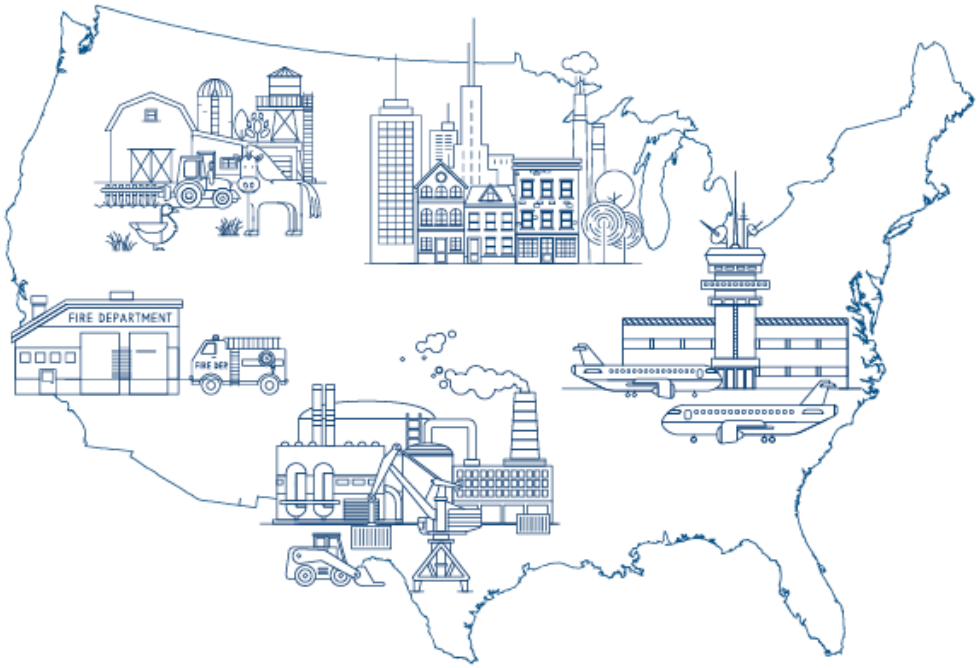
CYBER THREAT BRIEFING (2026)

Ryan Lewis
Cybersecurity Advisor
US Department of Homeland Security
Cybersecurity and Infrastructure Security Agency – Region IV

Cybersecurity and Infrastructure Security Agency (CISA)

As America's Cyber Defense Agency and the National Coordinator for critical infrastructure resiliency and security, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

Integrated Operations



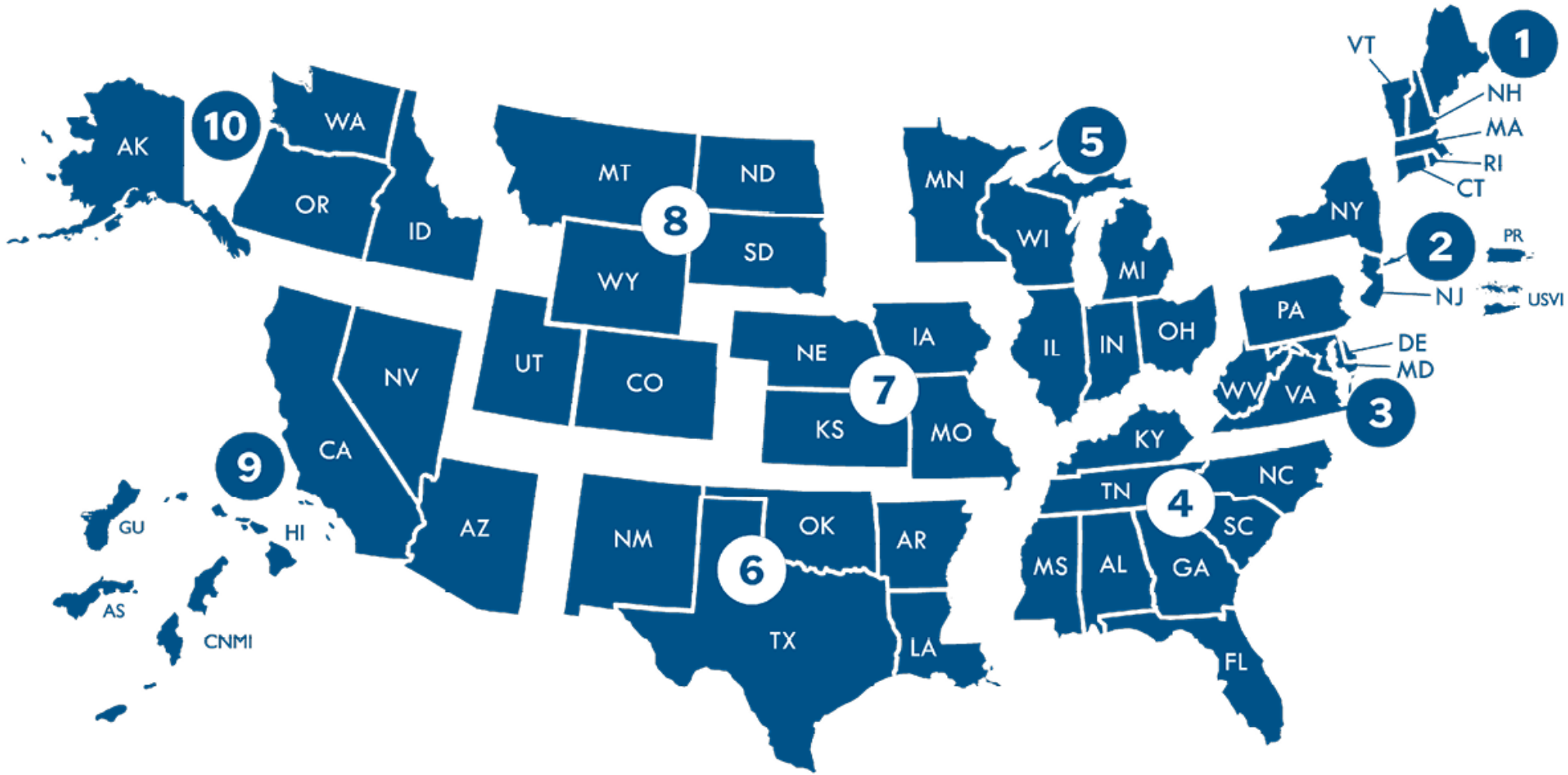
CISA's Integrated Operations Division enhances the resilience of our nation's critical infrastructure by taking an integrated approach to delivering services and sharing information. By meeting our stakeholders where they are, we help critical infrastructure owners and operators mitigate risk.

