Sun City Summerlin Computer Club
Seminar

Cyber Security Refresher
2023

Tom Burt

November 29, 2023

Seminar Agenda

- **Introduction**
- **Data Loss**
- **Identity Theft**
- **Malware Ransomware Attacks**
- **Home Network Security**
- **Scams**
- **SPAM / Unwanted Ads**

Thanks to Jeff Wilkinson! I used some of his images.

Introduction

- **“Cyber Security” is a very broad topic. Computer Technology touches so many aspects of modern life.**
  - **Desktop and laptop PCs**
  - **Smart phones and landline phones**
  - **Televisions**
  - **Smart Home Devices (Alexa)**
  - **Automobiles**
- **We spend a lot of time “on line”**
  - **Social Media, News, Sports, Entertainment, Shopping, Investing, Banking, …**
- **All of these offer opportunities for adverse events.**
- **Our seminar today will review these to refresh and update you on risks, defenses and mitigations.**

Data Loss Overview

- **Data loss occurs when data stored on your PC or phone or a storage device, including “the cloud” is suddenly no longer available.**
  - **Documents, pictures, videos, financial information, databases, emails …**
- **Common causes …**
  - **Hard drive / solid state drive failure (mechanical or corruption)**
  - **Lost flash drive / memory card**
  - **Accidental deletion**
  - **Malicious software attacks - may delete or encrypt data or entire device**
  - **Forgotten password**
  - **Fire or flood, lightning strike, power surge**
  - **Theft**

Data Loss – Backing Up (1)

- **"Backing up" means *making a copy* of all or part of your device's hard or solid-state drive to another hard or flash drive.**
- **Why do it?**
  - **Hard drives are electro-mechanical devices – they BREAK DOWN. (but hard drive MTBFs are now 100,000+ operating hours)**
  - **Drives, their folders and files can become CORRUPT.**
  - **Even solid-state drives can fail, wear out or become corrupt.**
  - **Humans are fallible!! Sooner or later, you will DELETE or overwrite a file when you didn't mean to.**
  - **Malware of all kinds may attack your PC and DESTROY data.**
  - **Lightning may strike, fires happen, floods happen.**
- **Without backups, you may lose irreplaceable data**
  - **Family photos, music, videos, financial records, e-mail, …**
- **Replacing lost software may be difficult and expensive.**

Data Loss – Backing Up (2)

- **Disc Imaging**
  - **A disc image is a *copy* of an entire disc drive into a single big file on another (usually external) disc drive.**
  - **Disc images are compressed – about 2 to 1.**
  - **Images only contain "used" areas of the original partition(s).**
  - **A backup drive can normally hold *multiple* disc images.**
  - **Disc images are not directly bootable but contain all boot information.**
  - **A disc image can be *restored* (copied back) to a disc drive (including a replacement for a failed drive). Usually done by booting from a rescue DVD or flash drive.**
  - **With software help, a disc image file can be "mounted" as a logical drive. (This allows individual files to be retrieved from the image).**

Data Loss - Backup Tools

- Macrium Reflect 8 (annual subscription)
  - https://www.macrium.com/reflectfree
- Acronis Cyber Protect Home (annual subscription)
  - https://www.acronis.com/en-us/ or http://ugr7.com/
- CASPER by Future Systems Software
  - https://www.fssdev.com/products/casper/
- EaseUS ToDo Backup (free edition)
  - https://www.easeus.com/backup-software/tb-free.html
- Windows File History (built-in to Windows 8, 10 & 11)
- Windows File Explorer (built-in to Windows 8, 10 & 11)
- MacOS Time Machine

