EMPOWER Invest well. Live a little.™

Exploring Advancements in AI and Cybersecurity

Trish McGinity, CISSP, CCSK
Head of Cybersecurity Communications

Agenda

1. Why should I be concerned?
2. What good security looks like: Cybersecurity and AI
3. Fraud protection & Security Guarantee
4. Continuous and extensive oversight (DOL/SEC/SPARK)
5. Protect your data, your identity, and your money
6. Questions and answers

Invest well. Live a little.™

Why should I be concerned? Cybersecurity Trends

Breach versus fraud

SECURITY BREACH

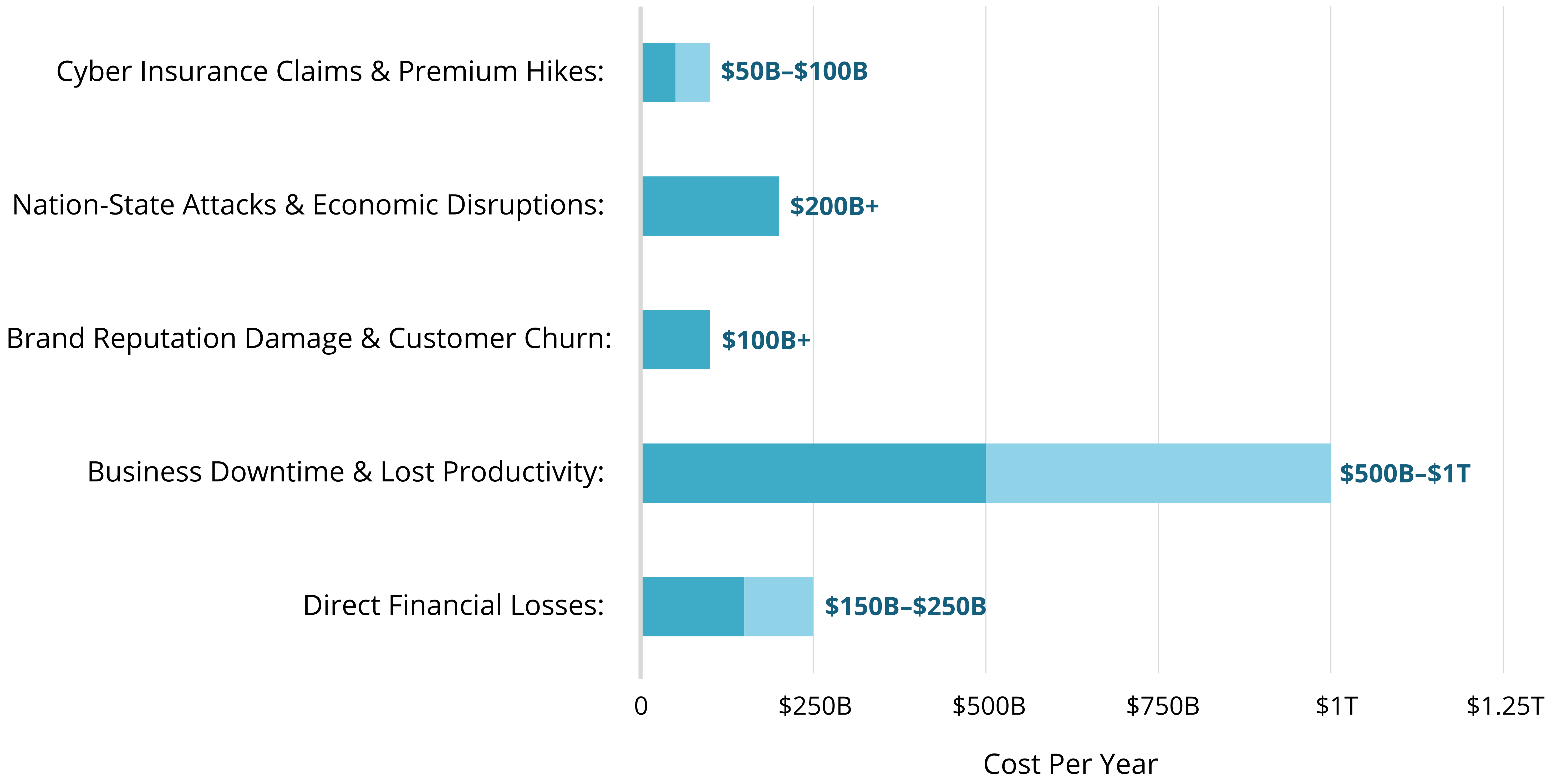
A confirmed **compromise** of an **information system** within the authority or responsibility of the recordkeeper that results in the unauthorized acquisition; disclosure; modification; or use of unencrypted **personal data**, or encrypted personal data where the encryption key has also been compromised, and a potential risk of identity theft or fraud against the data subject

CYBER FRAUD

A confirmed compromise of an **individual's financial account** by a fraudster using information within the fraudster’s possession or control that results in **wrongful financial** or personal gain or illegal access to a financial account

The Escalating Economic Threat of Cybercrime

The Global Cost of Cybercrime (2025 Projection)



The Bottom Line:

Cybercrime was a $1.2 Trillion problem in 2025

[The True Cost of Cybercrime: Why Global Damages Could Reach $1.2 – $1.5 Trillion by End of Year 2025. March 2025.]

