

21 SECURITY BEST PRACTICES FOR WORKING REMOTELY IN 2022

The global pandemic has forced companies worldwide to rapidly shift and adapt to a primarily remote workforce and decentralized network environments. Unfortunately, employees who are worried about a potentially deadly virus, or who feel underprepared and overwhelmed by the various challenges of working from home, have quickly become the number one target for cybercriminals.

Working remotely is rapidly becoming a new standard operating procedure, which is why we've put together a list of 21 best practices to help you maintain a strong security strategy in 2022, regardless of where or how you get your work done.



01

INSTALL ESSENTIAL SECURITY PROTECTIONS

Ensure all your devices, whether company-issued or personal, are protected by actively licensed antivirus and antimalware solutions.



06

SECURE PERSONAL DEVICES

If you have permission to work and access company systems with your personal device, it is imperative that you implement encryption for all data assets and internet traffic and make certain your device is password-protected.



02

KEEP HARDWARE & SOFTWARE UPDATED

Cybercriminals will exploit security vulnerabilities in your hardware and software systems. To keep your systems as secure as possible, you need to install security patches right away.



07

FOLLOW COMPANY PASSWORD POLICIES

Weak passwords and bad password hygiene will impair even the best security strategies. Make sure you are adhering to your company's password policies and criteria requirements.



03

SECURE YOUR HOME NETWORK

When working from home, make sure you're using a wireless network that is secure and password-protected. Never use the default internet router credentials. Always change them to maximize security.



08

NO PERSONAL DEVICES WITHOUT A BYOD POLICY

Using an unsecure personal device for work can expose your company's network and systems to security risks and cyberthreats or even data theft. Do not use a personal device for work without adhering to your company's BYOD policy.



04

USE A VPN TO ACCESS COMPANY RESOURCES

Using a VPN, or virtual private network, while accessing company data or applications helps protect your privacy by encrypting all traffic and data being transmitted.



09

LEARN ABOUT AND ADHERE TO ALL COMPANY SECURITY POLICIES

An essential security practice when working remotely is to follow your company's IT and security policies. This helps you securely access your company's data, networks and resources, and minimize risks.



05

ENABLE MULTIFACTOR AUTHENTICATION

Multifactor authentication enforces strict control over who logs in to company systems and applications, ultimately protecting against unauthorized access of confidential data should your individual credentials be compromised.



10

BEWARE OF PHISHING SCAMS

Security risk is one of the trade-offs of remote work and threat actors can easily execute phishing scams. Be cognizant! Read emails carefully before responding and avoid malicious links.



11

BACK UP EVERYTHING

Data loss can result from a variety of incidents, such as system failures or accidental deletions, and can cause costly downtime. Make sure all files and data are backed up regularly and securely according to your company's backup policies.



16

COMPANY-ISSUED DEVICES ARE FOR YOUR USE ONLY!

Never allow family or friends to use your company-issued devices or any devices that contain private, sensitive or restricted company data or systems.



12

AVOID USING PUBLIC WIFI

Although it's free, public WiFi is unsecure and can expose your device and any confidential or sensitive company data to significant security risks. If using a public WiFi connection is unavoidable, always use a secure VPN.



17

AVOID PRINTING OR WRITING DOWN SENSITIVE INFORMATION

Avoid the risks that come with protecting documented, confidential information by never printing or writing down any sensitive or private data. If necessary, keep records securely locked and out of view.



13

SECURE ONLINE/VIRTUAL MEETINGS

Unlike in-person meetings, authenticating attendees is difficult in online meetings. Use one-time PINs or access codes and MFA to ensure only authorized personnel are attending the meetings.



18

PAY ATTENTION TO PRYING EYES

While working from a public place, such as a coffee shop or a library, pay close attention to prying eyes. Skilled shoulder surfers could easily identify sensitive information and obtain your credentials.



14

LOCK YOUR DEVICE OR LOG OUT WHEN NOT IN USE

An unlocked device is an invitation for trouble. Make it a habit to lock your device when unattended.



19

COMPANY DEVICES ARE NOT FOR PERSONAL USE

Using company-issued devices for personal activities, such as online shopping, gaming or social networking, puts your company's sensitive data at risk and could introduce malware into the devices.



15

NEVER SHARE PASSWORDS OR ACCOUNT CREDENTIALS

Never share your passwords or login credentials with anyone — colleagues, family members or friends.



20

STICK TO COMPANY-APPROVED COMMUNICATION RESOURCES

Do not use personal emails for business communication. Always use company-provided resources, such as corporate emails and collaboration tools, to communicate or share documents and other information.



21

COMPLETE SECURITY AWARENESS TRAINING

Make sure you complete the training programs to learn the strategies, measures and actions needed to protect yourself and your company.



If you need help securing your home working environments, devices or data, contact us today. Make sure that remote workforce security is a part of your cybersecurity strategy in 2022.