CYBER SCAMS

Jason Burt
Cybersecurity Advisor (CSA)
Region IV

Overview

- CISA
- Cybersecurity Advisor Program
- Targets of Opportunity
- Common Cyber Scams
- Avoiding Cyber Scams
- Questions

CISA

- CISA consists of:

Cybersecurity Division

National Risk Management Center

Emergency Communications Division

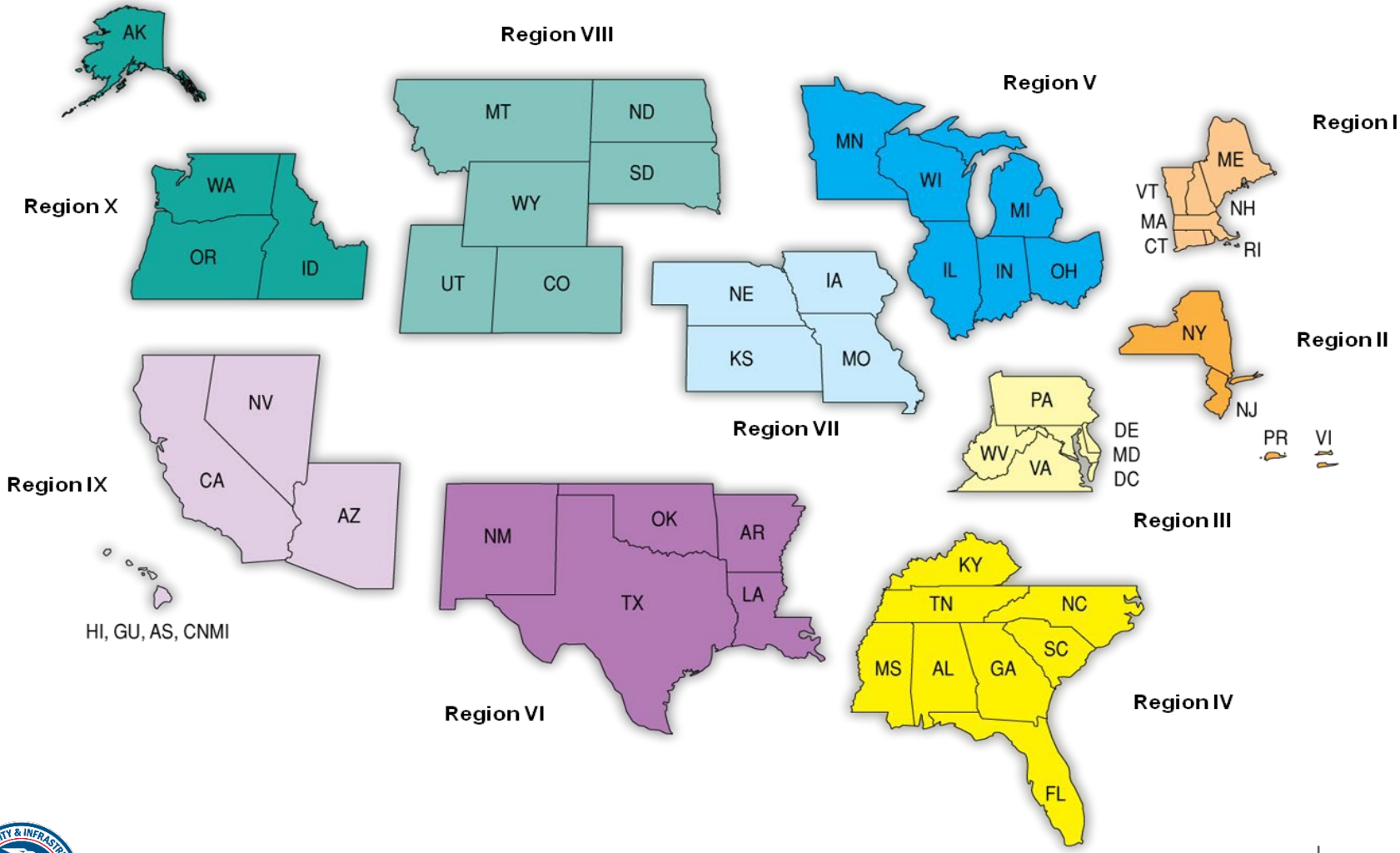
Infrastructure Security Division

CISA Mission and Vision

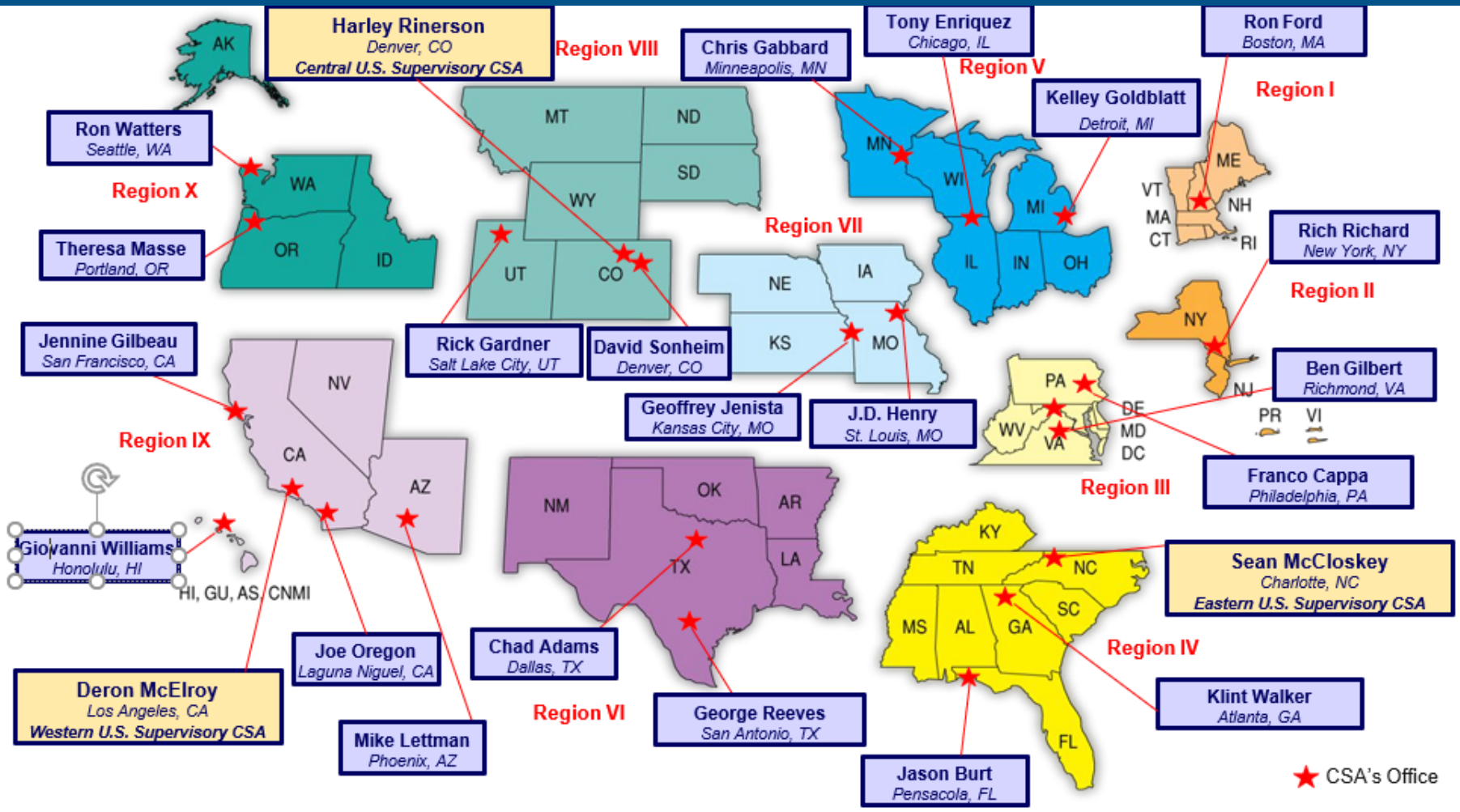
- Cybersecurity and Infrastructure Security Agency (CISA) mission:
  - Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

- CISA vision:
  - A Nation with secure, resilient, and reliable critical infrastructure upon which the American way of life can thrive

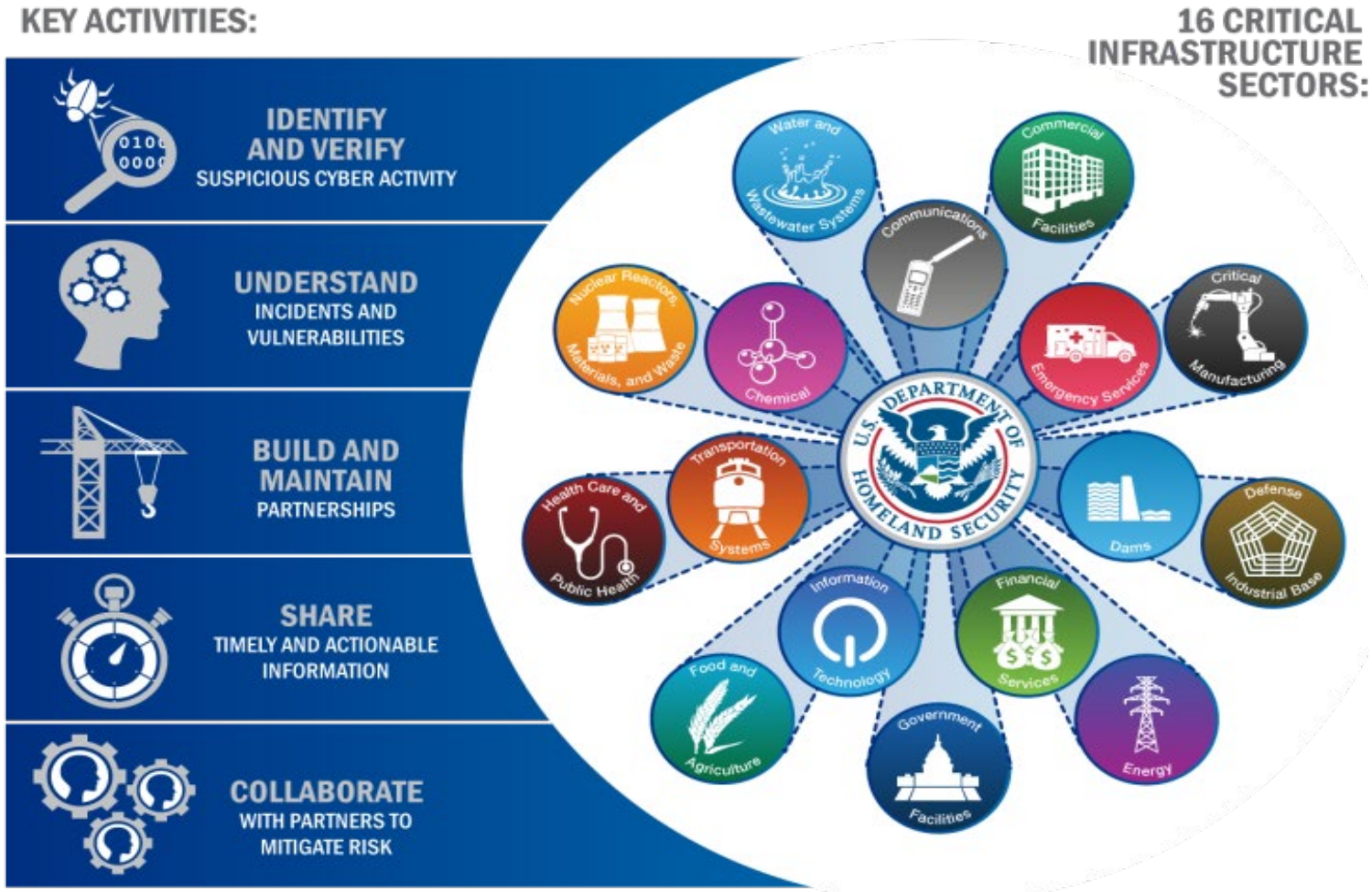
CSA Program


AK
Region VIII
MT
ND
SD
WY
UT
CO
Region V
MN
WI
MI
IL
IN
OH
Region I
ME
VT
NH
MA
CT
RI
Region X
WA
OR
ID
NE
IA
KS
MO
Region VII
NY
Region II
NJ
PR
VI
PA
WV
VA
DE
MD
DC
Region III
NV
CA
AZ
Region IX
HI, GU, AS, CNMI
NM
OK
AR
TX
LA
Region VI
KY
TN
NC
SC
MS
AL
GA
FL
Region IV

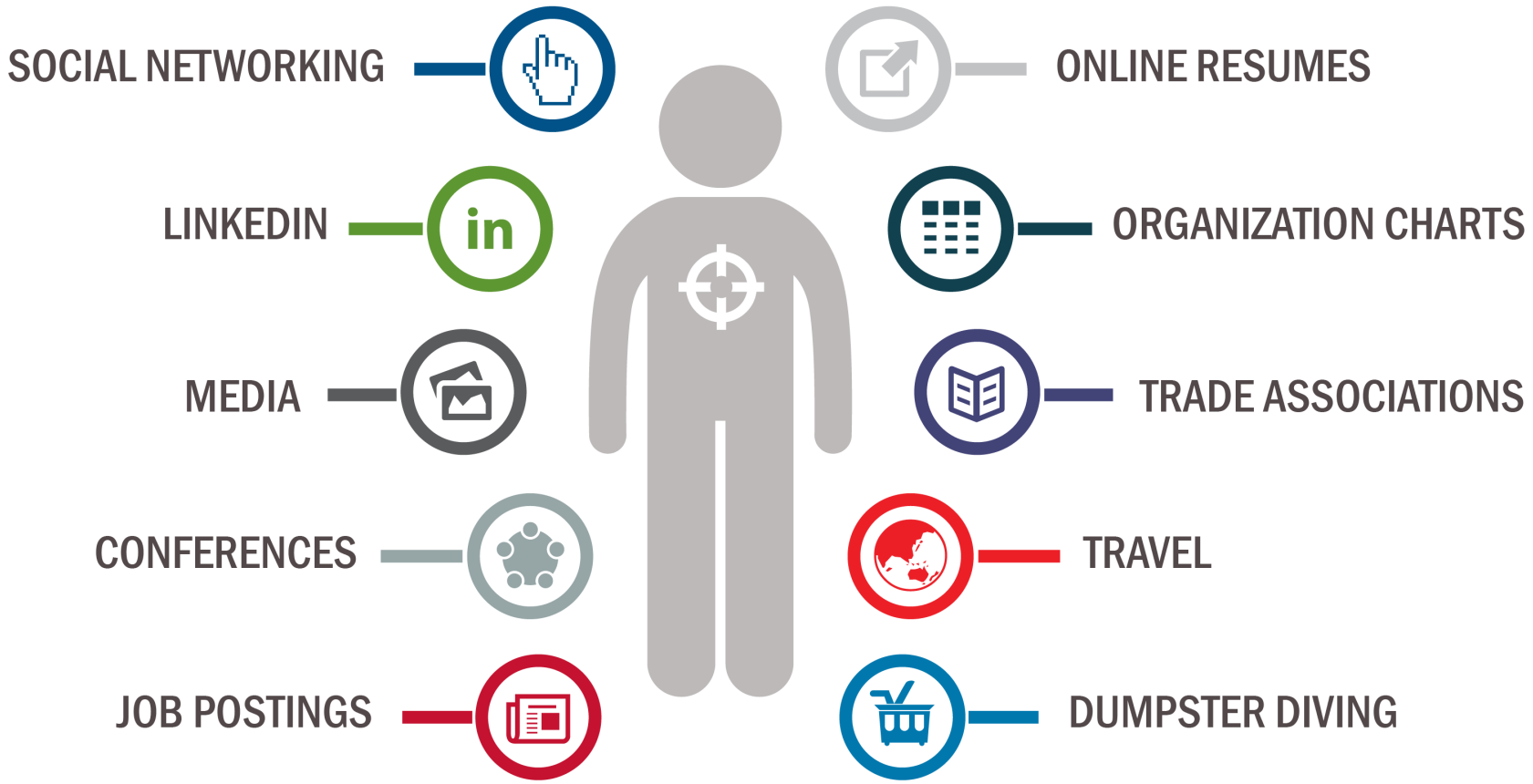
CSA Program


Harley Rinerson
Denver, CO
Central U.S. Supervisory CSA
Region VIII
Chris Gabbard
Minneapolis, MN
Tony Enriquez
Chicago, IL
Region V
Ron Ford
Boston, MA
Region I
Kelley Goldblatt
Detroit, MI
Ron Watters
Seattle, WA
Region X
Theresa Masse
Portland, OR
Rich Richard
New York, NY
Region II
Jennine Gilbeau
San Francisco, CA
Rick Gardner
Salt Lake City, UT
David Sonheim
Denver, CO
Region VII
Geoffrey Jenista
Kansas City, MO
J.D. Henry
St. Louis, MO
Ben Gilbert
Richmond, VA
Region IX
Franco Cappa
Philadelphia, PA
Region III
Giovanni Williams
Honolulu, HI
HI, GU, AS, CNMI
Joe Oregon
Laguna Niguel, CA
Chad Adams
Dallas, TX
Sean McCloskey
Charlotte, NC
Eastern U.S. Supervisory CSA
Region IV
Deron McElroy
Los Angeles, CA
Western U.S. Supervisory CSA
Mike Lettman
Phoenix, AZ
Region VI
George Reeves
San Antonio, TX
Klint Walker
Atlanta, GA
Jason Burt
Pensacola, FL
CSA's Office
AK
WA
OR
ID
MT
ND
SD
WY
UT
CO
NE
IA
KS
MO
MN
WI
MI
IL
IN
OH
ME
VT
NH
MA
CT
RI
NY
NJ
PA
WV
VA
DE
MD
DC
PR
VI
NV
CA
AZ
NM
OK
AR
TX
LA
KY
TN
NC
SC
MS
AL
GA
FL

Protecting Critical Infrastructure



Targets of Opportunity



E-mail Scams

- Bogus business opportunities
- Chain letters
- Work-at-home schemes
- Health and diet scams
- Easy money
- “Free” goods
- Investment opportunities

Phishing

- Phishing emails are crafted to look as if they've been sent by a legitimate organization.
- Purpose:
  - Fool you into visiting malicious websites in order to download viruses
  - Fool you into revealing personal information (SSN, Banking, Passwords)

  - visible link: http://www.yourbank.com/accounts/
  - actual link to bogus site: http://itcare.co.kr/data/yourbank/index.html

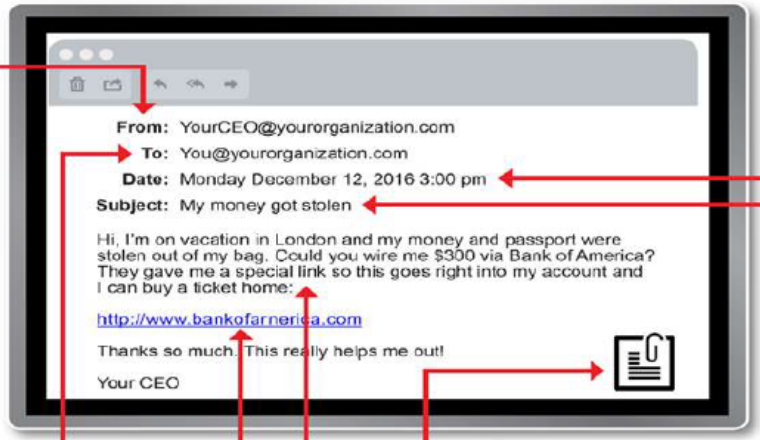
Phishing

- Common phishing tactics:
  - Fake emails from online payment, auction, and ISP services
    - Claim there is a problem with your account and request for you to access a bogus website to provide personal and account info.
  - Fake Patriot Act violations
    - Claim to be from the FDIC. Requires info to “verify identity”
  - Fake communications from the IT department
    - Attempts to gain access to organization’s networks and computers
  - Low-tech solutions of any of the above, asking for you to fax back information on a printed form you can download from a malicious website.

Phishing Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

What to look for…

- Email posing as virtual postcard
- Email masquerading as security bulletin from a software vendor requesting the recipient apply an attached “patch”
- Email with the subject line “funny” encouraging the recipient to view the attached “joke”
- Email claiming to be from an antivirus vendor encouraging the recipient to install the attached “virus sweeper” free of charge

Avoid being a victim….

- Filter Spam
- Regard Unsolicited Email with Suspicion (even from legitimate addresses)
- Treat Email Attachments with Caution!
- Install and Update Anti-virus Software
- Use Long Uncommon Pass Phrases and Multi-Factor Authentication

QUESTIONS??

For more information:
CyberAdvisor@cisa.gov

Questions?
Email: Jason.Burt@cisa.dhs.gov
Phone: (202) 578-9954


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY