How Can Your Email Account be Hijacked?

An email account can be hijacked in a number of ways. **Phishing** attacks in which a hacker subtly persuades a user into revealing login passwords are a common hijacking technique. A message, purportedly from your bank or other trusted partner, may tell you that a "security check" requires you to respond with your password. Such claims are always bogus; legitimate organizations never ask you to reveal your password via email, phone, or other means.

Many forms of **malware** (viruses, spyware, etc.) attack for the purpose of gaining access to your computer, in order to *enslave it* in a botnet, and use it as a *spam spewing device*. This can happen without you even knowing, until people from all over the world start accusing YOU of being a spammer!

Keylogger spyware installed on your computer can record every keystroke you type and send the results to a remote operator who can then read your password from the log file. This is not likely to happen unless you are using a public computer.

Failing to log out of an account when you've finished a session makes it easy for anyone who has access to the computer you used to hijack your account. Always log out of accounts accessed from shared computers, such as those in libraries, computer labs, Internet cafes, etc. A browser's auto-fill forms feature may reveal your password to someone who uses the same computer you use.

Server-level attacks against email providers, online stores, or financial institutions go after the password database, attempting to crack its security and harvest thousands or millions of email addresses and passwords in one swoop. There's not much you can do to prevent this type of attack except to host email only with a reputable service provider who pays attention to security, and use a secure password.

Network packet monitoring software (called “sniffers”) can sniff out passwords sent over unsecured wireless connections. You should be aware of this type of attack if you use **free wifi** in a coffee shop, airport, hotel, etc. Use encrypted (https) connections when logging in or emailing over unsecured public wireless networks.

It's also a good idea to enable the **firewall** (just type *firewall* in the search box of the Start menu) built into your laptop, even when using secured hotspots. A

personal firewall can protect your data against other hotspot users. If you are connecting via wifi on a Windows computer, choose the "Public" option when asked what type of network you're on.

You should **disable file and printer sharing** on your laptop before going out in public with it. Whatever data you allow to be shared on a network is available to other users of a wireless hotspot.

If you use webmail, or any other website that requires a login password, look for the "https" in the website address. As long as you're on a page with an address that begins with https, the data you send and receive is protected from sniffers and snoopers. That *s* is your assurance that your connection is encrypted. If you use Outlook, Thunderbird, Windows Live Mail or another desktop email program, adjust your account settings to require a secure connection when sending or receiving mail.

Your connection is almost always encrypted when using online banking, or making a purchase on the web. But other venues, such as online forums or your web-based email may NOT use an encrypted connection. Gmail, Yahoo Mail, Outlook.com, and Facebook are fully encrypted, so you're safe there. Be aware that some sites offer a secure login page, but after you're logged in, they revert to non-encrypted mode! (For mobile users, the Gmail app on Android smartphones and tablets is secure.)

What does all this mean? **If you don't see HTTPS in the address bar** of your browser, anything you read or post online, as well as any email you send or receive while using a public wifi connection may be exposed. If you enter a username and password on a website that doesn't offer HTTPS encryption, it's the equivalent to holding up a sign with your login credentials.

Consider **disabling your device's WiFi adapter when it's not in use**. This prevents your device from automatically connecting to any wireless hotspot you may pass. On smartphones, this will be found in the Settings dialog. Most laptops have a button or switch that makes enabling and disabling a WiFi adapter quick and easy.