HOW CISA IS CARRYING OUT ITS INTEGRATED OPERATIONS MISSION:

- Provide Operational Visibility to Understand, Manage, and Reduce Risk to the Nation
- Offer a Unified Regional Approach to Sharing Information and Delivering CISA Services

CISA Regions

1. Boston, MA
2. New York, NY
3. Philadelphia, PA
4. Atlanta, GA
5. Chicago, IL
6. Dallas, TX
7. Kansas City, MO
8. Denver, CO
9. Oakland, CA
10. Seattle, WA



CISA.GOV/REGIONS

Today's Risk Landscape

America remains at risk from a variety of threats:

What Is Cybersecurity?

Cybersecurity is the protection of computer systems and networks from attacks by malicious actors that could cause unauthorized information disclosure, theft, or damage to hardware, software or data.

Wherever there is technology, there needs to be cybersecurity.

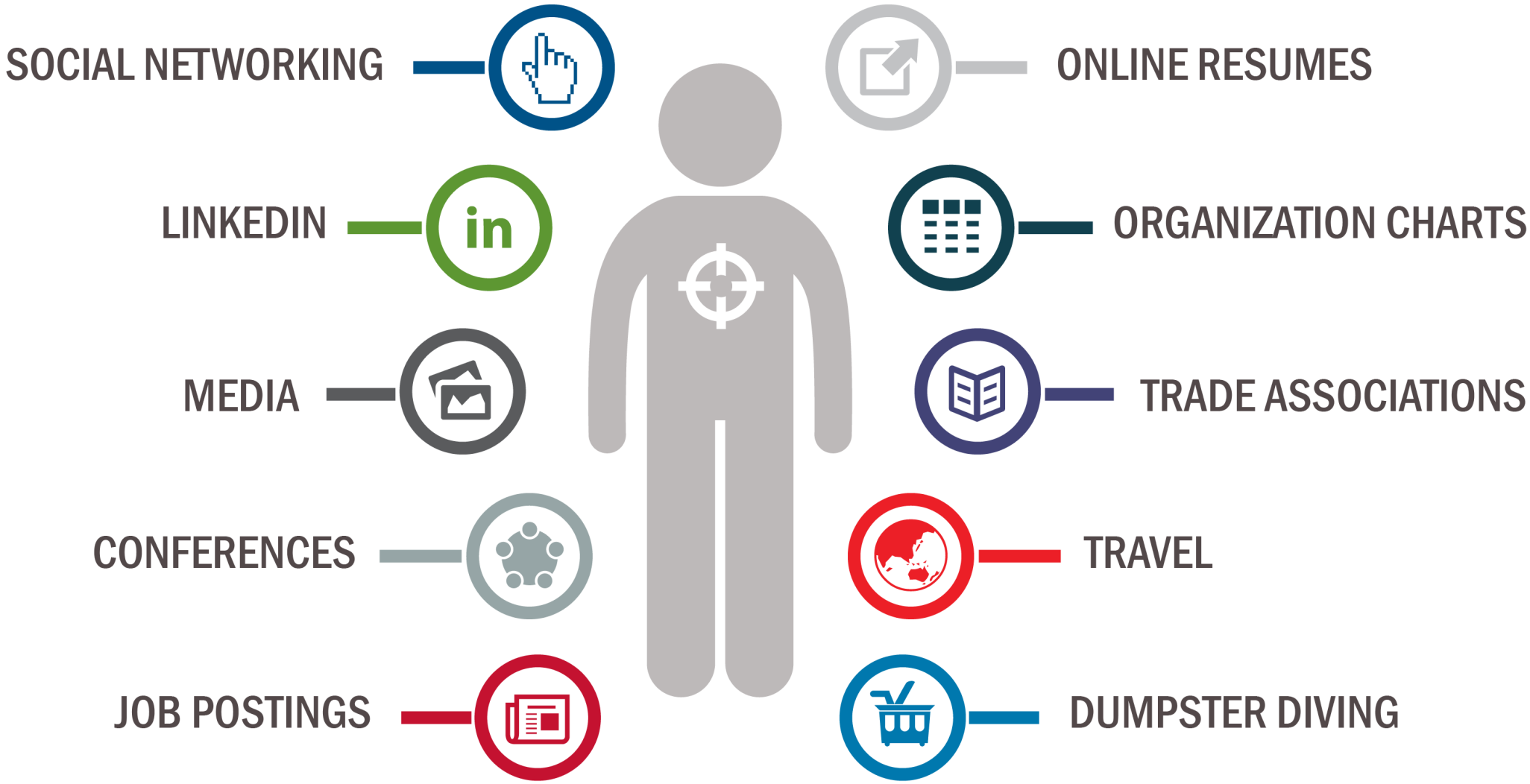
Ryan Lewis
June 3, 2026

Why Is it Important?

