Subject: Topics for Thanksgiving Dinner with the Family (Technology Safety)

11/21/2022

Not sure what to talk about with your family at the Thanksgiving table, technology security is a great topic, and you may just help save Aunt Sally's photos and Uncle Buck's recipe for Mushroom Soup.

Topic 1: Keeping your computer up-to-date

Keeping your computer up-to-date with the most recent patches is one of the most significant tasks you can perform to keep your computer safe.

Windows Users - Microsoft releases new patches on the second Tuesday of every month. Occasionally additional Patches are released outside of the regular schedule.

Microsoft Windows Update Link - This link outlines how to turn on automatic updates

MacOS Users - Apple releases updates every two to three months

macOS Update Link – This link outlines how to manually and automatically check for updates

Chromebook Users – Chromebooks are updated often; sometimes, mutiple updates will come out in a week.

Chromebook Update Link – This link outlines how to update your Chromebook and the notification color code system.

Topic 2: Passwords

A strong password is a password that is long and complex.

Length - Experts vary on the minimum length of a password. Most experts agree that 12 or longer is a minimum

Complexity – Passwords need to be complex (Upper and Lower Case letters, numbers, and Special Characters) but also need to be memorable. I suggest using a passphrase. A passphrase is a sentence-like string of words, numbers, and characters used for authentication that is longer than a traditional password, easy to remember, and difficult to crack.

https://www.useapassphrase.com/ is a site that will check the strength of passwords. For example, the password "Turkey(82)Drive7:45am " is estimated to take over 33,000,000 centuries to crack; very secure. Easy for the user to remember

- Turkey = street the Jr./Sr. HS is on
- (82) = street address of the Jr./Sr. HS

- Drive7:45am = start time of the Jr./Sr. HS

Topic 3: General Tips for recognizing Spam/Phishing email

1. The sender's address isn't correct. Check if this address matches the name of the sender and whether the domain of the company is correct. To see this, you must make sure your email client displays the sender's email address and not just their display name. Sometimes you need to train hawk eyes at the address since spammers have some convincing tricks up their sleeve. For example: From 'Joseph Monastero irr_1@badguy.com
2. The sender doesn't seem to know the addressee. Is the recipient's name spelled out in the email, and are you being addressed as you would expect from the sender? Does the signature match how this sender would usually sign their emails to you? Your bank usually does not address you in generic ways like "Dear customer." If the email is legit and clearly intended for you, then they will use your full name.
3. Embedded links have weird URLs. Always hover first over the links in the email. Do not click immediately. Does the destination URL match the destination site you would expect? (Once again, train those eagle eyes.) Will it download a file? Are they using a link-shortening service? When in doubt, if you have a shortcut to the site of the company sending you the email, use that method instead of clicking the link in the email.
4. The language, spelling, and grammar are "off." Is the email full of spelling errors, or does it look like someone used an online translation service to translate the mail into your language?
5. The content is bizarre or unbelievable. If it is too good to be true, it probably isn't true. People with lost relatives that leave you huge estates or suitcases full of dollars in some far-away country are not as common as these scammers would have us believe. You can recognize when email spam is trying to phish for money by its promises to deliver great gain in return for a small investment. For historical reasons, we call this type of spam "Nigerian prince" or "419" spam. Tips were pulled from Malwarebytes Labs - June 19, 2018 https://blog.malwarebytes.com/101/2018/06/five-easy-ways-to-recognize-anddispose-of-malicious-emails/

Good methods on Preventing Phishing Federal Trade Commission https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Topic 4. Artemis-I – Space Program - https://www.nasa.gov/artemis-1

A cool topic (Below is the overview from NASA)

Artemis I, formerly Exploration Mission-1,will be the first integrated flight test of NASA's Deep Space Exploration Systems: the Orion spacecraft, Space Launch System (SLS) rocket, with the newly upgraded Exploration Ground Systems at Kennedy Space Center in Cape Canaveral, Florida.

The primary operation goal of the mission is to ensure a safe crew module entry, descent, splashdown, and recovery. In addition to sending Orion on its journey around the Moon, SLS will carry 10 small satellites that will perform their own science and technology investigations. The first in a series of increasingly complex missions, Artemis I will provide a foundation for human deep space exploration and demonstrate our commitment and capability to extend human existence to the Moon and beyond prior to the first flight with crew on Artemis II.

Artemis I is foundational to the space economy, fueling new industries and technologies, supporting job growth, and furthering the demand for a highly skilled work force. Men and women in all fifty states are hard at work building the Deep Space Exploration Systems to support missions to deep space. NASA prime contractors, Aerojet Rocketdyne, Boeing, Jacobs, Lockheed Martin, and Northrop Grumman currently have over 3,200 suppliers contributing to the milestone achievement that heralds the success of America's human spaceflight program.

Enjoy the time with your family and friends

With respect
Joe