for the future is a far more flexible approach to remote work - however with increased remote work comes a new set of cyber security concerns. Introduce these 10 tips to your employees for enhanced cyber awareness.

1. Use strong passwords (and never repeat them) Password security is still as important as ever. Password crackers that use brute force can be used gain access to accounts, which reinforces the importance of creating passwords that are obscure, long, and contain different combinations of upper and lower case letters, numbers, and special characters. Organisations may use Single Sign-On, available via services like Azure Active Directory, for users to log into all enterprise applications using the one password.

To show the importance of not reusing passwords, point your employees in the direction of Have I Been Pwned. With this website, people are able to enter their email addresses and see how many data leaks they have been involved in. You'd be surprised at how many times personal data like names and address, and even cleartext passwords have been leaked. If passwords are reused, then hackers can use this information on other websites to gain access to other information and services - or even use information as blackmail.

2. Do not use public Wi-Fi Working from home won't always be just working from home. Once travel restrictions are lifted, this will include working while on the road, at the coffee shop, at a friend's house, or in the airport. With each location comes a different type of network access. While most establishments offer a secure Wi-Fi link, others use a public Wi-Fi access point. You should stress to your employees that these access points are not secure and can be subject to Man in the Middle attacks.

Instead, if there are no secure networks available, encourage your employees to use mobile or 4G networks, available by hotspotting their phone. An enterprise VPN should be used at all times.

3. Beware of email links and attachments While you may have sophisticated email scanning tools and technologies in place, such as Mailguard, to catch out scam emails, these cannot uncover every single attack attempt. Email scammers operate either in a targeted or untargeted way to try and elicit a response from recipients - generally downloading malware, logging into a fake website to steal credentials, or having them to wire funds to the scammer. While the 'Nigerian prince' scam is well-known, an email that looks like it's from a known supplier may be far more convincing.

Educating your team about the types of email scams, so they know what to be on the lookout for, is essential. Remind the team:

To carefully check the sender's email address matches the known email domain

Not to open attachments from unknown senders

Not to click on links in emails from unknown senders

To be wary of links even from known senders - if there is a known website visit that instead

You can take a look at Scamwatch.gov.au for up to date info on common scams in Australia.

4. Similarly, beware of other social engineering techniques Just as scammers operate via email, they can operate via other communication avenues, too. This includes phone calls, contacts on social media, random encounters in day to day life, or people at the door. The more business-critical your employees' role, or the more important data/funds they have access to, the more appealing they are as a target.

Social engineering could be as simple as a call 'from Telstra to reset your internet' or as convoluted as becoming friends with an employee to steal passwords by watching over their shoulder at home.

5. Switch on Multi-Factor Authentication (MFA) One of the best ways to prevent passwords from being stolen (like in the above case) is by switching on Multi-Factor Authentication (MFA) as default for your employees. This way, when an employee logs on by using a password, they will need to verify the login attempt by another means. With MFA, this generally involves keying in a code sent via SMS, or an app like Google Authenticator.

You can encourage employees to switch on MFA for all their important personal apps also, such as banking and email.

6. Do not download unauthorised software on devices used for work Software and apps are both easy to download, but can wreak havoc on systems if they contain spyware or malware. It is impossible to police what your employees download on their own computers - that is their property to do with as they please, after all - which makes it a better idea to have company-owned equipment with a strict no download policy, other than company-authorised software.

The other option is to deploy a solution such as Amazon Workspaces. This creates virtual desktops on employees' own devices, however, your

organisational data never is stored on the machine, creating a walled garden type effect.

7. Keep software updated Many of the continuous updates that we see rolled out to software across the course of the week are actually security patches. Software security patches (in the form of updates) are small changes to software that ensure that vulnerabilities recently discovered are closed up - so attackers can't use them to their advantage.

Setting up an environment that rolls out automatic updates of all your employees' workplace software is critical to ensuring ongoing cyber security. You should encourage employees to update their own software whenever prompted, including system updates (e.g. Windows, Android, iOS).

8. Keep devices in a secure place when not in use If an attacker were to gain access to an employee's computer, would they be able to gain access to company data, too, somehow? If this is the case, then it's important that you provide a secure place for employees to keep their devices when not in use. This can be in the form of in-home safes, lockable bags, and other physical safety measures.

With solutions like Amazon Workspaces, where no organisational data is stored on the device, the security of the device itself when not in use is not an issue for business.

9. Secure your home properly Similarly, a safe home means that the contents within are more secure. Locks, alarms, and other measures are recommended. The same building safety that you practice at work should be encouraged among your employees at home, perhaps boosted by a security stipend.

10. Keep up to date with organisational cyber security training As an organisation offering work from home flexibility, the most important cyber security tip for you is to keep up to date with employee training. The more training that your team have in cyber security, staying up to date with the latest security practices, and reinforcing known lessons, the more cyber aware they will be overall.

It is up to you to have regular training packages available to your team that are comprehensive and up to date. This can be combined with email blasts and reference materials.

Building a security culture Building a security culture is not a simple tick and flick activity, it is a comprehensive series of practices that all employees need to engage in. Cyber security awareness is something that each employee needs to be trained in, with ongoing learning in the field across the course of their tenure.

Working from home, whether it's full time or ad hoc, can be a successful practice that leads to greater levels of enjoyment and productivity among employees. However, organisational security is of the greatest importance - which means heightened levels of cyber security are necessary. Putting controls in place on the organisational IT side of things will be the most effective block to security vulnerabilities, but employees still need to do their bit, too.

Find out about our Cyber Security Consulting and Advisory Services

Contacts

Stevie

mailto: Stevie@evolocity.com.au