INDIANA UNIVERSITY OF PENNSYLVANIA: NATIONAL CYBERSECURITY AWARENESS MONTH 2023

Derek Mueller
Cybersecurity Advisor – State Coordinator Pennsylvania
Region III (MD, PA, DE, DC, VA, WV)
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

Cybersecurity Awareness Month

- Launched in 2004
- Co-managed by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA)
- Collaborative effort between government and industry to raise cybersecurity awareness
- Ensures that everyone has the resources they need to be safe and secure online.

October is Cybersecurity Awareness Month

CISA

STRATEGIC PLAN 2023–2025

GOAL 1

CYBER DEFENSE:

Spearhead the National Effort to Ensure Defense and Resilience of Cyberspace

GOAL 2

RISK REDUCTION & RESILIENCE:

Reduce Risks to, and Strengthen Resilience of, America's Critical Infrastructure

GOAL 3

OPERATIONAL COLLABORATION:

Strengthen Whole-of-Nation Operational Collaboration and Information Sharing

GOAL 4

AGENCY UNIFICATION:

Unify as One CISA Through Integrated Functions, Capabilities, and Workforce

What is Cybersecurity?

- Defined as "the protection of computer systems and networks from attacks by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data..."
- Wherever there is technology, there needs to be cybersecurity.

Why is it Important?

- Implementing cybersecurity best practices is important for individuals as well as organizations of all sizes to protect personal, financial and sensitive information.
- For both government and private entities, developing and implementing tailored cybersecurity plans and processes is key to protecting and maintaining business operations.

Feelings Toward Cybersecurity

- **78%** of people consider staying secure online a priority
- **34%** noted they often feel overwhelmed by information and, as a result, minimize their online actions
- **46%** felt frustrated while staying secure online
- **39%** of users trying to keep safe felt information on how to stay secure online is confusing

Findings from Oh Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2022

Our Online Behaviors

- **Only 33% of individuals create unique passwords for all accounts**
  - Only 18% of individuals have downloaded a password manager
- **43% of respondents have never heard of multifactor authentication (MFA)**
  - Out of the 57% of the participants who had heard about it:
    - 79% applied it at least once and 94% of them reporting that they were still using MFA
- **92% of respondents took action after a security training**
  - 58% say they are better at recognizing phishing
  - 45% started using strong and unique passwords
  - 40% started using MFA
  - 40% started regularly installing software updates

Findings from Oh Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2022

Who – Cyber Threat Actors

Nation States

Hacktivists

Cyber Criminals

How – Avenues for attack

- Social Engineering
- Vulnerability Exploitation
- Misconfigurations & Poor Security Practices
- Physical Access and Hands On Exploitation
- Phishing
- Insider Threat

Action Steps

4 Easy Ways to Stay Safe Online

Use Strong Passwords and a Password Manager

Turn on Multifactor Authentication

Recognize and Report Phishing Attacks

Update Your Software

Use Strong Passwords

CREATE STRONG PASSWORDS:

- **Long**
  - At least 16 characters
- **Unique**
  - NEVER reuse passwords
- **Complex**
  - Upper- and lower-case letters
  - Numbers
  - Special characters
  - Spaces

Use a Password Manager

WHY USE A PASSWORD MANAGER?

- Stores your passwords
- Alerts you of duplicate passwords
- Generates strong new passwords
- Some automatically fill your login credentials into website to make sign-in easy

Encryption ensures that password managers never "know" what your passwords are, keeping them safe from cyber attacks.

Turn on Multifactor Authentication

WHAT IS IT?

- **A code sent to your phone or email**
- **An authenticator app**
- **A security key**
- **Biometrics**
  Fingerprint
  Facial recognition

Turn on Multifactor Authentication

WHERE SHOULD YOU USE MFA?

- **Email**
- **Accounts with financial information**
  Ex: Online store
- **Accounts with personal information**
  Ex: Social media

Recognize and Report Phishing

PHISHING RED FLAGS:

- **A tone that's urgent or makes you scared**

"Click this link immediately or your account will be closed"

- **Bad spellings, bad grammar**
- **Requests to send personal info**
- **Sender email address doesn't match the company it's coming from**

Ex: Amazon.com vs. Amaz0n.com

- **An email you weren't expecting**

Recognize and Report Phishing

WHAT TO DO

Do NOT

- Don't click any links
- Don't click any attachments
- Don't send personal info

Do

- Verify
- Contact that person directly if it's someone you know
- Report it to your IT department or email/phone provider
- DELETE IT

Update Your Software

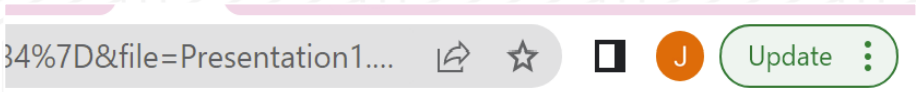
WHY?

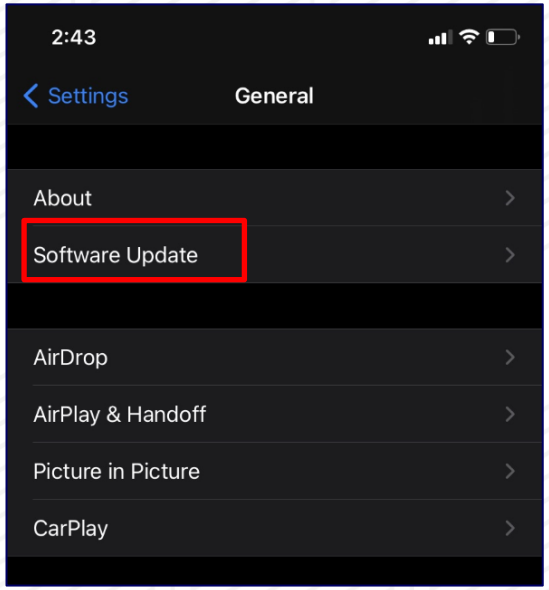
- Updates ensure your devices and apps are protected from the latest threats
- Don't click "remind me later", it could leave you vulnerable to cyber threats
- Automatic updates are the easiest way to stay secure

Update Your Software

WHERE TO FIND AVAILABLE UPDATES

- Check for notifications to your phone or computer
- Look in your phone, browser or app settings
- Check the upper corner of your browser for any alerts





Building a Strong Cybersecurity Culture

- **Use basic cybersecurity training.** This helps familiarize staff with cybersecurity concepts and activities associated with implementing cybersecurity best practices.
- **Identify available cybersecurity training resources.** Cybersecurity training resources—on topics like phishing and good email practices—are available through professional association, educational institutions, as well as private sector and government sources.
- **Stay current on cybersecurity events and incidents.** This helps identify lessons learned and helps to maintain vigilance and agility to cybersecurity trends.
- **Encourage employees to make good choices online** and **learn about risks** like phishing and business email compromise.

CISA Website – cisa.gov

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About | REPORT A CYBER ISSUE

SHARE:

ShieldsUp

Prepare for, respond to, and mitigate the impact of cyberattacks.

LEARN MORE

Secure Our World Resources and Tip Sheets

Learn more about the four ways to stay safe online with Secure Our World Tip Sheets, translated in various languages.

SECURE OUR WORLD RESOURCES AND TIP SHEETS

SEP 29, 2023 ■ BLOG

Defending Democracy and Standing Up for Civil Society

SEP 29, 2023 ■ BLOG

Transforming Vulnerability Management: CISA Adds OASIS CSAF 2.0 Standard to ICS Advisories

SEP 28, 2023 ■ BLOG

Region 8 Invites You to Secure Our World

VIEW MORE NEWS

Cisco Releases Security Advisories for Multiple Products

OCT 05, 2023 ■ ALERT

CISA Adds Three Known Exploited Vulnerabilities to Catalog

OCT 05, 2023 ■ ALERT

CISA Releases Three Industrial Control Systems Advisories

VIEW ALL ALERTS & ADVISORIES

SUBSCRIBE TO UPDATES

Ways to Get Involved

AT WORK

- Publicize resources and activities
  - Intranet
  - Website
  - Emails to employees/customers
- Promotions
  - Discounts
  - Giveaways
- Hold a contest
  - Phishing simulation
  - Poster contest

AT HOME

- Share helpful tips and resources
  - Kids
  - Parents
  - Friends
- Hold a family “tech talk”
  - Discuss how each family member can protect their devices, accounts, and personal information.
- Create a culture of security in your family

Ways to Get Involved Cont.

IN YOUR COMMUNITY

- Volunteer to teach others in your community
- Reach out to
  - Your kid's school
  - A library/community center
  - Senior center
  - Place of worship

ONLINE

- Join on the conversation on social media using
  - **#CybersecurityAwarenessMonth**
  - **#SecureOurWorld**

What's It Worth - Avg. Dark Web Price (USD)

Credit card details, account balance up to 5,000 ($120)

Credit card details, account balance up to 1,000 ($80)

Stolen online banking logins, minimum $2,000 on account ($65)

Cashapp verified account ($800)

Stolen PayPal account details, minimum $100 balances ($15)

50 Hacked PayPal account logins ($150)

Crypto.com verified account ($250)

Binance verified account ($260)

USA verified LocalBitcoins account ($120)

Utility bill templates ($25)

New York driver's license ($70)

US driver's license (avg.) ($150)

10 million USA email addresses ($120)

Netflix account, 1-year subscription ($25)

Uber hacked acct. ($15)

Uber driver hacked acct. ($35)

Hacked Facebook account ($45)

Hacked Instagram account ($40)

Hacked Twitter account ($25)

Hacked Gmail account ($65)

Additional Resources

CISA

- Report a Cyber Issue
- Secure by Design
- Cross-Sector Cybersecurity Performance Goals
- Cyber Resource Hub
- Cybersecurity Training & Exercises
- CISA YouTube Channel

NCA

- Resources and Guides
- Videos and On-Demand Webinars

Other Federal Reporting Resources

FBI 24x7 CyWatch: (855) 292-3937 or CyWatch@fbi.gov

FBI Cyber Complaint Center: www.ic3.gov

For individuals who are victims of an online/digital crime

Federal Trade Commission – reportfraud.ftc.gov

For individuals who are victims of bad business practices or taken advantage of by online companies

Identity Theft Resources – IdentityTheft.gov

For individuals who believe they may be victims of Identity Theft

For more information, visit **cisa.gov** or contact **central@cisa.dhs.gov**

Derek Mueller
Cybersecurity Advisor – State Coordinator Pennsylvania
Region III (MD, PA, DE, DC, VA, WV)
Derek.mueller@cisa.dhs.gov
Cybersecurity and Infrastructure Security Agency