Implementing cybersecurity best practices helps protect intellectual property and other sensitive data, as well as networks and systems that support your operations.

Ryan Lewis
June 3, 2026

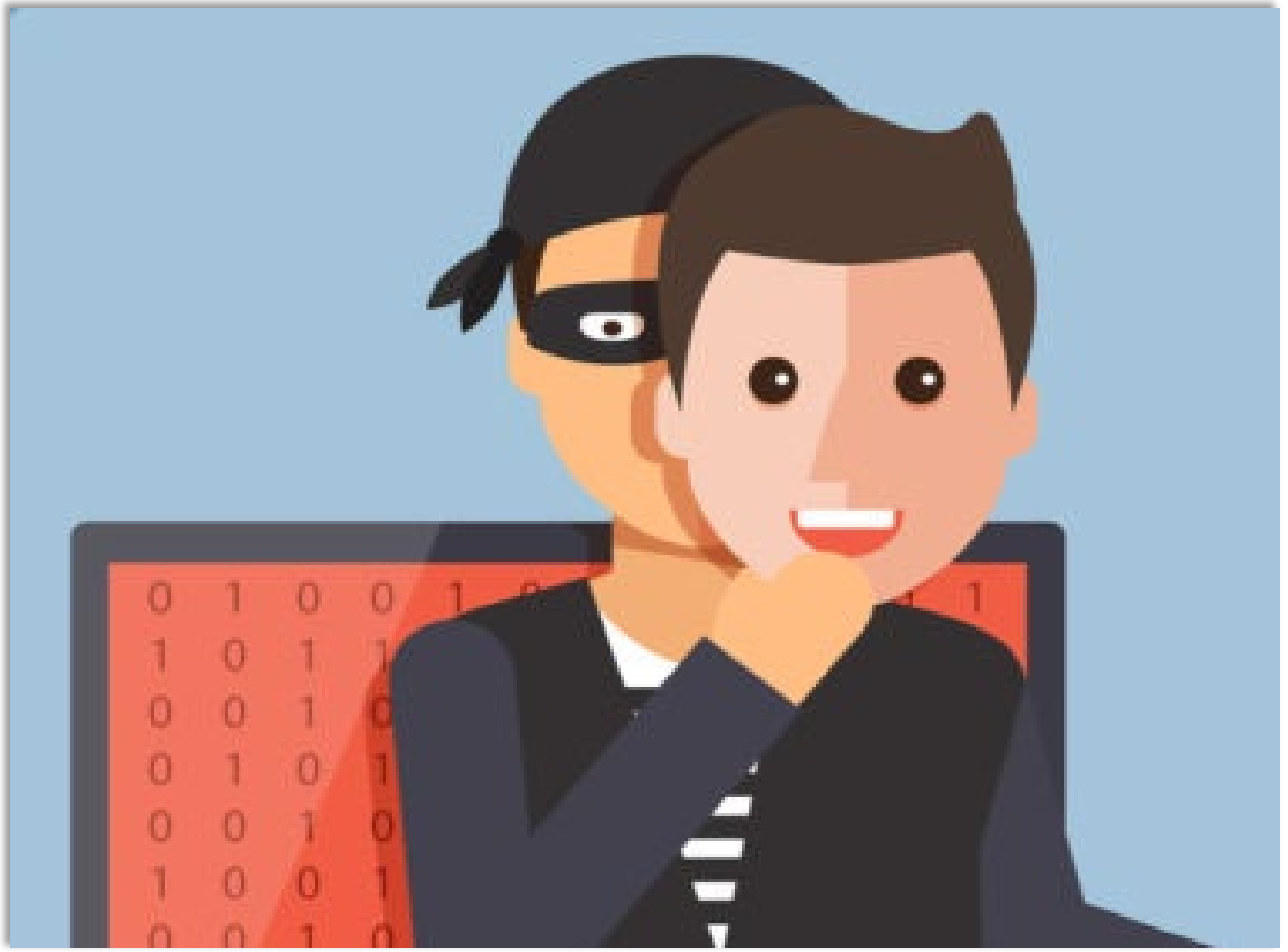
How Are You Targeted? – Human Vulnerabilities