FBI crime statistics[1]

#1&2
crime loss
Investment & business email compromise[1]

#1
crime vector
Phishing & Spoofing[2]

$11.4
billion
cryptocurrency investor losses in 2025[3]

$893
million
AI scams (fake social profiles, voice clones, ID docs, videos)[4]

2025 Victims by age range (crimes reported to FBI)[5]

Age range	2025 total count	2024 total Loss	2025 total Loss	total increase from 2024
Under 20	31,254	$22.5 million	$67.1 million	198%
20-29	112,069	$540.1 million	$563.1 million	4.26%
30-39	153,293	$1.4 billion	$1.742 billion	24.4%
40-49	167,066	$2.2 billion	$2.957 billion	34.4%
50-59	124,820	$2.5 billion	$3.676 billion	18.28%
Over 60	**201,266**	**$4.8 billion**	**$7.748 billion**	**61.42%**

1 Federal Bureau of Investigation - 2025_IC3Report.pdf
2 2025_IC3Report.pdf
3. Can You Write Off Crypto Losses on Your Taxes? - Experian
4. 2025_IC3Report.pdf
5. 2025_IC3Report.pdf
6.. BEC Trends: Payroll Diversion Dominates and Sneaky Multi-Persona Attacks Emerge (trustwave.com)
7. Who experiences scams? A story for all ages | Federal Trade Commission (ftc.gov)

- Business email compromise schemes resulted in **nearly $3 billion** in losses, remaining one of the most financially damaging fraud types.[2]
- Investment scams generated **$8.6 billion in losses** in 2025, making it the costliest form of cybercrime.[2]
- Payment diversion scams involve fraudsters creating a **false sense of urgency** — often after claiming a supplier's **bank details have changed**. Always verify bank account changes through a known contact method before sending funds.[6]
- 2026 AFP Survey indicates payments fraud remains widespread, with **76% of organizations** reported **attempted or actual fraud** in 2025.[8]
- **Checks** remain the payment method most frequently impacted by fraud. In 2025, **58% of organizations** reported **check fraud**, outpacing **ACH fraud** and **wire fraud.**[8]

What changed in cyber risk this year?

1. Fraud is the primary source of loss

- Investment scams, BEC, and payment diversion dominate losses
- Cyber is now **financial crime, not just data breaches**

2. AI is accelerating attacks

- Voice cloning, impersonation, and personalized scams
- Faster phishing, better social engineering
- Attackers scale with automation

3. Your attack surface is expanding

- APIs = faster integration **+ more exposure**
- Third-party vendors extend your risk footprint

4. Future risks are becoming current

- "Harvest now, decrypt later" (quantum risk)
- Data stolen today may be exposed later

Cyber risk now has 3 defining characteristics:

1. **Faster** → attacks happen in minutes, not days
2. **More convincing** → AI removes "red flags"
3. **More connected** → vendors + platforms = shared risk

Bottom line:
More frequent, more financial, more systemic losses

What You Should Do About It ?

1. Protect against fraud (highest ROI)
- Verify all payment or account changes offline
- Train teams on impersonation + urgency tactics
- Watch for investment/crypto scams

2. Secure identity & access
- Enable **MFA everywhere**
- Use **password managers**
- Monitor account activity and alerts

3. Manage third-party & ecosystem risk
- Treat vendors as **extensions of your business**
- Require:
  - security reviews
  - breach notification standards
  - incident response alignment

4. Prepare for what's next (AI + quantum)
- Understand how your data is used in AI tools
- Plan long-term for encryption changes
- Stay aligned with regulatory expectations

The most effective controls are still simple: Pause, Verify, Protect

Polling Question

How long does it take an average hacker with AI to crack a complex password with 8 characters?

Under an hour	About 7 hours	About 24 hours	About 2 - 3 days
A	B	C	D

Security Hero, “An AI <Just cracked your> password” (Octber 1, 2023), securityhero.io

RO4828783-0925

Time it takes to crack your password using AI

# of characters	Numbers only	Lowercase letters	Upper and lowercase letters	Numbers, upper and lowercase letters	Numbers, upper and lowercase letters, symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	4 seconds
7	Instantly	Instantly	22 seconds	42 seconds	6 minutes
8	Instantly	3 seconds	19 minutes	48 minutes	7 hours
9	Instantly	1 minutes	11 hours	2 days	2 weeks
10	Instantly	1 hours	4 weeks	6 months	5 years
11	Instantly	23 hours	4 years	38 years	356 years
12	25 seconds	3 weeks	289 years	2K years	30K years
13	3 minutes	11 months	16K years	91K years	2M years
14	36 minutes	49 years	827K years	9M years	187M years
15	5 hours	890 years	47M years	613M years	14Bn years
16	2 days	23K years	2Bn years	26Bn years	1Tn years
17	3 weeks	812K years	539.72M years	2Tn years	95Tn years
18	10 months	22M years	7.23Bn years	96Tn years	6Qn years

Security Hero, “An AI <Just cracked your> password” (Octber 1, 2023), securityhero.io

AI and other scams to watch out for

Impersonation scams: celebrities, co-workers, family

Voiceprint scams: Thieves may be able to capture a recording of your voice (from videos on social media or other means) and then use an AI program to generate an imitation “deepfake” version that can be used to impersonate you to family/friends. Create a safe word or phrase.

Cryptocurrency scams: A type of fraud in which criminals lure victims to download fraudulent investing apps while building trust and convincing victims to invest in cryptocurrency platforms. The fraudsters control the platforms and eventually take all the money and vanish.

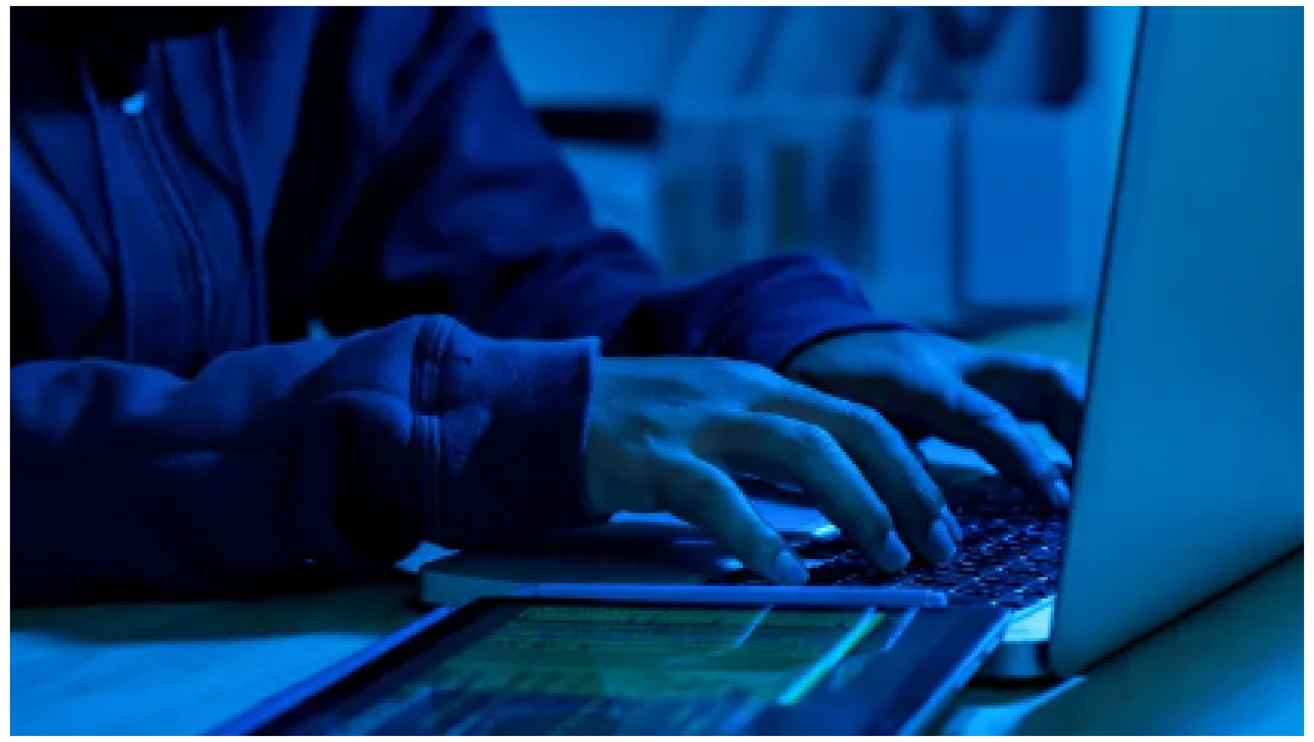
AI used in romance scams: Fraudsters use AI chatbot to interact with victims, generate fake profiles, and generate language tailored to specific victims based on their profiles.

AI recruiter scams: Scammers collect your personal information from your employment forms or tell you to buy equipment or training.

Watch out for:
QR code redirect
Gift cards
Venmo/Zelle apps
Checks in your mailbox
Delayed deliveries

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN
2 minute read
Published 2:31 AM EST, Sun February 4, 2024



Authorities are increasingly concerned at the damaging potential posed by artificial intelligence technology. boonchai wedmakawand/Moment RF/Getty Images

AI is ready for its close up

This video was generated by Artificial Intelligence and with the permission of the individual whose likeness and voice are used in the video.

