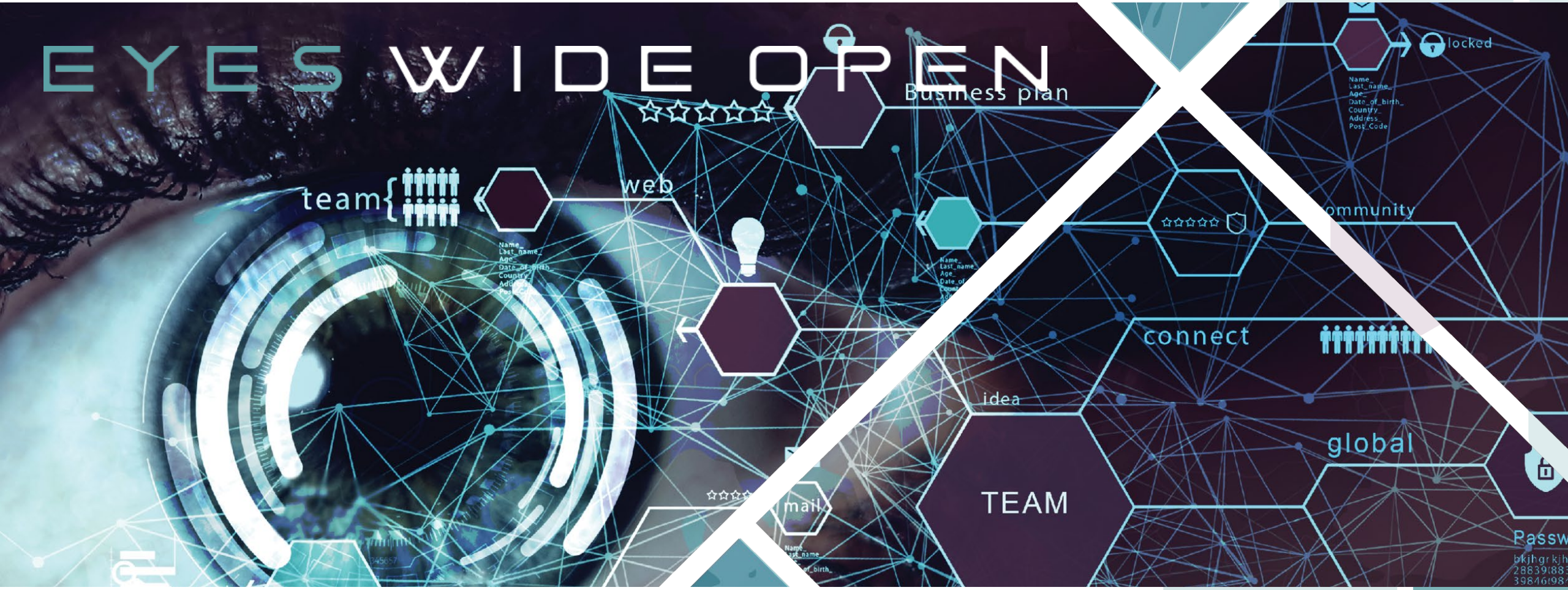
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island



DHS Intelligence and Analysis Threat Assessment

Karissa Zamora

Intelligence & Analysis,
DHS – Office of
Regional Intelligence

Nontechnical Actions to Enhance Cybersecurity Posture

Chris Gabbard

Cybersecurity Advisor,
Region 5, CISA

US Department of Homeland Security

CISA | CYBERSECURITY ANI
INFRASTRUCTURE SECURIT
AGENCY

DHS Office of Intelligence & Analysis (I&A) Cyber Mission Center

Cyber Summit: Cyber Threat Actor Overview

25 Oct 2022

The overall classification of this exchange is:

UNCLASSIFIED

(U) Warning: This product may contain US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. US person information is highlighted with the label USPER and should be protected in accordance with constitutional requirements and all federal and state privacy and civil liberties laws.

DISCLAIMER

(U) This presentation addresses a variety of Homeland security issues and provides operational and intelligence advice and assistance to federal, state, local, and tribal Homeland security, law enforcement, and private sector security officials so they may deter, prevent, preempt, or respond to foreign threats against the United States.

