**🛡️ Phishing Scam Mitigation Strategies \*\*SAGE\*\*\***

🔹 1. Build Awareness & Spot the Signs

Check the sender address → scammers often use addresses that look similar to trusted companies.

Look for urgency or fear tactics → “Your account will be locked!” is a red flag.

Hover over links before clicking → see if the URL is strange or doesn’t match the company.

Poor grammar or spelling → legit companies rarely make big mistakes.

🔹 2. Technical Protections

Enable spam filters in email accounts.

Use multi-factor authentication (MFA) on important accounts (banking, email)

Keep software & browsers updated → reduces risk from malicious links.

Install reputable security software with phishing site protection.

🔹 3. Safe Habits

Never click suspicious links → instead, go directly to the website by typing the URL.

Don’t download unexpected attachments (especially .zip, .exe, .pdf from unknown senders).

Verify with a phone call if an email or text looks odd, even if it seems to come from a friend.

🔹 4. Education for Elderly Users

Use real-world examples of phishing emails (print screenshots, circle red flags).

Teach the “pause and think” rule before clicking or replying.

Encourage use of a trusted buddy system → if unsure, show the message to a friend/family before acting.

Use simple analogies:

“Just like a stranger at your door asking for money — don’t hand it over.”

🔹 5. Community Support

Host small workshops at libraries, senior centers, or churches.

Share weekly tips in simple language (like “Never click on an email that asks for gift cards”).

Encourage elderly users to teach each other — peer learning reinforces habits.

Provide a printable checklist with “Top 5 Rules to Avoid Phishing.”

✅ Example Elderly-Friendly Teaching Approach:

Show them two emails side by side (real vs fake).

Point out sender address, urgency, bad links.

Role-play: “If you see this, what should you do?”

Have them teach a friend — teaching reinforces learning.

[How to Prevent Phishing Scams: A Guide for Seniors](https://www.ncoa.org/article/how-to-prevent-phishing-scams-a-guide-for-seniors/)

How to Prevent Phishing Scams: A Guide for Seniors

[**Scam and Fraud Prevention**](https://www.ncoa.org/older-adults/money/management/avoiding-scams/)

Dec 09, 2021

6 min read

Print Page

Share



**Key Takeaways**

* Phishing is one of the internet’s oldest and most well-known scams. There are many types of phishing attacks used by cyber criminals.
* Unlike spam (junk mail), phishing attacks are deliberate attempts to steal your information and use it in unlawful ways.
* Knowing how to spot phishing emails is the first step in keeping your sensitive personal information safe from thieves.

Elderly scams are a multi-million dollar business that robs seniors of their hard-earned savings, retirement funds, and even government benefits.

The financial damage can be devastating: in 2020, the Internet Crime Complaint Center (IC3) [reported](https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud) losses in excess of $966 million for people age 60 and over.

While there are many methods cyber criminals use to defraud older adults, [phishing](https://www.avast.com/c-phishing#gref) is one of the internet’s oldest and most well-known scams.

What is phishing?

Phishing is a type of internet hoax in which scammers use email and other methods to steal personal information, such as financial details or account passwords. This approach earned its unusual name because it uses attractive “bait” to lure people to websites and solicit their data under false pretenses.

Phishing is not the same as spam. While spam is just another term for junk mail and unwanted ads, phishing attacks are deliberate attempts to steal your information and use it in harmful ways.

How does phishing work?

There are three main components to a phishing scam:

1. The attack is conducted via electronic communications. Although email is common, phishing can also be carried out via text messages, social media accounts, voicemail, and even phone calls.
2. All forms of phishing aim to convince you that a fake communication is real and credible. The attacker claims to be an individual or organization that’s familiar and trustworthy to you.
3. The goal of a phishing attack is to obtain sensitive personal information, such as login credentials, bank details, or credit card numbers.

