◊ Change the default name of your wireless network. Leaving the default name could allow criminal actors to pinpoint your specific router. This allows them to exploit any weaknesses the router might have.

◊ Use WPA2 secure access mode with a strong Wi-Fi Password (15-20 characters, alphanumerical, and symbols). Also, ensure you change it regularly.

◊ Change the default admin login information, and disable remote access on your router. When remote access is disabled, you have to be directly connected to the network to change settings in the router.

◊ If your home router has a "Guest Network" capability, consider enabling it, so you don't have to give visitors access to your main network. Be sure to change the default password to prevent casual users from accessing your network, especially in high-density residential areas.

Connecting to any Wi-Fi that you do not have control of is risky. However, if you are going to connect to a publicly accessible secured Wi-Fi or network—never connect to unsecured Wi-Fi or networks!—follow these steps:

◊ Check the legitimacy of the Wi-Fi to which you want to connect. Criminal actors can name their Wi-Fi anything to entice you to connect (e.g., Free Wi-Fi, Airport Wi-Fi, Coffee Shop Wi-Fi).

◊ Use a VPN to access the Internet after connecting to the Wi-Fi network. This will secure and encrypt your transmitted data in addition to the security provided by websites using secure (https) connections.

◊ Today, most devices, during the initial network or Wi-Fi connection, will offer the option to make your device discoverable. Make sure your device is undiscoverable.

INSIDER THREAT

from a cybersecurity perspective

Wanda T. Jones-Heath
Chief Information Security Officer
(CISO), DAF
Twitter: @SAF_DCIO
@SAF_CISO
https://www.safcn.af.mil/ciso/

Air Force Cybersecurity
To assure the effectiveness of
Air Force's core
missions by increasing the
cybersecurity and resiliency
of systems and information

The Accidental or Unknowing Insider

Normally, when we discuss the insider threat, we refer to employees or contactors who knowingly use their authorized access to sensitive information or privileged accounts to do harm to the company or organization.

However, another form of insider threat should be recognized, which is the unknowing or accidental insider. This type of insider does not intend to harm their company or organization. Instead, their actions lead to breaches in the network, access to accounts, or compromised sensitive information. These actions may be induced by cybercriminals or simply the lack of adherence to good practice.

The following sections explain a few of the most common ways that accounts, systems, devices, or information can be compromised by an unknowing insider.

Phishing and Vishing

Phishing is the easiest way for criminal actors to gain access. Phishing is defined as the fraudulent practice of sending seemingly legitimate emails from reputable companies in order to entice individuals to provide personal or sensitive information, click on malicious links, or open harmful attachments. Vishing is the telephone equivalent: criminals pose as agents of legitimate companies and request sensitive information.

In 2019, the FBI's Internet Crime Complaint Center (IC3) received 23,775 complaints in regard to email compromise that resulted in the loss of over $1.7 billion.

Here are a few ways and techniques to help you identify and avoid phishing attacks:

◊ Do not give personal information, account information, or usernames and passwords to anyone who requests them via email or over the telephone. Legitimate companies and organizations will not request this information via unsecure email or telephone.

◊ If you receive such a request, contact the company's customer support function through their website or published phone numbers.

◊ Do not click or use the link in the email as it could lead you to a fake site that looks identical to the real site or lead you to download malicious software.

◊ Do not open any attachments received via email before they are scanned with an anti-malware application. Attachments can run scripts or install malicious software onto your device.

Unlocked Systems or Devices

CACs are always removed from our systems before we leave our workstations. This ensures that the system is locked, and you keep positive control of your CAC. But do you lock your personal computer or device when you leave them unattended? You should. Even at home, when no one else has access to it, you should make it a habit to log out of or lock your device.

When you leave your device unlocked, you leave your information vulnerable, which can potentially allow unauthorized actors access. This would allow them to assume your identity on any application, social media, bank, or email account that you are still logged into on that system.

Whether it is your personal device or GFE, lock the system when it is not in use.

Passwords

Passwords are the key to everything virtual. Whether it is an account; application; device; or system, it is protected by a password or Personal Identification Number (PIN). Today, most sites and applications have specific requirements that assist in strong password generation. Even with a strong password, you still need to follow additional steps to secure your accounts and devices. Here are a few:

◊ Change your password regularly.

◊ Do not reuse your password. Always make them unique. This includes mirroring or changing one character in the password (e.g., 1234 to 4321 or 1234 to 1235). Consider using passphrases to construct secure passwords.

◊ Do not use personal information in your passwords. Personal information in this case refers to anything in your day-to-day life as well as PII (i.e., pet names, kid's names, street addresses, phone numbers, birthdays, anniversaries, etc.).

◊ Do not discuss your passwords, give them to anyone, or write them down.

◊ Consider using a password "vault" application. These applications eliminate the need to write down passwords and allow for construction of site-unique, strong passwords that do not rely on human memory.

Unsecured Networks & Wi-Fi

Another easy way for criminal actors to gain access to your devices, systems, and information is through unsecured networks or Wi-Fi. Once criminal actors gain access to your home network, your devices connected to that network become vulnerable.

Follow these easy tips to secure your home network: