CYBER-SECURITY ESSENTIALS

Remote Work Best Practices

Working remotely offers flexibility, but it also expands the ways cyber-threats can reach you. Outside the office, the usual safety nets, namely IT oversight, threat detection tools and physical security, may not be readily available. This, in turn, can permit cyber-criminals to exploit potential vulnerabilities and launch damaging attacks.

A weak Wi-Fi password, a convincing phishing email or an unlocked laptop left unattended can all open the door to serious risks, both for you and your employer. Fortunately, many of these risks can be managed with smart habits. This article provides more information on common remote work threats and related mitigation strategies.

Common Remote Work Threats

Cyber-criminals have been targeting businesses for decades, continually seeking new ways to compromise confidential systems and data. Depending on a company's size, it may receive dozens or thousands of attack attempts each day. These attempts are typically blocked by IT teams and workplace security tools. However, when employees work remotely, these safeguards aren't guaranteed.

Here are some of the most common cyber-threats facing remote workers:

- **Phishing scams**—This attack method utilises deceptive electronic communications to manipulate recipients into sharing sensitive information, clicking on dangerous links or opening harmful attachments. While emails are the most prevalent delivery method for phishing scams, cyber-criminals may also use text messages, social media interactions, fake or misleading websites, or even phone calls.
- **Malware**—Malicious software, also called malware, is software designed to damage, disrupt or gain unauthorised access to devices, networks or data. Malware includes viruses, ransomware, spyware, trojans and other harmful programs. This software can perform a variety of tasks, typically hidden from the user. For instance, they might store passwords, track website activity or download personal files.
- **Brute-force attacks**—This attack method involves repeated attempts to log into someone's account until their credentials are cracked. Such attacks also frequently use credential-stuffing tactics, where usernames and passwords stolen from one breach are automatically tested against other accounts. These attempts are most successful when individuals reuse credentials across multiple accounts.
- **Shoulder-surfing incidents**—This attack method involves cyber-criminals stealing sensitive data, whether it's through no-tech means (eg peering over an employee's shoulder and writing notes on what they see), low-tech means (eg zooming in on a smartphone camera to peer at classified records from a distance) or high-tech means (eg leveraging a professional camera and other advanced equipment to surreptitiously record confidential information displayed on a screen).

Altogether, these threats can lead to costly and disruptive attacks, such as data breaches, account takeovers and ransomware incidents.

MACKAY
Corporate Insurance Brokers

Provided by MacKay Corporate Insurance Brokers

Mitigation Strategies

Considering the risks of remote work, it's crucial to take steps to boost your security. Whether you are working from home or a public location (eg a hotel, airport or coffee shop), follow these best practices:

- **Protect your device.** Only use devices specifically designated for work purposes. Never allow family or other household members to use these devices. When working from home, ensure a secure connection to your private Wi-Fi network, regularly update your router's firmware and lock your device whenever it's not in use. When working from a public location, maintain a proper distance from onlookers, dim your screen to make it harder for others to read and don't leave your device unattended. In any location, always connect to your employer's virtual private network or other secure access solution before handling company resources and keep all security software up to date.
- **Maintain data security.** Keep sensitive information safe by using only company-approved tools and applications for communication (eg email, direct messaging and video conferencing) and file sharing. Remain aware of your physical surroundings and the visibility of your screen to ensure maximum privacy.
- **Use strong passwords.** Utilise hard-to-guess passwords across your work accounts, applications and devices. The National Cyber Security Centre recommends using three random words combined into a single passphrase (eg "carpetmonkeybridge") to make passwords memorable yet difficult to crack. Never reuse passwords or share your credentials with others. In addition to creating strong passwords, use your employer's multifactor authentication services as an extra layer of security.
- **Recognise phishing scams.** Be prepared to identify key indicators of phishing scams (eg unknown or copycat senders, generic or threatening language, unsolicited links or attachments, and unusual or sensitive requests) and act accordingly. Never respond to these messages or answer any prompts without first verifying them through an alternative channel.
- **Enable company safeguards.** Ensure corporate security tools remain enabled on your device, including endpoint protection software, host firewalls and automatic updates. Ask your employer for more information on these resources.
- **Report potential incidents promptly.** If you notice any unusual activity or suspect a possible cyber-threat while working remotely, report these issues immediately. This may entail using a built-in alert system on your device, flagging concerning messages or other content for further review, or contacting the IT team directly.

For More Information

Cyber-attacks targeting remote workers are an ongoing, pervasive threat; nevertheless, you aren't defenceless against them. By understanding key risks and implementing proper precautions, you can help stay one step ahead of cyber-criminals.

Cyber-security can be challenging, but you don't have to navigate this topic alone. Contact your employer for more information on cyber-security best practices.