(U) WARNING: While unclassified, the material in this presentation should be considered sensitive and is not authorized to be reproduced, copied, transmitted, recorded, or photographed without the express written consent of the Department of Homeland Security, Office of Intelligence & Analysis. Requests for authorization to further disseminate this presentation or information contained therein must be submitted to I&A's Rocky Mountain Region at IARockyMountainRegion@hq.dhs.gov

Cyber Threat Actors

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

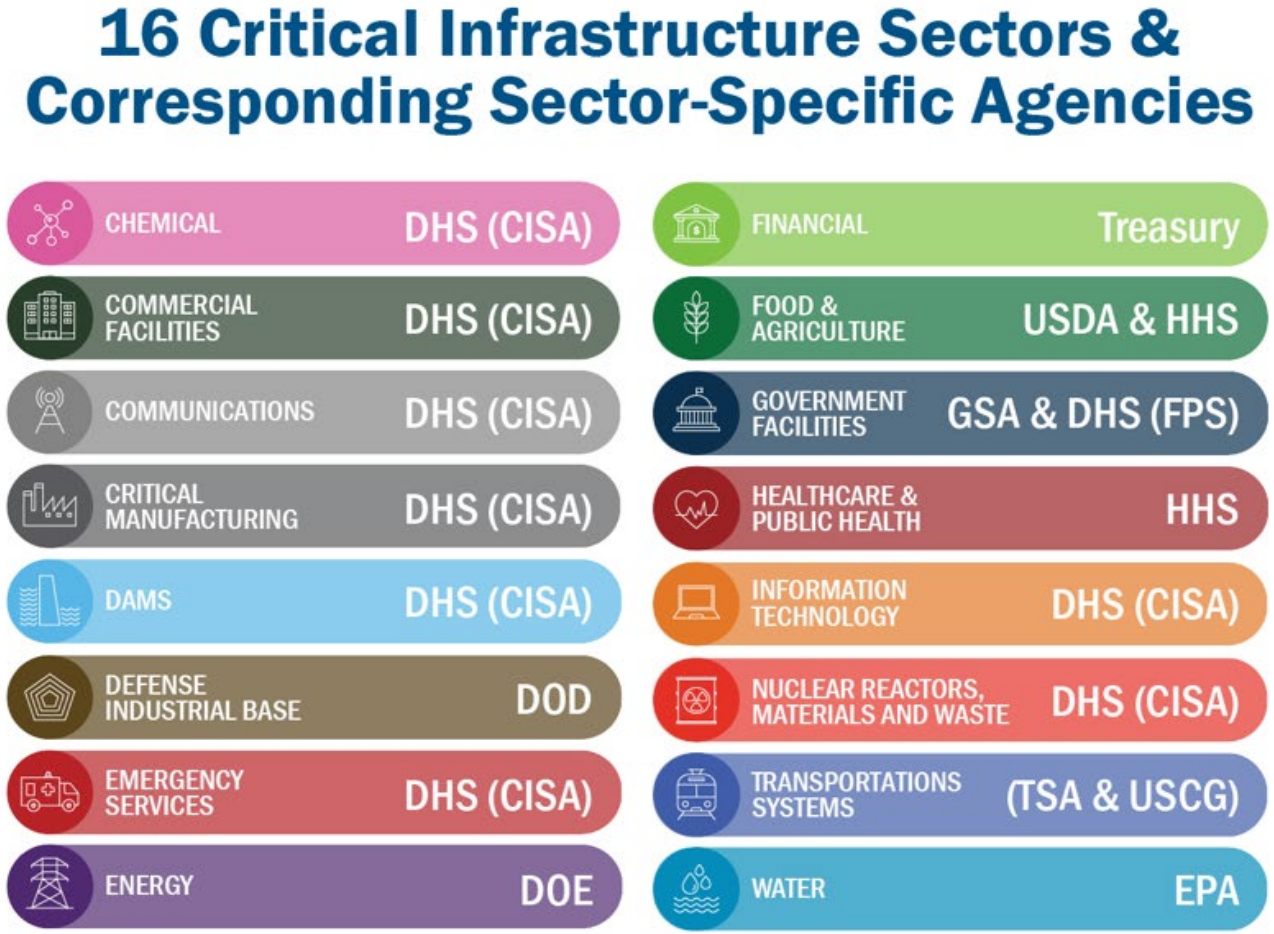
months | years | decades

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

Critical Infrastructure



80% of critical infrastructure is owned and/or operated by the private sector

Cybersecurity Awareness Month

Since 2004, October is celebrated as Cybersecurity Awareness Month, previously called National Cybersecurity Awareness Month. Now in its 19th year, Cybersecurity Awareness Month is a collaborative effort between government and industry to raise cybersecurity awareness nationwide and help ensure that all Americans have the resources they need to be safe and secure online.

The CISA is the federal lead for Cybersecurity Awareness Month with the National Cybersecurity Alliance (NCA) as co-lead.

CYBERSECURITY AWARENESS MONTH 2022

National Cybersecurity Alliance (staysafeonline.org)

Cybersecurity Awareness Month

Many users share some common misconceptions about their role in cybersecurity

- I’m not important enough to be at risk of a cyberattack
- My devices are “secure enough” right out of the box
- Cybersecurity Problems are I.T.’s problems
- The human factor will always be a vulnerability

CYBERSECURITY AWARENESS MONTH 2022

Theme

The 2022 Campaign theme, See Yourself in Cyber, emphasizes that while cybersecurity may seem like a complex subject, ultimately, it's really all about people. This October, we will focus on the "people" part of cybersecurity, providing information and resources to help Americans make smart decisions on the job, at home, at school, and in the future.