Data Loss – Cloud Backup for Data

- **Google Cloud (Google Drive) - *FREE***
  - **https://drive.google.com/drive/u/0/my-drive**
  - **Requires a Google / Gmail account**
  - **15-17 GB of free cloud storage**
  - **Install Google Drive app (Windows / Mac)**
  - **Specify a set of folders to be monitored and backed up to the Google Drive Cloud whenever a change is detected.**
- **Microsoft OneDrive - FREE**
  - **https://onedrive.live.com/about/en-us/**
  - **Requires a Microsoft Account**
  - **5 GB free (1 TB free if subscribed to Office 365)**
  - **Syncs from a OneDrive folder on your PC or device to your OneDrive cloud storage.**

Data Loss - Where to Buy a Back Up Drive

- **Shop the usual on-line tech stores:**
  - **www.amazon.com, www.walmart.com**
  - **www.newegg.com, www.bestbuy.com, www.officedepot.com**

- **For disc imaging, web search for a specific brand / size:**
  - **external "hard drive" "usb 3" 5-tb**
  - **Lots of hits – typical price about $110 for a 5 TB disc drive.**
  - **Ultra-slim drives may be slower.**

- **For just backing up data files, consider a flash drive or SD Card**
  - **USB 3 64GB, 128GB & 256 GB drives/cards quite affordable.**
  - **128GB USB 3 flash drive costs about $11.**

Identity Theft - Overview

- **Identity Theft occurs when a malicious actor or group obtains details of your personal information and your financial accounts.**
  - **Commonly this is used to open new credit accounts or use existing credit accounts and charge goods or services to them.**
  - **Thieves may impersonate you to gain access to your bank and brokerage accounts.**

- **Often, identity theft starts when information you gave to online merchants or services is stolen by "hackers" and sold on the "dark web" to other malicious actors.**
- **Every time you make an online purchase using a credit card, you've left a record on file that might leak.**
  - **You can't assume that all employees of merchants or services are honest, careful and reliable. They're human. Some are naive or not conscientious or not well-trained.**
- **Hackers often use "social engineering" (cons) to persuade people to give them information or allow them access.**

Identity Theft - Prevention (1)

- **Credit Bureau Freezes**
  - **Set up web accounts at Experian, Equifax and Trans Union.**
  - **Activate freezes on each account. Only unfreeze when applying for new credit.**
  - **This prevents bad actors from opening credit in your name.**

- **Change passwords on all financial accounts regularly.**
  - **Yes! It's a hassle, but nothing like having to deal with identity theft.**
  - **Avoid using the same ID and password on multiple accounts.**
  - **Use STRONG passwords (long, mixed digits, upper/lower case, special characters)**
  - **Use multi-factor authentication (see next slide)**
  - **Use biometric authentication if available (see next slide).**
  - **Set up a "verbal password" (if possible) to be used on all phone interactions.**

- **Use a password manager to manage your passwords**
  - **https://www.wired.com/story/best-password-managers/**

Identity Theft - Prevention (2)

- **Multi-factor Authentication**
  - https://www.keepersecurity.com/blog/2023/06/27/types-of-multi-factor-authentication-mfa/
  - **Combines something you know (Login ID, password) with something you have (smartphone, email, digital key device).**
  - **Problem is the details vary for each service provider you deal with.**
  - **Can also be difficult when cell service is poor or phone unavailable.**

- **Biometric Authentication**
  - https://ondato.com/blog/benefits-of-biometric-authentication/
  - **Facial recognition, fingerprint recognition, iris scan, …**
  - **Requires a webcam or other reading device (easy on smartphones, laptops).**
  - **Biometric data has to be registered at each institution, website you interact with.**
  - **Might be affected by changes such as beard, glasses, hair style, weight change.**
  - **Need a fallback protocol to simple ID / Password if biometrics aren't working.**

Identity Theft – Phishing Examples

- **Watch Out for Phishing Attempts**
  - **https://en.wikipedia.org/wiki/Phishing**
  - **Scam emails, phone calls, texts that attempt to trick the user into revealing personal details or to run malicious software. Caller-ID info can be "spoofed".**
  - **Phishing phone calls may just want to record your voice to use later in AI deep fakes.**
  - **Emails may be broad-based or targeted to specific individuals (spear-phishing).**
  - **Emails often have attachments that can execute malware or have links to fake websites.**
  - **Be skeptical! Check links by hovering your mouse.**