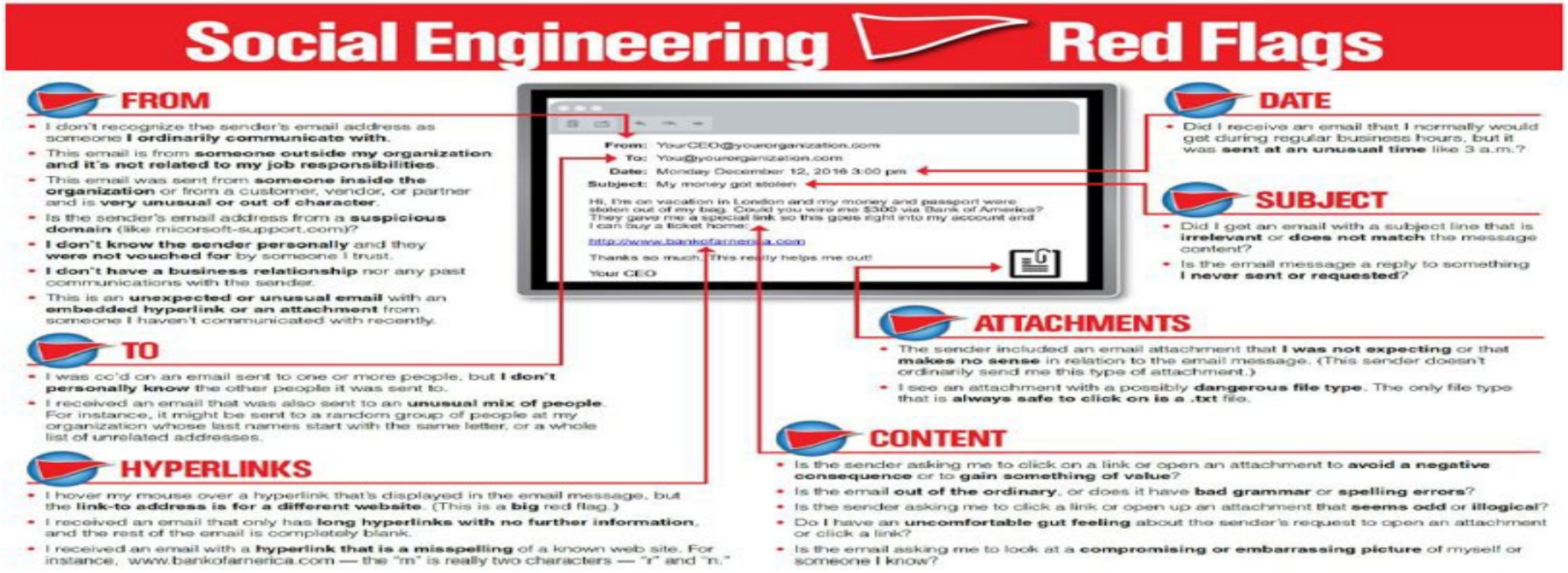
SOCIAL ENGINEERING

Social Engineering

Use of deception, through manipulation of human behavior, to target and manipulate you into divulging confidential or personal information and using it for fraudulent purposes.



SOCIAL ENGINEERING



Especially under the prevailing conditions – Always Pause and Ask:

Is this message expected?

Do I recognize the sender of this email?

Is there something odd about the email address?

Verify the email address/domain by hovering the cursor over an email address or embedded link, without clicking; the actual destination appears in a text box or bubble.

Is there a needlessly urgent call to action in the email?

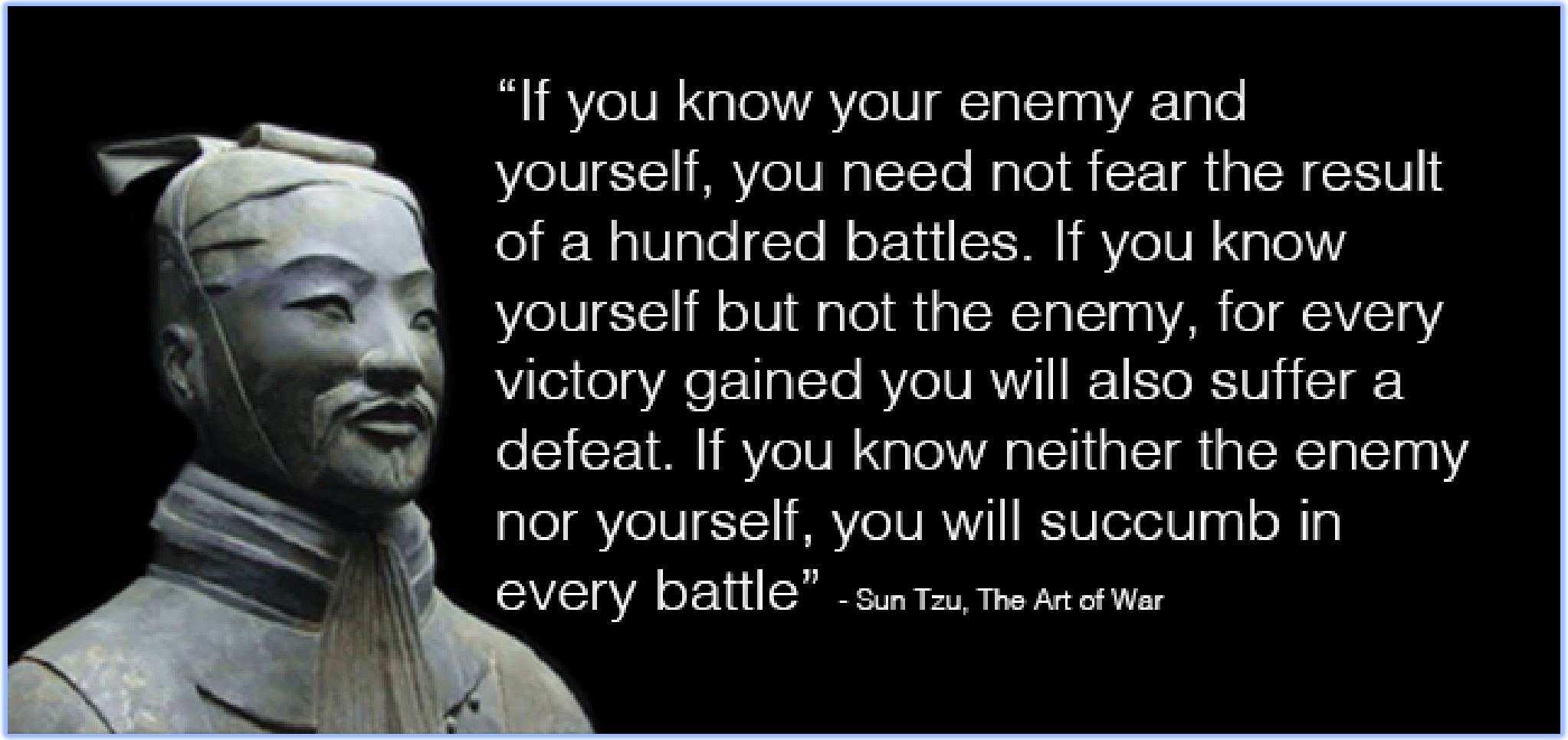
Is the action sought odd or unfamiliar?

Are my network access credentials requested after clicking to open a link?

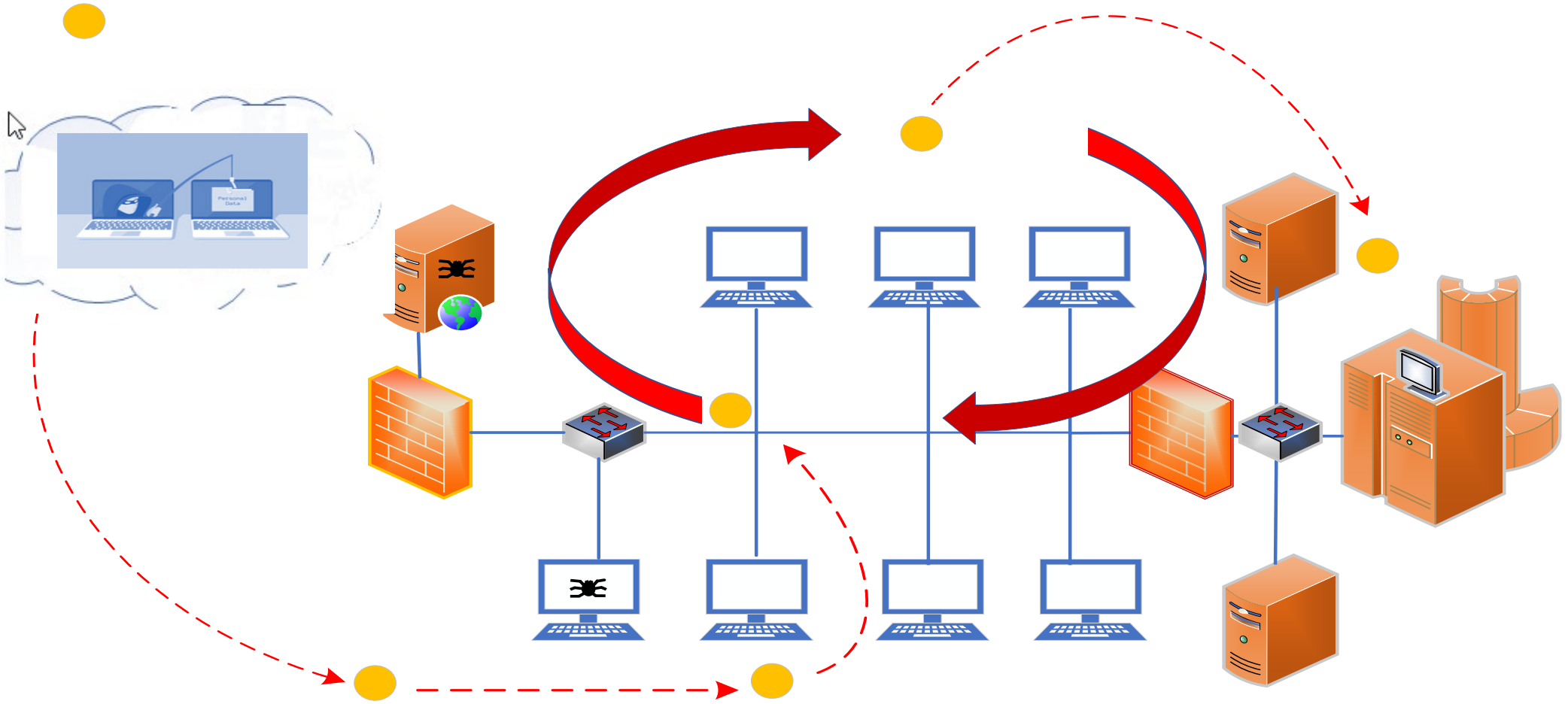
NEVER enter user name and password in these circumstances!

