



Taking Control of Your Privacy

Faisal Kaleem

Will Lee

9/27/2024

Objectives

- Understand online privacy basics
- Importance of Privacy
 - Why privacy matters, especially for older adults
 - Protect personal and financial information
 - Stay safe from identity theft and scams
- Managing Privacy
- Recognize common scams and how to avoid them

The 2023 Medicare Scam

- Medicare scam surged across the U.S., specifically targeting older adults
 - Scammers posed as Medicare representatives, offering "**free**" medical devices, such as knee braces, back supports, or genetic testing kits.
 - The asked for personal information, including Medicare numbers
 - The scammers used **high-pressure tactics**, creating a sense of urgency, claiming that the **offer was for a limited time**
-

The 2023 Medicare Scam

- Impact

- Financial Loss
- Medical Identity Theft
- Emotional Distress

- Why It Works:

- Older adults are often targeted because they are **perceived as more trusting and less familiar with modern scam tactics**
- The use of **medical and official-sounding language** makes the scam more convincing



The 2024 Grandparent Bail Scam

- Scam **exploited the love and concern** older adults have for their grandchildren.
 - Fraudsters posed as **distressed grandchildren, lawyers, or law enforcement officers**, calling seniors and claiming that their grandchild was in jail or involved in a car accident.
 - They would **urgently request money** to cover bail, legal fees, or medical expenses, often asking for **large sums of cash, gift cards, or wire transfers.**
-

The 2024 Grandparent Bail Scam

- Impact

- Financial Loss
- Emotional Manipulation
- Widespread Reach

- Why It Worked

- **Emotional Tactics:** The scammers expertly **exploited the natural instinct** of grandparents to protect their grandchildren, making it difficult for victims to think critically in the moment.
 - **Use of AI Technology:** Scammers used **AI-generated voices** that closely mimicked the voices of the victims' real grandchildren, making the calls seem even more authentic and convincing.
-

Understanding Online Privacy

- Online privacy is about **protecting your PII and PHI** from unauthorized access and misuse
 - PII (Personally Identifiable Information)
names, email addresses, and financial data
 - PHI (Protected Health Information)
Your health-related information.
 - PII and PHI can be sold or used for **identity theft** and **fraudulent medical claims**
 - Privacy vs Security
 - Privacy is about **controlling** your personal information
 - Security is about **protecting** that information from threats
 - Privacy Policy: <https://tosdr.org/>
-

Managing Privacy: Global Layer

- Secure vs. Public WiFi

- Public WiFi networks (coffee shops, airports, and hotels) are usually **unsecured**

- Risks

- Data interception while being transmitted

- Communication Interception (man-in-the-middle)

- Malware Injection

- Fake Hotspots:** Fake WiFi with similar names as legitimate network

- Best Practices

- Always use password-protected WiFi networks at trusted locations

- Avoid performing sensitive transactions over unsecure Public WiFi

- Use a **strong password** for your home WiFi and use the latest encryption standard (WPA3)

- Turn off automatic WiFi connections and using “Forget” options for previously connected **public** networks.



Managing Privacy: Global Layer

- VPNs (Virtual Private Networks)
 - VPN creates a secure, encrypted connection (tunnel) to the Internet
 - VPNs hide IP addresses, encrypt data, and prevent tracking by websites or ISPs
 - Hides your online activities from your Internet Service Provider (ISP) and potential eavesdroppers
 - A **must** when using **public WiFi**, as it adds a secure layer of protection
- **Choosing a VPN**
 - Try to avoid FREE VPNs
 - Look for user-friendly VPNs with clear instructions for installation and use

Managing Privacy: Local Layer

- Use Browsers with Enhanced Privacy
 - Mozilla Firefox, Brave, or DuckDuckGo
 - Utilize Browser Security Features
 - Tracking Protection to block trackers that collect data about your **browsing habits**
 - Sandboxing prevent malware from spreading if a webpage is compromised
 - Adjust Browser Privacy Settings
 - Disable **third-party cookies** to prevent third-parties from tracking your activities
 - Enable 'Do Not Track'
 - Use Private Browsing (Incognito) Mode to enhance your privacy on **shared or public devices**
-

Managing Privacy: Local Layer

- Extensions and Add-ons for Privacy
 - **Ad Blockers** (AdBlock Plus) to block intrusive ads and trackers
 - **Https Everywhere** to automatically switches website connection **from insecure (http) to secure (https)** and provide protection against data interception
 - **Privacy Badger** blocks tracker that track your **browsing habits without consent**
- Managing Cookies
 - **Clear cookies** manually or set them to clear automatically when you close the browser. (Exceptions can be made for trusted sites)
 - Configure browser to block all third-party cookies
 - Strictly-necessary cookies vs All cookies
- Browsing History
 - Clear history regularly to maintain your privacy, especially on shared devices
 - Browser Cleaning Tools like CCleaner can help clean many things automatically
- Ad Tracking
 - Opt-Out of Personalized Ads to limit the amount of data collected by advertisers

Managing Privacy: Local Layer

- Email Privacy Issues

- Phishing Scams

- **Tracking Pixels** are tiny, invisible images embedded in emails that notify the sender when an email is opened, providing information about your location, device, and engagement

- Email Privacy Settings

- Choose a Secure Email Provider that prioritize privacy and security, such as ProtonMail, Tutanota, or Zoho Mail

- Enable 2FA on your email account to add an extra layer of security



Phishing Email Example

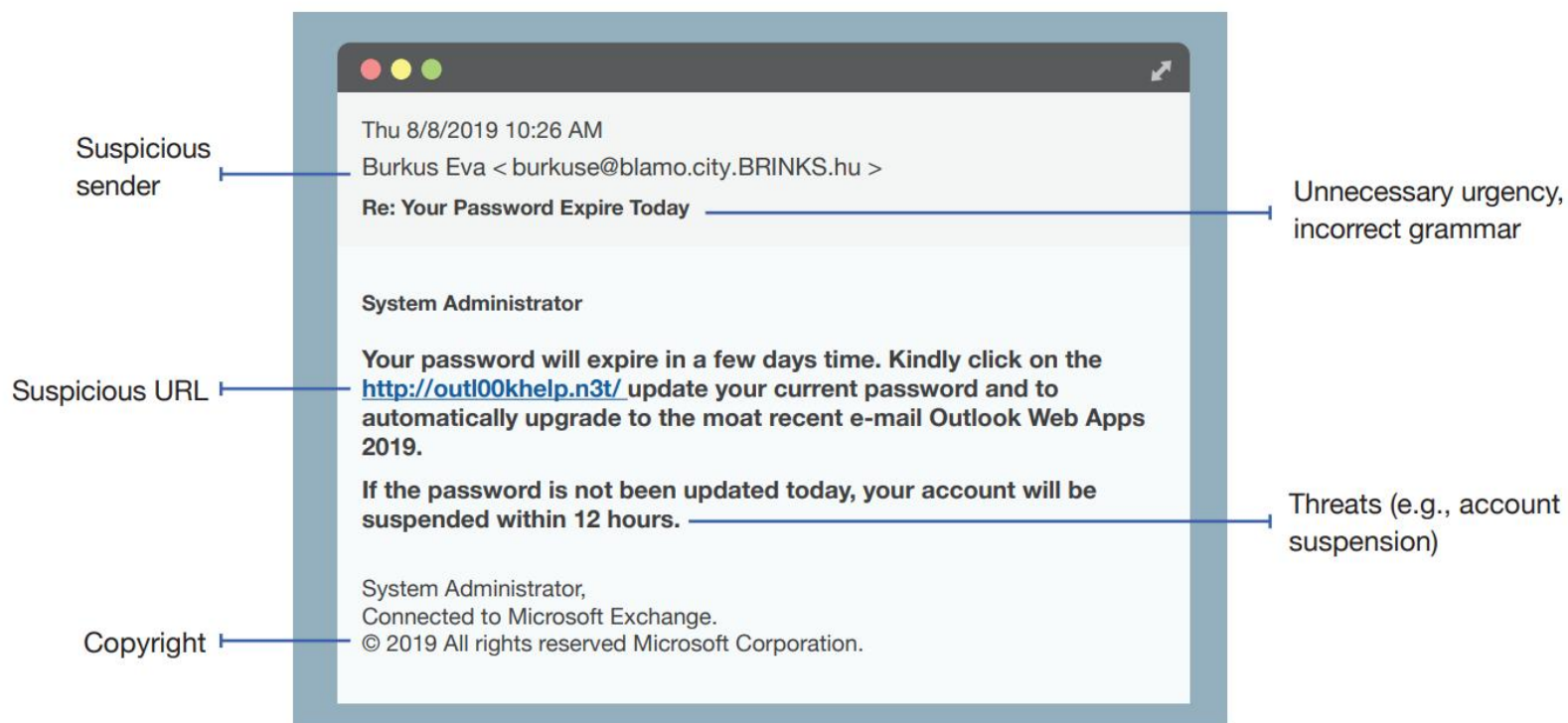


Figure 1: Example of phishing email characteristics

Note: email address and URL above are fictitious

Managing Privacy: Local Layer

- Privacy Settings in Popular Email Services

- Gmail

Confidential Mode: Use this feature to send emails that automatically expire after a set time and cannot be forwarded, copied, or printed by the recipient

Disable Read Receipts and Images: Adjust settings to block read receipts and prevent images from automatically loading, which can stop tracking pixels from notifying senders


Secure Connection: Always ensure that your connection is secure by checking for HTTPS in the address bar when accessing Gmail

- Outlook:

Encrypt Emails: Use Outlook's built-in encryption options to send emails securely. You can select "Encrypt" in the options menu when composing an email

Disable External Content: Adjust settings to block automatic downloading of external content, such as images, which helps prevent tracking and malicious code from being loaded

Junk Mail Settings: Adjust the junk mail filter settings to automatically block suspicious or potentially harmful emails



Managing Privacy: Local Layer

- Managing Spam and Phishing

Spam Filters: Ensure that your email's spam filter is enabled and set to the highest protection level. Most providers allow you to mark emails as spam, which helps improve the filter's accuracy over time

Report Phishing: If you receive a phishing email, report it to your email provider. Most providers have an option to report phishing, which helps protect you and others from similar attacks

- Avoiding Tracking Pixels

Turn Off Automatic Image Loading: Prevent tracking pixels from loading by disabling automatic image loading in your email settings. This stops the invisible trackers from reporting back to the sender when you open the email.

Use Privacy-Focused Extensions: Consider using browser extensions like Privacy Badger or Ghostery, which can block tracking pixels in emails when viewed in a web browser.



Managing Privacy: Local Layer

- Email Encryption Tools

PGP (Pretty Good Privacy): PGP is a popular tool for encrypting emails. It uses public and private keys to encrypt messages, ensuring that only the intended recipient can decrypt and read them

Secure Email Apps: Apps like ProtonMail and Tutanota offer built-in end-to-end encryption, making it easy to send secure messages without needing extra tools.

- Regularly Update Your Email Password

Use Strong, Unique Passwords: Your email password should be complex, with a mix of letters, numbers, and symbols. Avoid using easily guessed information like names or birthdays

Change Passwords Regularly: Regularly update your password, especially if you suspect a breach or receive phishing attempts that target your account



Managing Privacy: Local Layer

- Limit Sharing Personal Information via Email

Avoid Sharing Sensitive Data: Refrain from sending sensitive information (e.g., Social Security numbers, passwords) via email. If necessary, use encrypted email services to protect the content

Beware of Unsolicited Requests: Never respond to unsolicited requests for personal information, even if the email appears legitimate. Instead, contact the organization directly using verified contact information

- Secure Email on Mobile Devices

Set Up Screen Lock: Ensure your mobile device is protected with a strong passcode, fingerprint, or face recognition to prevent unauthorized access to your email

Enable Remote Wipe: Set up remote wipe capabilities, which allow you to erase your device if it's lost or stolen, protecting your email and other sensitive data



Managing Privacy: Personal Layer

- Android/Apple Device

- **Location Settings:** Set location access to "**While Using the App**" or "**Never**" unless absolutely necessary. Disable location access for apps that don't need it, and regularly review which apps have location permissions
 - **Limit App Permissions:** Go to your device's privacy settings to **review and manage app permissions**, such as access to your camera, microphone, contacts, and photos. **Revoke permissions** that are unnecessary or seem suspicious
 - **Privacy Checkup Tools:** Use built-in privacy tools on **Android (Privacy Dashboard)** and **iOS (App Privacy Report)** to review which apps access sensitive data most frequently and adjust settings accordingly
 - **Uninstall Unused Apps:** Delete apps you no longer use to reduce potential privacy and security risks. Apps often continue collecting data even when not actively used.
-

Managing Privacy: Personal Layer

• Settings to Enhance App Privacy:

- **Limit Background Data:** Prevent apps from running and collecting data in the background when you're not actively using them. This can be adjusted in the app's settings on both Android and iOS.
- **Update Apps Regularly:** Keep your apps updated to ensure you have the latest privacy and security patches. Developers often release updates to fix vulnerabilities that could be exploited by hackers.



