wef Member Association

Water Environment Federation
the water quality people®

PARTNERING FOR MUTUAL SUCCESS

Data Privacy and Cyber Security

Lynn Thomson – Sr. Director, Information Technology

Andy Decker – Sr. Manger, Network Systems

Simple ways to improve cyber security

Safe Email Practices

- Hover over links
- Beware of attachments
- Look for spoofed domains

Safe Web Browsing Practices

- Think before you click
- Always use HTTPS
- No saved passwords
- Avoid free public Wi-Fi

Email and Web Protection

- Firewalls
- Open DNS
- Email scans

Social Engineering Red Flags

FROM:

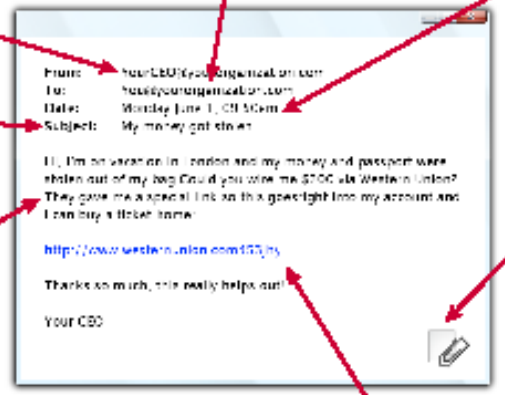
- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner 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 hadn't communicated with recently.

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, a seemingly random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

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**?

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 these types of attachment(s).)
- 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.

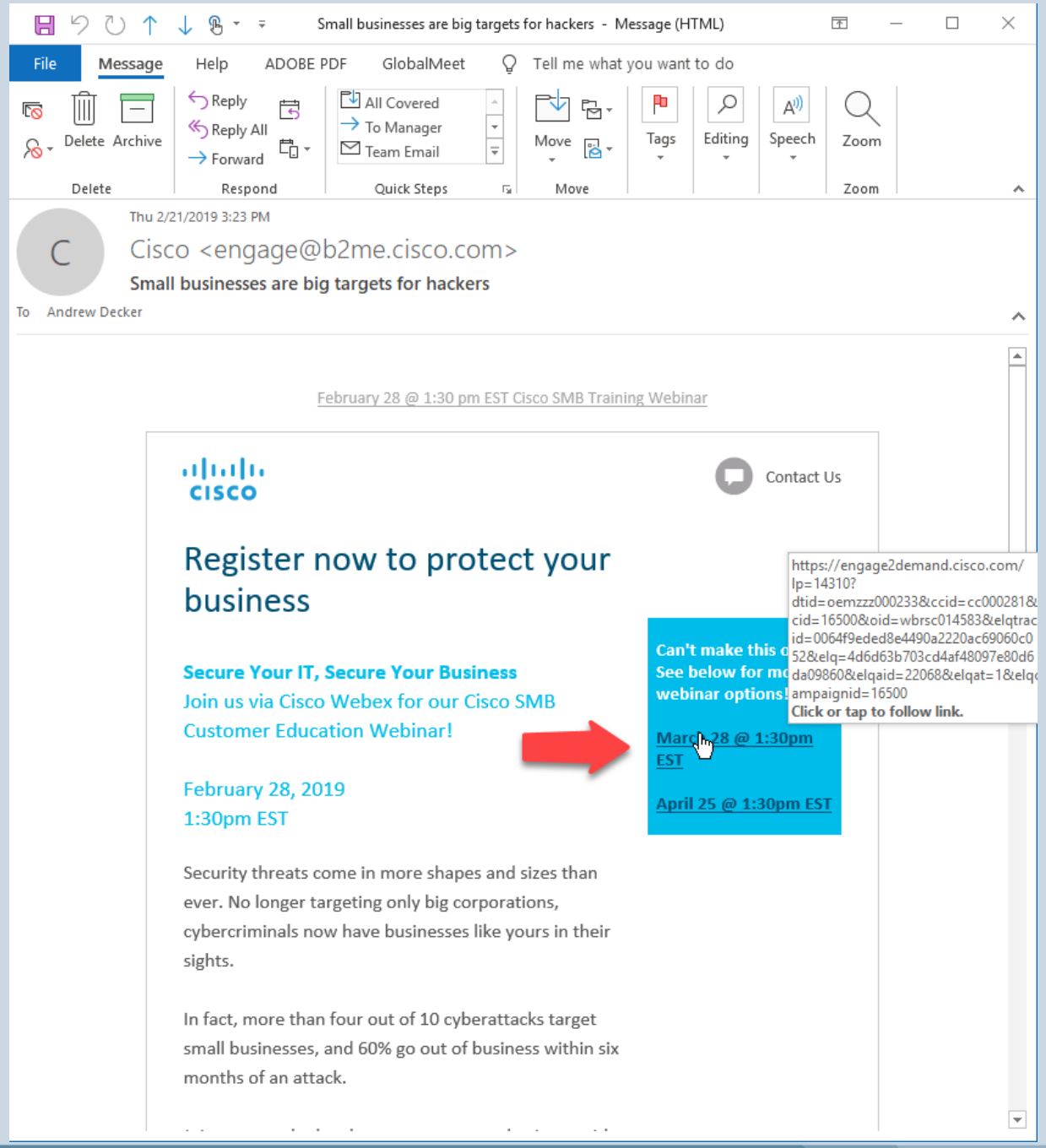
CONTENT:

