



Lifelong Education & Aging Resource Network

Health • Wealth • Lifestyle • Caregiving

ONLINE FRAUD AND SCAMS

Some of the most common types include **phishing and social engineering**.

You may encounter these scams on a website, in an email or text message, or even in a pop-up window on your computer.

Phishing

Scammers use **fake emails or text messages to “fish” for information**.

These fake messages can look real, but link to **fake websites**. The website may look like a trusted, well-known company, organization or government agency, but it's all a trick to get your information – such as your Social Security number or bank number and credit card account numbers.

Malicious Software

A fake email can also be used to **infect your computer with malicious software**, referred to as malware, or a virus as soon as you open the email. Malware is a tool used by scammers that can take many different shapes. For example, malware can lead to viruses that infect your computer or “spyware” that tracks your online activities.

You may be able to tell when malware has been installed on your computer or device if you see **these signs: pop-up ads appear and they are hard to close; new or unfamiliar toolbar icons appear on the screen; or your computer or mobile device is not responding as fast as it used to**.

Social engineering

It's a new name for an old con-artist trick. In this scam, a fraudster tries to gain your trust by convincing you they are someone they are not, in order to get personal information from you.

These fraudsters can approach you by **phone, email, text or social media**.

Goals

To steal your money or collect information like your passwords or credit card numbers. Scams can also cause problems for your computer by infecting it with viruses or malware.

Phishing and social engineering may be encountered:

- while searching a website
- in an email or text message
- in a pop-up window on on your computer

Recognizing scams

- Have you heard of the person or organization before?
- Can you tell who the email message is from?
- Does the email look professional?
- Do they claim that they can fix your computer?
- Are they asking for your information?
- Are they trying to rush you into a quick action before taking the time to think about it?
- Is it too good to be true?

Here are some dos and don'ts:

- Don't give out personal information to something that could be a scam.
- Don't reply or engage them.
- Don't click on any links in a scam email.
- Don't download any email attachments or files on an untrustworthy website.
- Do be skeptical.
- Do look up their contact information on your own, from a statement you've received in the mail or from their official website.
- Do try using another method to close the pop-up window.

Reporting Scams

- phishing@irs.gov.
- Put the message in spam or junk folder. This helps email providers identify and prevent scams.
- File official complaints with the Federal Trade Commission by visiting their website at reportfraud.ftc.gov

Provided by AT&T Connected Learning + Public Library Association

None of the other companies whose names or logos appear in these educational materials have been involved in the creation of these materials, or approve, sponsor, or are affiliated in any way with these materials.