Email hygiene

Phishing – when a con-artist “phishes” for victims—is far and away the most common attack over the internet. An attacker sends a malicious email to a victim and persuades the victim to open an attachment or visit a compromised website. After the victim bites, the attacker owns the victim computer, tablet, or cell phone.

Spear-phishing is when a con-artist tailors a solicitation specifically for a victim. Spear-phishing is scary because it means somebody did homework on that victim. See *Social Media*, below.

One of the best phishing war stories is the one about Hilary Clinton's campaign manager, John Podesta, and the Democrats in 2016. Podesta opened an email claiming to come from Google and it said he needed to reset his Gmail password. He followed the link, logged into what he thought was Google, and gave Russian attackers his email password. And that was one link in a chain of events that led to the Democrats airing their dirty laundry on Wikileaks.

Poor email hygiene is on both sides of the political aisle. Apparently, Colin Powell, Republican former Secretary of State, also fell for a similar scheme.

Phishing attacks are successful because anyone can impersonate anyone else in an email. It’s an architectural weakness from the dawn of the internet. There are lots of proposals to address this problem, but nobody has a foolproof solution and none are coming in the foreseeable future.

Don’t trust emails claiming to come from your bank or your best friend. Don’t open attachments unless somebody you trust looks you in the eye and promises the attachments aren't malicious. Hover over links and make sure they point where they claim to point before following them.

Here are a few links for more information:

- How to spot a phishy email from a mile away: http://dgregscott.com/week-2-day-2-spot-phishy-email-mile-away/
- How to spot a phishy email http://dgregscott.com/spot-phishy-email/
- Spam and phishing: Recognizing phishing scams: http://dgregscott.com/spam-phishing-mini-seminar/

You probably don't keep national security secrets in your computer. But you do keep information important to you, and if you fall for a phishing scheme, somebody else will own you, your devices, and all the information inside. Don't be a victim. Do be smarter than politicians who should know better.

For your own protection, learn how to spot phishy spam emails and learn how to decipher email headers. Don't hide behind, "I'm not technical," because identity thieves prey on the unprepared.