NADA Retirement from EMPOWER

2023 Cybersecurity: Best practices overview

Agenda topics

- Global trends in cybersecurity — what we're seeing.
- DOL's cybersecurity best practices: How Empower meets and exceeds the DOL guidelines. Ask your relationship manager for our response to these guidelines.
- Ways Empower protects data.
- What we can all do to improve data security.
- Q&A

Global trends, threats, and vulnerability statistics

- 70% of ransomware attacks include data exfiltration, including theft of corporate data, usernames, and passwords.[+]
- 48% fewer victims paying a ransom from 2019 to 2022.[++]
- The three most common compromise points for ransomware are phishing; unpatched, exploitable vulnerabilities; and remote desktop protocol (RDP sessions).[+++]
- CVE global annual vulnerability stats: 2021 had 20,100+ new vulnerabilities. 2022 had 25,000+ new vulnerabilities (Data as of 12/31/22).

You are now being redirected. Empower Retirement, LLC and its affiliates are not affiliated with the author or responsible for the third-party content provided.

- Global records stolen (per billion): 93 billion records stolen from 2019 through 2022.[++++]

What are the bad actors up to?

- Phishing through email: No. 1 successful attack platform for bad actors.[1]
- Organized crime is trending up (targeting CARES Act, unemployment insurance, Social Security Administration, Paycheck Protection Program).[2]
- "Families behaving badly" is trending up.[2]
- 2022 FBI PSA: Cybercriminals tampering with QR codes to steal victim funds.[3]
- Ransomware grew 1,070% year over year.[4]
- Smishing (SMS/text message phishing) attempts are increasing.[5]
- Increasing ransomware-as-a-service: Cybercriminals acting like capital investors are funding startup cybercriminal organizations, such as Darkside ransomware.[6]
- 7x increase in cryptocurrency losses in 2021 over 2020.[7]
- Shortened URL links are now used as phishing hooks.[8]

Please note the difference between breach and fraud. Empower has not experienced a security breach of our systems. If a bad actor attempts to access a participant account, Empower has a multilayer fraud control environment to protect your account and data.

DOL's cybersecurity best practices

Learn how Empower meets and exceeds these guidelines.

- 12 cybersecurity program best practices for recordkeepers and service providers
- Six tips for plan sponsors
- Nine online security tips

Please ask your relationship manager for more information on Empower's response to the DOL cybersecurity guidelines.

Ways Empower protects data

For plan sponsor clients:

- A modern platform
- Annual SOC 2 Type II reports
- Third-party validation
- Quarterly risk assessments
- Penetration testing
- Dark web monitoring
- Fraud prevention
- Cloud technology
- Ongoing disaster recovery exercises

For participants, we:

- Encrypt your data.
- Do not sell your data.
- Partner with cybersecurity leaders to keep your information safe.
- Have your back if you're the victim of an ID theft or email compromise.
- Have an Empower Security Guarantee.

Empower cybersecurity best practices

Five best practices for plan sponsors to increase plan security:

1. Provide accurate, up-to-date contact information for your participants.
2. Set up a secure file transfers protocol (SFTP) and forced email encryption (TLS) with your provider and other third parties with whom you exchange sensitive data and emails. (Please ask your relationship manager for more information.)
3. Provide security awareness training — especially for topics such as phishing.
4. Promptly inform us of any breaches or fraud so we can put additional protections on your account.
5. Use e-delivery for all participant communications and go paper-free for statements.

Seven steps to better security for participants:

1. Register your account with **nada401k.com**.
2. Provide all available email addresses and phone numbers for security alerts.
3. Use a password manager (e.g., Bitwarden, 1Password, KeePass).[9]
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 with the three major credit bureaus and only unfreeze your credit for the time you want additional credit.

Empower Security Guarantee

We will restore losses from your participants' accounts that result from unauthorized transactions that occur through no fault of their own.

Reimbursements associated with the Empower Security Guarantee are subject to certain conditions. View details

SECURITY GUARANTEE

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

1

Change your password(s), then **notify** all your financial institutions, including Empower. We can put additional protections on your account.

2

Notify all three major credit bureaus:

Equifax:
800-525-6285 | equifax.com

Experian:
888-397-3742 | experian.com

TransUnion:
800-916-8800 | transunion.com

3

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**).

You are now being redirected. Empower Retirement, LLC and its affiliates are not affiliated with the author or responsible for the third-party content provided.

Industry links and resources

SPARK Institute

(Society of Professional Asset Managers and Recordkeepers)

Leading nonprofit association regarded as a major voice influencing federal retirement policy and a thought leader for data security.

- Data Security Oversight Board: 16 control objectives
- Cybersecurity conferences and training

NIST

(National Institute of Standards and Technology)

NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. and global industries, including financial services. NIST CSF provides a cost-effective, adaptable, and flexible framework that any organization can use for creating and maintaining an information security program. NIST 800-53 and NIST 800-171 provide security controls for implementing NIST CSF.

- Quick Start Guide
- Informational videos
- Awareness, education, training, and workforce development
- Cybersecurity supply chain projects
- Ransomware resources

CISA.gov

(Cybersecurity & Infrastructure Security Agency)

All services are available at no cost to federal agencies, state and local governments, critical infrastructure, and private organizations.

- Security assessments
- Cybersecurity training

FBI IC3

(Federal Bureau of Investigation Internet Crime Complaint Center IC3)

Small businesses should immediately report any threats and incidents to the FBI's IC3. The IC3 accepts online internet crime complaints from the actual victim or a third party to the complainant.

- File a complaint
- Consumer and industry alerts

You are now being redirected. Empower Retirement, LLC and its affiliates are not affiliated with the author or responsible for the third-party content provided.

NADA Retirement from EMPOWER

Empower's cybersecurity resource library

Please ask your relationship manager for these materials:

- Empower Recordkeeping Technology and Cybersecurity Guide
- Empower's Response to the DOL's Cybersecurity Guidelines
- Empower Overview DOL EBSA Cybersecurity Guidance
- CISO cybersecurity videos
- Cobranded participant communications campaigns
- White paper: Defense-in-Depth Protecting your Plan
- SOC 2 Type II Report + AICPA SOC 2 Overview

› Get started at **nada401k.com**

+Health IT Security, Phishing Top Entry Point, February 2021.

++Improved security and backups result in low number of ransom payments, Covware.com, January 2023.

+++xorlab, Most Common Ransomware Attack Vectors, February 2022.

++++The biggest data breaches and leaks of 2022, CSHub.com.

*Risk Based Security: A Flashpoint Company, "New Research: No. of Records Exposed Increased 141% in 2020", January 21, 2021.

**Risk Based Security: A Flashpoint Company, "Data Breach Report: 2021 Year End," February 4, 2022.

1 2021 Verizon DBIR Figure 20 Top Action varieties in breaches.

2 Empower Proprietary Research 2021.

3 FBI Public Service Announcement, January 2022.

4 Fortinet, "FortiGuard Labs Global Threat Landscape report," September 2021.

5 ITPro, "Smishing attacks increase 700% in first six months of 2021."

6 TechTarget, "Darkside Ransomware funded by cybercriminal 'investors,'" June 2021.

7 DataDrivenInvestor, July 2022

8 Proofpoint, "State of the Phish – Annual report," 2021.

9 Empower Retirement, LLC and its affiliates are not affiliated with Bitwarden, 1Password, KeePass or other password manager organizations.

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