Top 3 tips to avoid getting scammed

1

Pause before you act

Scammers use urgency to make you rush. Take a moment before you click or share - especially if wire or bank numbers are changed.

2

Check before you trust

Verify directly with the person or company using official contact information – not the message you received.

3

Protect your info

Use strong passwords and MFA. Share details only when you're sure it's safe.

Staying cautious keeps your data — and money — safer.

EMPOWER Invest well. Live a little.™

What good security looks like: Cybersecurity, AI and Security Guarantee

Secure recordkeeping system built for scale and reliability

Innovation and technology

Our proprietary platform is cloud- and server-based for simplified administration.

We store your data in the U.S.

Innovation Lab supports new tech advances.

Client-protection program

Meets or exceeds DOL cybersecurity best practices[1]

Cyber and fraud teams partner with key groups and governing bodies.

Clean, unqualified SOC 2 Type II report

Everything we do starts with our commitment to protecting your data

We will restore account losses that occur through no fault of the participant

SECURITY GUARANTEE

No eligibility requirements for participants
There is no limit to what we reimburse
100% whole

Empower has not experienced a cybersecurity breach

For more information regarding account security, including Empower Security Guarantee, visit **empower.com** and, from the list of additional links at the bottom of the page, click *Security center*.

1 DOL Cybersecurity Best Practices #2 Conducted audit by Verizon.

Our Technology Innovation Lab accelerates technology adoption to benefit our clients

1

Artificial intelligence

- Advanced machine learning
- Hyper-automation
- Knowledge assistance
- Quantitative insights
- New content and code creation

2

Data and analytics

- Descriptive and diagnostic analytics
- Predictive and prescriptive analytics
- Cognitive analytics

3

Emerging technology

- No-code, low-code platforms
- NexGen Cloud
- Biometrics
- Blockchain and distributed ledger
- Quantum computing

*

Our mission

To **ignite innovation** by testing new capabilities, **accelerating new technologies**, and differentiating the customer experience through **safe and transparent experimentation**

Everything we do starts with our commitment to protecting customer data

AI potential benefits to clients

Personalized experiences

Management of risk and fraud

Compliance related to trade monitoring and customer due diligence

Enabled transparency

Streamlined operations

ML/AI uses at Empower today*

Call fraud detection to keep customers safer

Customer Service **Chatbot** to offer faster time to resolution and next best action

Scaled and enriched **call quality analysis and agent coaching**

Customer Care Center **interactive voice response** to extend access during off-peak hours

Piloting **AI companion technology** to help boost creativity and productivity

AI future innovation

Software development with paired programming to **improve quality and productivity** while accelerating time to market for new features

Increased **quantity** of customer call analytics

Customer Care Center management

Next best action (NBA) will give associates suggested insights to serve participants **expanding to mobile/web** for anytime/ anywhere service.[1]

* Representative sample list

1 Anticipated for the second half of 2025.

Some tools described above may not be implemented or their availability is subject to change without notice.

Cybersecurity and artificial intelligence

1 Enable AI adoption at Empower

As AI transforms the workplace, Empower is developing its capability to use the technology.
The security team is:

Dedicating architecture resources to enable experiments.

Building reusable patterns.

Learning and identifying new risks.

2 Adopt AI for cybersecurity

The security team, as most teams, must do more with less and do it faster. So we are:

Building agentic AI technologies to support our teams' workflows.

Experimenting with agentic AI use cases for a faster Security Operations Center (SOC).

Building AI monitoring.

3 Mitigate new AI-enabled external threats

As external criminal actors also build upon AI technology to improve their effectiveness, we must:

Closely track advances in capabilities of models.

Build a strategic plan to execute cybersecurity at AI speed.

Footnotes/Open Sans (Body), 18pt/ As of date.

EMPOWER®
Invest well. Live a little.™

Continuous and extensive oversight

Cybersecurity attestation, legislation, and regulation

AICPA

SOC 2
Type II reports

+

SPARK INSTITUTE
SHAPING AMERICA'S RETIREMENT

SPARK Institute
and Empower

17
cybersecurity control objectives

Employee Benefits Security Administration (EBSA) & United States Department of Labor (DOL)

12
cybersecurity program best practices for recordkeepers and service providers

6
tips for plan sponsors:
how to select a service provider with strong cybersecurity practices

9
online security tips

Securities and Exchange Commission (SEC)

Two laws for public companies

1. Four-day cybersecurity incident disclosure
2. Annual disclosure of cybersecurity risk management, strategy, and governance

Highly regulated

Gramm-Leach-Bliley Act (GLBA)
Federal Financial Inst Examination Council (FFIEC)
Department of Labor (DOL)
Sarbanes-Oxley Act (SOX)
U.S. Securities and Exchange Commission (SEC)
Financial Industry Regulatory Authority (FINRA)
State Department of Insurance (DOI)
Division of Banking (DOB)
Fair and Accurate Credit Transactions Act (FACTA)
New York State Dept of Financial Services (NY DFS)
Federal laws
State laws

DOL's six tips for hiring a service provider with strong cybersecurity practices[1]

DOL	Empower
1. Security standards, practices, and policies	NIST 800-53
2. Validation, implementation, and compliance of security practices	• AICPA SOC 2 Type II – compliance reports • Verizon Certification 14 years – quarterly risk assessments • Penetration testing • Dark web monitoring • Development code testing
3. Service provider's track record in the industry	• Plan Advisor: #1 Value for Price[3] • Plan Advisor: #1 Overall Service[3]
4. Service provider response to past security breaches if applicable[2]	Empower has not had a breach
5. Insurance policies that would cover losses caused by cybersecurity and identity theft breaches	Cyber liability insurance + Empower Security Guarantee
6. Service agreements that document ongoing compliance with cybersecurity and information security standards	SOC 2 Type II, Verizon Certification, data security and privacy addendum

1 DOL, "Tips For Hiring a Service Provider With Strong Cybersecurity Practices," accessed March 2025.

2 Empower's response to the DOL's cybersecurity best practices, 2025.

3 2023 PLANADVISER Retirement Plan Adviser Survey as of February 2024.

Eight questions to ask your Recordkeeper

1. Do you offer a formal **Security Guarantee** for the protection of personal information and account balances?

    1. Are all participants are automatically opted in? E.g., are there are any eligibility requirements to qualify for the security Guarantee — do they need to register, look at monthly statements, keep contact info up to date, etc.?
    2. Will your recordkeeper make participants 100% whole in the event of fraud (through no fault of the participant)? E.g., is there a limit to what your Recordkeeper will reimburse?
    3. Which accounts are covered vs not covered? E.g. DC, DB, Non-qual. (Empower's Security Guarantee covers all Empower branded accounts — except Optum)

2. Has the recordkeeper had a **data security breach** where they needed to notify affected individuals or clients of loss of their personal identifiable information, including Class 1 data?

3. Does the recordkeeper own or rent their recordkeeping platform?

4. How do you **test the security of your controls** with third-party cybersecurity experts and third-party penetration testers? Do they have a clean/unqualified SOC 2 type 2 report?

5. Is any part of their **recordkeeping platform mainframe-based**?

6. Is **participant recordkeeping and trust data integrated**?

7. Does your system update using batch processing or **real-time functionality**?

8. How is your organization leveraging the **SPARK best practices** and Industry Standards, including a SOC2 security report that is specific to your recordkeeping environment? Please provide your SOC2 report along with the mapping of SPARK 17 best practices for ease of comparison.

Protect your data, your identity, and your money

FOR PLAN SPONSOR OR FINANCIAL PROFESSIONAL USE ONLY.

How to increase your plan's security with Empower

1

We need current participant contact information.

Payroll integration provides accurate and timely participant data.

2

The **most secure** way to share information is through the Plan Service Center (PSC) portal.

We can set up forced email encryption (TLS) to secure emails.

3

Provide security awareness training on topics like phishing.

4

Tell us (your recordkeeper) about any breaches, fraud, or identity theft.

5

Use e-delivery for all participant communications and go paper-free for statements.

Take action if you suspect unusual activity

1 Change your passwords

Change your password and if you have reused the compromised password, change it in all places.

Change all email passwords and add multifactor authentication to your email accounts.

2 Notify all major credit bureaus and your financial institutions

Equifax:
800-685-1111
equifax.com

Experian:
888-397-3742
experian.com

TransUnion:
800-680-7289
transunion.com

Notify all your financial institutions

3 File a report

If you are a victim of online crime, file a report with the FBI's Internet Crime Complaint Center (IC3.gov) as soon as possible.

Contact financial institutions like Empower immediately if you suspect any unusual activity on any of your financial accounts. We can add additional protections to your account.

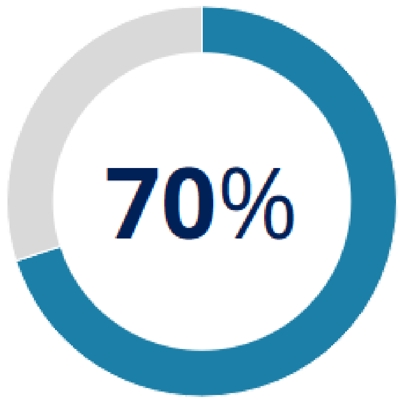
The credit bureaus listed are not affiliated with Empower Retirement, LLC and its affiliates.
These best practices are for informational purposes only. They apply to U.S. residents. Security risks and recommendations change frequently.
Check the Security Center on **empower.com** for updates.
Follow the alerts, recommendations, and announcements from your service providers, law enforcement agencies, and consumer protection agencies..

