



# Beware of cyber crimes

***“In 2023, the FBI Internet Crime Complaint Center (IC3) received a record number of complaints from the American public: 880,418 with potential losses exceeding \$12.5 billion. Nearly a 10% increase in complaints and a 22% increase in losses compared to 2022...”***

Access to the internet and the conveniences it offers have altered how we behave in our daily activities. From basic communication, shopping and banking to complicated financial transactions and gaming and entertainment, we now rely on computers and technology more than ever before.

We post details about our lives on social media, or various companies disclose our personal information without our knowledge or permission. At the same time, all of these “innocent” activities expose that information to cybercriminals.

With easy access to computers and the convenience of online technology and anonymity, cybercriminals can exploit cybercrimes for financial gain, espionage, sabotage, and cyberbullying.

To cybercriminals, your personal information has value: Here are examples of prices cybercriminals will pay for your financial data:<sup>2</sup>

- Credit card details (account balance up to \$5,000): \$20 in 2020 and \$240 in 2021
- Hacked Facebook account: \$75 in 2020 and \$65 in 2021

## What gets stolen online and how?

- Social Security number
- Online payment service login info
- Credit or debit card
- Driver’s license
- Loyalty accounts
- Diplomas
- Passports
- Medical records
- Subscription services
- General non-financial logins

Cybercrime takes many formats: phone calls, emails, text SMS, and of course online, and the consequences are enormous, whether financial or reputational, and can lead to self-harm and even suicide.

## What to do about it?

***“The strongest cybersecurity defense is not a sophisticated tool or technology, it’s the people and their vigilance to spot suspicious activity. Humans are the best sensors for cyber-threats.”***

– Aryn Gilani, Director of Threat Management at Group 1001

Be very cautious and vigilant when online or when dealing with unknown actors.<sup>3</sup>

- Protect your systems and data.
- Keep systems and software up to date.
- Install a strong, reputable anti-virus program.
- Create a strong and unique passphrase for each online account you hold.
  - Using the same passphrase across several accounts makes you more vulnerable if one account is breached.

- Do not open any attachments unless you are expecting a document or invoice and have verified the sender’s email address.
- Protect your connections.
- Be careful when connecting to a public Wi-Fi network.
  - Do not conduct any sensitive transactions, including purchases, when on a public network.

much more difficult to hack versus passwords with fewer characters.<sup>4</sup>

**Hint:**

*Adding “!” to the end of your password is not “securely” changing it*

## The importance of passwords

Having strong passwords is extremely important to keep your information safe. Consider the following steps when creating passwords:

- Use a password manager for unique, strong passwords.
- Enable a multifactor authenticator (MFA) on your accounts.
  - MFA is something you know, you have, you are.
- Check your passwords periodically.
- Change all exposed passwords.

Remember that most hacked passwords are nicknames, terms of endearment, TV characters, TV shows, colors, cities, countries, etc. Consider 12-character passwords with at least one uppercase letter + symbol + number, which are

## Check your own information and report abuse

Check if your email has been compromised in a data breach: <https://haveibeenpwned.com>

Check if your phone number or email address has been leaked:

<https://cybernews.com/personal-data-leak-check/>

Report bitcoin abuse and other malicious crypto activity: <https://www.chainabuse.com>

Have information regarding a cybercrime? Contact Homeland Security Investigations (HSI) at

1-877-4-HSI-TIP or contact your local HSI office.

Sources:

<sup>1</sup> [https://www.ic3.gov/AnnualReport/Reports/2023\\_IC3Report.pdf](https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf).

<sup>2</sup> <https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it>.

<sup>3</sup> <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/on-the-internet>.

<sup>4</sup> <https://www.cisa.gov/secure-our-world/use-strong-passwords>.

## 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**

© 2024 Delaware Life Insurance Company. All rights reserved.