With all phishing attacks, the scammer delivers a carefully crafted pitch aimed at getting you to click a link, download an attachment, or provide specific personal information. In some cases, you may even be asked to make a payment, and most recently [we’ve seen scammers using the COVID-19 vaccine rollout](https://www.ncoa.org/article/how-seniors-can-avoid-covid-vaccine-scams/) to steal Medicare numbers and personal information. Some common phishing attack examples include:

* **A plea for help:** With a goal of tugging at your heartstrings, the attacker sends you an email pretending to be a good friend or relative (e.g., your grandchild). They claim to be in financial dire straits and request your assistance immediately. How are cyber criminals able to impersonate people you know? With social media, scammers have access to more of our personal information than ever before. This allows them to make their messages highly targeted—and often very believable.
* **You’re the grand prize winner:**You receive a text message congratulating you on being the winner of a very big prize, whether it's an irresistible travel package deal or free tickets to the event of the year. You're asked to provide your personal details in order to claim your award.
* **Your bank account has been compromised:**You get an “urgent” notice that appears to be from your bank, alerting you of suspicious activity on your account. You're then asked to click a link that takes you to a website, where you'll be prompted to confirm your bank account information.
* **The government is after you:**Few things in life are as jarring as an authoritatively worded notice from the Internal Revenue Service (IRS). Scammers know this, which is why many phishing emails appear to be from the U.S. government. An email like this typically has a threatening tone and mentions big, scary penalties—unless you provide the payment or personal data they demand.

These types of phishing attacks have a flip side, too. In some cases, they’re sent during tax season, offering you a generous refund after you confirm your financial details.

Why does phishing work so well?

Emails, text messages, voicemail messages, and even voice calls are not authenticated. This means that, just like a postcard sent through the mail, there’s no real way to validate where they came from. That gives scammers plenty of freedom to mimic trusted brands in their communications.

 “Phishing is one of the most common and pervasive threats. A 2021 report by Avast found that the chances of consumers encountering phishing scams has increased by 20% in the June-October period, compared to the first five months of the same year," said Emma McGowan, a privacy and security expert at Avast.

Sophisticated phishers are very skilled at creating spoof email templates and websites that are almost indistinguishable from the real thing, right down to the URL (website address) and security certificates. You may think you’re receiving a credible message from a bank, online store, or credit card company. And if you’re not paying close attention, you might not notice the trickery until it’s too late.

How do you avoid phishing scams?

Knowing how to stop phishing emails and texts means knowing what to look for. While scammers are always changing their approaches to evade detection, certain red flags can help tip you off to trouble. Some [telltale signs](https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams) of a phishing email or text message include:

* Offers that seem too good to be true
* High-pressure sales pitches that stress urgency
* Alerts that there’s a problem with your account (e.g. suspicious activity or outdated payment information)
* [Shortened](https://whatis.techtarget.com/definition/URL-shortening) or misspelled links
* Emails that don't address you by name
* Messages with poor grammar and spelling
* Direct requests or demands for payment
* Requests to confirm personal information

The best defense against a phishing scam is to verify with the person or organizations who sent the email or message before clicking on anything," McGowan continued.

Remember that you can never be 100% certain that the sender of an email, text message, voicemail, or phone call is who they say they are. That’s why it’s important to approach every communication with a healthy dose of skepticism. Here are some personal cybersecurity best practices to keep in mind:

1. Don’t click on any links found within emails or text messages if the original message was not initiated by you.
2. Navigate to trusted websites by typing the web address directly into the browser address bar—instead of clicking on a link.
3. Verify [security certificates](https://www.makeuseof.com/tag/website-security-certificate-care/) of websites by clicking the small padlock icon in the left corner of the browser address bar. Make sure the URL begins with “HTTPS.” An HTTPS connection is protected by a special type of security technology, which means that any information you send through the website is kept private.
4. Do not send personal information in email or text messages. Again, this information is not secure, and you can’t be sure who the recipient is.
5. Never give out personal information over the phone during calls that are not initiated by you. Always double-check to make sure you’re using the correct phone number of the person or business you’re trying to contact.

When it comes to preventing phishing scams, education is a powerful way to protect yourself. Installing reputable antivirus software on your devices is another. Many of these software programs contain an anti-phishing tool that detects and blocks phishing attempts before they reach you. There are a number of trusted options [available for free](https://www.digitaltrends.com/computing/best-free-antivirus-software/) on the web.

*This content on phishing was developed in partnership with*[*Avast*](https://www.avast.com/?utm_source=ncoa&utm_medium=blog&utm_campaign=elders&utm_content=phishing)*. Learn more about Avast’s*[*privacy and security software*](https://www.avast.com/avast-one?utm_source=ncoa&utm_medium=blog&utm_campaign=elders&utm_content=phishing)*and how it can help protect your information and data.*