Ten Tips to Stay Cyber-Safe When Working Remotely

CHUBB®

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 in different ways.

Cyber criminals know that when more people are communicating online, they're interacting with technology in different ways - even sometimes using networks or software for the first time. Bad actors often attempt to take advantage of such situations, using 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 suggesting ways to possible help you prevent issues from happening in the first place. Following these ten tips may help your business and your employees stay cyber-safe, even in periods of uncertainty.

1. **Prepare for IT resourcing issues from both a people and a technology perspective.** When more people are connecting remotely, technology call centers 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 recognize 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.
3. **Make sure your resources are aligned - before an incident occurs.** Organizations 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, organizations 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; organizations should carefully review those as well.

5. **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 organizations provide a VPN to their employees to ensure secure, remote access for work use, and personal VPN accounts are available from various service providers.
6. **Use strong passwords.** Many 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 to ensure you have strong, unique passwords for everything, because passwords are the foundation of sound online security practices.
7. **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 defense 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.
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 organization's private information and/or freeze their computers or networks. If you're unsure of the source, go to the organization'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 organization. Don't feel rushed; take the time to research the request and whether it's appropriate before responding.

Minimize Your Cyber Risks

Every commercial Chubb cyber policy provides access to a variety of resources to help organizations prepare for and quickly respond to disruptive cyber incidents, including:

- Online cyber security training that can be shared with employees to educate them on how to identify potential threats, protect sensitive data, and escalate issues to the right people when necessary.
- Password management software that can be deployed to employees, ensuring they always use secure and complex passwords.
- Cyber security rating services, providing objective, quantitative measurements on your company's security performance.
- Ransomware identification software, to help identify ransomware attacks from incoming malware, then mitigate the spread to other exposed devices on a company's network.

Chubb's personal cyber policyholders also have access to premier consulting, investigative, and crisis management services to help prevent incidents from happening.

Visit www.chubb.com/cyber to learn more about keeping your organization protected against cyber risk, or www.chubb.com/online-you-protected for additional tips on protecting your personal data at home.

Chubb. Insured.℠