coast mountain college

RESOURCE INF-015G

Wireless Wi-Fi Connectivity Guideline

Purpose

The purpose of this guideline is to secure and protect the information assets owned by Coast Mountain College (CMTN) and to establish awareness and safe practices for connecting to free and unsecured Wi-Fi which may be provided by the College.

Overview

CMTN provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. CMTN grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

Definitions

Keylogger: The action of recording or logging the keystrokes on a keyboard.

Wi-Fi: A term for certain types of wireless local area networks (WLANs) that use specifications in the 802.11 family.

Wireless: A term used to describe telecommunications in which electromagnetic waves, rather than some form of wire, carry the signal over all or part of the communication path.

Wireless Access Point (AP): A device that allows wireless devices to connect to a wired network using Wi-Fi or related standards.

Scope

This guideline addresses the wireless connection of CMTN-owned devices in remote locations.

Details

Coast Mountain College Wi-Fi Network

The CMTN Wi-Fi network is provided on a best-effort basis, primarily as a convenience to employees and others who may receive permission to access it. For employee business use, it is designed to be a supplement to, and not a substitute for, the production-wired local area network. For non-employees, it is also provided as a convenience, primarily as a way for members to access CMTN online products and services.

Staff may easily demonstrate CMTN online products and services to members or prospects. Wi-Fi access points, located at the Court Street facilities and in most branch offices, allow for compatible wireless device connectivity.

Microwaves, cordless telephones, neighboring APs, and other radio frequency (RF) devices that operate on the same frequencies as Wi-Fi are known sources of Wi-Fi signal interference. Wi-Fi bandwidth is shared by everyone connected to a given Wi-Fi access point (AP). As the number of Wi-Fi connections increases, the bandwidth available to each connection decreases and performance deteriorates. Therefore, the number and placement of APs in a given building is a considered design decision. Due to many variables out of direct CMTN control, availability, bandwidth, and access is not guaranteed.

The CMTN Wi-Fi network and connection to the Internet shall be:

- secured with a passphrase and encryption, in accordance with current industry practice
    - Passphrases will be of appropriate complexity and changed at appropriate intervals, balancing security practice with the intended convenient business use of the Wi-Fi.
- physically or logically separate from the CMTN production-wired local area network (LAN) and its resources
- provided as a convenience for the use of CMTN employees, their vendors while visiting the College, the members of CMTN, and other visitors with CMTN's express permission via provision of an appropriate passphrase
- optionally provided to members and qualifying visitors, by CMTN staff, with the provision of an appropriate passphrase and may be accessed only with the agreement to acceptable use policy statements provided online or in a written or verbal format
- accessed by employees only in accordance with INF-001, *Acceptable Use of Information Systems Policy* and its cross-referenced policies
- used for access to the CMTN production LAN only for business use and with the approved use of a CMTN-issued virtual private network (VPN) connection.

CMTN's Wi-Fi service may be changed, the passphrase re-issued or rescinded, the network made unavailable, or otherwise removed without notice for the security or sustainability of CMTN business.

Public Wi-Fi Usage

When using Wi-Fi on a mobile device in a public establishment, the following precautions should be followed.

Do:

- As with any Internet-connected device, defend your laptop, tablet, phone, etc. against Internet threats. Make sure your computer or device has the latest antivirus software, turn on the firewall, never perform a download on a public Internet connection, and use strong passwords.
- Look around before selecting a place to sit, consider a seat with your back to a wall and position your device so that someone nearby cannot easily see the screen.
- Assume all Wi-Fi links are suspicious, so choose a connection carefully. A rogue wireless link may have been set up by a hacker. Actively choose the one that is known to be the network you expect and have reason to trust.
- Try to confirm that a given Wi-Fi link is legitimate. Check the security level of the network by choosing the most secure connection, even if you have to pay for access. A password-protected connection (one that is unique for your use) is better than one with a widely shared passphrase and infinitely better than one without a passphrase.

- Consider that one of two similar-appearing service set identifiers (SSIDs) or connection names may be rogue and could have been setup by a hacker. Inquire of the manager of the establishment for information about their official Wi-Fi access point.
- Avoid free Wi-Fi with no encryption. Even if your website or other activity is using https (with a lock symbol in your browser) or other secure protocols, you are at much greater risk of snooping, eavesdropping, and hacking when on an open Wi- Fi connection (such as at Starbuck's, McDonald's, some hotels).
- Seek out Wi-Fi connections that use current industry-accepted encryption methods and that generally require obtaining a passphrase from the establishment.
- Consider using your cell phone data plan for sensitive activities rather than untrusted Wi-Fi, or your own mobile hotspot if you have one or have been provided with one.
- If you must use an open Wi-Fi, do not engage in high-risk transactions or highly- confidential communication without first connecting to a virtual private network (VPN).
- If sensitive information absolutely must be entered while using a public network, limit your activity and make sure that, at a minimum, your web browser connection is encrypted with the locked padlock icon visible in the corner of the browser window, and make sure the web address begins with https://. If possible, save your financial transactions for when you are on a trusted and secured connection, at home, for instance. Passwords, credit card numbers, online banking logins, and other financial information is less secure on a public network.
- Avoid visiting sites that can make it easier or more tempting for hackers to steal your data (for example, banking, social media, and any site where your credit card information is stored).
- If you need to connect to the CMTN network and are authorized to do so, choose a trusted and encrypted Wi-Fi AP or use your personal hotspot. In every case, you must use your CMTN-provided VPN at all times. The VPN tunnel encrypts your information and communications and besides, hackers are much less likely to be able to penetrate this tunnel and will prefer to seek less secure targets.
- In general, turn off your wireless network on your computer, tablet, or phone when you are not using it to prevent automatic connection to open and possibly dangerous APs. Set your device to not connect automatically to public or unknown and untrusted networks.

Finally,

Do Not:

- Leave your device unattended, not even for a moment. Your device may be subject to loss or theft, and even if it is still where you left it, a thief could have installed a keylogger to capture your keystrokes or other malware to monitor or intercept the device or connection.
- Email or originate other messages of a confidential nature or conduct banking or other sensitive activities, and definitely not when connected to an open, unencrypted Wi-Fi.
- Allow automatic connection to or connection to the first Wi-Fi AP your device finds, as it may be a rogue AP set up by a thief. Rather, choose the one that is known to be the network you expect and have reason to trust.

Related Policies, Guidelines, and Other Resources

- INF-001, *Acceptable Use of Information Systems Policy*