OKLAHOMA
Office of Management
& Enterprise Services

Checklist for Securing Remote Workers

Instructions

Use this checklist to ensure that you are implementing all IT security best practices when you are working from home or away from the office.

	Checklist Item	Rationale	Instructions
☐	Change your wireless router's default administrator credentials	Default username and passwords for wireless routers can be easily obtained online by hackers. If these aren't changed, wireless routers can be used by malicious individuals who gained access to your wireless network.	Enter your router's IP address into your web browser and log in with the default username and password, which are often both "admin." Instructions will vary by router. Create a password with at least 12 characters with a combination of uppercase and lowercase letters (HJW, dsn), symbols (!@#$), and numbers (12345), and write it down somewhere that is physically secure and not in plain text on a device or in an IT application.
☐	Create a complicated password for wireless internet access	The wireless password should not be the same password that gives you administrative rights over the wireless network. Create a password that doesn't use easily guessed personal information like last name or phone number.	Create a password with at least 12 characters with a combination of upper-case and lower-case letters (HJW, dsn), symbols (!@#$), and numbers (12345), and write it down somewhere that is physically secure and not in plain text on a device or in an IT application.
☐	Change home network name to something bland and unattractive	People often use last names for their home network when they should really be choosing something bland and unattractive to hackers. If your last name and phone number can be found on the internet, then hackers can find these too. Use something inconspicuous instead.	Log in to your Wi-Fi router using the router's IP address. Go to settings and look for the option entitled "Wi-Fi name" or "SSID." Enter a new SSID, save your settings, then log out.
☐	Hide your network SSID	Along with changing the SSID to something that is less attractive to hackers, users can go one step further and create a hidden network for added security and peace of mind. This step may require a little more effort when you need to connect to the network, but it will be that much more difficult to find a non-broadcasting network.	Log in to your Wi-Fi router settings and look for the option entitled "Wi-Fi name" or "SSID." Click on the box that says "Hide SSID" and your network will no longer broadcast to the public. You will have to search for the SSID manually whenever you need to access the network.
☐	Strengthen your Wi-Fi encryption	Most routers will have automatic settings, but WPA2 AES is the newest and strongest encryption available in most consumer routers. If your router	To switch to WPA2 AES, go to your wireless settings in the router settings page, which is generally the same page you used to name your SSID.

	Checklist Item	Rationale	Instructions
		does not allow you to switch to WPA2 AES, you might have an older router that needs to be upgraded.	Choose WPA2 (sometimes WPA/WPA2) and then click on AES under the encryption options.
☐	Turn off remote management	Remote management doesn't mean you can't connect to the network when at home. Instead, if this feature is turned on and you cannot encrypt management access, this can allow hackers to remotely access the home network without being physically near your home.	While this varies by router, go to your system settings and go to the administration or administrative tools settings. Under remote management, disable remote management. Save and close settings.
☐	Consider limiting or turning off WPS	WPS was built into routers with ease of use in mind, but it also leads to a widespread security vulnerability in most consumer Wi-Fi routers. Weigh the convenience of setting up access to the Wi-Fi network against the overall security of the network if you decide to turn WPS on or off.	As this varies by router, you want to go to system settings and go to the administration or administrative tools settings. Under WPS, uncheck the box that enables WPS. Save and close settings.
☐	Make sure router firmware is up to date	Having up-to-date firmware means your router will be better protected from vulnerabilities in older hardware. Check to see if the manufacturer is still pushing out firmware updates for your home router and modem, because if updates have ended, this makes older, unsupported products more vulnerable to attacks.	Read the manufacturer's website to see what version your wireless router's firmware should be. Under system settings, check your firmware by clicking on check for upgrade. If you are up not up to date, make sure to allow the newest version to be downloaded and installed.
☐	Ensure that your firewall is turned on	If there is a firewall included on the Wi-Fi router, you should refer to the user's guide on the manufacturer's website for how to turn it on. Turning on your firewall blocks malicious traffic going in or out of your network, making this an easy win for best security practices.	Read the user's guide on the manufacturer's website for how to turn on your Wi-Fi. Normally, under security settings, you can check a box to make sure that the firewall is turned on. Save and then close settings.
☐	Install an antivirus or anti-malware (artificial intelligence or signature based)	If you do not use Microsoft Windows 10 and do not have access to Windows Defender by default, refer to your service desk for advice on which antivirus or anti-malware program you should have installed on your endpoint device.	Check with your service desk for the appropriate antivirus you should install and what settings should be turned on.
☐	Use encrypted protocols for connecting to company resources (VPN, IPsec, and SSL)	If your organization has a defined remote work access policy, make sure to follow use the proper encrypted protocols for connecting to company resources. If using the VPN is general practice, the VPN should be the only way that users can access sensitive information when working from home. Other encrypted protocols may be used by your organization.	Follow your organization's remote work access policy to access sensitive information on the corporate network.
☐	Make sure device is encrypted	It is important to make sure that your mobile work device (laptop, company managed cell phone) are encrypted.	Check with your service desk to make sure that BitLocker is turned on as you work remotely.

	Checklist Item	Rationale	Instructions
		Microsoft Windows 10 ensures that devices can be encrypted using BitLocker that will protect your drive and stop any unauthorized changes to your system such as firmware-level malware.	
☐	Ensure device is up to date	You should make sure that your device is up to date and running the latest configuration to avoid any security vulnerabilities. Check with your service desk to see whether or not they will run updates outside of normal work hours.	Go to your operating system's settings menu and search for updates. Run a check to see if there are updates that need to be installed. If there are new updates, install them and then close the settings menu.
☐	Avoid public Wi-Fi	It is strongly advised that you should not work remotely using public Wi-Fi to conduct company business unless it is done securely through an encrypted protocol. Connecting to public Wi-Fi opens your activity up to malicious attackers that look for vulnerable endpoint devices.	Use an encrypted network that is private and preferably managed by yourself or by a trusted IT team.
☐	Use multi-factor authentication (MFA)	Multi-factor authentication is an additional layer of security to check against the identity of a person accessing company information and applications. Multi-factor authentication is a staple of security best practices that is even more important when working from home.	If presented as a choice, always use MFA whenever accessing your company's resources.
☐	Be aware of targeted spear phishing attacks	For users that cannot walk over and check to see if someone really sent them that urgent email, now is a good time to remind everyone to be diligent and watch out for urgent requests that may break company policy.	Use the right collaboration tools, preferably one that uses videoconferencing, to verify the identity of suspicious or fraudulent phishing emails, then report any suspicious emails to security or service desk.
☐	Ensure area around your laptop/desktop/mobile device is clear	Make sure that no one is looking over your shoulder or potentially looking at your screen if you are working in a public space. Maintaining the privacy of your company's information must be ensured when working in public.	Do not leave your computer on and unattended, lock your computer screens when you are away from the device, and ensure that the space around you is clear of lines of sight. This includes public spaces such as a home shared with roommates.
☐	Do not leave your laptop or mobile device in your car	Do not leave your laptop or mobile device in your car because of the risks of car theft. Make sure to keep them in a secure space, like a locked home office, locked drawer, or home safe when not the device is not in use.	Make sure that you do not leave your laptop unattended and continue to leave it in a secure place when not in use.