Cyber Scam Prevention for Seniors: Briefing- **Briefing**

Executive Summary:

This briefing document summarizes the key themes and actionable advice presented in a formal presentation aimed at protecting seniors from cyber scams. The presentation, led by Corey Limer and David Nublaku, highlighted the increasing prevalence and financial impact of online scams targeting older adults. The core message emphasized a "stop, think, act" approach to online interactions, coupled with awareness of common scam tactics and the importance of strong password security. The presenters also addressed audience questions and offered practical tips for identifying and avoiding online threats.

Main Themes and Important Ideas/Facts:

1. **The Pervasiveness and Impact of Cyber Scams:**
    - The internet offers numerous benefits, including connecting with family, but also presents risks, particularly for those less familiar with evolving technologies.
    - Cyber scams are widespread and financially damaging. In 2023, individuals over 60 in the US lost **$3.4 billion** to elder fraud.
    - The financial incentive is a primary driver for the continuation of these scams. As Corey Limer stated, *"that's why you see all these scams right? that's a lot I mean people people are getting money from it."*
2. **Common Online Scam Tactics:**

The presentation outlined several prevalent scam types:

- **Grandparent Scam:** Impersonating a grandchild in distress to solicit urgent financial help, often through untraceable methods like gift cards or wire transfers. The scammers often create a sense of urgency to prevent critical thinking. As Limer noted, *"the message invokes a sense of urgency but that urgency is to make us not think and react."*
- **Romance Scam:** Building emotional connections through fake online profiles and then requesting financial assistance. Corey Limer shared an example of his mother-in-law being targeted.
- **Accidental Deposit Scam:** Claiming to have mistakenly sent money and requesting it back, often aiming to obtain financial information.
- **Tech Support Scam:** Contacting individuals with false warnings of viruses or computer problems to gain access to their devices or solicit payment for unnecessary services.
- **UPS or Delivery Tech Scams:** Sending fake notifications about delivery issues to trick recipients into clicking malicious links or providing personal information.

3. **The "Stop, Think, Act" Approach to Online Safety:**

This is presented as a fundamental strategy for preventing cyber scams.

- **Stop:** Pause before reacting to any unexpected online message or request.
- **Think:** Evaluate the legitimacy of the request. Consider if the message was expected, if the request makes sense, and if it creates a sense of urgency. As Corey Limer advised, *"most legitimate requests are not urgent."*
- **Act:** If the message or request seems suspicious, verify it through known and trusted channels (e.g., contacting family members directly, visiting official websites or apps). Avoid clicking on links in unsolicited messages.

4. **Key Actions to Protect Yourself Online:**

- **Verify unexpected messages:** Contact family members directly if you receive a message claiming to be from them in distress. Hang up and call back using known contact information. David Nublaku shared an example of a neighbor who avoided a scam by doing this.
- **Be wary of urgency:** Legitimate organizations rarely demand immediate action.
- **Avoid clicking suspicious links:** Always type website addresses directly into your browser or use official apps instead of clicking on links in emails or texts. Corey Limer cautioned, *"take a breath before clicking link. Often times you'll see a link um computer programmers can disguise uh malicious links in a nice text link that says this is a friendly link but behind it might be bad code."*
- **Trust your instincts:** If something feels like a scam, it likely is.
- **Report suspicious activity:** Marking messages as spam or reporting them can help prevent future scams.
- **Keep software updated:** Regular updates include security patches that protect against known vulnerabilities. David Nublaku emphasized the importance of updates, comparing them to changing "the keys to the doors" of your digital life.

5. **Password Security:**
   - Using strong, unique passwords for different online accounts is crucial.
   - Avoid using easily guessable information like birthdays or common phrases.
   - David Nublaku highlighted the risk of using the same password across multiple platforms, as a breach in one less secure site could compromise other more sensitive accounts.
   - He suggested using a combination of uppercase and lowercase letters, numbers, and special characters.
   - Corey Limer shared a mnemonic technique for creating and remembering complex passwords.
6. **Phishing Scams:**
   - These scams often involve emails or messages that look legitimate, sometimes including correct logos and formatting of well-known organizations.
   - The goal is to trick individuals into revealing personal information like passwords or financial details.
   - The crucial rule for online safety is **never to click email links**, even if they appear to come from trusted sources.
7. **Actionable Recommendations:**
   - Adopt the "stop, think, act" approach to all online interactions, especially unexpected messages or requests.
   - Be highly suspicious of any communication that creates a strong sense of urgency.
   - Never share personal or financial information in response to unsolicited requests via email, text, or phone.
   - Independently verify the legitimacy of requests by contacting the supposed sender through known and trusted channels.
   - Create strong, unique passwords for all online accounts and consider using a password manager or mnemonic techniques to remember them.
   - Enable two-factor authentication whenever possible for added security.

- Keep all devices and software updated regularly.
- Be wary of offers that seem too good to be true.
- Report suspicious emails, texts, and phone calls to the relevant authorities and service providers.
- If you believe you have been a victim of a scam, report it immediately.

8. **For More Information**
   - **Golden Tech Tips**: goldentechtips.com | youtube.com/@GoldenTechTips | corey@goldentechtips.com
   - **Aspire Wellness**: youtube.com/@Aspirewellnesszelienople | lutheranseniorlife.org/location/passavant-community
   - Ask for help at your local senior center or library

Remember: You're not alone! It's always okay to ask for help with technology.