Be Attentive – and Protect Yourself and the Network

KNOW THY ENEMY



MECHANICS OF A CYBER ATTACK



NEXT STEPS

BUILD RESILIENCE

National Security Memorandum on Critical Infrastructure Security and Resilience

- Published On April 30, 2024, by the White House National Security Council (NSC)
- This memo builds on the important work that the Cybersecurity and Infrastructure Security Agency (CISA) and agencies across the federal government
- It also replaces Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience

FOUR ESSENTIAL BEHAVIORS

Update software

Use strong passwords and a password manager

Turn on multifactor authentication (MFA)

Recognize and report phishing

UPDATE SOFTWARE

What should you remember about updates?

- Updates are the easiest way to ensure your devices and apps are protected from the latest threats.
- Updates only protect you if you install them, so:
  - Install them right away.
    (Don't click "remind me later.")
  - Enable automatic updates
    for convenience.

USE STRONG PASSWORDS

What makes a strong password?

Long

- At least 16 characters

Random

- Upper- and lower-case letters
- Numbers
- Special characters
- Spaces
- Consider passphrases (5-7 unrelated words).

Unique

- Different for each account
- NEVER reuse passwords.

POP QUIZ #1

How many online accounts does the average American use?

A. 12

B. 100

C. 38

POP QUIZ #1

How many online accounts does the average American use?

~~A. 12~~

B. 100

~~C. 38~~

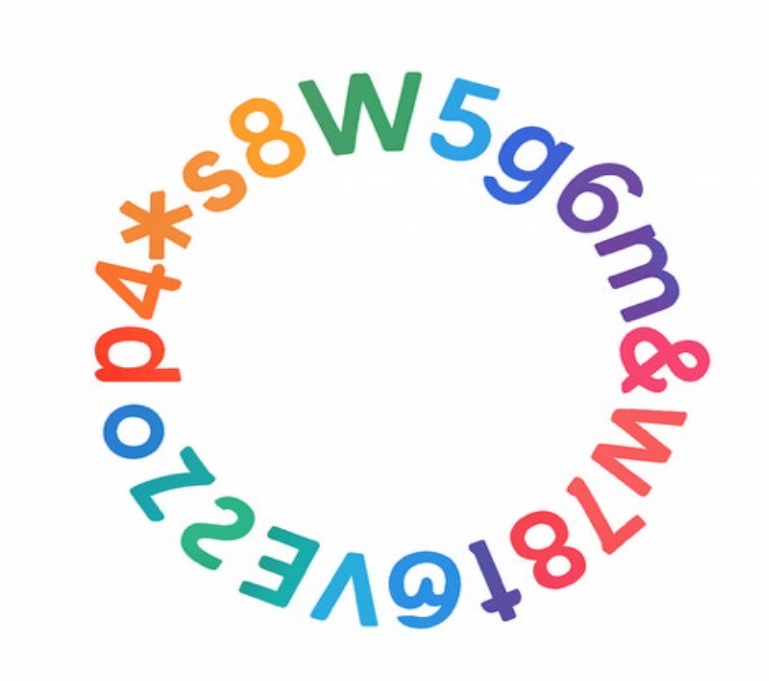
POP QUIZ #2

How many unique passwords are used for those accounts?

A. 8

B. 1

C. 20



POP QUIZ #2

How many unique passwords are used for those accounts?

A. 8 (same pw for 12)

~~B. 1~~

~~C. 20~~

USE A PASSWORD MANAGER

Why use a password manager?

- Stores your passwords.
- Alerts you of duplicate passwords.
- Generates strong passwords.
- Fills in your login credentials on websites to make sign-in easy.
- Won't fall for a phishing website, even if you do.

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

TURN ON MFA EVERYWHERE

What is MFA and where should you use it?

Multifactor authentication (MFA) provides an extra layer of security for your accounts by requiring a quick second step to verify your identity when logging in. Use it on every account that offers it, especially:

- Email
- Accounts with financial information
  Ex: Banks, online stores
- Accounts with personal information
  Ex: Social media

Turn on Multifactor Authentication

Which MFA methods are best?

Choose the most secure MFA method available. Here are some options, from most to least secure:

Security key:
your device. It provides the best protection against phishing and is easy to use.

Authenticator app with number matching: An app prompts you to enter a number on your phone. You enter a number shown on the login screen to confirm your identity

Authenticator app with one-time code:

Biometrics: Uses your fingerprint or face to confirm your identity.

Text or email code: A one-time code is sent to your phone or email. Least secure method

Ryan Lewis
June 3, 2026

RECOGNIZE AND REPORT PHISHING

How can you tell if a message is phishing?

A tone that's urgent or makes you scared

Ex: "Click this link immediately or your account will be closed."

Sender email address doesn't match the company it's coming from

Ex: Amazon.com vs. Amaz0n.com

Unexpected communications such as an email or attachment you weren't expecting

Requests to send personal info

Legitimate organizations don't ask for personal information through email or an unexpected call.

Misspelled words, bad grammar and odd URLs

Be aware that AI will make spotting these more challenging—stay diligent.

Recognize and Report Phishing

What should you do if you spot a phish?

DO

- Verify that the communication is real and contact the sender directly through known phone numbers or emails.
- Report it to your IT department or email/phone provider.
- Use email filters. Many email services have filters that can help prevent phishing messages
-

DON'T

- Don't click any links you don’t trust, even “unsubscribe” (just delete).
- Don't click any attachments you were not expecting or recognize.
- Don't send personal info online or share over the phone.

Ryan Lewis
June 3, 2026

REPORT INCIDENTS

Why report cyber incidents?

- For situational awareness
- For decision making
- Requesting response assistance

When to report a cyber incident?

If there is a suspected or confirmed cyber attack or incident that:

- Affects core or critical business functions;
- Results in the loss of data, system confidentiality, integrity, and/ or availability; or control of systems;
- Indicates malicious software is present on critical systems

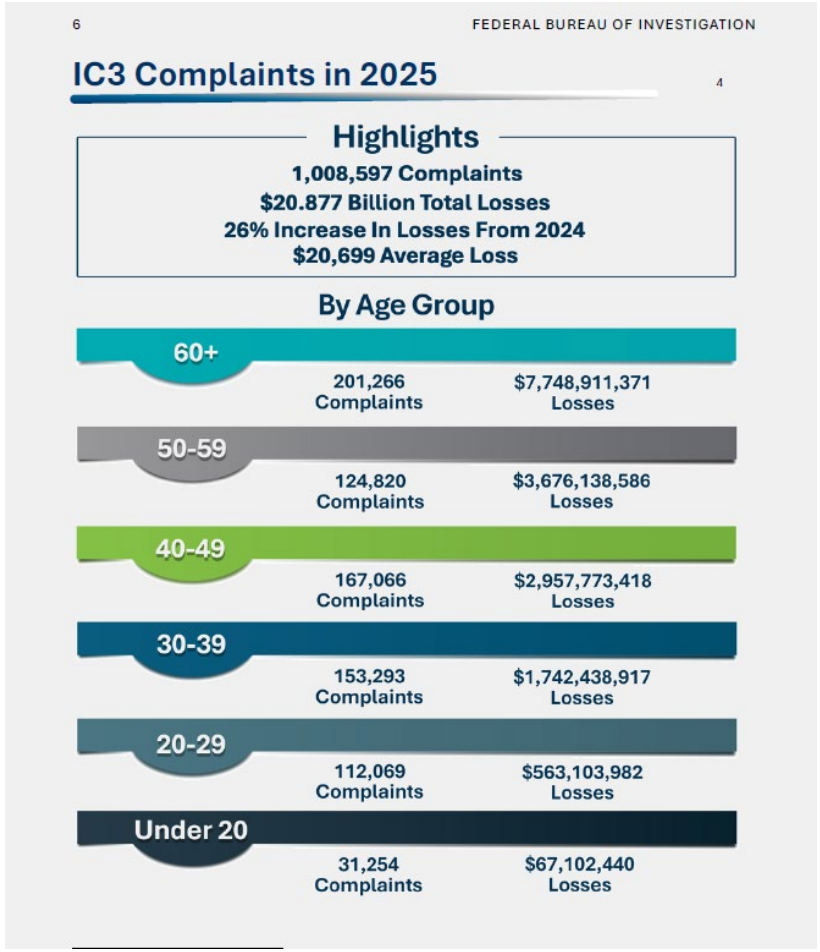
Who to report cyber incidents to?

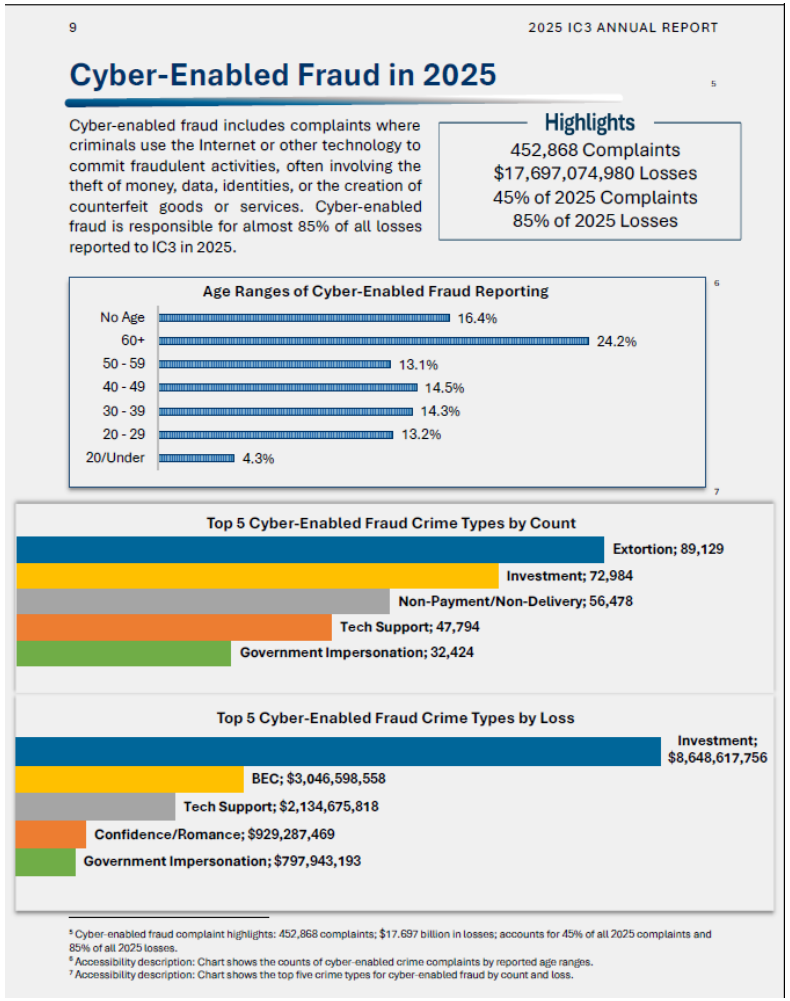
- Leadership, public affairs, legal and other internal stakeholders
- Relevant vendors
- Law enforcement and other government agencies
- Cyber insurance providers
- Appropriate 3rd party incident response teams

Report Cyber Incident Information to CISA and the

- **How do you report a cyber incident, or suspected cyber incident?**
  - Use the online form at: cisa.gov/report
- **Welcome to the Internet Crime Complaint Center**
  - https://www.ic3.gov/
- **Subscribe to the CISA Community Bulletin**
  - Sign up for the CISA Community Bulletin to learn how you can spread cybersecurity awareness across the country to people of all ages. Organizations and individuals will learn about CISA services, programs, and products and how they can use them to advocate and promote cybersecurity within their organizations and to their stakeholders.

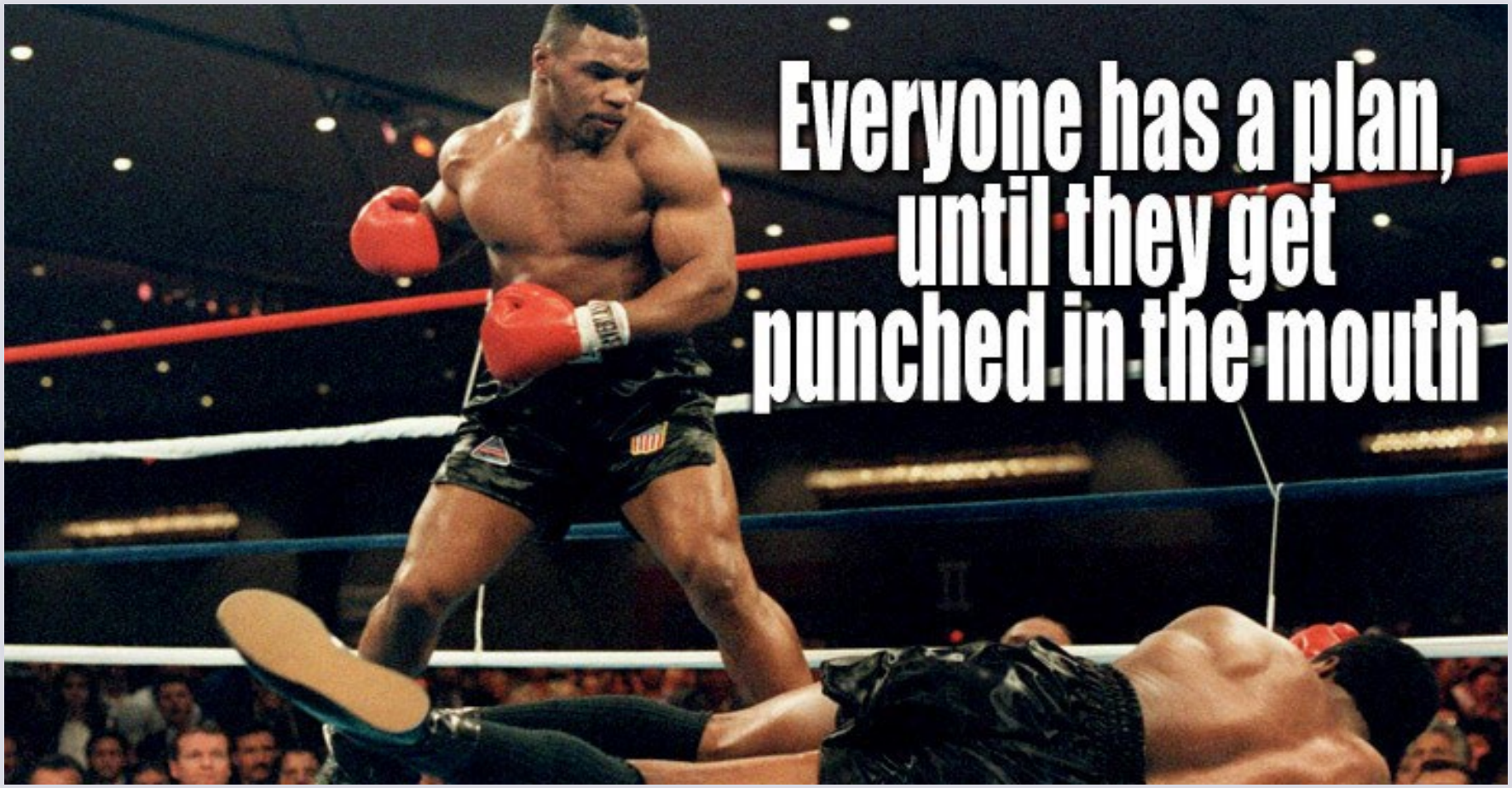
IC3 Complaints in 2025





Domestic Financial Fraud Kill Chain (D-FFKC) Process

BOTTOM LINE



For more information:

www.cisa.gov

Questions?

Ryan.Lewis@cisa.dhs.gov
(202) 975-9453


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY