Guarding Our **Loved Ones:**

Understanding Cyber Scams

Exploiting the Elderly

Office of Information Technology
Division of Information Security
JULY 2023

The **Indian Health Service** (IHS) Division of Information Security is happy to bring you important information and practical tips to protect your beloved seniors from the growing threat of cyber scams. In this newsletter, we'll look at typical cyber scams aimed at seniors and talk about safety precautions that senior citizens and family members can take to stay secure online.

THE GROWING THREAT

Cybercriminals are significantly targeting susceptible individuals, particularly the elderly, through complex and deceptive tactics. It is important for us to understand the various cyber scams common today to effectively safeguard our loved ones. Below are some common scams to be aware of:

- **Phishing Scams:** A common type of online scam, phishing involves cybercriminals sending deceptive emails or messages while pretending to be reputable organizations, with the objective of tricking individuals into disclosing personal details or downloading malicious software. Here's a detailed look at what phishing entails:
  - Phishing scams often begin with emails that appear to come from familiar entities such as banks, internet service providers, or even charities. These messages are designed to alarm recipients into responding, typically by indicating an urgent need to update account information or verify identities.
  - A prominent example of a phishing scam is the "Bank Email Scam". The scammer will send an email that closely resembles official correspondence from your bank, usually warning of a security issue requiring immediate attention. They include a link leading to a fraudulent website, designed to steal login credentials or other sensitive data.

  You can help seniors to avoid phishing scams by encouraging them to use following behaviors:
  - **Instill prudence:** Encourage your elderly family members to scrutinize any email that requests sensitive information, regardless of how authentic it appears. Explain that legitimate organizations rarely, if ever, request personal data via email.
  - **Validate source:** Encourage them to verify the sender's identity by contacting the official organization directly, using official contact details, not those provided in the suspicious email.
  - **Pause and evaluate:** When receiving an email requesting personal or financial information, seniors should pause and evaluate the email carefully. Scammers often create a sense of urgency to pressure victims into responding without thinking.

    Teach your elderly family members not to rush into providing help. Legitimate institutions and actual family members will appreciate their desire to verify the situation. When receiving an email requesting personal or financial information, seniors should pause and evaluate the email carefully. Scammers often create a sense of urgency to pressure victims into responding without thinking.
  - **Check the sender's email address:** Ask your loved ones to inspect the sender's email address closely. Scammers often use email addresses that closely resemble legitimate ones but may have slight variations or misspellings. Legitimate emails from banks or financial institutions should come from official domain names.
- **Tech Support Scammers:** These scammers pose as tech support personnel and try to access victims' devices remotely, frequently claiming to fix problems that don't exist. They may request payment or install malware to steal personal information.
  - One example of a tech support scam is the "Microsoft Tech Support" scam. Scammers often cold call unsuspecting individuals, posing as Microsoft representatives. They use various tactics to create a sense of urgency and convince victims that their computer is infected with viruses or experiencing technical problems. Here's how you can help your loved ones protect themselves:

- **Encourage skepticism:** Teach your elderly family members to be cautious when receiving unsolicited calls or pop-up messages claiming to be from tech support. Remind them that legitimate tech support companies, like Microsoft, will not contact them proactively unless they have previously requested assistance.
- **Verify legitimacy:** Instruct them to ask for the caller's name, company, and contact information. Advise them not to provide any personal information or grant remote access to their devices during such calls. They should hang up and independently contact the official tech support channels of the company in question to verify the legitimacy of the call. Note that they should not use the contact information provided in the pop-up or in the call.
- **Educate about payment requests:** Scammers often request payment for their fraudulent tech support services. Remind your loved ones that legitimate tech support companies will not ask for payment upfront. Inform them that they should never share credit card information or make any financial transactions during these calls.
- **Seek trusted help:** Encourage your family members to consult with a trusted family member, friend, or a local computer technician if they have concerns about their computer's security or performance.

- **Romance Scams:** Cybercriminals build false online relationships with seniors, earning their trust, and exploiting this trust to extract money or personal information. Below is a detailed examination of how this scam operates:
  - Romance scams typically originate on online dating platforms or social media. The scammer creates a fake profile, initiates a relationship, and, over time, convinces the victim to send money, gifts, or personal details.
  - One common example is the "Long-Distance Lover" scam. The scammer forms a relationship with the victim, often professing love quickly. They then concoct a variety of reasons for needing money, including travel costs to visit the victim or medical expenses.

  You can help seniors avoid romance scams by encouraging them to use following behaviors:
  - **Promote skepticism:** Teach your elderly loved ones to approach online relationships with caution. Warn them that scammers can spend a significant amount of time building trust before asking for money.
  - **Verify information:** Encourage your family members to do background checks on potential online partners and ask detailed questions about the person's story. Reverse image searches can be used to verify profile pictures.
  - **Discuss money requests:** Remind family members that legitimate potential partners will not ask for money early in relationships, especially not under desperate or emergency circumstances.

- **Impersonation Scams:** These scams involve fraudsters posing as government officials, bank representatives, or even distressed family members, aiming to obtain financial aid or sensitive information. Let's delve into this type of scam a bit deeper:
  - Impersonation scams typically involve phone calls or emails from people claiming to represent a trusted organization or being a distressed family member. The scammer usually presents a problem that requires immediate financial assistance or personal information. Ask your loved ones to inspect the sender's email address closely. Scammers often use email addresses that closely resemble legitimate ones but may have slight variations or misspellings. Legitimate emails from banks or financial institutions should come from official domain names.
  - A prime example is the "Grandparent Scam". In this scam, fraudsters pose as grandchildren in distress, often claiming to be in an accident or legal trouble and needing money urgently.

  You can help seniors to avoid impersonation scams by encouraging them to use following behaviors:
  - **Encourage caution:** Teach your elderly family members not to rush into providing help. Legitimate institutions and actual family members will appreciate their desire to verify the situation. When receiving an email requesting personal or financial information, seniors should pause and evaluate the email carefully. Scammers often create a sense of urgency to pressure victims into responding without thinking.
  - **Validate authenticity:** Urge family members to independently contact the organization or family member mentioned to confirm the request's legitimacy.
  - **Don't use unusual payment methods:** Scammers often request funds via wire transfer, gift cards, or cryptocurrency. Make sure your loved ones know that such payment methods are red flags.
  - **Do not click on links:** Recommend to seniors to avoid clicking on any links provided in an email. Instead, they should independently open a web browser and manually type in the official website address of their bank or financial institution.

PRECAUTIONS FOR OUR LOVED ONES

Protecting our elderly loved ones requires a proactive approach. These are essential precautions to help prevent cyber scams:

- **Educate and Raise Awareness:** Inform your older family members about the existence and tactics of cyber scammers. Encourage open communication and caution them against disclosing sensitive information electronically.
- **Use Strong Passwords and Two-Factor Authentication:** Advise your loved ones to use strong, unique passwords for their online accounts and to enable two-factor authentication whenever possible. To make this process easier, suggest they think about using a password manager.

TIPS FROM THE FEDERAL TRADE COMMISSION

The Federal Trade Commission offers the following tips for protecting us from cyber criminals.

- **Don't wire money.** Wiring money is like sending cash. Once you send it, you usually can't get it back. Don't wire money even if someone sends you a check, tells you to deposit it, and wire some of the money back to them. That's a fake check scam, and the bank will want you to repay the money you withdrew and sent. That may also be a money mule scam that will involve you in moving stolen money.
- **Don't pay with a gift card.** Gift cards are for gifts. As soon as you tell someone the numbers on the back of the gift card, they get control of the card and your money is gone forever. No legitimate business or government agency will insist that you pay with a gift card.
- **Don't pay with cryptocurrency.** If someone requires you to pay for something with Bitcoin, Ether, or some other type of cryptocurrency, they're probably a scammer. Cryptocurrency payments don't come with legal protections. If you pay with cryptocurrency, you usually can't get your money back unless the person you paid sends it back.

RESOURCES AND ASSISTANCE

It's critical to be aware of where to turn if you suspect any activity or your loved ones fall victim to cyber scams. The following list provides some resources:

- **Local Authorities:** Contact local law enforcement if you suspect a cybercrime has occurred.
- **Consumer Protection Agencies:** Inform your loved ones about consumer protection agencies that specialize in handling fraud and cybercrime cases:
  - Federal Trade Commission: https://reportfraud.ftc.gov/#/
  - National Elder Fraud Hotline: 833–FRAUD–11 or 833–372–8311
  - Your state's Attorney General office
  - Your local FBI field office: https://www.fbi.gov/contact-us/field-offices.
    The FBI suggests that you provide as many of the following details as possible:
    - Names of the scammer and/or company
    - Dates of contact
    - Methods of communication
    - Phone numbers, email addresses, mailing addresses, and websites used by the perpetrator
    - Methods of payment
    - Where you sent funds, including wire transfers and prepaid cards (provide financial institution names, account names, and account numbers)
    - Descriptions of your interactions with the scammer and the instructions you were given
    - Whenever possible, you should keep original documentation, emails, faxes, and logs of communications.
- **Cybersecurity Resources:** Familiarize yourself with resources that provide aid and guidance in the event of cyber scams.
  - Internet Crime Complaint Center (IC3)
  - Cyber-Seniors
  - AARP

Please contact cybersecurity@ihs.gov with any questions or comments about this newsletter.

NOTE: *Products mentioned in this document are for informational purposes only and do not signify an endorsement.*