Safe web browsing

INFOSEC

The big problem online is malware, right?

Staying safe online means being on the lookout for phishing attacks, spoofing and fraudulent sites, and being careful about what information you give out.

Wait, what's spoofing?

"Spoofing" is when attackers copy identities and imagery to impersonate sites, email addresses or links. Spoofed sites are especially dangerous. Often, the only difference is a single letter in the URL. Always make sure it's is the real thing.

How can I spot a phony link?

Hover your mouse over the link. Does the URL displayed contain a lot of random letters and numbers? Is it using HTTP instead of HTTPS? All of these are red flags.

http://gsdjx5sc4m.com/h4xyouraccounts325/

What should I do if I get a suspicious browser warning?

Close the entire tab or window. Don't click any "close" or X buttons it may offer, since those can be concealing malware download links. Run an antivirus scan, just in case.

What's the difference between HTTP and HTTPS?

HTTP stands for Hypertext Transfer Protocol. HTTPS, or HTTP Secure, is an updated version of HTTP where the communication protocol is encrypted. This is much safer than ordinary HTTP. Never send sensitive information over any site that doesn't use HTTPS!

I just got a browser pop-up about my computer having a virus. What should I do?

Don't click it! The phony browser warning is a common trick online. If it wants you to interact with it, such as clicking a button or running a scan, it's not a real warning. Real browser warnings will ask you not to do something.

UPDATE YOUR ANTIVIRUS

What's one thing I can do to stay safe while browsing?

Use safe channels when you're browsing. Visit sites through bookmarks rather than following links. If you have to follow a link, inspect it before clicking on it. Secure your connection by setting up a VPN, or Virtual Private Network.