WORK-FROM-HOME SECURITY GUIDANCE

Use the guidance provided in this document to improve the security of WFH. 4 Pages 20-882

These documents have been voluntarily contributed by NOREX Members with the full knowledge that other Members may use them in any manner they see fit. NOREX and its Members shall not be held liable for any statements or interpretations contained within the documents.

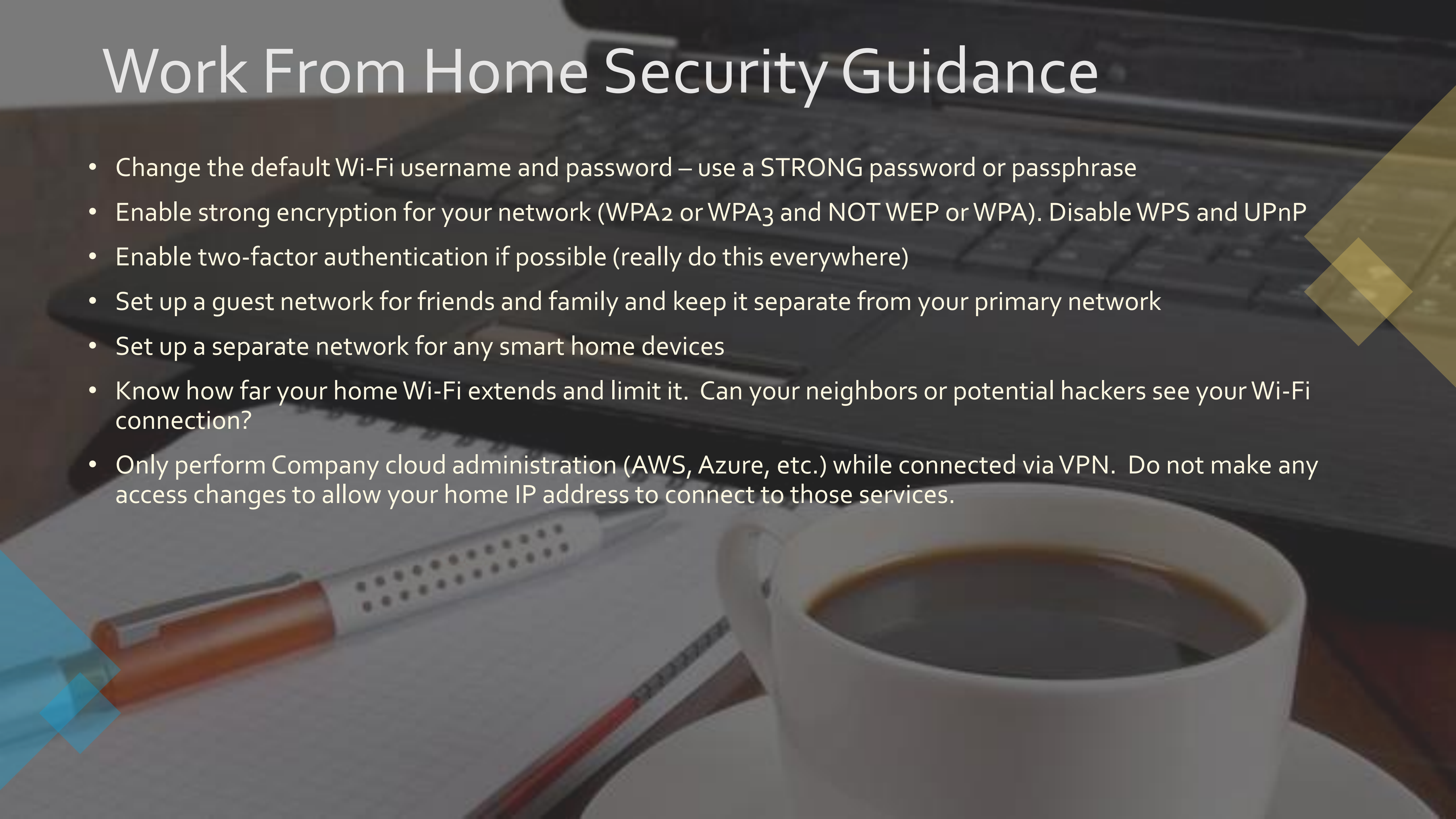
Work From Home Security Guidance

Use the guidance provided in this document to improve the security of working from home. The guidance included will reduce the risk to Company and increase the security of your own home computing environment, including any Smart Home technologies you may have.

Work From Home Security Guidance

- Be vigilant to watch your email for phishing attempts
- Ensure your system is up to date with all patches and do not turn off automatic patching for your device
- Use only Company provided or managed devices when connecting to Company networks or resources whenever possible
- Only use authorized software on your devices
- Protect your login and password - do not share it or allow anyone to use your device
- Ensure your device is not connected to multiple networks while using Company's VPN (dual-homed)
- Make sure you've changed the default admin password for your internet router/mode
- Make sure your software and firmware on your router/modem and Wi-Fi device (if different) is updated
- Configure your router/modem firewall to limit traffic. Refer to your router support website for instructions or contact your ISP.

Work From Home Security Guidance



- Change the default Wi-Fi username and password – use a STRONG password or passphrase
- Enable strong encryption for your network (WPA2 or WPA3 and NOT WEP or WPA). Disable WPS and UPnP
- Enable two-factor authentication if possible (really do this everywhere)
- Set up a guest network for friends and family and keep it separate from your primary network
- Set up a separate network for any smart home devices
- Know how far your home Wi-Fi extends and limit it. Can your neighbors or potential hackers see your Wi-Fi connection?
- Only perform Company cloud administration (AWS, Azure, etc.) while connected via VPN. Do not make any access changes to allow your home IP address to connect to those services.

“SMART HOME” Security Tips

- Change the default Wi-Fi username/password – use a STRONG password
- Enable two-factor authentication if possible (really do this everywhere)
- Check the default privacy and security settings
- Disable features you aren't using
- Keep your software up to date
- Avoid using public Wi-Fi to manage your devices
- Know how your devices work, what data is stored and what those devices communicate with
- Choose well-known brands - avoid kick-starter, Indiegogo, etc.