sam
seamless network

A Summary of the NSA's Recommendations for Device Security

February 2023

- **Secure electronic devices** - Such as computers, laptops, printers, mobile phones, tablets, security cameras, home appliances, cars, and other "Internet of Things" (IoT) devices, must all be secured to reduce the risk of compromise. Schedule frequent device reboots.

- **Use the most updated version of your devices' OS** - Enable automatic update functionality when available, or install patches and updates from a trusted vendor on a monthly basis.

- **Secure and update routing devices** - Consider using a personally owned router instead of the one provided to you by your ISP. Disable remote admin on the router. Keep routing devices updated with the latest patches, and replace them when they reach end-of-life for support. Ensure that your personally owned routing device supports basic firewall capabilities (including NAT) to prevent scanning of your internal systems.

- **Segment and protect your Wi-Fi network** - Create a separate wireless network for guests, and preferably a separate one also for your IoT devices. Ensure your WAP is capable of Wi-Fi Protected Access 3 (WPA3). Use a strong passphrase with a minimum length of 20 characters and protected management frames for added security. Change the default service set identifier to something unique.

- **Leverage security software** - Including anti-virus, anti-phishing, anti-malware, safe browsing, and firewall capabilities as a layered defense mechanism. This can be provided via the OS or a separate product, it should be installed on computers, laptops, and tablets. Full disk encryption should be implemented where possible on these devices.

- **Protect passwords** - Passwords and answers to challenge questions should be strong, unique, and difficult to guess. They should not be stored in plain text form on the system. It is highly recommended to use a password manager.

- **Limit use of the administrator account** - Create a non-privileged "user" account for normal, everyday activities, and use the admin account for maintenance, installations and updates.

- **Safeguard against eavesdropping** - Limit sensitive conversations when near baby monitors, audio recording toys, home assistants, and smart devices – their microphones might be listening even when they're not being used.

- **Exercise secure user habits** - Back up data on external drives, avoid connecting mobile devices to public charging stations, leave computers in sleep mode, and regularly reboot computers to apply updates – this will help you minimize ransomware risks.

- **Ensure confidentiality during telework** - Use a VPN when connecting to your corporate network from home. When connecting to other work services, make sure it is also done through a secure tunnel. If using commercial collaboration services, choose one that provides strong encryption.

The full set of recommendations, including advice on how to practice safer online behavior, can be found at the NSA's Central Security Service website, here.

Please note that this is not an official NSA document. The information presented here is based on NSA's latest Cybersecurity Information Sheet.

Logos of the National Security Agency and Central Security Service used under Public domain, via Wikimedia Commons.