Ten Tips to Stay Cyber-Safe When Working Remotely

Whether for work or personal use, our reliance on technology has never been higher. As this reliance grows, so do the associated cyber risks. And when more people are working or studying from home, the potential for a cyber incident increases significantly.

Cyber criminals know that when more people are communicating online, it's much easier for them to use deception to gain access to protected information. At the same time, corporate IT and operations teams are working overtime to keep networks running without interruption – potentially impacting their ability to detect malicious activity quickly.

This makes protecting confidential information more challenging than ever. At Chubb, we look for ways to do more for our clients, like helping you prevent issues from happening in the first place. Following these ten tips can your business and your employees stay cyber safe, even in periods of uncertainty.

Best Practices for your Company

1. **Prepare for IT resourcing issues from both a people and a technology perspective**
   When more people are connecting remotely, technology call centres may face a higher call volume than normal, and more resources may be needed outside of standard business hours. Simultaneously, network bandwidth, data storage capabilities, and computing power are put to the test. Despite this increase in traffic, attention to detail cannot falter. Businesses are encouraged to keep a close eye on these needs, prepare a plan to reallocate resources as necessary, and recognise that this dependency may increase over time.

2. **Ensure your network, software, and applications are up-to-date**
   Remote access technologies have known vulnerabilities – and are all too often the weak link that bad actors use to gain access to protected information. Make sure all software and applications are updated and patch any weaknesses that are identified.

Ten tips to stay cyber-safe when working remotely, Australia. Published 03/2020.

3. **Make sure your resources are aligned – before an incident occurs**
Organisations should make sure their business continuity plans, disaster recovery teams, and cyber incident response plans are in alignment. Bad actors know that dependency on your network and its availability is never higher than when more people are accessing it remotely and will attempt to take advantage of the situation.

4. **Review your existing policies and closely monitor any necessary security exceptions**
When IT resources are stretched, organisations may need to make some exceptions to published security policies, standards, or practices. Implement a thorough review process to ensure such exceptions are closely monitored and solved. Also, most work from home policies weren't originally drafted to address a global conversion to remote work; organisations should carefully review those as well.

5. **Use multifactor authentication - now is the time to implement if you haven't already**
Traditional user login and password accounts are easy for bad actors to penetrate. Whenever possible, set up multifactor authentication on your accounts. This requires you to provide at least two authenticating factors, or proofs of identity, before you can access protected data, giving you a second line of defence against criminal activity. This additional level of protection is particularly critical when more people are accessing networks remotely, giving bad actors more entry points to access private networks.

Best Practices for your Employees

6. **Only connect to the Internet through a secure network.**
When connected to a public network, any information you share online or via a mobile app could be accessed by someone else. Always use a Virtual Private Network (VPN) to encrypt your activity. Most organisations provide a VPN to their employees to ensure secure, remote access for work use, and personal VPN accounts are available from various service providers. Access via personal devices while working remotely should be limited to encryted company VPN channels.

7. **Use strong passwords**
Most people use the same or similar version of a password for everything, even between work and home. Unfortunately, this means a single stolen password can be reused on multiple sites to unlock dozens of accounts for hackers. Remembering secure and complex passwords for every account can be difficult, if not impossible. Use password management software such as Dashlane to ensure you have strong, unique passwords for everything, because passwords are the foundation of sound online security practices.

8. **Only click on links, open attachments and download software from trusted resources**
Most people want to stay informed with the latest information, especially during periods of uncertainty. Bad actors know this and will attempt to take advantage by masking malicious links as something informative. Once clicked, that malicious link can be used to gain access to an individual's or organisation's private information, and/or freeze their computers or networks. If you're unsure of the source, go to the organisation's website. If it's important, the information will be posted there as well.

9. **Verify website URLs before sharing confidential information**
Bad actors can create fake websites where both the URL and homepage look remarkably similar to a site you trust – such as your healthcare provider, bank, or email provider. Instead of following a link in an email, type the URL in by hand. Also, make sure the site you visit has HTTPS in the URL; these sites are more secure than those with HTTP.

10. **Don't respond to requests for information from unknown sources – especially if the request is for personally identifiable information or passwords**
Bad actors will attempt to con people into sharing confidential information by pretending to be someone you know or work with. Take extra care in identifying who you're sharing information with – even if you think the request came from a trusted resource or organisation. Don't feel rushed; take the time to research the request and whether it's appropriate before responding.

Additional Resources

The Chubb website hosts a variety of Insights and resources to help you and your business mitigate cyber risks.

Please visit www.chubb.com/au-cyber

Contact us

Chubb Insurance Australia Limited
ABN: 23 001 642 020 AFSL: 239687

Grosvenor Place
Level 38, 225 George Street
Sydney NSW 2000
O +61 2 9335 3200
F +61 2 9335 3411
www.chubb.com/au

Chubb. Insured.℠

This content is brought to you by Chubb Insurance Australia Limited ("Chubb") as a convenience to readers and is not intended to constitute advice (professional or otherwise) or recommendations upon which a reader may rely. Chubb Insurance Australia Limited (Chubb) makes no warranty or guarantee about the accuracy, completeness, or adequacy of the content. Readers relying on any content do so at their own risk. It is the responsibility of the reader to evaluate the quality and accuracy of the content. Reference in this content (if any) to any specific commercial product, process, or service, and links from this content to other third party websites, do not constitute or imply an endorsement or recommendation by Chubb and shall not be used for advertising or service/product endorsement purposes. Ten tips to stay cyber-safe when working remotely. Published 03/2020. Chubb10-649-0320.