CYBERSECURITY AWARENESS MONTH 2022

Action Steps

This year's campaign goal is to have everyone implement these four action steps to increase online security:

- **Enable Multi-Factor Authentication**: You need more than a password to protect your online accounts, and enabling MFA makes it 99% less likely you will get hacked
- **Use Strong Passwords**: Use passwords that are long, unique, and randomly generated.
- **Recognize and Report Phishing**: If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.
- **Update Your Software**: Don't delay – if you see a software updated notification, act promptly. Better yet, turn on automatic updates.

CYBERSECURITY AWARENESS MONTH 2022

Enable Multi-Factor Authentication

- It's More than a Password: Why We all Need Multi-factor Authentication
- If you can do just one thing to protect your online valuables, set up Multi-factor Authentication.
- It goes by many names: Two Factor Authentication. Multifactor Authentication. Two Step Factor Authentication. MFA. 2FA. They all mean the same thing: opting-into an extra step when trusted websites and applications ask you to confirm you're really who you say you are.

CYBERSECURITY AWARENESS MONTH 2022

Use Strong Passwords

- Creating strong passwords is an easy way to improve your cyber security. Strong passwords include one uppercase letter, one lowercase letter, at least one number and 11 or more characters. Be sure to use different passwords for different accounts.
- Use password managers to generate and remember different, complex passwords for each of your accounts. A password manager will encrypt passwords securing them for you!
- Put cybersecurity first by protecting the information stored on devices. Much of a user's personal information is stored either on their computer, smartphone, tablet or possibly someone else's system.

CYBERSECURITY AWARENESS MONTH 2022

Use Strong Passwords

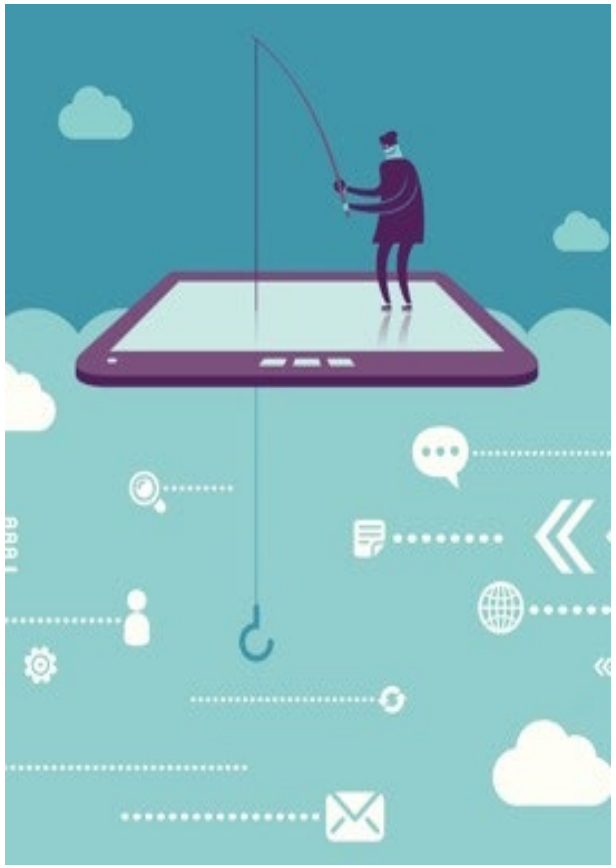
TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number 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	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

> Learn about our methodology at hivesystems.io/password

Recognize and Report Phishing



- Have you ever seen a link that looks a little off? It looks like something you've seen before, but it says you need to change or enter a password. Or maybe it asks you to verify personal information.
- It's likely a phishing scheme: a link or webpage that looks legitimate, but it's a trick designed by bad actors to have you reveal your passwords, social security number, credit card numbers, or other sensitive information. Once they have that information, they can use it on legitimate sites.

CYBERSECURITY AWARENESS MONTH 2022

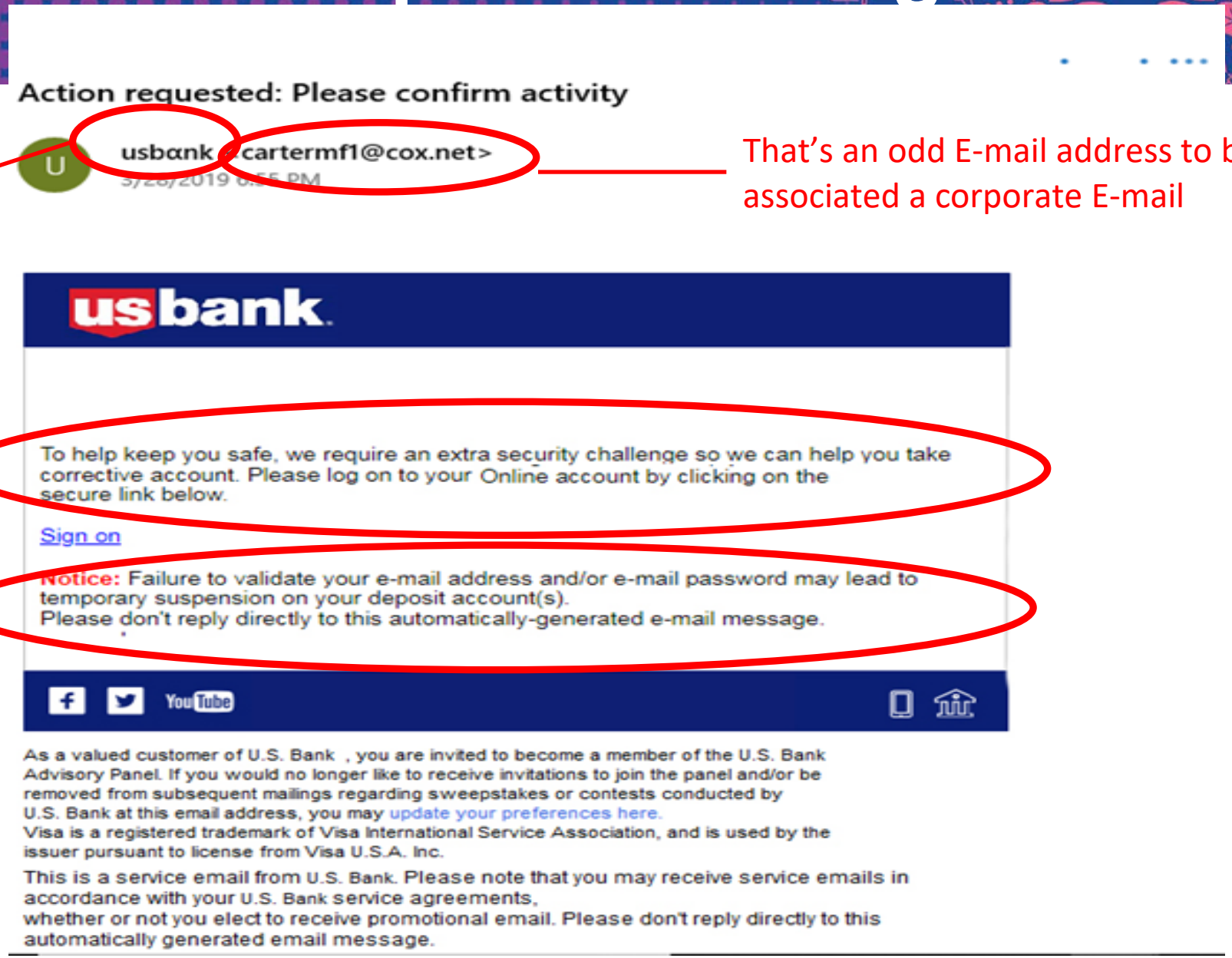
Recognize and Report Phishing

Notice anything unusual about the “a” in usbank?

That’s an odd E-mail address to be associated a corporate E-mail

“take corrective account”
Is that how we normally speak?

Threatens adverse action for not complying



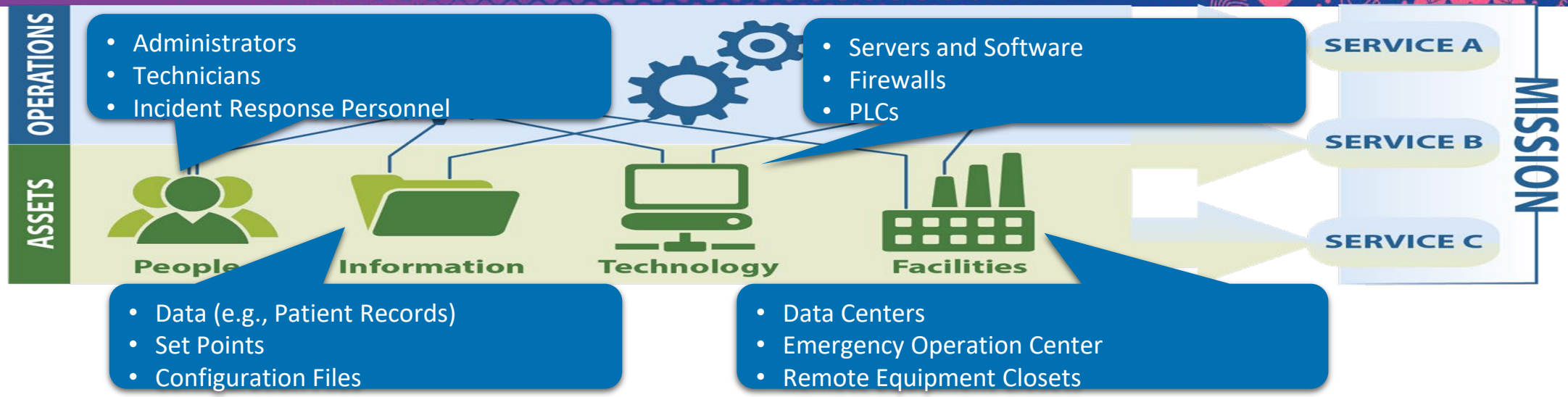
CYBERSECURITY AWARENESS MONTH 2022

Update Your Software

- Bad actors will exploit flaws in the system. Network defenders are working hard to fix them as soon as they can, but their work relies on all of us updating our software with their latest fixes.
- Update the operating system on your mobile phones, tablets, and laptops. And update your applications – especially the web browsers – on all your devic on automatic updates for all devices, applicati operating systems.

CYBERSECURITY AWARENESS MONTH 2022

Update Your Software

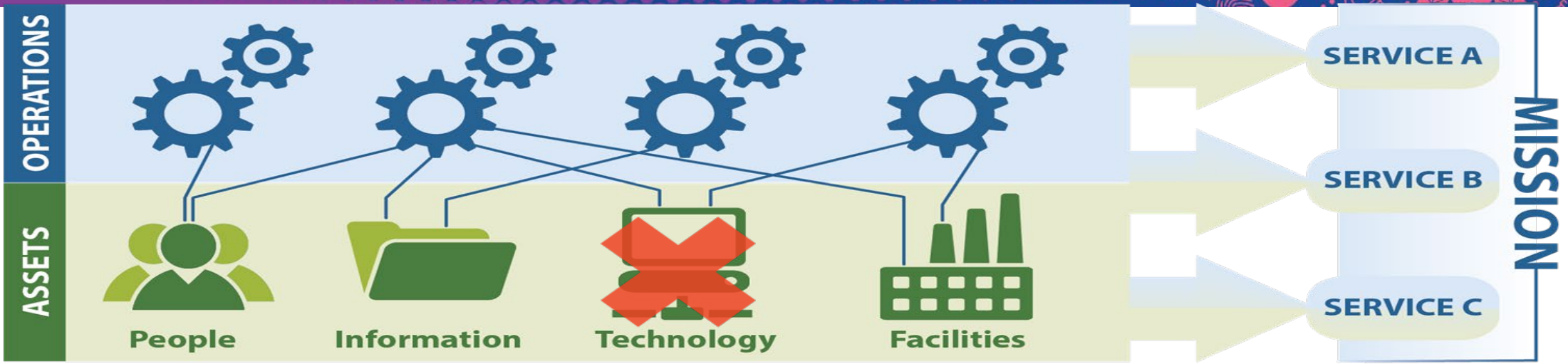


Organizations use **assets (people, information, technology, and facilities)** to provide operational **services** and accomplish **missions.**

- **People** – Those who operate and monitor the service
- **Information** – Data associated with the service
- **Technology** – Systems that automate and support the service
- **Facilities** – Where the service is performed

CYBERSECURITY AWARENESS MONTH 2022

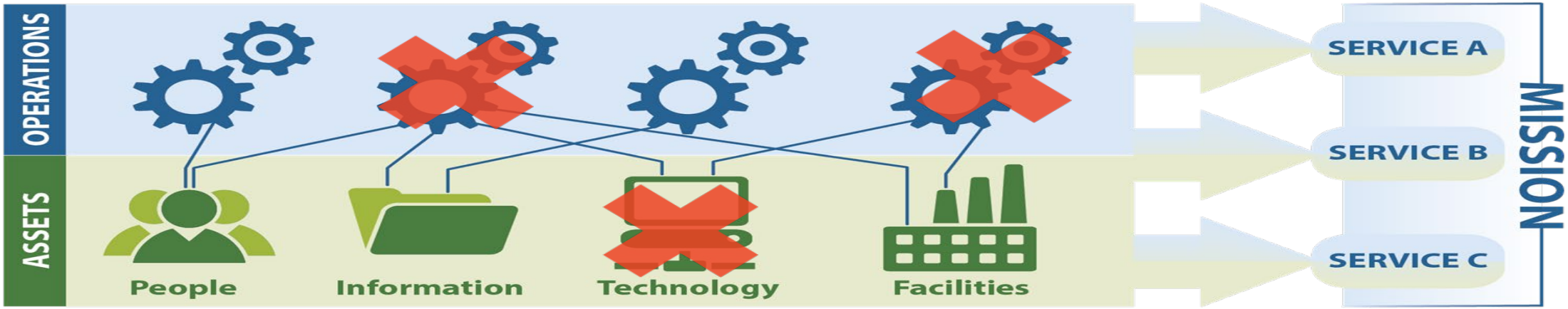
Update Your Software



Disruptions affect assets first.

CYBERSECURITY AWARENESS MONTH 2022

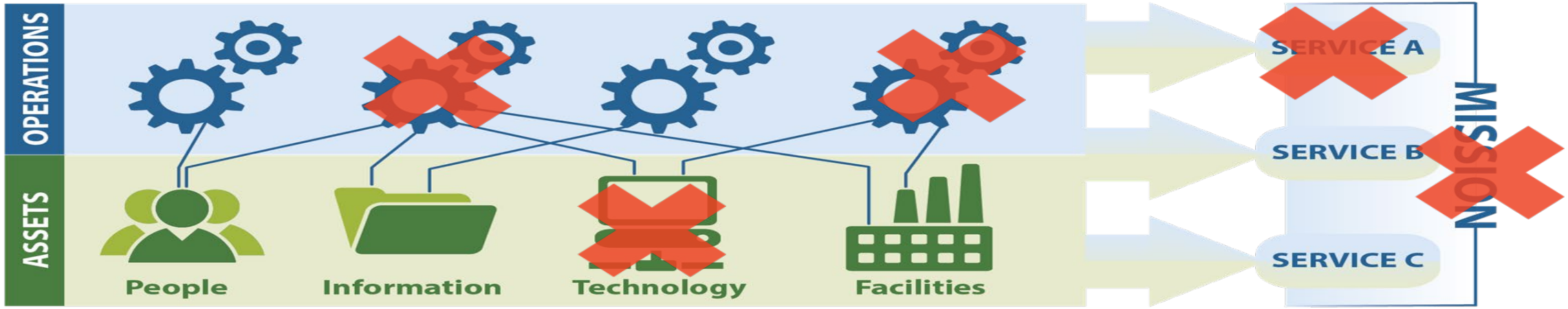
Update Your Software



Disruption of assets leads to disruption of business processes.

CYBERSECURITY AWARENESS MONTH 2022

Update Your Software



Disruption of business processes can lead to mission failure.

CYBERSECURITY AWARENESS MONTH 2022

Report a Cyber Issue

"If You See Something, Say Something" is a long standing national anti-terrorism campaign for reporting suspicious activity to law enforcement.

When cyber incidents are reported quickly, we can use this information to render assistance and as warning to prevent other organizations and entities from falling victim to a similar attack.

- Contact Minnesota Fusion Center at (651) 793-3730 or mn.fc@state.mn.us
- Contact CISA at central@cisa.gov or 888-282-0870
- FBI Field Office: http://www.fbi.gov/contact-us/field or the FBI's 24-7 Cyber Watch at 855-292-3937 or by e-mail at cywatch@fbi.gov

CYBERSECURITY AWARENESS MONTH 2022

Resources

CISA Shields Up

- Known Exploited Vulnerabilities Catalog
- Cybersecurity Advisories
- Cyber Essentials Toolkits
- Cyber Hygiene and Web Scanning Services
- Mis-, Dis-, and Malinformation Resources
- Emergency Communications Resources

Communications & Cyber Resiliency Toolkit

Cyber Resource Hub

- Cyber Hygiene Services
- Vulnerability Scanning
- Web Application Scanning
- Cybersecurity Evaluation Tool (CSET) and On-Site Cybersecurity Consulting
  - Ransomware Readiness Assessment

Cybersecurity Training & Exercises

CYBERSECURITY AWARENESS MONTH 2022

SHIELDS UP

Website

For complete information and resources on Cybersecurity Awareness Month, go to:

www.cisa.gov/cybersecurity-awareness-month

CYBERSECURITY
AWARENESS
MONTH 2022

Small Bites

- Reset password (length beats complexity)
  - If you can, implement MFA
- Sign up for Vulnerability Scanning and/or Web Application Scanning
- Set up a meeting with department heads to identify and make a list of critical services for the organization
  - Each department should make their specific list ahead of time
- At the meeting mentioned above, combine and reconcile the lists into one
  - Once that list is created, prioritize and establish the order of recovery

Questions?

For more information:
www.cisa.gov

Chris Gabbard
Cybersecurity Advisor
Region 5 – Minnesota District
Phone: 612-716-3044
Email: christopher.gabbard@cisa.dhs.gov

CYBERSECURITY AWARENESS MONTH 2022

For more information:

www.cisa.gov

www.cisa.gov/shields-up

Questions?

CISARegion5@hq.dhs.gov


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA