May 17, 2022

Airlines Clearing House
Revenue Accounting Committee Meeting

Understanding Cyber Security Trends and Safeguarding Your Business

VP Charles Banks, Manager of Information Security

Agenda

Welcome

Navigating the Cyber Risk Landscape

Phishing & Social Engineering

Prevention Strategies & Response

Q&A

My disclaimer

This presentation is meant to educate you — not to scare you.

But I do want you to take action when you leave.

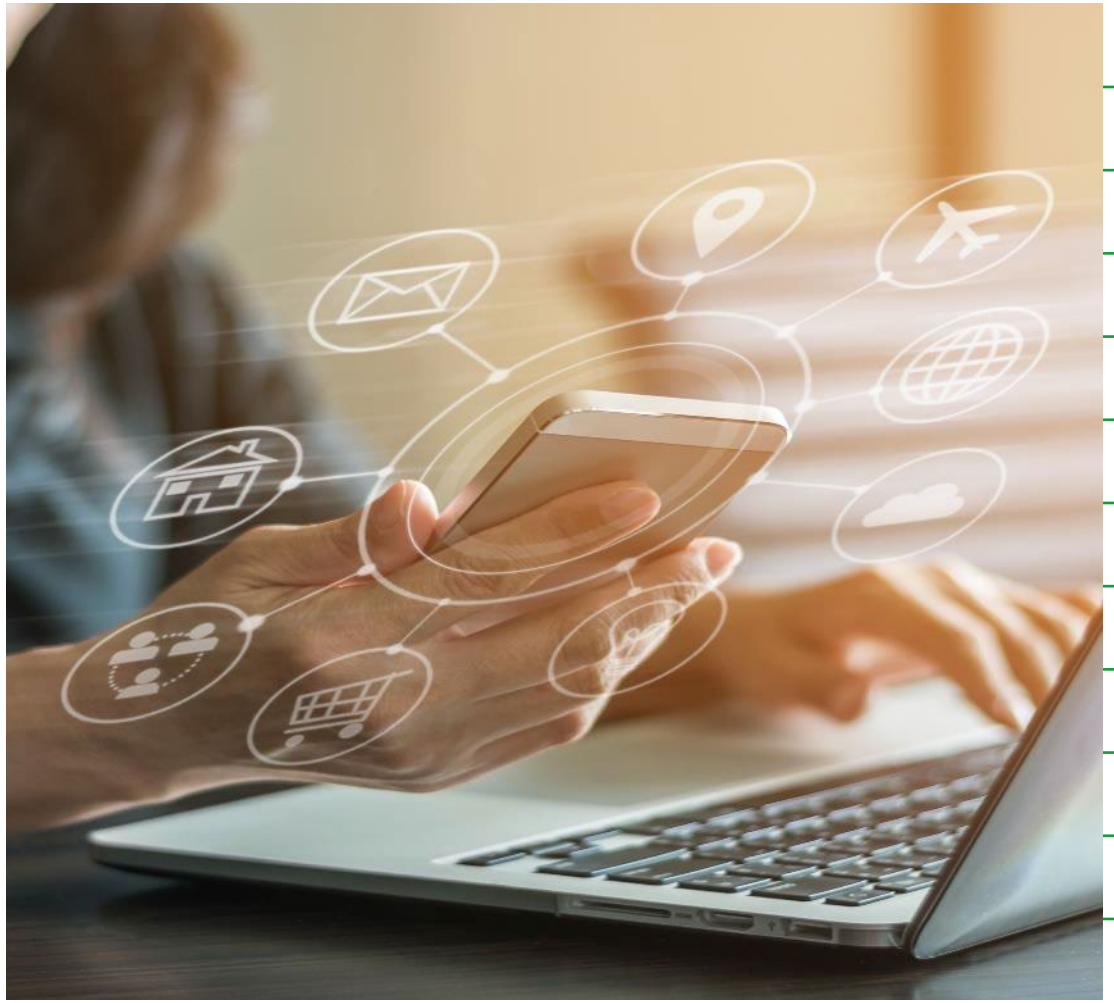
Cyber-physical “Internet of Things”

By 2022:

30 billion devices will be connected with online data volume increasing **50x**

Source: Forbes, Vice, Cisco IBSG, University of Michigan, ABC News, Qmed, Network World

What happens in an internet minute?



167M TikTok users watch videos

44M Facebook Live views

12M people send iMessages

6M people shop online

5.7M Google searches

2M Snapchat users send chats

694K YouTube users' stream

304K Dollars sent through Venmo

283K Dollars spent online on Amazon

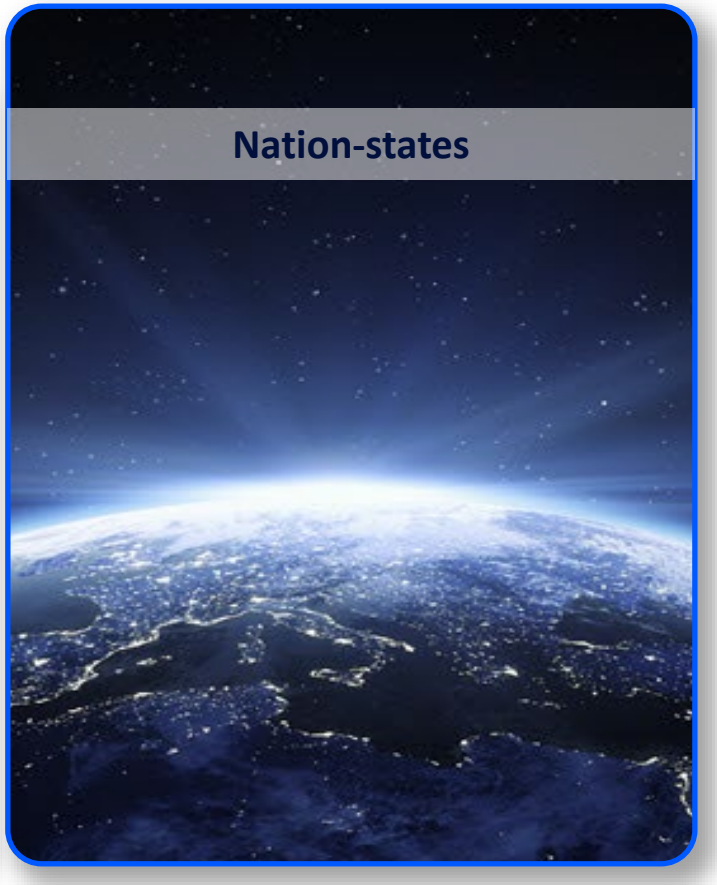
100K Teams users send messages

65K Instagram users share photos

856 Users host Zoom webinars

Source: July 2021, Data Never Sleeps 9.0.

Rapidly evolving threats — Current Landscape



Theft + Disruption + Destruction

Cyber Risks to Financial Institutions in Eastern Europe amid Russia-Ukraine Conflict

Impacted Industry: FSI

These threats target banks and other financial institutions in Western Ukraine and Eastern Europe

Sophistication: Highly Sophisticated

A new round of **wiper malware** was observed targeting Ukrainian government and financial institutions