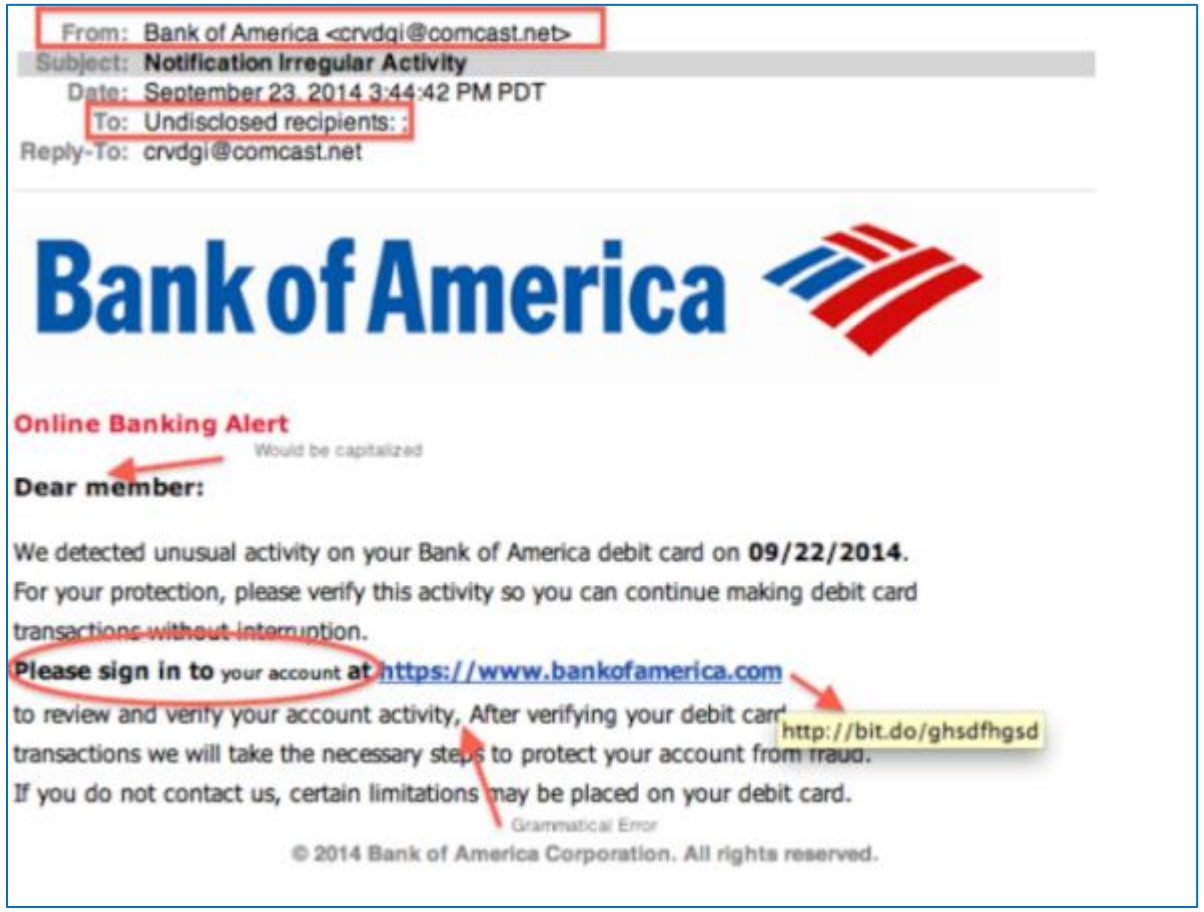
- **Phishing emails have gotten very sophisticated due to use of AI-based text writers and image editors.**
  - **Let's look at a few examples …**

- **Phishing phone calls often prey upon seniors**
  - **E.g. Bank/Broker needs to verify your account information**

