Aaron Poppas, infrastructure security engineer at GPM Corporation, talks about how you can protect your personal information and help thwart cybercriminals.

Residents of senior living communities and post-acute and long-term care facilities are prime targets for computer hackers seeking private information they can use and sell. Fortunately, there are many steps one can take to keep personal information secure.

First and foremost, don’t give any personal data — including date of birth, social security number, bank account or credit card numbers, medical information, and Medicare/Medicaid beneficiary information — to anyone in an unsolicited phone call or email.

Make sure you have strong passwords for each online account you have. Avoid using obvious information such as your name and date of birth, and don’t use the same password for all accounts. Of course, it can be challenging to remember all this information, so keep reminders about your usernames and passwords someplace secure, in a locked drawer, for example. Don’t put them on a sticky note on your desk or refrigerator.

Another key step is protecting yourself against “phishing.” This is when hackers get into your computer system and gain access to your information by getting you to open an email attachment containing malicious program or click on a link to a fake site asking for your passwords.

Phishing generally starts with an email containing a subject line designed to get you to open the message and click on the attachment. Most commonly, the subject is related to a financial issue (e.g., a problem with your bank account or credit card), or it offers something free or discounted.

How do you tell when something is a phishing email? There are a few hints:
• The message may seem to be from your bank, your insurance company, or one of your friends, but email address or the link doesn’t match. For instance, instead of mary-smith@gmail.com, the return address is info1@newvision.com or instead of capitalone.com, the URL is capitalone.com.
• The attachment file may have an .exe, .bat, .cmd, or .dmg at the end of its name.
• The message will include a request to enter a password. Don’t click on any links or enter any such passwords.

It is important to realize that a cyberattack can happen to anyone. If you do open a phishing message, you can minimize the damage by changing all your online passwords, and you may be able to put a special alert on key accounts such as your banking, credit cards, and mortgage company.

Some other cybersecurity tips include:
• Purchase and install antivirus software.
• Don’t leave devices open, turned on, or unlocked when they are out of your sight/control.
• When you leave a site (such as after checking your bank account), always remember to log out.
• Don’t accept “friend requests” or other offered connections on Facebook or other social media sites unless you know the person or the individual has been recommended or referred by a trusted source.

If your loved one has Alzheimer’s disease or other cognitive impairment, you may want to take steps to limit or secure their computer use. For instance, you can block certain sites, enable them to receive email only from select sources, and give them “pay as you go” cards with limited funds instead of credit cards.

Questions to Ask Your Practitioners
• Will you ever contact me via email about medical issues? What should I do if I get an email from you or your office?
• Do I have to give out my email address to practitioners, health insurance companies, community/facility administrators, and others?
• How do you secure my loved one’s or my personal information?

What You Can Do
• Use your email carefully. Don’t open or respond to emails from unfamiliar sources. Report any suspicious emails to the facility/community administrators.
• Don’t share private information, such as your credit card number or SSN, via email.
• Be very suspicious of an offer or promise that seems too good to be true or uses extreme urgency.
• When in doubt, err on the side of caution.

For More Information
• Federal Trade Commission, FTC Complaint Assistant (for reporting phishing emails and other online scams), https://ftc.gov/complaint