Cybersecurity Best Practices

Senior Center

Introductions

What are some of your favorite technology tools?

Agenda

- Best Practices for passwords
- Emails and online scams
- Social media and personal information
- Avoid Romantic Scammers Online
- Protecting your devices
- Managing Photos
- Additional Tips
- Q&A and Troubleshooting

Password Best Practices

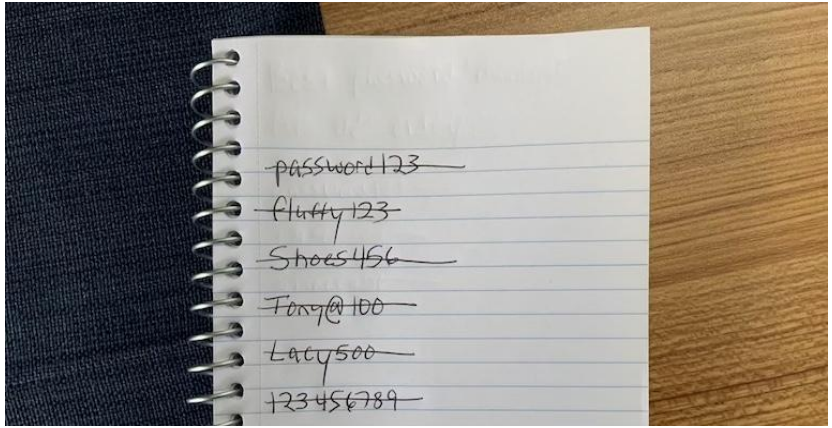
- Don't use personal information: Avoid birthdays, addresses, pet names, or anything easily guessed by someone who knows you.
- Mix it up: Use a combination of uppercase and lowercase letters, numbers, and symbols (@, #, $, etc.).
  - A password generator can help
- Length matters: Aim for longer passwords, ideally at least 12 characters.
- Passphrases are powerful: Consider a memorable phrase instead of a single word. Use a favorite quote or song lyric with added complexity (e.g., "EarlyBirdGetsTheWorm2023!").

Password Best Practices

- Two-factor authentication - Whenever possible, you should use two-factor authentication.
- Be very suspicious of emails that ask you to share your passwords or personal details.
- Never reveal your passwords to others.
- Never use the same passwords for all or really any of your online activity.
- Ask for help: Don't hesitate to ask family members or tech-savvy friends to help set up strong passwords and password managers.
- Senior resources: Many organizations offer resources specifically geared towards senior citizens and online safety. check websites like AARP's Senior Planet (https://seniorplanet.org/strong-passwords/).

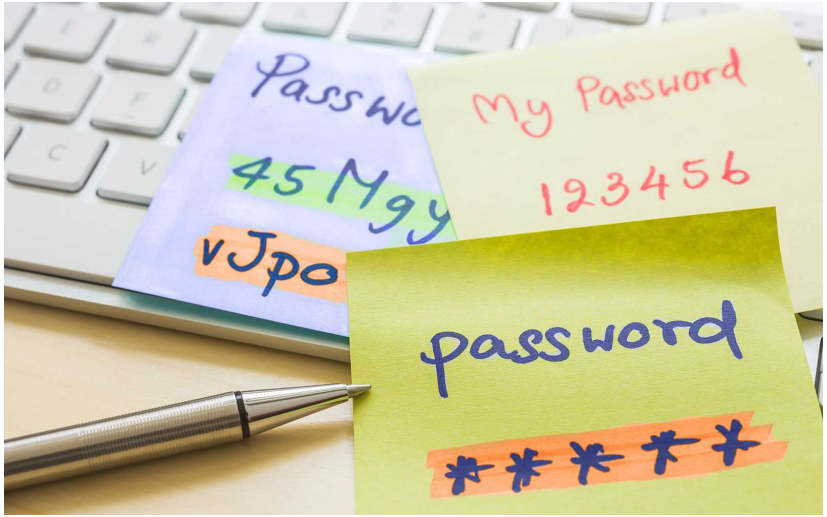
How Do I Keep Track of all my Passwords?

- Consider using a password manager: This tool helps store and manage complex passwords securely.
  - Google Password manager
  - iCloud Keychain access
  - Nordpass
  - 1Password
  - Dashlane
  - Bitwarden



How Do I Keep Track of all my Passwords?

- List passwords on your computer in a spreadsheet, Word processing document or a notes app. But you must make sure you encrypt, another word for lock, the file with a master password or passphrase in case someone gains access to your computer, phone or tablet.
- As a last resort, write them down. Just not on a sticky note under your keyboard.



Emails and Online Scams: Key Terms

- **Spam** - unsolicited bulk commercial email messages.
- **Phishing/Spear phishing** - tricking individuals into disclosing sensitive personal information or taking a potentially dangerous action, such as opening an infected attachment or visiting a compromised web link. Spear: researched and crafted attack that targets an individual or group.
- **Spoofing** - tricking or deceiving you or your system. Typically done by faking the identity of another user.

Emails and Online Scams: Red Flags

Knowing how to stop phishing emails and texts means knowing what to look for. While scammers are always changing their approaches to evade detection, certain red flags can help tip you off to trouble. Some telltale signs of a phishing email or text message include:

- Offers that seem too good to be true
- High-pressure sales pitches that stress urgency
- Alerts that there's a problem with your account (e.g. suspicious activity or outdated payment information)
- Shortened or misspelled links
- Emails that don't address you by name
- Messages with poor grammar and spelling
- Direct requests or demands for payment
- Requests to confirm personal information

Emails and Online Scams Example #1

From: Chase Bank <noreply@chasebank-security.com>
Reply-To: Chase Bank <noreply@chasebank-security.com>
Subject: Action Required! Important Security Notification On Your Chase Account

CHASE

Important Notification on Sensitive Account Features

Hello jennifer_sebbas@nobl.k12.in.us,

We wanted to let you know that your account requires an important update. We strongly recommend you to upload the following informations metioned below:

What should I update?

Click the link below to update your primary E-mail address and contact information for preventive measure.

Complete one-time verification process.

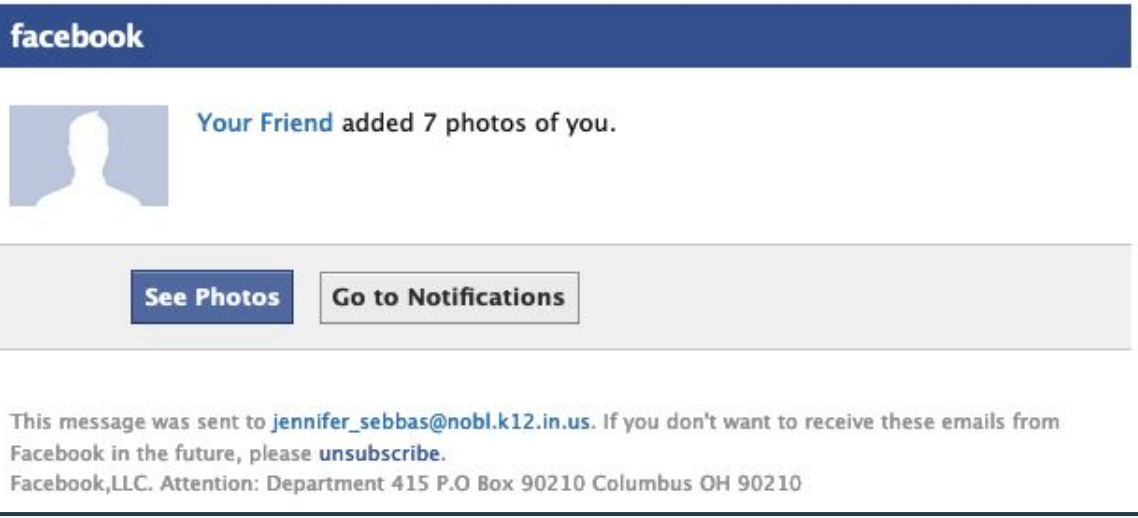
Thanks for choosing Chase Bank.

Chase Client Commitment: Protecting your information and identity is our priority. Chase will never send unsolicited emails asking clients to provide, update or verify their personal or account information, such as passwords, Social Security numbers, personal identification numbers (PINs), credit or debit card numbers, or other confidential information. Learn more about security on our website.

Chase Bank, Member FDIC. Chase Financial Corporation. Chase Bank and the Chase logo are service marks of the Chase Financial Corporation.

Emails and Online Scams Example #2

From: Facebook <notify@facebook.authentication.com>
Reply-To: Facebook <notify@facebook.authentication.com>
Subject: Your friend tagged you in photos on Facebook



Emails and Online Scams: Topic Examples

- **A plea for help:** With a goal of tugging at your heartstrings, the attacker sends you an email pretending to be a good friend or relative (e.g., your grandchild). They claim to be in financial dire straits and request your assistance immediately. How are cyber criminals able to impersonate people you know? With social media, scammers have access to more of our personal information than ever before. This allows them to make their messages highly targeted—and often very believable.
- **You're the grand prize winner:** You receive a text message congratulating you on being the winner of a very big prize, whether it's an irresistible travel package deal or free tickets to the event of the year. You're asked to provide your personal details in order to claim your award.
- **Your bank account has been compromised:** You get an "urgent" notice that appears to be from your bank, alerting you of suspicious activity on your account. You're then asked to click a link that takes you to a website, where you'll be prompted to confirm your bank account information.
- **The government is after you:** Few things in life are as jarring as an authoritatively worded notice from the Internal Revenue Service (IRS). Scammers know this, which is why many phishing emails appear to be from the U.S. government. An email like this typically has a threatening tone and mentions big, scary penalties—unless you provide the payment or personal data they demand.

Social Media and Personal Information

1. Read the privacy policy. While breaches can still happen, ensure you understand what the company is collecting about you and how that information is being used. If you're not comfortable, don't use the service.

2. Ask not to be tracked. Apple gives you an option to not have an app track you, something that's not available on Windows or Android devices. If you opt out, these app companies won't know where you've gone before and after your social media visit.

3. Use strong passwords. Don't just use long and strong passwords with eight or more letters, numbers, symbols, etc. Keep away from your kids' and pets' names. And don't use the same password for more than one site or app.

4. Opt for two-factor authentication. Social media sites and apps should give you the option to prove it's really you with not just your password but also a one-time code sent to your mobile device that must be typed in.

Social Media and Personal Information

5. Think twice before posting. Do you really need to show vacation photos before you've returned home, advertising that your place is empty? And if you're upset about a topic on the news, take a deep breath and make sure you don't write something you'll regret later.

6. Avoid scams. Know that scam artists come after your money in many ways, so don't be naive when you receive a message about an "urgent" opportunity. Just delete, block and report.

7. Close unused accounts and delete your data. Don't just deactivate your account. Your information may remain on a company's servers, so ask the social media platform to delete your data

Avoid Romantic Scammers Online

Guarding Personal Information:

- Don't overshare online: Keep dating profiles and social media accounts light on personal details like address, phone number, or financial information.
- Be cautious with photos: Avoid sending revealing photos or those with identifiable details like your home in the background.
- Slow and steady wins the race: Don't rush into sharing personal information or moving conversations off the dating platform/app.

Avoid Romantic Scammers Online

Spotting Red Flags:

- Too good to be true? It probably is: Be wary of profiles that seem unrealistically perfect or shower you with excessive compliments early on.
- Love at lightning speed? Take a step back: If someone professes deep feelings very quickly and pressures you into a relationship, be cautious.
- Financial Woes? A big red flag: Never send money or financial aid to someone you haven't met in person, regardless of their story.
- Excuses for Meeting Up? A Reason to Doubt: If someone constantly cancels plans to meet in person with excuses, it's a red flag.

Avoid Romantic Scammers Online

Staying Safe:

- Trust your gut: If something feels off, end communication. Don't be afraid to block someone if necessary.
- Talk to someone you trust: Discuss your online dating experiences with a friend, family member, or trusted confidant.
- Reverse image search photos: Use a search engine to see if the person's profile picture appears elsewhere online, potentially linked to a different identity.
- Keep online dating on the platform: Scammers often try to move conversations quickly to personal email or phone numbers. Keep communication within the dating platform for safety features and reporting options.

Protecting Your Devices

- **Keep software up-to-date**: Regularly update your operating system (Windows, Mac, etc.), web browser, and other software. Updates often contain security patches to fix vulnerabilities.
- **Install reputable security software**: Consider antivirus and anti-malware software from a trusted brand to help protect against malicious programs.
    - Enable automatic updates: This ensures you have the latest security patches.
- **Be cautious about free software downloads**: Only download software from trusted sources.

Protecting Your Devices

- **Use strong passwords and enable two-factor authentication (2FA)**:
- This was covered in the previous password tips section, but it's crucial for device security as well.
- **Be mindful of public Wi-Fi**: Avoid using public Wi-Fi for sensitive activities like online banking. If necessary, use a Virtual Private Network (VPN) for added security.
- **Secure your physical device**: Don't leave your laptop, phone, or tablet unattended in public places.
    - Don’t leave your devices unattended in a vehicle.

Managing Photos

Gathering and Sorting:

Start with printed photos: Decide which ones to keep, scan (explained later), or discard. Consider sentimental value and duplicate photos.

Download digital photos: Gather photos from phones, cameras, and social media (if comfortable). Organize by download date for a starting point.

Managing Photos

Digitizing and Saving:

Scan printed photos: Many libraries and senior centers offer scanning services or rent scanners. Consider asking tech-savvy family or friends for help.

External hard drive storage: Store digital photos on an external hard drive for safekeeping. Look for user-friendly drives with clear labeling options.

Cloud storage: Consider cloud storage services (Dropbox, Google Drive) for additional backup, but ensure privacy settings are understood.

Managing Photos

Organizing and Sharing:

Simple folder structure: Use clear folder names like "Year - Event" or "Family - Last Name" for easy browsing.

Photo organizer software: Explore user-friendly photo organizer software that helps categorize and search photos by date, location, or keywords.

Google Photos, Photos App for iOS

Sharing with loved ones: Create digital albums or slideshows to share with family and friends. Many photo storage services offer these features.

Managing Photos

Organizing and Sharing:

Utilize Metadata: Many photo management software and platforms allow you to add metadata such as tags, keywords, and captions to your photos.

Organize by Date: Within each event or category folder, organize your photos chronologically. This makes it easier to track the progression of events over time.

Tag Faces: Some photo management software automatically detects faces in your photos and allows you to tag them with the names of the people in the image.

Managing Photos

Additional Tips:

Start small, set achievable goals: Don't try to tackle everything at once.

Focus on the fun! Relive memories while sorting photos.

Ask for help: Don't be afraid to ask family or friends for assistance with technology or organization.

Consider professional services: Photo organizing companies can help with large collections or complex tasks.

Additional Tips

Calendars: Online calendar available with email account, such as Yahoo & Google

- Google Calendar: Google Calendar is a free tool that many of your family members may already have. You can create a calendar or multiple calendars and share them with your family members. How to sync Google Calendar with a phone or tablet.
- iPhone Calendar

Caring for the device:

- If it's not the only phone in the house, power it down at night (including your computer). If it's the only phone in the house, occasionally restart it when possible.
- Clean computer screens with a microfiber cloth. Clean keyboards and smartphones with a small amount of rubbing alcohol on a cotton ball.

Additional Tips

CyberSecurity Cont'd:

- Be cautious of public Wi-Fi: Avoid using public Wi-Fi for sensitive activities like online banking.
- Be wary of unsolicited phone calls and texts: Don't share personal information with unknown callers or texters.
- Talk to a trusted person: If unsure about something online, ask a trusted family member or friend for help.

Website Resources:

- AARP: Personal Technology
- National Council On Aging: Avoiding Scams

Q & A and Troubleshooting