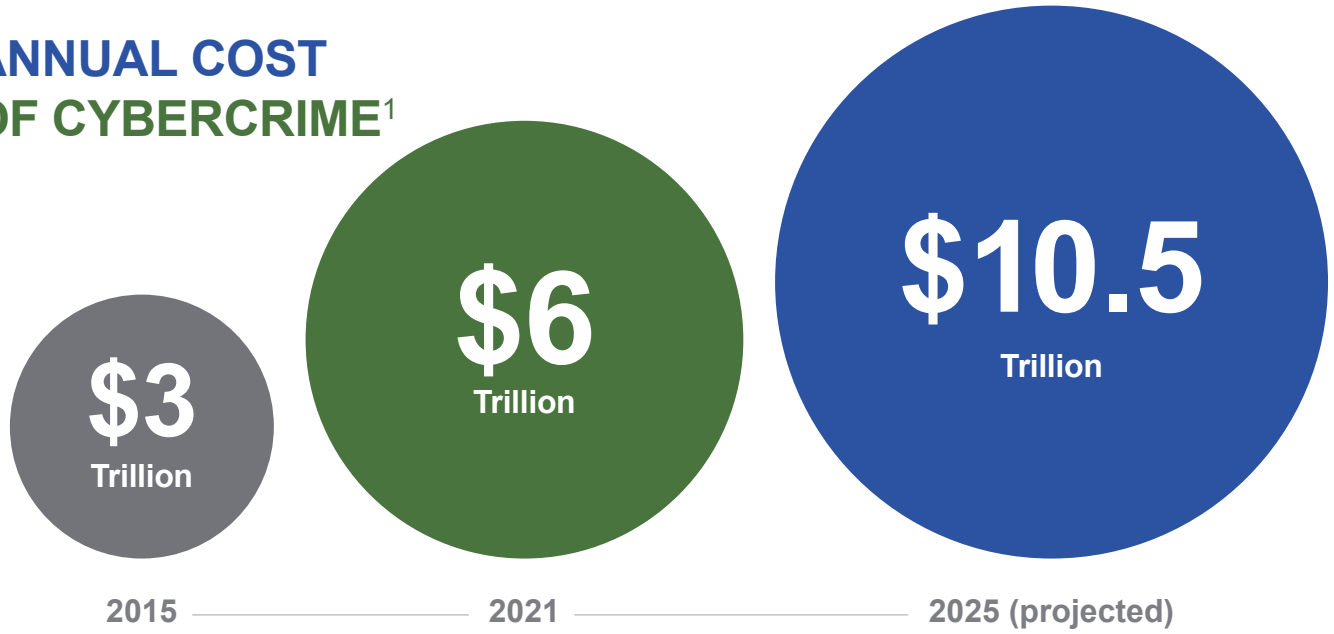
CYBERSECURITY: PROTECT YOUR RETIREMENT SAVINGS

Tips to Help You Keep Your Savings Safe Online

ANNUAL COST OF CYBERCRIME[1]



With trillions of dollars in America's retirement savings plans, your hard earned savings aren't immune to cybercriminals.

HACKERS ARE SMART; THEY ONLY NEED A FEW THINGS TO DRAIN AN ACCOUNT:

When it comes to keeping your retirement savings from falling into the hands of cybercriminals, your employer isn't the only one responsible. While they likely have cybersecurity measures in place, you also play a critical role in safeguarding your retirement accounts.

THIS EASY-TO-USE CHECKLIST OF ONLINE SECURITY TIPS CAN HELP YOU KEEP YOUR RETIREMENT SAVINGS SAFE FROM CYBERTHIEVES.[2]

- ☐ **Regularly monitor online accounts:** Set up and monitor your retirement accounts online and check in regularly to help reduce the risk of fraud and identity theft.
- ☐ **Create strong, unique passwords:**
  - **Avoid dictionary words and common letter and number sequences (i.e., "abc", "123").**
  - **Passwords should be longer than 14 characters.**
  - **Never write your passwords down, and don't share or reuse passwords.**
  - **Change your passwords frequently, at least every 120 days or when there's been a security breach.**
- ☐ **Use two-factor or multi-factor authentication:** This security method requires a secondary form of identity verification, such as entering a code you receive by email or text in real-time.
- ☐ **Keep contact information up-to-date:** Make sure your retirement account contact information is current so you can be reached should a problem arise. Choose multiple contact methods, such as email and text.
- ☐ **Close or delete unused online accounts:** Keep your online presence as minimal as possible to maximize security and reduce risk. Sign up for account notifications to keep tabs on unusual activity, such as unauthorized logins or transactions.
- ☐ **Use private Wi-Fi networks:** Avoid accessing your retirement accounts and other sensitive information using public hotspots in airports, libraries and coffee shops, for example. These aren't secure and, therefore, are easily accessed by cybercriminals. Your cell phone and home Wi-Fi network are more secure options.
- ☐ **Beware of phishing attacks**: Cybercriminals use phishing scams to try to trick you into giving up passwords, account numbers and other sensitive information to gain access to your accounts. Often, a phishing message will look like it is coming from a trusted organization to entice you to click on a fraudulent link or offer up some confidential information. Don't fall for it!

Telltale warning signs of phishing attacks may include:

- **A text or email you weren't expecting from someone you don't know or a service you don't use**
- **Requests for your account numbers or personal information, such as passwords or answers to security questions. (Legitimate providers will never ask you for this information via email or text.)**
- **Offers or messages that seem too good to be true, urgent or that are overly aggressive or scary**
- **Strange or mismatched sender addresses**
- **Short, odd or mismatched links (you can often spot them by hovering over the link without clicking on it. If it goes to a destination you don't recognize, don't click on it.)**
- **Spelling mistakes or poor grammar**
- **Anything else that makes you feel uneasy**

- ☐ **Install trustworthy antivirus software and keep apps and software up to date:** Make sure to have the latest antivirus software installed on all your computers and mobile devices and download recent upgrades and patches to protect them from viruses and malware. Many vendors offer automatic updates.
- ☐ **Recognize how to report and respond to identity theft and cybersecurity fraud:**
  You can report cybersecurity incidents to the FBI and Department of Homeland Security at the following websites:
  - **FBI Cyber Incident Reporting**
    www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf
  - **Cybersecurity & Infrastructure Security Agency Report Cyber Incidents**
    www.cisa.gov/reporting-cyber-incidents

We hope this information helps you keep your savings safe and away from cyber criminals. For more best practice guides and educational material on savings, budgeting and other financial wellness, CONTACT US.

NORTHEAST BENEFIT SERVICES INC.

Larry Kavanaugh, Jr. AIF®, CPFA, CLU, ChFC

950-A Union Rd. Suite 31
Buffalo, NY 14224
716.674.7200

L.Kavanaugh@nebstpa.com www.nebstpa.com

[1] Morgan, Steve. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025." Cybersecurity Ventures. 13 Nov. 2020.

[2] Employee Benefits Security Administration (EBSA) and U.S. Department of Labor (DOL). "Online Security Tips."