

Your naked computer in the wild! Staying safe on public Wi-Fi!

BRIAN MENDONCA
PHOENIX IT SUPPORT

DEPARTMENTS OF
ENTOMOLOGY AND NEMATOTOLOGY
PLANT PATHOLOGY
PHOENIX CLUSTER



Fact: Not every network you connect to is secure!

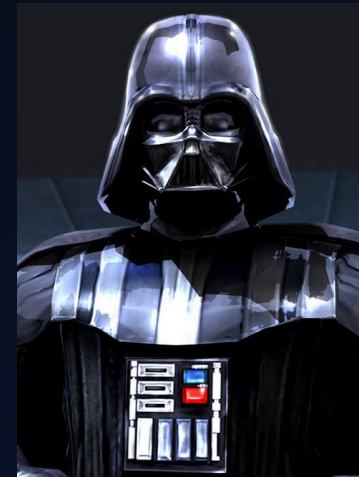
- Any network where other people you don't know or trust can connect to should be considered insecure.
- Insecure networks can be spied on and manipulated by bad guys.
- Today, we will go over some of the techniques the hackers use and how you can protect yourself!

Network Map

Potential Unfriendlies

The router you connect to for internet

Your laptop



You trust the networks you regularly connect to, but....

- This is the way how trouble can happen....
 - Moobilenet
 - Moobilenetx
 - Attwifi (Wifi commonly found at most Starbucks)
 - Marriott_Guest (Hotel wifi)
 - 2WIRE790 (Commonly given by AT&T for home routers)
- Just because it looks trustworthy, doesn't mean it is. Here's why....

Network Spoofing

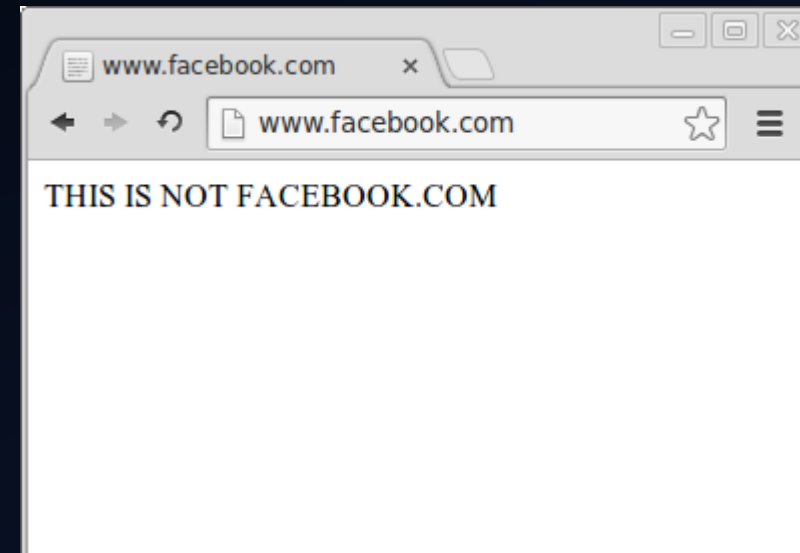
- Bad guys can make fake “wireless routers” that have the same name as the Wifi you normally connect.
- If your computer connects to a fake network that it thinks it knows and trusts, then it connects to the hacker’s network.

I'm moobilenet!
You know me
already! Connect
to me!



Then more trouble...

- Depending on how in depth the hackers went, they would be able to set up very authentic looking webpages that most victims would try to log in:
 - Facebook
 - Gmail
 - Ebay
 - Amazon
- The point is to collect your usernames/password attempts as you try to log into the fake website

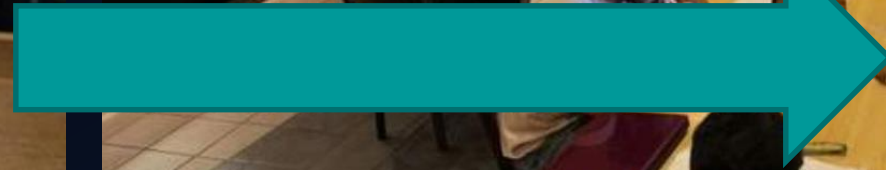
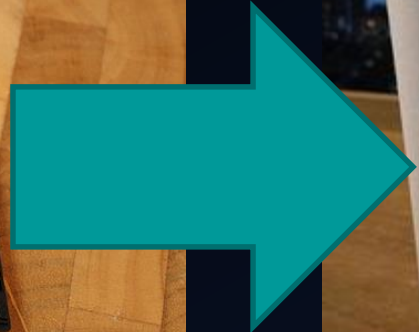






Real life application time! Here's how it is for hackers!

