Nefarious Networks [1]

Nefa

Sharon settled into the coffe
inhaled the sweet scent of her la
day off, she was feeling productive
get a little work done as the latte
her WiFi settings, expecting to v
boxes in order to connect to the
surprise, the first network on the li
WiFi-Officalxx". Excellent, she thoug
the university

Sharon frowned. Something
something very suspicious about
named network. Although she d
she knew better than to linger there
she could safely connect to the r
the campus VPN, she connected
and started up her VPN connectio
her, her intuitions were right. Altho
legitimate, fake networks are an
and can be used by criminals to m
and harvest your personal d
connecting to trusted networks a

Image note: The image that was initially used with this campaign has been switched out for the image above due to concerns about the appearance of the woman depicted. A number of people thought the woman appeared to be wearing a head scarf, leading them to believe that she was a Muslim woman. Please know that was not the case and it was not our intent to depict a Muslim woman. In fact the woman in the original image is an employee of the Office of Information Technology who has long dark hair. We blur the images in order to guard their identities and also lend a bit of intrigue to the stories. We apologize for the wrong impression the image and text may have provided.

Be Watchful of your WiFi

When the Internet first became popular, the only way you could connect to it was physically. This meant you had to manually take a cable (often an Ethernet cable) and connect it to your computer or laptop. This cable then connected you to a local network which connected to the Internet. While inconvenient for the end user, physical cables helped protect our organization. They allowed us to control who had and did not have access to our networks. However, users needed a simpler and faster way to connect to networks, one that did not require physical cables. Although they are incredibly convenient and revolutionized how with think about connectivity, Wi-Fi networks come with their own unique risks which you need to be aware of.

1. ### Monitoring

   First, remember that when you connect to a wireless network that anyone else can intercept and monitor your activity. All your online activity is simply converted into radio signals that are broadcast into the open air. These signals can then be intercepted by anyone close enough to you. This is especially true in public places such as hotels, airports, cafes, or conferences. Since anyone can intercept your Wi-Fi signals, just about anything you do online can be monitored.

   The best way to protect yourself is to **encrypt** all your online activities. When you're browsing on a public Wi-Fi network and aren't connecting to sites that use HTTPS (the encryption standard for web browsing), anyone on that network can see what you're doing; they can grab passwords sent in plain text, or they can potentially steal your browser cookies and pretend they're you. HTTPS is a significantly more secure version of HTTP, which is the protocol you generally use to load up your webpages (whether you're aware of it or not). HTTP stands for Hypertext Transfer Protocol, so HTTPS stands for the same thing but with "Secure" on the end of it. It means when you enter your password or your phone number or anything personal on Facebook—or any other site offering HTTPS—that data will be encrypted as it flies through the great tubes of the internet.Checking for web encryption is easy, just look at your browser's menu bar. If the URL begins with HTTPS, you're safe.

   HTTPS is enabled by default on most reputable websites, but many sites have varying

degrees of safety. For encryption across the whole internet, the Electronic Frontiers Foundation recommends HTTPS Everywhere [2] (Chrome/Firefox Add-On) or SSL Enforcer [3] (Chrome Extension).

In addition, it's a good idea to check to see if you can use a VPN (Virtual Private Network) [4] for remotely connecting back to our organization. This will allow you to use the UCB Wireless Network from anywhere, giving you the security benefits of the university's network wherever you go.

2.

Connecting to a WiFi Network

Connecting to a wireless network first begins by selecting the network you want to connect to. In crowded or public places, there is often multiple networks to choose from. However, always be careful which network you are connecting to. Cyber criminals can create counterfeit or fake wireless networks that are designed to harm or monitor everything you do. To protect yourself, always make sure you are joining a trusted network. When you are at work, your network administrator will tell you which wireless networks you can join. These networks almost always will require a login and password. You can trust these networks as they are administered by our organization. When you want to connect to Wi-Fi networks in public places (such as hotels or airports) look for posted signs telling you which wireless networks are legitimate and how to join them. By making sure you only connect to trusted wireless networks, you protect yourself against these and other attacks.

That doesn't mean you should avoid your local coffeeshop's WiFi like the plague. Here are some tips for staying safe while out and about:

TURN OFF SHARING - When you're at home, you may share files, printers, or even allow remote login from other computers on your network. When you're on a public network, you'll want to turn these things off, as anyone can access them—they don't even need to be a hacker, and depending on your setup, some of that stuff probably isn't even password protected.

For Windows: Open your Control Panel, then browse to Network and Internet > Network and Sharing Center, then click Choose Change Advanced Sharing Settings. Once here, you should definitely turn off file and printer sharing, and you may as well turn off network discovery and Public folder sharing. Some of this is done automatically by Windows if you specify the network as public.

For Mac: Go to System Preferences > Sharing and make sure all the boxes are unchecked. You'll also want to turn off network discovery, which will be in the same place. This will prevent others from even seeing your machine on the network, meaning you're less likely to be targeted. On Windows (as I mentioned), it's just another check box under advanced sharing settings. On OS X, it will be called "stealth mode" and be under your firewall's advanced settings.

ENABLE YOUR FIREWALL - Most OSes come with at least a basic firewall

nowadays, and it's a simple step to keeping unwanted local users from poking at your computer. You may already be using a firewall, but just in case, go into your security settings (in Windows under Control Panel > System and Security > Windows Firewall; and on a Mac under System Preferences > Security & Privacy > Firewall) and make sure your firewall is turned on. You can also edit which applications are allowed access by clicking on "allow a program or feature" in Windows and "advanced" in OS X. Your firewall is not an end-all, be-all protector, but it's always a good idea to make sure it's turned on.

3.

Creating a Wireless Network

If you are going to install a Wi- Fi wireless network at home, take the following steps to protect yourself.

• Be sure to change the default administrative login and password on your Wi-Fi access point. The simplest way for cyber criminals to hack into any Wi-Fi network is simply scan the entire Internet and log into Wi-Fi access points with default logins and passwords.

• By default, most WiFi networks are open, allowing anyone to join them. Make sure your wireless network requires a login and password to join it. This protects your home network from cyber criminals accessing your computers, or protects you from criminals using your wireless network to attack others.

• By default, most Wi-Fi networks are in the clear, meaning anyone can intercept and monitor your activity. Make sure you enable the latest version of encryption in your Wi-Fi network. This ensures your activities cannot be monitored. Remember, older versions of encryption (such as WEP) are outdated and offer little security. Your router should come with detailed instructions on how to configure various levels of security.

UCCS Help Desk [5]	**UC Denver & Anschutz Help Desk** [6]	**CU Boulder Help Desk**
719.225.3536	303.724.4357	303.735.4357
helpdesk@uccs.edu [8]	UCD-ITS-HELPDESK@ucdenver.edu [9]	help@colorado.edu [10]

Source URL:https://www.cu.edu/nefarious-networks

Links
[1] https://www.cu.edu/nefarious-networks

[2] https://www.eff.org/https-everywhere [3] https://chrome.google.com/webstore/detail/kb-ssl-enforcer/flcpelgcagfhfoegekianiofphddckof?hl=en [4] https://oit.colorado.edu/services/network-internet-services/vpn [5] http://www.uccs.edu/~helpdesk/ [6] https://www1.ucdenver.edu/offices/office-of-information-technology/ [7] https://oit.colorado.edu/support/it-service-center [8] mailto:helpdesk@uccs.edu [9] mailto:UCD-ITS-HELPDESK@ucdenver.edu [10] mailto:help@colorado.edu [11] mailto:help@cu.edu