- 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?

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" & "n".

KnowBe4
Human error. Conquered.


Small businesses are big targets for hackers - Message (HTML)
File
Message
Help
ADOBE PDF
GlobalMeet
Tell me what you want to do
Delete
Archive
Reply
Reply All
Forward
All Covered
To Manager
Team Email
Move
Tags
Editing
Speech
Zoom
Thu 2/21/2019 3:23 PM
Cisco <engage@b2me.cisco.com>
Small businesses are big targets for hackers
To Andrew Decker
February 28 @ 1:30 pm EST Cisco SMB Training Webinar
Contact Us
Register now to protect your business
Secure Your IT, Secure Your Business
Join us via Cisco Webex for our Cisco SMB Customer Education Webinar!
February 28, 2019
1:30pm EST
Security threats come in more shapes and sizes than ever. No longer targeting only big corporations, cybercriminals now have businesses like yours in their sights.
In fact, more than four out of 10 cyberattacks target small businesses, and 60% go out of business within six months of an attack.
April 25 @ 1:30pm EST
Click or tap to follow link.

Simple ways to improve cyber security

Passwords	Multi-factor Authentication	Biometrics
• Strong passwords • Use password managers • Avoid free public W-Fi • Always use HTTPS	• Text codes • Authenticator app	• Fingerprint scans • Facial recognition • Eye scans

Simple ways to improve cyber security

Software patching

- Firmware
- Operating systems
- Applications

Data Backups

- Removable drives
- Cloud storage

Cloud services

- Office 365 email
- OneDrive
- SharePoint

Most important way to improve cyber security

Have a plan

- Multi-layered approach
- Talk to your vendors and hosting providers
- Security standards
- Third part assessments

What is Data Privacy?

Data Privacy is the branch of information security dealing with the proper handling of data concerning consent, notice, sensitivity, and regulatory concerns. It is a **fundamental right** of the individual.

Data privacy is at the forefront of regulatory action now as a result of the European Unions GDPR regulations and Facebooks Cambridge Analytics scandal.

What is GDPR

General Data Protection Regulation (Get Data Protection Right)

Regulation designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.

What is happening in the U.S.

As of March 2018, all 50 U.S. States, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have all enacted breach notification laws that require businesses to notify consumers if their personal information is compromised.

Several U.S. states have also started/enacted legislation expanding consumer privacy and data protection laws covering areas such as:

- Data breach notification requirements
- Changes in data processing operations
- Information security requirements mandate
- Expansion of the personal data definitions
- Providing individuals with greater control over their personal data

States who have or are in the process of implementing data privacy protections

Alabama	Arizona	Colorado	Iowa
Louisiana	Nebraska	Oregon	South Carolina
South Dakota	Vermont	Virginia	California (2020 – California Computer Protection Act (CCP))

What does this mean for Associations?

Be aware of the information we collect	Is the information safe	What information am I able to share without customer permission
• How does this information help us serve our member? • How often is this information updated?	• Is it encrypted or sitting on a desktop in an easily accessible Excel file? • Is your software platform adhering to your state/federal data security regulations?	• Sharing with 3rd parties, i.e. Exhibitors • Sharing internally with committee chairs

How may data privacy impact you?

- Changes how you store your member information
- What information you supply to 3rd parties
- Need to Opt-in instead of Opting-out for materials sent

Questions