Account registration and protection

As of 9/30/2025

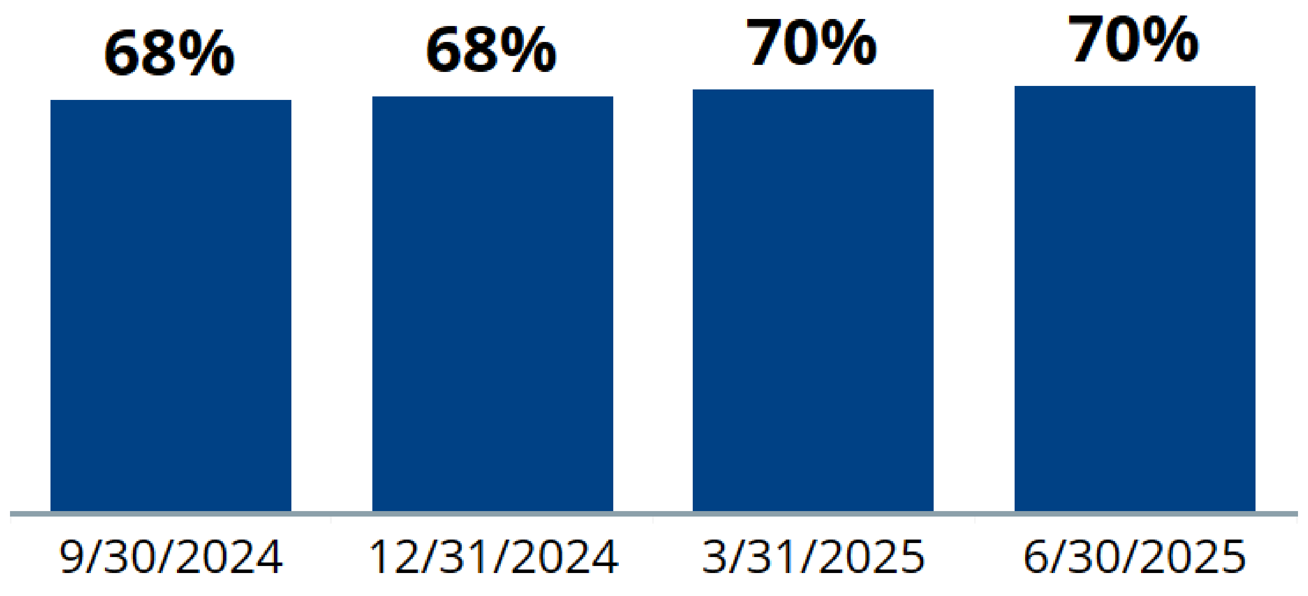
The insights below are based on all participants with a balance, regardless of their eligibility and employment status. The account registration and login activity is inclusive of both the website and the mobile app.

Percent of registered accounts



18,074 out of **25,776** participants with a balance have registered their online account

Trending



Participants missing contact information

Participants with missing contact information by registration status

	Registered participants	Not registered participants
! No phone and no email[1]	14 (0.1%)	620 (8.0%)
No personal email	843 (4.7%)	5,832 (75.7%)
No work email	2,542 (14.1%)	2,563 (33.3%)
No mobile phone	1,069 (5.9%)	7,364 (95.6%)
No home phone	3,003 (16.6%)	2,008 (26.1%)

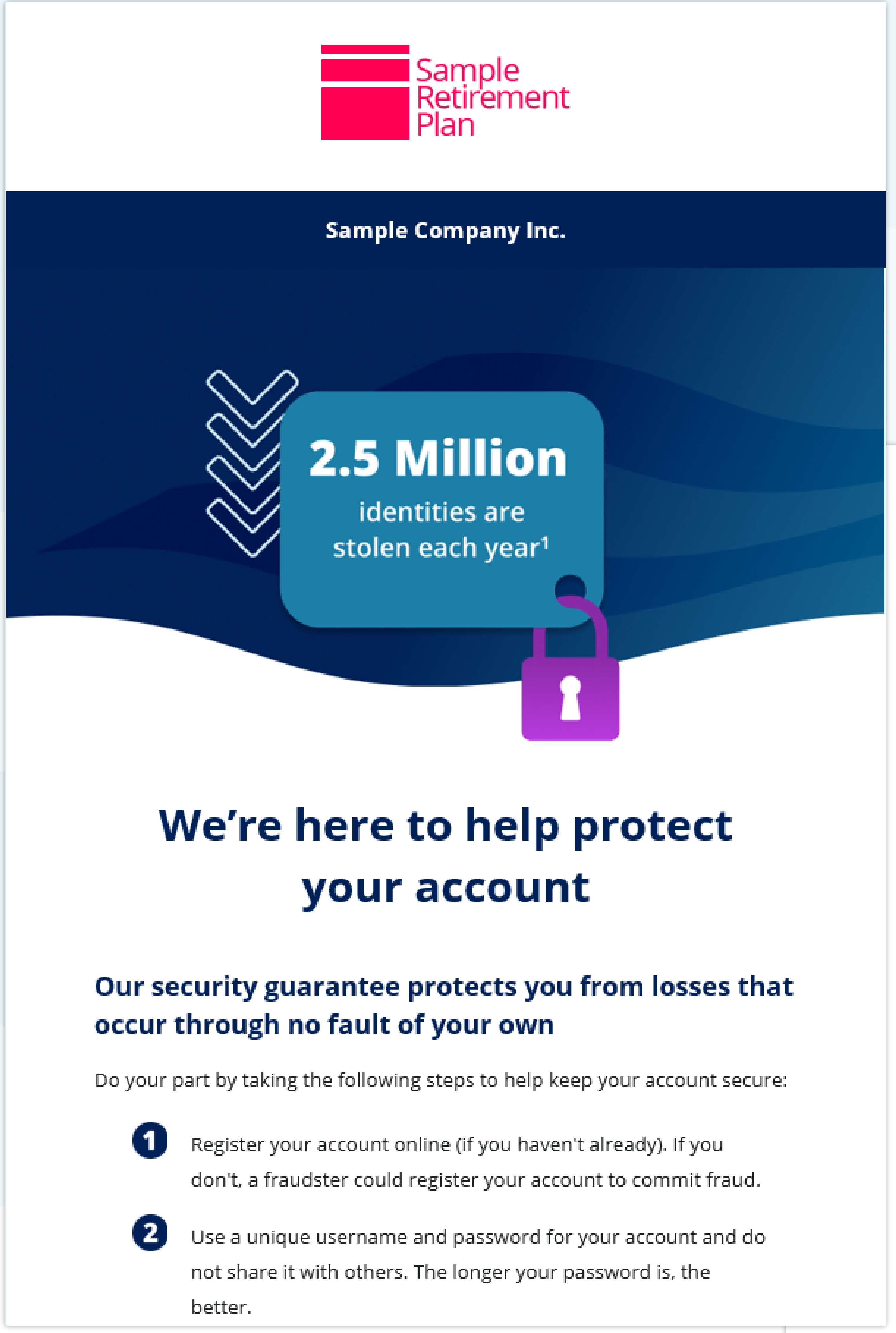
Login activity

Most recent login

	Participants with a balance
! Never logged in	7,702 (29.9%)
Within past month	4,996 (19.4%)
1-6 months ago	5,268 (20.4%)
7-12 months ago	2,085 (8.1%)
More than 12 months ago	5,725 (22.2%)

[1]Phone and email considers mobile and home phone, international phone numbers, and work and personal email

Are you leveraging our participant communications campaigns?



Sample Retirement Plan

Sample Company Inc.

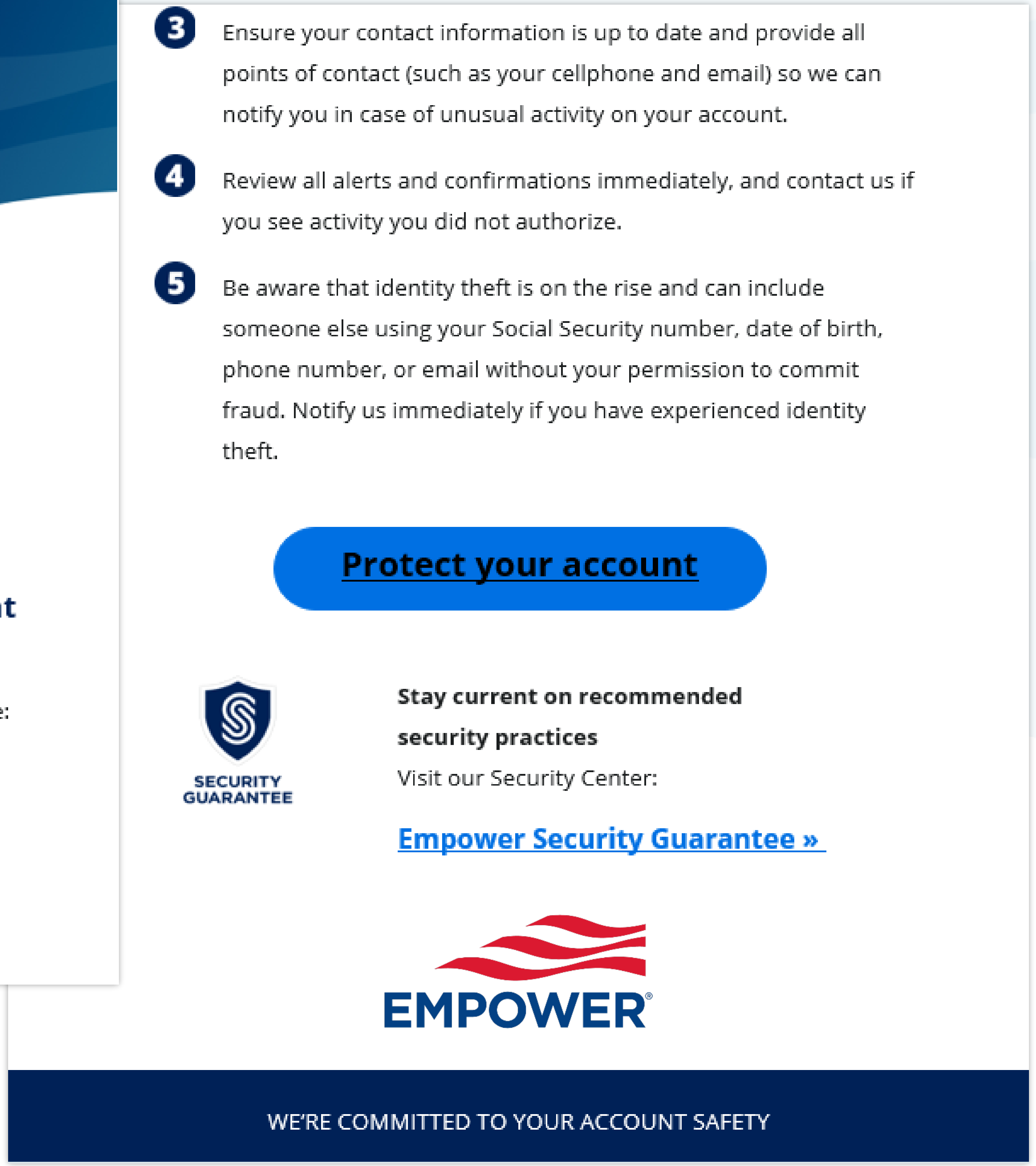
2.5 Million identities are stolen each year[1]

We're here to help protect your account

Our security guarantee protects you from losses that occur through no fault of your own

Do your part by taking the following steps to help keep your account secure:

1. Register your account online (if you haven't already). If you don't, a fraudster could register your account to commit fraud.
2. Use a unique username and password for your account and do not share it with others. The longer your password is, the better.



3. Ensure your contact information is up to date and provide all points of contact (such as your cellphone and email) so we can notify you in case of unusual activity on your account.
4. Review all alerts and confirmations immediately, and contact us if you see activity you did not authorize.
5. Be aware that identity theft is on the rise and can include someone else using your Social Security number, date of birth, phone number, or email without your permission to commit fraud. Notify us immediately if you have experienced identity theft.

Protect your account

SECURITY GUARANTEE

Stay current on recommended security practices

Visit our Security Center:

Empower Security Guarantee »

EMPOWER

WE'RE COMMITTED TO YOUR ACCOUNT SAFETY

FOR ILLUSTRATIVE PURPOSES ONLY.

Online security tips

Department of Labor: Nine online security tips[1]

1. **Register**, set up, and routinely monitor your online account.
2. Use strong and unique passwords.
3. Use multifactor authentication (MFA).
4. Keep personal contact information current.
5. Close or delete unused accounts.
6. Be wary of free Wi-Fi (use a VPN).
7. Beware of phishing attacks.
8. Use antivirus software and keep apps and software current.
9. Know how to report identity theft and cybersecurity incidents.

You: Seven steps to better security[2]

1. **Register** your account on Empower.
2. Provide all available **emails** and **phone numbers.**
3. Use a **password manager** (e.g., Bitwarden, 1Password, Keeper).
4. **Use multifactor authentication** (MFA).
5. Leave MFA enabled by **not clicking** "remember this device."
6. **Pay attention** to security alerts.
7. Freeze your **credit** (and your family's).

1 DOL, Online Security Tips, February 2021.

2 Empower proprietary research.

What to do if you're a victim of fraud and/or identity theft?

1 Protect

Change your password(s), then notify all your financial institutions, including Empower via our Customer Service Center: 844-773-6797.

We can put additional protections on your account.

2 Alert

Notify all three major credit bureaus:

Equifax: 800-685-1111
equifax.com

Experian: 888-397-3742
experian.com

TransUnion: 800-680-7289
transunion.com

3 Report

If you discover that you have become a victim of a cybercrime, immediately file a report with your local law enforcement authorities and with the FBI's Internet Crime Complaint Center (IC3.gov).

90 second Account Security Tips video with Vanessa Welch

EMPOWER Invest well. Live a little.™

Questions & Answers

Disclosures

Empower refers to the products and services offered by Empower Annuity Insurance Company of America and its subsidiaries. This material is for informational purposes only and is not intended to provide investment, legal, or tax recommendations or advice.

WSA-SPP-WF-3335057-0525(4120801) RO4325722-0425

EMPOWER® Invest well. Live a little.™

Thank you