Managing Privacy: Personal Layer

• Managing Privacy Settings on Social Media:

- **Limit Profile Visibility:** Set your **profile to private or limit** who can see your posts and information (e.g., only friends or specific groups). Adjust the audience settings for each post **to ensure your content isn't shared more broadly than intended.**
- **Turn Off Location Sharing:** Disable location sharing on social media platforms to **prevent your posts from broadcasting your location.** On platforms like Facebook, you can turn off location history and prevent location tracking entirely.
- **Control Who Can Contact You:** Adjust settings to control who can send friend requests, message you, or see your profile. Enable filters to reduce unwanted messages or requests from strangers.
- **Review App Permissions:** Disconnect or remove third-party apps and services linked to your social media accounts, especially those you no longer use or that seem outdated.

Recognizing and Avoiding SCAMS

• Grandparent Scam (Emergency Scam)

- **How It Works:** Scammers call **posing as a grandchild or a lawyer**, claiming that the grandchild is in trouble—such as being arrested, involved in an accident, or stuck abroad—and urgently needs money for bail, legal fees, or travel expenses
- **Why It Works:** The scam relies on **emotional manipulation**, exploiting the grandparent's desire to help their loved ones quickly
- **How to Recognize and Avoid:**
 - **Verify the caller's identity** by contacting other family members directly
 - Be wary of **requests for secrecy and urgent payment** demands
 - Never send money or share personal information without verification

https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf



Recognizing and Avoiding SCAMS

• Medicare and Health Insurance Scams

- **How It Works:** Scammers **pose as Medicare representatives or healthcare providers**, offering free medical equipment or services in exchange for personal information, like Medicare numbers. They may also ask for payment for services that are usually free or covered by insurance
- **Why It Works:** Older adults rely heavily on Medicare, making them prime targets for scams involving health concerns
- **How to Recognize and Avoid:**
 - Medicare will never call or visit** to sell you anything
 - Do not give out Medicare or health insurance numbers over the phone
 - Verify any offers by contacting Medicare directly

Recognizing and Avoiding SCAMS

• Tech Support Scams

- **How It Works:** Scammers **pretend to be from well-known tech companies** like Microsoft or Apple, claiming that your computer has a virus or other technical issue. They **request remote access** to your computer or ask for payment for unnecessary services
- **Why It Works:** Older adults may be less familiar with technology, making them vulnerable to convincing-sounding claims about their devices
- **How to Recognize and Avoid:**
 - Legitimate companies do not make unsolicited tech support calls
 - Never give remote access to your computer to unknown callers**
 - Hang up and contact the company directly using official contact information

Recognizing and Avoiding SCAMS

• Sweepstakes and Lottery Scams

- **How It Works:** Scammers inform victims that they have **won a lottery or sweepstakes** but need to pay a fee, tax, or processing charge to claim the prize. The prize never materializes, and the fees are lost
- **Why It Works:** The promise of a large reward can be enticing, especially when presented as a **once-in-a-lifetime opportunity**
- **How to Recognize and Avoid:**
 - You cannot win a contest you didn't enter
 - Legitimate lotteries do not ask for money upfront
 - Never send money or provide personal information to claim a prize

Recognizing and Avoiding SCAMS

• Phishing Scams

- **How It Works:** Phishing involves **fraudulent emails, texts, or phone calls** designed to trick individuals into revealing personal information, such as Social Security numbers, bank account details, or passwords
- **Why It Works:** The messages often **appear to come from legitimate sources** like banks, government agencies, or companies you trust
- **How to Recognize and Avoid:**
Look out for **generic greetings, spelling errors, and urgent requests** for information
Verify the sender by contacting the organization directly through **official channels**
Never click on suspicious links or download attachments from unknown sources



