Delaware Life®

Delaware Life Income Planning Institute®

Online safety vs. cyber scams

Cyber scams are nothing new, but they have become more prevalent and easier to create due to the advent of artificial intelligence, ChatGPT, and other technological advances. According to the FBI's Internet Crime Complaint Center (IC3):

"In 2024, IC3 received a number of complaints from the American public: 859,532 complaints were registered, with a record loss exceeding $16.6 billion. This is 33% increase in losses suffered, compared to 2023."

These numbers are likely higher because not all incidents and losses are readily reported to the authorities.

Think you are not worth being the target of online predators? Think again! Hackers don't need to know how much is in your bank account to want to get into it. Your identity, your financial data, what's in your email—it's all valuable. Cybercriminals will cast a wide net. They are not playing by any rules, they are persistent, and they want to get to you one way or another. They're counting on you thinking you're not a target.

How can you reduce the chances of falling for the scams? Learn the signs! Here are 10 easy, commonsense cyber hygiene practices you can use to protect yourself online.

Delaware Life's online safety checklist

- ☐ 1) **Turn on multifactor authentication.** Implementing multifactor authentication on your accounts can help reduce the likelihood you'll get hacked. It is an extra step on top of your password (which can be more easily cracked or stolen) in which trusted websites and applications ask you to confirm you're really who you say you are. Your bank, your social media network, your school, your workplace—they want to make sure you're the one accessing your information. Multifactor authentication can be a) something you know, b) something you have, or c) something you are.
- ☐ 2) **Update your software.** Turn on automatic updates to ensure your software stays up to date. Bad actors are constantly upgrading their hacking tools and techniques. Network defenders, anti-virus safety protocols, and firewalls are intended to fix any flaws or glitches. It is up to you to update your software with the latest fixes.
- ☐ 3) **Think before you click.** More than 90% of successful cyberattacks start with a phishing email. If it's a link you don't recognize, trust your instincts and think before you click. Phishing could come via email, a text message, or even a phone call. Implement Zero Trust environment.
- ☐ 4) **Be cautious while online in public places.** Don't use public Wi-Fi in internet cafes, hotel lobbies, airports, or anywhere internet access is not secure.
- ☐ 5) **Utilize cognitive security.** This is the mental piece of online security. Hackers are persistent and don't play by any rules; they want to get to a desired target one way or another. Before you click, ask some critical questions:
  a) Why am I receiving this?
  b) What's the story behind it? What emotions do they want to evoke?
  c) What do they want me to do or believe?

6) **Use strong passwords or even better a passphrase.** Make your passwords as strong as possible by creating the longest password or passphrase permissible, using various characters such as lower case, upper case, and special characters. Be sure to customize your standard password for different sites. Even better, use a password manager to generate and store your unique passwords.

7) **Don't answer calls from unknown numbers.** If you don't recognize the number and it is a legitimate call, the caller will leave a voicemail. If it is not, they won't leave a voicemail and will disconnect.

8) **Don't give out personal information.** Keep your private information private. This includes your full name, employer, job title, account numbers, Social Security number, mother's maiden name, home address, date of birth, family members, passwords, or any other identifying information. Guard your information from unexpected calls, emails, texts, and all other suspicious activity.

9) **Educate yourself and your family.** Establish computer usage guidelines for your family, and help your children understand how to use the computer, other connected devices, and the internet safely. Have candid, age-appropriate conversations with younger users to help them understand the dos and don'ts of cybersecurity.

10) **Beware of deep fakes.** Bad actors can develop scams via inexpensive or free tools by using images, video, and voice recordings. For example, voice cloning is used to spread misinformation that ranges from mass robocalls/robotexts (e.g., campaign messages) to individual calls for extortion of money (e.g., loved one kidnapped or in an accident.)

"Voicemails, public speaking, and videos are used to produce voice cloning and only three seconds of the recording is needed to create a 'deep fake.'"

— Greg Bohl, Chief Data Officer, Transaction Network Services

Sources:

https://www.cisa.gov/cybersecurity-awareness-month;

https://www.cisa.gov/topics/cybersecurity-best-practices;

https://www.cisa.gov/topics/cybersecurity-best-practices/identity-theft-and-personal-cyber-threats;

https://www.cisa.gov/secure-our-world/use-strong-passwords;

https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf;

https://www.fbi.gov/contact-us/field-offices/philadelphia/news/fbi-philadelphia-emphasizes-strong-passwords-for-cybersecurity-awareness-month;

https://www.fcc.gov/sites/default/files/CAC-Minutes-26June2024.pdf; all accessed 12/24/2025

delawarelife.com

Annuities are issued by Delaware Life Insurance Company, and variable annuities are distributed by Clarendon Insurance Agency, Inc. (member FINRA). Both companies are members of Group One Thousand One (Group 1001).

This communication is for informational purposes only. It is not intended to provide, and should not be interpreted as, medical or Social Security, individualized investment, legal, or tax advice. To obtain such advice, please consult with the appropriate professional.

Guarantees are backed by the financial strength and claims-paying ability of Delaware Life Insurance Company (Zionsville, IN).

Withdrawals of taxable amounts are subject to ordinary income and, if made before age 59½, may be subject to a 10% federal income tax penalty.

NOT FDIC INSURED | MAY LOSE VALUE | NO BANK OR CREDIT UNION GUARANTEE
NOT A DEPOSIT | NOT INSURED BY ANY FEDERAL GOVERNMENT AGENCY OR NCUA/NCUSIF

© 2026 Delaware Life Insurance Company. All rights reserved.