- Buy honeypot hardware and program it to put out the bait.
- Hide it in coffee cup
- Go to Starbucks
- Profit.

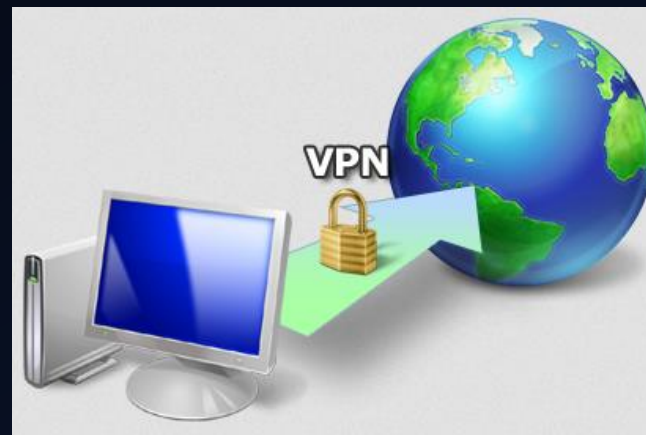


Your counter attack!

- It's not necessarily antivirus software or firewalls that protect you from this style of hack (but you should still have them!)
- Good computing behavior and being vigilant will protect your computer more than anything else when you are traveling away from your home network.

Defense Mode:

- Avoid connecting to public wireless networks unless absolutely necessary. Do not connect to open wireless networks you are unfamiliar.
- If you have a VPN (Virtual Private Network), use it. Many free and paid ones available. Tip: Paid ones are usually worth it. Can you trust the free VPN provider with your data?



Defense Mode:

- No VPN? Consider purchasing personal mobile hotspots. Smartphone LTE/4G tethering is good too.
- Avoid typing in passwords or sensitive information when on a possibly insecure network. Anything you type or send can be taken and used against you.
- Be on the lookout for suspicious people within the Wi-Fi range.
- Leaving campus for a trip? Plan your IT needs ahead a few weeks in advance.

Other strategies for when insecurity is certain

- Change your passwords/passphrases before going on your trip. After you return, change them back, even if you don't think the account has been stolen.
- If your account gets stolen, make sure you have a way to regain access to that account such as a recovery email address, tech support numbers, ways to prove your identity and account ownership to whoever is managing the account. Do these preparations BEFORE YOU LEAVE HOME.
- Enable two-factor authentication where you can. What is two factor-authentication?

How Phoenix IT and Campus IT are helping you

- Network Scanning: Automated tools are running on the network (including Moobilenet), looking for people who are trying to sniff or manipulate network traffic.
- Vulnerability scanning: Computers on our networks are regularly scanned for hacked and/or hackable machines.
- Website Scanning: Website applications are kept up to date with the current secure code practices and SSL certificates. You can verify a website's authenticity with these certs.
- CAS Authentication; all major UC Davis websites require CAS authentication; you can verify that you are actually entering your password on the legit website by viewing the certificate.

University of California, Davis

Identity verified

Permissions

Connection


The identity of University of California, Davis at Davis, CA US has been verified by COMODO Extended Validation Secure Server CA but does not have public audit records.

[Certificate information](#)



Your connection to cas.ucdavis.edu is encrypted with 128-bit encryption.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses DHE_RSA as the key exchange mechanism.



Site information

You first visited this site on Dec 18, 2014.

[What do these mean?](#)



UC DAVIS UNIVERSITY OF CALIFORNIA

Central Authentication Service (CAS)

Check the URL!  University of California, Davis (US)

The URL might not look exactly like this, but it will include a padlock, "University of California, Davis" and start with cas.ucdavis.edu

Secure Log In

Login ID:

Passphrase:

LOG IN

To access this secure UC Davis web page, please enter your UC Davis login ID and Kerberos passphrase.

For optimal security, please Log out and exit your web browser when you are done.

[Need Help?](#)

[Verify Site Certificate](#)



SECURITY NOTICES

Protect your campus computing account login ID and passphrase. Use them only for campus websites and campus online services.

UC Davis will never ask you to provide your passphrase via phone or email. A message that asks you to is probably a *phishing scam*. Delete it without responding.

Be extremely wary of messages that ask you enter your passphrase into a non-UC Davis website. If you have doubts about a message or website, or think you have been tricked into submitting your passphrase or personal information, call the IT Express Computing Services Help Desk at 530-754-HELP (4357).



QUESTIONS?