Recognizing and Avoiding SCAMS

• Romance Scams

- **How It Works:** Scammers create **fake online profiles** on dating sites or social media, **building romantic relationships** with victims and then requesting money for emergencies, travel, or medical expenses
- **Why It Works:** Scammers prey on **loneliness** and the **emotional connection** they build with their victims
- **How to Recognize and Avoid:**
 - Be wary of people who **profess love quickly or avoid meeting in person**
 - Never send money to someone you haven't met in person**
 - Use **reverse image search** tools to check if their profile pictures are stolen from someone else

Recognizing and Avoiding SCAMS

• Charity Scams

- **How It Works:** Scammers pose as **charitable organizations**, especially after natural disasters or major events, asking for donations that never reach those in need.
- **Why It Works:** Older adults are **often generous and sympathetic** to charitable causes, making them susceptible to appeals for help
- **How to Recognize and Avoid:**
Verify the legitimacy of charities through trusted sites like **Charity Navigator or the Better Business Bureau**
Be cautious of high-pressure tactics and **requests for immediate donations**

Recognizing and Avoiding SCAMS

• Investment Scams (Ponzi Schemes)

- **How It Works:** Scammers offer fake investment opportunities with promises of high returns and little risk. These scams often target **retirees** looking to grow their savings.
- **Why It Works:** The promise of a **secure investment with high returns** can be very appealing, especially for those worried about retirement savings.
- **How to Recognize and Avoid:**
 - Be skeptical of investments that seem too good to be true.
 - Research the investment and consult with a licensed financial advisor.
 - Avoid investments that pressure you into **making quick decisions**.

Recognizing and Avoiding SCAMS

• IRS or Government Impersonation Scams

- **How It Works:** Scammers pretend to be **IRS or government officials**, claiming that the victim owes taxes or fines and demanding immediate payment via wire transfer, gift cards, or prepaid debit cards
- **Why It Works: Fear of legal trouble** can prompt quick action, especially when the call is aggressive and threatening
- **How to Recognize and Avoid:**
 - The **IRS will never call to demand** immediate payment without first sending a bill
 - Do not share personal information or make payments over the phone
 - Contact the IRS directly if you receive such a call**

Recognizing and Avoiding SCAMS

• Home Repair Scams

- **How It Works:** Scammers **go door-to-door** offering home improvement services at a low cost, taking payment upfront, and either performing shoddy work or disappearing without completing the job
- **Why It Works:** Older adults may have **difficulty maintaining their homes** and are targeted by scammers offering quick, cheap fixes
- **How to Recognize and Avoid:**
 - Do not hire contractors who solicit door-to-door
 - Get written estimates and **verify the contractor's credentials**
 - Pay only after work is completed to your satisfaction

Reporting Fraud or Scam

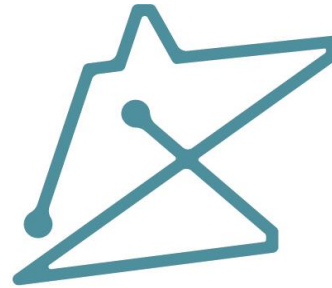
- [Federal Trade Commission \(FTC\)](#)
 - [FBI Internet Crime Complaint Center \(IC3\)](#)
 - [Consumer Financial Protection Bureau \(CFPB\)](#)
 - [AARP Fraud Watch Network](#)
 - [National Elder Fraud Hotline \(1-833-FRAUD-11\)](#)
 - [U.S. Senate Special Committee on Aging Fraud Hotline \(1-855-303-9470\)](#)
 - [Elder Justice Initiative \(Department of Justice\)](#)
 - [Social Security Administration \(SSA\) Fraud Hotline](#)
 - [Adult Protective Services \(APS\)](#)
 - [Minnesota Attorney General Complaint Filing](#)
-

Ten Tips

- Use Strong, Unique Passwords
 - Enable Two-Factor Authentication (2FA)
 - Be Cautious of Phishing Scams
 - Update Software Regularly (including Apps)
 - Limit What You Share on Social Media
 - Beware of Public WiFi
 - Monitor Your Accounts Regularly
 - Be Selective About Apps and Permissions
 - Review Privacy Settings Regularly
 - Ask for Help When in Doubt
-



DHS/NSA designated CAE-CD Institution



MN CYBER

Train. Test. Detect. Protect.



MINNESOTA STATE

Metro State University,
A member of Minnesota State

Faisal Kaleem
651-793-1238

Faisal.Kaleem@metrostate.edu

LinkedIn: Kaleemf

Twitter: @Kaleemf