Delaware Life®

Delaware Life Income Planning Institute®

Beware of cyber crimes

"In 2024, the FBI Internet Crime Complaint Center (IC3) received a record number of complaints from the American public: 859,532 with potential losses exceeding $16.0 billion - a 33% increase in losses compared to 2023..."[1]

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. The average price for your personal information can range from as little as $1 to more than $4,000.[2]

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, deep fakes, and of course online. The consequences are enormous, whether financial or reputational, and can lead to self-harm and even suicide. The FBI is also warning individuals and businesses to be aware of the escalating threat posed by cyber criminals utilizing artificial intelligence (AI) tools to conduct sophisticated phishing/social engineering attacks and voice/video cloning scams.[3]

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."

— Amyn Gilani, Director of Threat Management at Group 1001

Be very cautious and vigilant when online or when dealing with unknown actors.[4]

- Protect your systems and data.
- Consider a credit freeze at three major credit bureaus: Equifax, Experian, TransUnion.
- Limit your digital footprint or take steps to remove personal information online.
- 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.

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 much more difficult to hack versus passwords with fewer characters.[5]

Hint:

Adding "!" to the end of your password is not "securely" changing it

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:
[1] FBI Releases Annual Internet Crime Report, April 23, 2025; FBI Internet Crime Report, 2024
[2] Here's What Your Data Sells for on the Dark Web, June 30, 2025
[3] FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence, May 8, 2024
[4] FBI On the Internet: Be Cautious When Connected, no date given
[5] Cybersecurity & Infrastructure Security Agency: Use Strong Passwords, no date given

delawarelife.com