National Security Agency | Cybersecurity Information Sheet

Securing Wireless Devices in Public Settings

Telework has become an essential component of business, and many people are teleworking from home or during travel. While the owners of home networks can take steps to secure those networks, it can be difficult to ensure public networks (e.g., conference or hotel Wi-Fi®) are secure. Protecting personal and corporate data is essential at all times, but especially when teleworking in public settings. To ensure data, devices, and login credentials remain secure and uncompromised, cybersecurity is a crucial priority for users and businesses. This includes identifying higher-risk public networks and implementing security best practices while in public settings, whether connecting laptops, tablets, mobile phones, wearable accessories, or other devices with the ability to connect to the internet.

Accessing public Wi-Fi hotspots may be convenient to catch up on work or check email, but public Wi-Fi is often not configured securely. Using these networks may make users' data and devices more vulnerable to compromise, as cyber actors employ malicious access points (Masquerading [T1036][1]), redirect to malicious websites, inject malicious proxies, and eavesdrop on network traffic (Network Sniffing [T1040]).[1] In addition to Wi-Fi, cyber actors can compromise other common wireless technologies, such as Bluetooth® and Near Field Communications (NFC) (Exploit via Radio Interfaces [T1477]). These technologies must be properly configured to ensure user devices remain secure from compromises. The risk is not merely theoretical; these malicious techniques are publicly known and in use.[2]

This infosheet gives National Security System (NSS), Department of Defense (DoD), and Defense Industrial Base (DIB) users the best practices for securing devices when conducting business in public settings. It describes how to identify potentially vulnerable connections and protect common wireless technologies, and lists steps users can take to help secure their devices and data. While these best practices cannot ensure data and devices are fully protected, they do provide protective measures users can employ to improve their cybersecurity and reduce their risks.

[1] T1036 and similar notations identify MITRE ATT&CK® techniques.

Best practices for securing wireless devices

While technology settings and business controls may help keep security measures up-to-date, users should also be aware of the potential threats from connecting to publicly available Internet and take appropriate precautions. Before conducting business remotely or in public settings users should obtain explicit authorization from their organization to do so. Organizations may decide to require that users working like this adopt best practices such as the ones detailed here. The information that follows may be used to better protect users, devices, and data while teleworking.

Public Wi-Fi

Avoid connecting to public Wi-Fi, when possible, as there is an increased risk when using public Wi-Fi networks. Use a corporate or personal Wi-Fi hotspot with strong authentication and encryption whenever possible, as it will be more secure.

If users choose to connect to public Wi-Fi, they must take precautions. Data sent over public Wi-Fi—especially open public Wi-Fi that does not require a password to access—is vulnerable to theft or manipulation. Even if a public Wi-Fi network requires a password, it might not encrypt traffic going over it. If the Wi-Fi network does encrypt the data, malicious actors can decrypt it if they know the pre-shared key (Eavesdrop on Insecure Network Communication [T1439]). A malicious actor can also sometimes coerce the network into using insecure protocols or obsolete encryption algorithms (Downgrade to Insecure Protocols [T1466]).[3] Additionally, a malicious actor can set up a fake access point, also known as an evil twin, to mimic the nearby expected public Wi-Fi,[2] resulting in that actor having access to all data sent over the network. Unencrypted network traffic or traffic that is easily decrypted can be captured using open-source tools, exposing sensitive data. This includes, but is not limited to, personal and corporate login credentials (Network Sniffing [T1040]) that can lead directly to additional compromises.[4]

If connecting to a public Wi-Fi network, NSA strongly advises using a personal or corporate-provided virtual private network (VPN) to encrypt the traffic.[1],[3-6] In addition, users should incorporate secure browsing methods, such as only accessing websites that use Hypertext Transfer Protocol Secure (HTTPS). This is usually indicated by the URL beginning with “https://” or a lock symbol. These methods, as well as the ones listed in the “Do’s and Don’ts” section, will aid users in better protecting their information from Wi-Fi snooping (Network Sniffing [T1040]), man-in-the-middle techniques (Man-in-the-Middle [T1557]), server masquerades used to capture password hashes (such as the Responder tool) (Man-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay [T1557.001]), and evil twin mimics.

Bluetooth

Bluetooth technology transmits data wirelessly between devices within short distances. This feature is very convenient in private (i.e., non-public settings). However, keeping a device's Bluetooth feature enabled in a public setting can pose a cybersecurity risk. Malicious actors can scan for active Bluetooth signals, potentially giving them access to information about the targeted device. They can then leverage that information to compromise the device.[1] Other Bluetooth compromise techniques posing a cyber-threat in public settings include Bluejacking, Bluesnarfing, and Bluebugging to send, collect, or manipulate data and services on the device (Exploit via Radio Interfaces [T1477]). Additionally, the publicly released Bluetooth exploit, Blueborne, demonstrates that Bluetooth vulnerabilities can allow malicious actors complete control over a user's Bluetooth device. This could enable access to corporate data and networks.

NFC

NFC offers the benefit of contactless payments and other close device-to-device data transfers. As with any network protocol, there may be NFC vulnerabilities that can be exploited (Exploit via Radio Interfaces [T1477]). Due to NFC range limitations, opportunities to exploit vulnerabilities may be limited. However, NSA advises being aware of security risks with the technology and if possible, disable the function when it is not in use.

Do's and Don'ts

Complete security is never guaranteed, but to protect their devices and data in public settings when teleworking, NSS, DoD, and DIB users should adhere to the following Do's and Don'ts:

✓ DO'S	✗ DON'TS
((•)) FOR WIRELESS DEVICES	
All Devices • Keep software and applications updated with the latest patches.[3],[8],[9] • Use anti-virus/anti-malware software (if applicable). • Use multi-factor authentication (MFA) whenever possible.[1],[3-6],[9] ▪ MFA can assist in account/device security to defend against password hash captures. • Reboot regularly, especially for mobile phones after using untrusted Wi-Fi.[6] ***In Addition: For Laptops*** • Enable firewalls to restrict inbound and outbound connections by application.[5],[6] ***In Addition: For Windows Laptops*** • Disable Link-Local Multicast Name Resolution (LLMNR) if applicable.[10] • Disable Netbios Name Service (NBT-NS).[10]	***All Devices*** • Do not leave them unattended in public settings.[1],[6] • Do not use personal information in the names of the devices (i.e., John/Jane Smith's Computer).

• Configure Web-Proxy Autodiscovery Protocol (WPAD) to use only corporate proxy servers.[11],[12] ▪ In conjunction, disable Autodetect Proxy Settings.	

✓ DO'S	✗ DON'TS
FOR PUBLIC WI-FI	
All Devices • Connect to a personal/corporate wireless hotspot with strong authentication and encryption if possible. • Disable Wi-Fi when not in use.[6] • Ensure the device is connecting to the correct network. ▪ Disable Wi-Fi network auto-connect.[1],[3],[6] • If connecting to public Wi-Fi is necessary: ▪ Only connect to secure public Wi-Fi.[1],[5] ○ This usually requires a password or other forms of authentication, limiting who can connect. ○ Only connect to networks with WPA2-encryption at a minimum[2].	***All Devices*** • Do not connect to open Wi-Fi hotspots.[1],[3–6] • Do not enter most sensitive account passwords on sites/applications. • Avoid accessing personal data (e.g., bank accounts, medical, etc.).[1] • Do not have sensitive conversations.[6] • Avoid online shopping or financial transactions.[1] • Do not click unexpected links, attachments, or pop-ups.[6] ***In Addition: For Laptops*** • Do not set public Wi-Fi networks to be trusted networks. • Do not browse the Internet using the administrator's account for the device.

[2] Users can find this information in the Device Settings under Network Properties or Network Details in macOS®.

▪ Log out of the public Wi-Fi network and “Forget” the access point when finished using it. ▪ Delete unused Wi-Fi networks.[6] ▪ Use an IPsec VPN.[1],[3-6] ▪ Use HTTPS browsing protocols.[1],[5] ▪ Only browse to or use necessary websites and accounts. ***In Addition: For Laptops*** • Turn off the device file and printer sharing on public networks.[3],[5] • Use virtual machines (VMs) for an additional layer of security (if feasible) to contain drivers (e.g., Wi-Fi driver) and applications (e.g., web browsers) that process untrusted data from external sources.[13] ▪ The VM limits compromised adversarial activity. If compromised, the VM can be discarded.	

✅ **DO’S** ❌ **DON’TS**

FOR BLUETOOTH	
All Devices • Monitor Bluetooth connections by periodically checking what devices are currently connected to the device.	***All Devices*** • Do not use Bluetooth to communicate passwords or sensitive data.

• Disable the Bluetooth feature when it is not being used.[6] • Ensure the device is not left in discovery mode when Bluetooth is activated and discovery is not needed.[1],[6] • Use an allowlist or denylist of applications that can use the device's Bluetooth.	• Do not accept non-initiated pairing attempts.

✅ DO'S	❌ DON'TS
FOR NFC	
All Devices • Disable NFC feature when not needed (if possible).	***All Devices*** • Do not bring devices near other unknown electronic devices. (This can trigger automatic communication.) • Do not use NFC to communicate passwords or sensitive data.

Users should consider additional security measures, including limiting/disabling device location features, using strong device passwords, and only using trusted device accessories, such as original charging cords.[6]

Telework safely

The methods used to compromise devices and data are constantly evolving. As telework becomes more common, users are more frequently bringing themselves and their data into unsecured settings and risking exposure. By following the guidance in this infosheet and related guidance, users can identify potential threats and put best practices into action when teleworking in public settings.▪

Works cited

[1] Johansen, A.G. (2018), The do's and don'ts of using public Wi-Fi. Available at: https://us.norton.com/internetsecurity-wifi-the-dos-and-donts-of-using-public-wi-fi.html

[2] CBS Boston, (2018). Hacker Demonstrates Security Risk of Free Public Wi-Fi. Available at: https://www.youtube.com/watch?v=1OVTmrXGHyU/

[3] Johansen, A.G. (2020), Public Wi-Fi Security: Why public Wi-Fi is vulnerable to attack. Available at: https://us.norton.com/internetsecurity-wifi-public-wi-fi-security-101-what-makes-public-wi-fi-vulnerable-to-attack-and-how-to-stay-safe.html

[4] Hougen, A. (2020), Dangers of Public Wi-Fi: What you need to know in 2020. Available at: https://www.cloudwards.net/dangers-of-public-wifi/

[5] Griffith, E. (2020), 14 Tips for public Wi-Fi hotspot security. Available at: https://www.pcmag.com/how-to/14-tips-for-public-wi-fi-hotspot-security/

[6] NSA (2020). Mobile Device Best Practices. Available at: https://media.defense.gov/2020/Jul/28/2002465830/-1/-1/0/Mobile_Device_UOO155488-20_v1_1.PDF

[7] Cynet (2021). LLMNR & NBT-NS Poisoning and Credential Access Using Responder. Available at: https://www.cynet.com/attack-techniques-hands-on/llmnr-nbt-ns-poisoning-and-credential-access-using-responder/

[8] NSA (2019). Update and Upgrade Software Immediately. Available at: https://media.defense.gov/2019/Sep/09/2002180319/-1/-1/0/UPDATE AND UPGRADE SOFTWARE IMMEDIATELY.PDF

[9] NSA (2019). NSA's Top Ten Cybersecurity Mitigations Strategies. Available at: https://media.defense.gov/2019/Jul/16/2002158046/-1/-1/0/DDD-190716-666-071.PDF

[10] California Community Colleges (2021). Link Local Multicast Name Resolution (LLMNR0 and NetBIOS Name Service (NBT-NS). Available at https://cccsecuritycenter.org/remediation/llmnr-nbt-ns/

[11] CISA (2016). WPAD Name Collision Vulnerability. Available at https://us-cert.cisa.gov/ncas/alerts/TA16-144A

[12] Active Directory Security (2016). Securing Windows Workstations: Developing Secure Baseline. Available at https://adsecurity.org/?p=3299

[13] VMware® (2020). Creating Virtual Machines in VMware® Workstation. Available at https://www.kb.vmware.com/s/article/1018415/

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Trademarks

Wi-Fi is a registered trademark of Wi-Fi Alliance. • Bluetooth is a registered trademark of Bluetooth SIG, Inc. • VMware is a registered trademark of VMware, Inc. • MITRE ATT&CK is a registered trademark of The MITRE Corporation. • macOS is a registered trademark of Apple Inc. in the U.S. and other countries and regions. • Wi-Fi is a registered trademark of Wi-Fi Alliance.

Contact

Client Requirements / General Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media Inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov