A challenge for senior citizens who embrace the computer age is knowing how to avoid online fraud. Although people of all ages are at risk, statistics show that when it comes to online safety, seniors are more vulnerable. In fact, according to the DHS, “seniors are defrauded at twice the rate of the rest of the population.” Yes, there are swindlers out there — based in another country or maybe even in your neighborhood — who want to steal from you or your loved ones. But there are also reliable ways to spot a scam and steer clear of fraud. Here, we explain common scam types and show you how to safeguard your valuables, savings and online information.

WEB OF DECEIT

Why are seniors targeted?

They’re savers: Fraudsters assume seniors have lots of money sitting in their accounts.

It’s a low-risk crime: Scams on seniors often go unreported or can be difficult to prosecute.

60% of National Fraud Information Center callers are seniors

$16 Billion was stolen from 5.4 million U.S. consumers in 2016

67% of U.S. seniors have been the victim or target of at least one online scam or hack
PROTECTING SENIORS FROM ONLINE SCAMS

SENIORS’ INTERNET UNFAMILIARITY IS TARGETED:

- Fake IRS email scams
- Bogus Financial Institution “verify information” messages
- Virus spread via pop-up windows

“People who grew up in the 1930s, 1940s, and 1950s were generally raised to be polite and trusting.”
— FBI website, 2018

WHAT ARE THE MOST COMMON ONLINE SCAMS?

Grandparent Scam

Grandparents are targeted because they're protective and want to help those they love, when they are in a crisis. A grandparent scam could look like this:

1. A con artist emails you, posing as distressed relative in distress
2. He tells a variation of a “Grandma, it’s me” story
3. He describes their dire problem (car crash, arrest, need a lawyer, etc.)
4. The senior is asked to send money for expenses to get out of trouble

THE CON ARTIST THEN SAYS “DON’T TELL ANYONE!”
PROTECTING SENIORS FROM ONLINE SCAMS

What to watch for: Never pay anything in this situation. A strong sign of fraud is being asked to pay with a card such as an iTunes or MoneyPak card, which don’t offer the protection of a credit card.

What to do: Don’t respond to the email. Delete it. Call your family and check that they’re ok. Report it to the proper governmental authorities including the Internet Crime Complaint Center or the Federal Trade Commission.

Tech Support Scam

When using the computer, it can be difficult to tell the difference between a real warning and a fake one. A computer warning scam can happen like this:

1. You’re using the internet and a window pops up out of nowhere
2. It looks like a “computer hack” or “virus” warning
3. It uses the name of a computer company such as Apple or Microsoft
4. It says you need to download something to “fix” a computer issue
5. It’s a virus or program designed to steal your information
6. You punch in your account information and your savings get drained

What to watch for: Computer companies don’t usually approach consumers to offer support — it’s us who go to them.

IF A COMPUTER COMPANY CONTACTS YOU ON THE INTERNET — IT IS PROBABLY A SCAM.
PROTECTING SENIORS FROM ONLINE SCAMS

What to do: Close the pop-up window — do not open it and absolutely do not enter your bank account details. If you notice further similar windows, have a family member or trusted computer repair store run a check or install virus protection.

Remote Control Scam

Phonies offer a free security check over the phone to get you to give them remote access to your computer for a supposed diagnosis and fix. They gain access, add software and steal from your accounts.

15% of people have been called by scammers who pose as tech-support staff

Lottery Scam

Who wouldn’t be excited to hear they’ve won the lottery? Scammers recognize the lure of a lottery win, and turn it into online scams.

1 in 175 MILLION

Your odds of winning the lottery
How do lottery scammers target seniors online?

1. You receive an email telling you you’re a winner. Yay!

2. They ask you to enter your credit card number, or write a check to cover “administrative fees.”

3. The winnings may actually turn up in your account...

4. Only to be removed when the “winning” check is found to be fake.

What to watch out for: This is a common scam. Be wary of any email that mentions a lottery win. These scams often claim you have won a foreign lottery.

What to do: Remember the odds of winning the lottery are tiny, and delete the email in question. Report it to the proper governmental authorities including the Internet Crime Complaint Center or the Federal Trade Commission.
Seniors are often targeted because of their generosity and kind-heartedness. That’s what makes scammers pose as a charity — to target elderly people online. Here is how they often attempt to carry out such an act:

1. A natural disaster happens
2. Fake charities send out emails to you, asking for a donation
3. They pose as a legitimate charity, or make up their own identity
4. They play on your emotions — perhaps saying children need your help
5. There is no apparent identification or authorization
6. You pay using your credit card, but your bank account is then drained

Once you have donated to a nonprofit, it is likely that they will contact you through email to ask for continued support. Avoid any charity or fundraiser that refuses to provide detailed information about its identity, mission, costs, and how the donation will be used.
Here’s how to avoid a charity scam:

- Beware of any charity that asks you to send money overseas
- Delete emails with attachments — they probably are not real
- Investigate groups that make pleas over social media
- Criminals wait for disasters such as Hurricane Harvey and other natural devastations to set up websites asking for money. Only use authorized sites if you choose to donate.

WHEN CONSIDERING MAKING A CHARITY DONATION:

Do your research and don’t take an email request on face value or make a hurried decision. Ask family members for advice if you find something online about a charity you might like to support. Don’t support any charity by responding to a random email from an unknown source.
GENERAL RULES FOR AVOIDING ONLINE SCAMS

Don’t send money or give out personal information in response to an unexpected online request.

Do online searches for potential scams, such as “IRS scam”.

Don’t pay anything (fees, admin costs) upfront when someone promises something.

Government offices and trustworthy companies don’t ask you to pay with a reloadable card.

Be skeptical about free trials.

Sign up for free scam alerts. Click here to sign up!

When possible, purchase through a HTTPS site, as opposed to HTTP. The “S” stands for “secure”.

HTTPS sites are “secure” sites for making transactions. HTTP sites (notice there’s no “S”) are less safe. Steer away from these when prompted to enter personal details.
PROTECTING SENIORS FROM ONLINE SCAMS

DO YOU KNOW SOMEONE THAT YOU SUSPECT MAY BE VICTIM?

Here are some symptoms fraud victims can show:

• There are unusual changes in the person’s accounts, including atypical withdrawals, new people added, or sudden card use.
• The senior suddenly appears confused, unkempt, and afraid.
• Utility, rent, mortgage, medical, or other bills are unpaid.
• A caregiver won’t allow others access to the senior.
• There are piled up sweepstakes mailings, magazine subscriptions, or “free gifts,” which means they may be on “sucker lists.”

You should feel safe on the internet.

The internet need not be a threatening environment if you know what to look for, and don’t offer any personal information to unknown sources. Using only authorized sites, doing some research, and avoiding engagement with dubious emails and pop-ups will ensure you’ll stay perfectly safe from scammers.

Disclosure: The recommendations in this article are suggestions only, and are not to be taken as surefire solutions. Please know that when on the internet you are at your own risk.
PROTECTING SENIORS FROM ONLINE SCAMS

Sources

https://www.ag.state.mn.us/consumer/publications/seniorsguidefightfraud.asp
https://www.google.com/search?q=what+are+the+odds+of+winning+the+lottery&oq=what+are+the+odds+of+winning+the&aqs=chrome.0.0j69i57j0i4.5778j0j7&sourceid=chrome&ie=UTF-8
https://www.charitynavigator.org/index.cfm?bay=content.view&cpid=313
https://www.consumer.ftc.gov/articles/0060-10-things-you-can-do-avoid-fraud
https://www.homeinstead.com/370/blog/survey-two-thirds-of-seniors-have-been-scammed-online
https://www.consumer.ftc.gov/articles/0074-giving-charity
https://www.usa.gov/online-safety
https://www.instantssl.com/https-tutorials/what-is-https.html
https://www.dhs.gov/sites/default/files/publications/Cybersecurity%20for%20Older%20Americans_0.pdf