INSURANCE BOARD
Partners in Protection

Cyber & Finance Ministry for Seniors and Vulnerable Adults

Seniors and vulnerable adults in your congregation may be at greater risk of becoming victims of financial abuse or cyber-crime due to sophisticated schemes that target people within vulnerable populations. A safety net should be used to help protect people from becoming victims.

Cyber Crime

There is a running joke about the emails people receive in their spam folders from the king of a far-off country offering an inheritance if we would only send money to claim the reward. The joke ends when a vulnerable party is duped into sending thousands of dollars to an offshore account guaranteeing their life savings are gone forever. Victims may not be familiar with the dangers of the internet or the ominous "Dark Web." Education, awareness, and advice are the keys to prevention.

Teaching seniors and vulnerable adults how to practice cyber safety can go a long way toward protecting their identity, sensitive personal information, and financial resources. Providing resources and training, or a cyber resource helpline (supported by church members with a technical background) can make all the difference between a positive online experience for someone or a complete disaster.

Please see the tips below regarding tactics that can be used to protect seniors or vulnerable adults while online:

1. **Passwords:** Use passwords, including one to lock a device, and close out internet or computer sessions when done. A strong password is at least 12 characters long with a mix of letters, numbers, and symbols (and should not include personal information).
2. **Secure access to accounts:** Since passwords can be stolen, adding two-step authentication (a system to provide a one-time access code) to accounts provides a second layer of protection. Many online services, including apps and websites, offer free options that could help you protect information and ensure that the proper person is trying to access an account – not just someone with a password.
3. **Think then act:** Communications that create a sense of urgency, such as a problem with a bank account or taxes, are likely scams. Consideration should be given to reaching out directly to the company by phone to determine if the email is legitimate or not. A helpline with qualified congregants could offer assistance and answer questions for seniors or vulnerable adults.
4. **Delete it:** Clicking on links in emails is often how scammers get access to personal information. If an email looks unusual, even if the person knows the party who sent it, it's best to delete it. Scammers can use a friend's email address and send someone messages acting as them. It is best to turn on spam filters for an email account to help filter out unwanted or suspicious messages and senders.
5. **Online sharing:** One should be careful of what is shared publicly on social media sites. Adjusting the privacy settings on the site can limit who can see information and avoid giving a location.
6. **Security software:** Install security software from a reliable source on devices and keep it updated. It is best to run the anti-virus and anti-spyware software program regularly. Avoid security updates from pop-up ads or emails-they could be malware that could infect a computer. Hosting an information session where people can bring in their personal devices to have someone assist them with security measures, or even scheduling appointments with individuals to offer assistance may be helpful.
7. **Browser safety settings:** If someone searches for news, information, or products by using an internet browser, adjust the settings in each of those browsers to select the options for optimal security. The menu choices can often be found in the upper right corner of the browser. Consider clearing the browsing history at the end of a session to avoid leaving a trail of sensitive data.
8. **Firewall security on a computer:** The computer's operating system (OS) likely has a

Continues on next page

INSURANCE BOARD
Partners in Protection

Cyber & Finance Ministry for Seniors and Vulnerable Adults, 2

default firewall setting that will protect a computer from outsiders without needing adjustment. An antivirus software program can include additional firewall protection that can be adjusted separately-consider contacting a computer professional for assistance.

9. **Logging out:** Remember to log out of apps and websites when they are not being used. Leaving them open on the computer screen could make a system vulnerable to security and privacy risks.
10. **Support**: If a trusted person (family member or caregiver familiar with computers) is not available to assist with questions, consideration should be given to hiring a service to serve as a trusted source and to act as a second set of eyes and ears.

Financial Crime

The first step in protecting at-risk individuals is identifying those congregants who may be susceptible to exterior influences. Changes in behavior and emotional state may help identify who may need assistance. If someone is becoming withdrawn, it can be a sign of a changing mental or emotional state. If someone is limiting a person's ability to interact with others, their motives may be nefarious.

The second step is determining what assistance can be provided to create a safety net for those who need it. A program that creates awareness of issues and available assistance without causing shame can be a saving grace for seniors and vulnerable adults.

Protecting Against Financial Abuse

- Develop a program that helps build awareness and identifies people in your congregation who may be at risk for financial abuse.
- Provide helpful resources to help people recognize when someone may be trying to manipulate or take advantage of them.
- A ministry can provide resources offering financial guidance through regular meetings or seminars conducted by qualified church members who could also be enlisted as a direct contact for those needing advice.
- Sadly those who are closest to a vulnerable party and have access to them (caregivers, neighbors, or other family members) are often the same people that exploit seniors and vulnerable adults for financial advantage.
- Financial records can provide a window into possible abuse. A simple act such as reviewing a checkbook or banking statement may provide clues.
- Clues may include an abnormally large amount of cash withdrawals or small checks written regulary to one person.
- Other signs of financial abuse can be:
    - Changes in bank accounts
    - Altered financial documents (such as a will or power of attorney)
    - Unusual changes in spending habits
    - Secretive financial discussions
- Often, legal action is needed to protect the victim of exploitation from a predator. This can involve contesting a trust agreement or will.

Please consult experts, an attorney, and/or licensed financial or computer professionals for specific advice on any program to protect your ministry and its members.

Also, see these resources:

- U.S. Department of Justice Office of Justice Programs
- Insurance Board's Cybersecurity 101