

HOME OFFICE

Home Office & Home Network Checklist

When you work from home, your router protects your company. Most home routers are still running factory settings, and every smart device on the same network is a way in.

Router

- ☐ Change the router's default admin password to a long, unique passphrase
- ☐ Turn on automatic firmware updates, and replace a router that no longer receives updates
- ☐ Use WPA3 encryption (or WPA2-AES if WPA3 is not available) with a strong Wi-Fi passphrase
- ☐ Turn off remote administration, WPS, and Universal Plug and Play (UPnP) unless you need them
- ☐ Consider protective DNS that blocks known malicious sites, such as Quad9 or Cloudflare 1.1.1.2

Separate what you can

- ☐ Put visitors, smart TVs, cameras, speakers, and other smart devices on a guest network
- ☐ Keep work laptops off the network that children's gaming devices use, if your router supports it
- ☐ Change default passwords on printers, cameras, and other connected devices, and keep them updated

Workspace habits

- ☐ Lock your screen whenever you leave your desk, even at home
- ☐ Keep smart speakers away from where you take confidential calls
- ☐ Shred printed client or employee information instead of putting it in household trash
- ☐ Use your phone's hotspot instead of public Wi-Fi for sensitive work when traveling

Sources and further reading

NSA: Best Practices for Securing Your Home Network (PDF): https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF

CISA: Secure Our World: <https://www.cisa.gov/secure-our-world>

Need help rolling this out across your team? Request a consultation at nexussecurityadvisors.com/get-started.