Phishing Scams – Humor

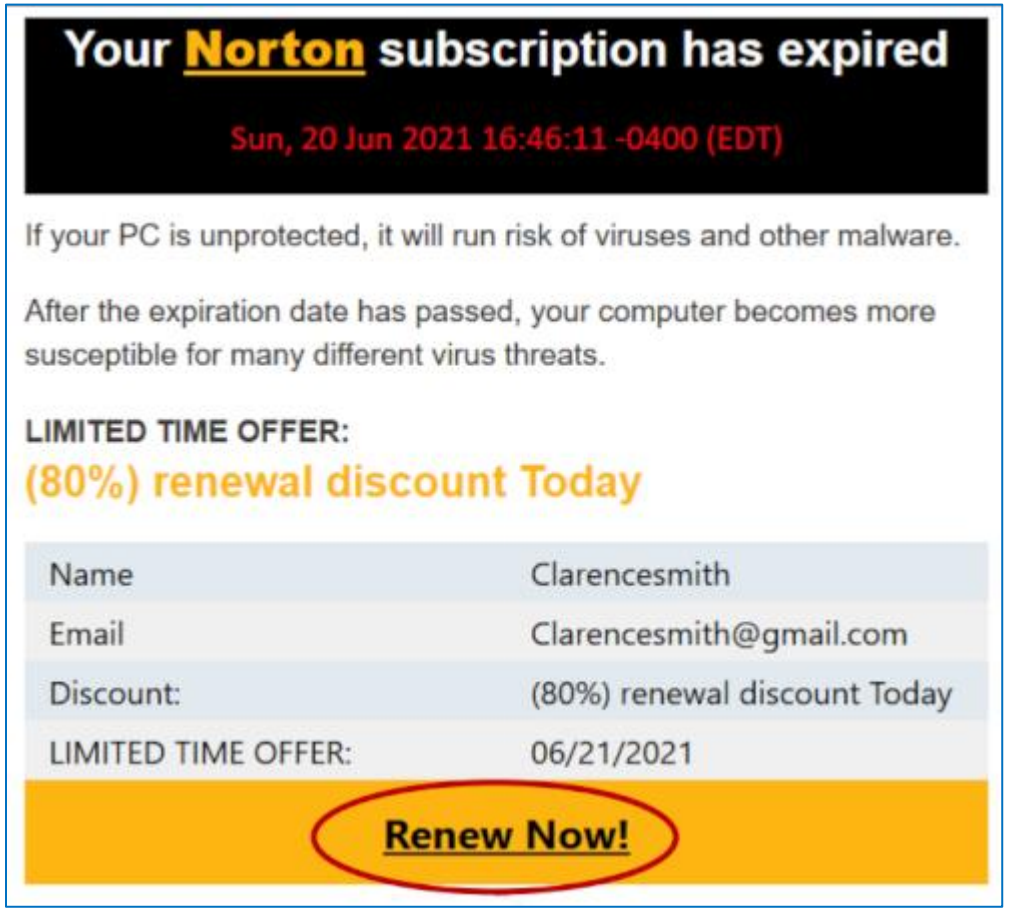
Source: dilbert.com

Phishing SCAM – Example 1



- **Clues that this email is a SCAM …**
  - From (Sender's) email address is not from B of A.
  - To: address is not a specific name.
  - Salutation is not a specific name.
  - Hover over the bankofamerica.com link and the actual link target is something else.
  - Grammatical error (comma should be period).
- **Goal of this email is to get you to click the fake link.**
  - Doing so will take you to a fake website (looks like B of A).
  - You will be asked to enter personal identification, account number(s) and your login credentials.
  - If you do this, they can empty your accounts.

Phishing SCAM – Example 2



Your Norton subscription has expired

Sun, 20 Jun 2021 16:46:11 -0400 (EDT)

If your PC is unprotected, it will run risk of viruses and other malware.

After the expiration date has passed, your computer becomes more susceptible for many different virus threats.

LIMITED TIME OFFER:

(80%) renewal discount Today

Name	Clarencesmith
Email	Clarencesmith@gmail.com
Discount:	(80%) renewal discount Today
LIMITED TIME OFFER:	06/21/2021

Renew Now!

- **No clues that this email is a SCAM except …**
  - **The Renew Now! link.**
  - **Hover over the link and it shows the actual link target is: https://gghj.s3.amazonaws.com/caa.html**
- **Goal of this email is to get you to click the fake link.**
  - **Doing so will take you to a fake website (looks like Norton).**
  - **You will be asked to enter personal information and a credit card number.**
  - **If you do this, they can use your credit card number to charge to your credit limit.**
- **You can check any hyperlink's domain (e.g. amazonaws.com) out at:**
  - **https://www.whois.com**

Malware Attacks - Overview

- **Malware (Malicious Software) is software that attempts to damage and / or steal data on your device or during your interactions with programs or the network.**
- **Windows PCs are most popular target, but ALL devices, including smartphones, are at some risk.**
- **There are various types of malware …**
  - **Spyware, including key loggers. Spyware scans your drives for "useful" information (account numbers, passwords, contact lists, tax returns, …) and sends it to the cybercrooks.**
  - **Data destroyers – attempt to wipe your data without any attempt at financial gain.**
  - **Ransomware – Encrypts your data and often makes it impossible to login to your PC. The cybercrooks demand you pay them a ransom, usually in Bitcoin, to get them to give you a decryption key and tool to resurrect your PC. (See next slide.)**
  - **SPAM Bots – Programs that hide on your device and use your network to send SPAM or malicious emails to other users.**
  - **Crypto Bots – Programs that hide on your device and perform crypto-mining for the financial benefit of cybercrooks.**

Ransomware Considerations

- **Ransomware is a virus infection that encrypts (scrambles) your PC's files and then demands a ransom in exchange for the decryption key / tool.**
  - **Sometimes ransomware has a time delay or event trigger (specific date/time).**
- **Ransomware scrambles files on *any attached disc drives*, including mapped network drives.**
  - **Files on File History backup drive are at risk.**
  - **Files in cloud folders on your PC are at risk.**
- **Best to frequently make a separate manual backup of essential / important data files. Back up to a flash drive, external hard drive or a cloud service.**
- **Also, it's wise to do a virus scan before making a clone or image backup.**
  - **You don't want to back up an infected hard drive.**

Ransomware Attack Screen

- **If you are a victim of ransomware:**
- **Contact your local FBI field office to request assistance:**
  - **Las Vegas Nevada FBI Office**
    700 East Charleston Boulevard
    Las Vegas, Nevada, 89104
    Phone 702-385-1281
- **File a report with the FBI's Internet Crime Complaint Center (IC3):**
  - **https://www.ic3.gov**

Malware Attacks – Prevention

- **Important to have a good anti-malware program that provides real-time detection and blocking as well as regular scans of your device's storage media.**
  - **Windows 10/11 (built-in) Windows Defender is very good and automatic.**
  - **macOS has built-in security: https://www.apple.com/macos/security/**
  - **Important to keep antivirus software up to date.**
  - **Important to keep your operating system up to date (fixes security holes).**

- **Be very careful when installing third-party software, especially if it's FREE.**
  - **Always use the "custom" install option so you can disallow installs of "tag-along" programs.**
  - **Stick with software from your device provider's app store or from well-known vendors.**

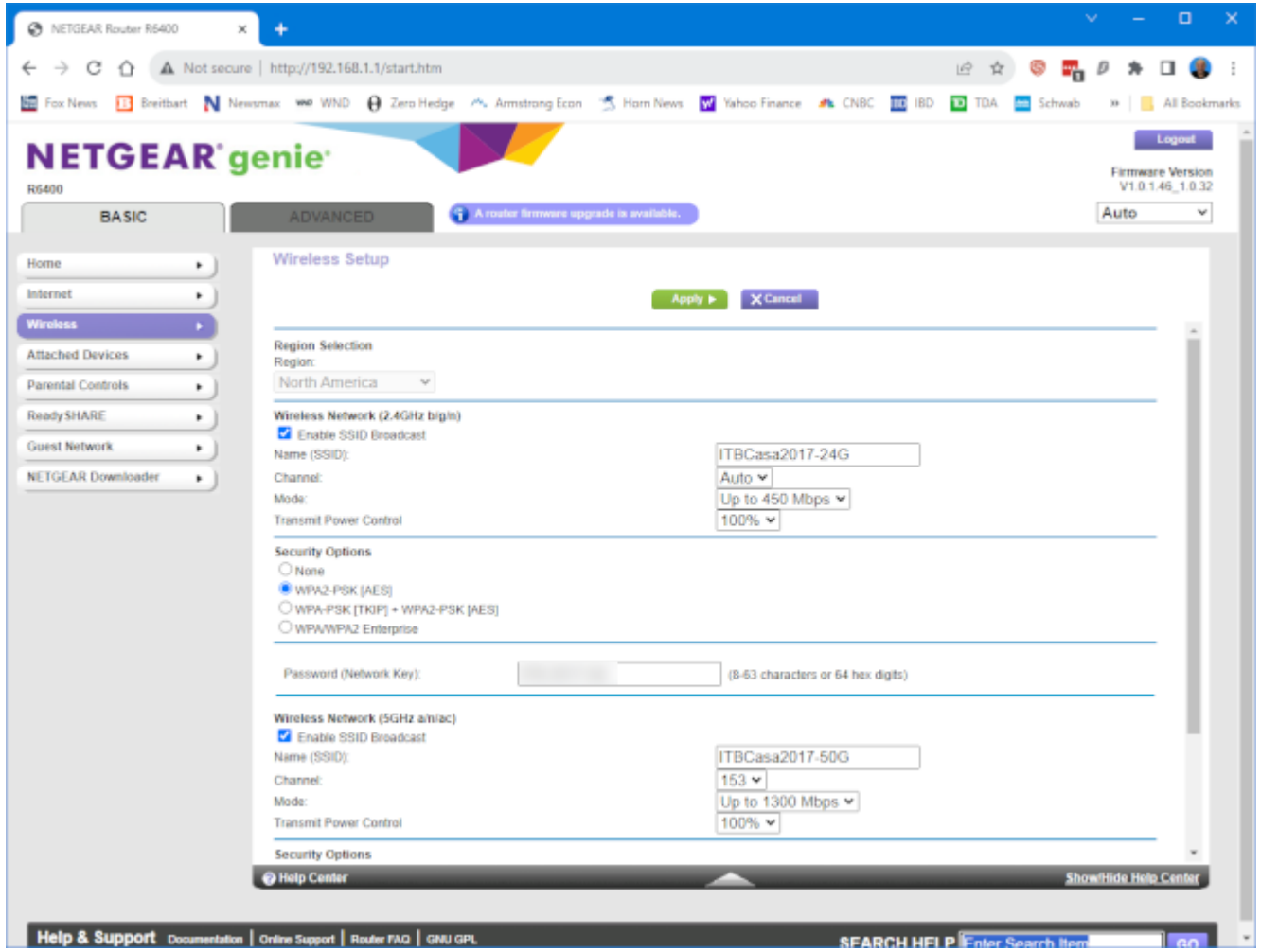
- **Don't directly open email attachments.**
  - **Save to a folder, right click and do an A/V scan first. Then open the saved attachment, if safe.**

- **Reboot your device regularly (once a day or once a week).**
  - **Helps clean out junk, makes your OS run better.**

Home Network Security – Overview

- **Most users have an in-home WiFi network**
  - **Typical setup has a home router that provides wired ethernet and wireless connections.**
  - **The home WiFi network uses radios operating in 2.4 GHz, 5 GHz or 6 GHz bands. These radios are low power but can have a range of 100 to 200 feet.**
- **This means someone outside your house could eavesdrop on your WiFi communications and possibly capture account numbers, IDs and passwords.**
  - **To prevent this, routers can use strong encryption of all radio traffic.**
  - **This encryption uses a passkey set up by the user. Only users with the passkey can connect.**
  - **Don't leave your WiFi network an open hotspot. Bad actors may use your net as a Botnet.**
- **It's important to configure your router securely.**
  - **Change the default Admin password.**
  - **Set up WiFi encryption passwords for all bands.**
  - **Set up Guest networks for each band. This allows visitors to reach the Internet, but not your in-home network.**
- **Reboot your router about once a week or more (power it off and back on)**
  - **Helps ensure no router viruses can spy on your network traffic.**
  - **Best to reboot late at night when not streaming TV.**

Home Network Security – Router Setup



- **Router setup accessed from your web browser:**
  - **Usually enter http://192.168.1.1 in your browser's address window.**
  - **Screen at left is for my Netgear AC1750 WiFi router. Yours may look a bit different.**
  - **You will need to login to the router. The setup guide will tell you the default login ID and password.**
  - **After logging in the first time, change these. Be sure to save the new ID and password.**
  - **Set up WiFI SSIDs and encryption passwords for each band.**
  - **Set up Guest networks for each band.**
  - **Connect your WiFi devices to your router.**

Scams – Overview

- **A Scam is an attempt to trick you in order to steal from you.**
- **Scams often try to get you to panic and act without thinking carefully.**
- **Scams take many forms – not all are "cyber"-related.**
  - **https://www.bottomlineinc.com/life/consumer-technology/warning-watch-out-for-these-ai-scams**
  - **Phone call from the IRS – You owe us money. Send via Zelle to <address>.**
  - **Phone call from grandson – in jail, needs bail. Send cash to <address>.**
  - **Web popup – Virus detected! Call this number to resolve.**
  - **Gift card scam – Email from someone you know & trust …**
    I'm tied up. Please buy some Amazon / Walmart gift cards and email the certificate #s to me @ <fake email address>.
  - **Email: Your account has been closed due to suspicious activity. Click here to reactivate.**
  - **Email: You've won a $500 loyalty gift. Click HERE to claim your gift.**

- **Let's look at a few more recent email examples …**

Scams – Things You Can Do

- **Be skeptical. Don’t panic. Take your time to check it out.**
  - **If it sounds too good to be true, it almost certainly is. (Old adage).**
  - **Legitimate businesses and government agencies won’t call you over the phone.**
  - **If you get a call or text purporting to be from a loved one, hang up and call / text them back. Use their known phone number from your Contacts list, not the number the call or text came from.**
  - **Don’t click links in emails purporting to be from merchants, financial institutions, government agencies. Instead, browse to the actual website to check your account activity, balances.**

- **Keep social media accounts private, visible only to a trusted circle of friends.**
  - **Keep personal information on social media accounts to a minimum.**

SPAM / Unwanted Ads

- **SPAM is the electronic equivalent of Junk mail**
  - **Predominantly ads – not malicious, just time wasting.**
  - **Show up as emails, text messages and robotic phone calls.**
  - **SPAMMERS send huge numbers of emails; if even 1% of recipients buy something, they make big money. AI and social media have made it possible for SPAMMERs to send targeted emails you're more likely to respond to.**
  - **Political ads can be especially noxious during campaign season.**
  - **SPAM may constitute 90% of emails in your inbox.**

- **What can you do to reduce the impact of SPAM?**
  - **Use an email service with a good SPAM blocker or tagger.**
  - **Use a throwaway email account for online purchases.**
  - **If your phone service is VOIP, try the free Nomorobo service.**
  - **Set up email filtering rules to route SPAM away from your Inbox to other folders. Example: I route all incoming "pizza" ads to a "pizza ads" folder.**

Final Questions and Answers