AKOUTO

eBook

Secure Remote Working

Cyber Security Checklist

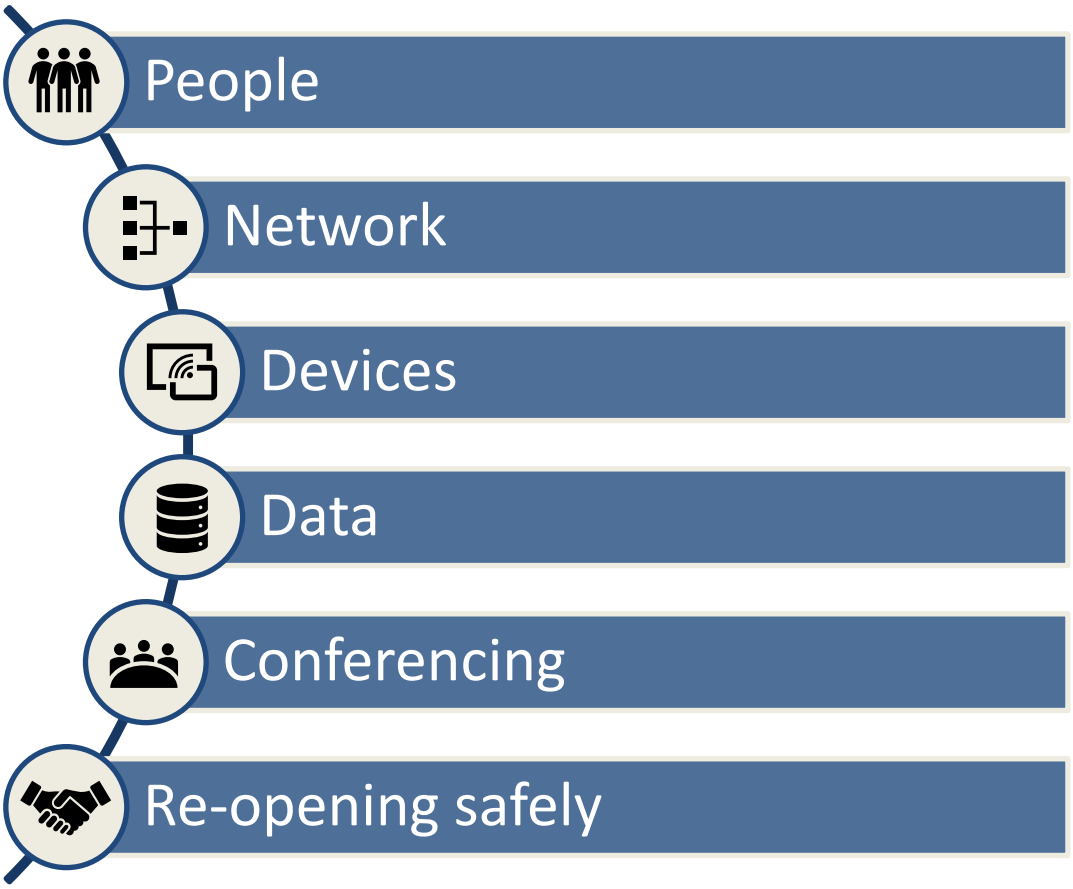
Secure Remote Working Cyber Security Checklist

There is a huge collection of tools and technologies that make remote working more efficient and effective than ever before. Laptops, Tablets, Smartphones, VPN, Webcams, Video Conferencing, Email, Instant Messaging, the list is seemingly endless.

Yet, these very same tools that enable today's flexible and mobile workforce are often exploited by hackers and cyber criminals to steal data, extort users and spread malware to other unsuspecting victims.

Contents

In this eBook we provide you with simple steps you can take to maintain a safe and healthy work environment, protect the systems and information you use while working remotely, and precautions you should take before resuming normal operations after an office closure.



Secure Remote Working Cyber Security Checklist

People

Cyber Awareness training: Take some time to follow cyber awareness training so you are up to date with the latest techniques and tricks that hackers use and what you can do to stay safe.	☐
Emergency Plan: Make sure you know who to contact in the event of a cyber incident. Have a printed sheet with contact information in case your computer is unusable.	☐
Confidentiality & Privacy: Be aware of who can overhear your confidential work conversations such as a spouse, room-mate or neighbour if you are taking calls in shared spaces, outside or with open windows.	☐
Workspace: Make sure your workspace is set up for a healthy posture and lighting. Use an external keyboard, mouse and screen (or laptop stand) and take breaks away from the keyboard.	☐
Connections: Maintain connections with colleagues through informal friendly interactions over phone, video or instant messaging.	☐

Network

No default logins: Make sure you are not using default usernames and passwords on any devices including routers, computers, cameras, TV, smart-thermostat or any other device connected to your network.	☐
Secure Wi-Fi: Make sure your Wi-Fi is password protected, does not use a default or easy to guess password, use a strong password with 10 or more characters and a secure protocol such as WPA.	☐
Network Segmentation: Keep all work devices on a separate network from personal and guest devices. Set up a guest Wi-Fi and separate wired network.	☐
VPN and Tethering: Avoid all public Wi-Fi if possible, prefer to tether your phone and use wireless data instead. If you must use public Wi-Fi use a VPN to protect your network traffic.	☐
DNS Firewall: Use a reputable DNS Firewall such as the free CIRA DNS Firewall or OpenDNS to add an extra layer of security to your network.	☐
Intrusion Prevention: If you handle sensitive or confidential information, use an Intrusion Prevention System like MySecurityConsole to protect your network.	☐

Secure Remote Working Cyber Security Checklist

Devices

Avoid Downloads: Only install what is absolutely necessary and do not trust downloads from untrusted sources or peer-to-peer file sharing services even if your virus scanner tells you a file is safe. Do not use work devices for personal downloads.	☐
Work Accounts: Keep all work related data on work related accounts, for example, do not use your personal email account to send work related files. Only use your work accounts on work devices, keep all personal activity on personal devices.	☐
Anti-Virus: Use a reputable anti-virus and firewall on all devices. Do not use free anti-virus products, Microsoft Defender which is standard on Windows 10 is safer than free offerings.	☐
Avoid Sharing: Do not allow other individuals including your partner, spouse, children or guests to use work devices even for a very short time or simple task.	☐
Password Protection: Use a password protected screen saver to make sure nobody can access your system when you are away from the keyboard or on a break.	☐
Drive Encryption: Use full drive encryption such as BitLocker on Windows to avoid data theft or exposure if your device is lost or stolen. Make sure you back up the decryption key and have secure backups of your data first.	☐
Update Software: Always keep software up to date with the latest patches and updates provided by vendors.	☐
Mobile Malware: Avoid installing apps on your mobile device if you don't need to, many applications in the legitimate app stores are malware in disguise.	☐
Lock Equipment: Store work devices in a secure spot when not in use, under lock and key if possible.	☐

Secure Remote Working Cyber Security Checklist

Data

Multi Factor Authentication: Enable MFA on all accounts that support it and use an authenticator app such as Google Authenticator. Make sure you regularly back up authenticator keys.	☐
Unique Passwords: Don't use the same password on different accounts, use unique, hard to guess passphrases that are 10 characters or longer.	☐
Professional Accounts: Don't use personal accounts or services such as email accounts or your personal Google Drive for work data. Only use professional accounts and services for work data.	☐
Encryption: Always password protect and encrypt files that contain sensitive, confidential or personal information before emailing or sharing them with colleagues.	☐
Backups: Set up secure, automated backups of your work files and data so you can recover the information you need in case of a virus or ransomware.	☐

Conferencing

Mute: Muting the microphone when you are not speaking improves the overall quality and prevents background conversations from being accidentally overheard.	☐
Cover Webcam: Use a webcam cover or a small piece of tape to cover your webcam when you are not using it. Don't trust the LED indicator to tell you when it is on.	☐
Clean Background: Check your background to make sure nothing sensitive or confidential is visible to other video conference participants.	☐
Lock Conference: Always require a PIN or passcode when setting up an online conference. Use unique codes for each participant if your platform supports it, or switch to a more secure service if not.	☐
Identify Participants: Keep an eye on conference participants and when in doubt don't be shy to challenge individuals to identify themselves.	☐

Secure Remote Working Cyber Security Checklist

Re-opening safely

Check Health and Safety Equipment: Make sure equipment such as smoke alarms, fire extinguishers, first aid kits and any other health and safety equipment are in good condition and working order.	☐
Software Updates: Make sure any systems that have been inactive or powered down are fully patched with the latest software updates before returning them into service. Backup important files first, sometimes updates can cause problems.	☐
Check Devices: Perform a full virus scan and double check any devices that have been used remotely in less secure environments for extended periods of time.	☐
Battery Backups: Check all battery backup systems to make sure they are in good working order and fully charged.	☐

www.akouto.com

info@akouto.com

1-877-707-0920