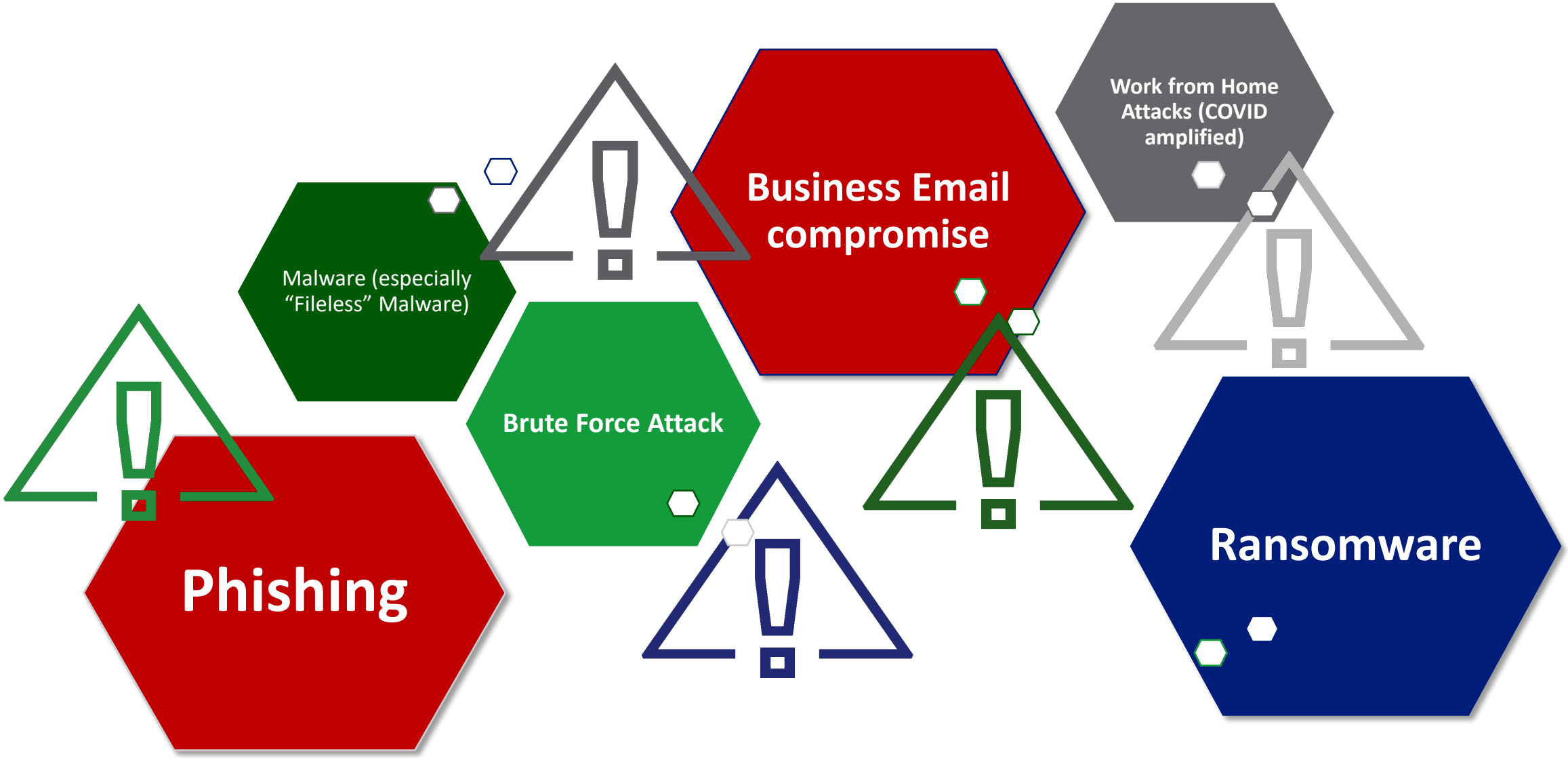
Intended Effect: Disruption

The goal is an escalation of war & disruption on financial transfers.

Assessment: Heightened Alert

Russian state-sponsored threat actors will continue to target the financial sector. These targets may include financial institutions that remain in Ukraine or operate in neighboring countries in Eastern Europe, as well as Western European and US-based financial institutions.

Top cybersecurity threats in 2021



Security Intelligence: https://securityintelligence.com/articles/cybersecurity-trends-and-emerging-threats-2021/

Threat landscape at a glance 2020 - 2021

Cybersecurity Executive Order

DEC 13

Discovery of a backdoor in the SolarWinds Orion business software was used to distribute malware. Impacted:

- **490 Fortune 500 firms affected**
- FireEye (major cybersecurity firm);
- Department of Homeland Security; and
- Treasury Department.

JAN 6

Four zero-day vulnerabilities in MS Exchange Server were actively exploited by state-sponsored threat groups and others to deploy backdoors and malware in widespread attacks.

MAY 7

Ransomware targeting computerized equipment impacting oil company's operations.

- $5M ransom paid

MAY 12

President Biden issued Executive Order in the wake of several major attacks to improve nation's cybersecurity and protect federal government networks.

MAY 25

SolarWinds hackers compromised USAID's Constant Contact email service account in external phishing attack.

MAY 30

Ransomware attack on the world's biggest meat processing company, JBS, escalated concerns about potential for a spike in meat prices and food supply as a national security threat.

- Ransom demand not disclosed.

JUL 2

IT company, victims of REvil ransomware attack. After paying ransom, received universal decryptor allowing customers to recover files.

- Ransom demand of $70 million (purportedly lowered to $40 million) paid.

Average cost of a data breach within United States businesses

Average cost of a data breach:

$4.24M

Cost difference where remote work was a factor causing breach:

$1.07M

Total breach cost due to lost business/ customer confidence

38%

Average number of days to identify and contain a data breach

287

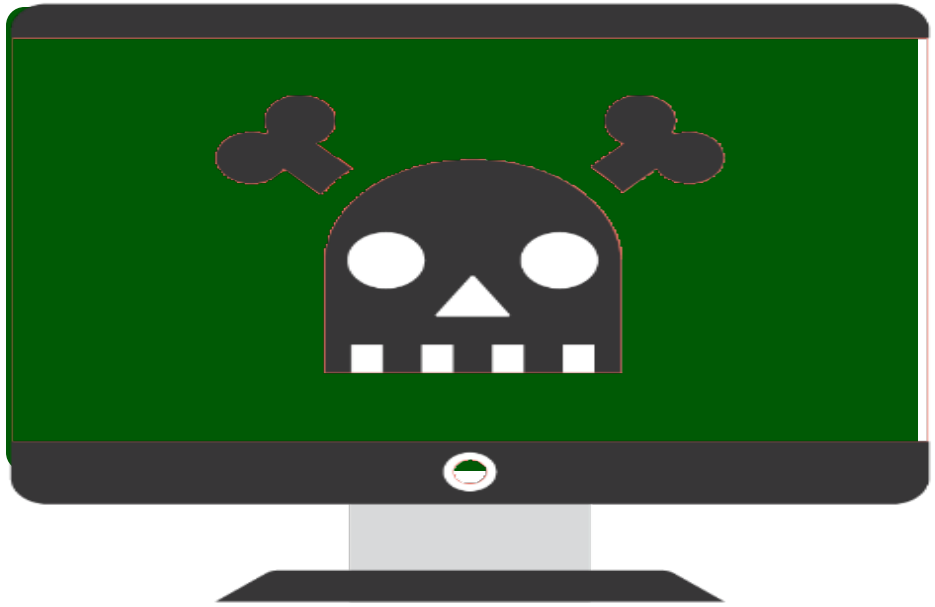
Source - IBM Ponemon: How much does a data breach cost? See end disclosures

What is Ransomware?

Ransomware is a type of malware attack that encrypts a victim's data until a payment is made to the attacker.

If the ransom payment is not made, the malicious actor publishes the data on data-leak-sites (DLS) or blocks access to the files in perpetuity.[1]

Payment demands are usually made in Bitcoin or another Cryptocurrency, which are very difficult to trace or recover.



Source: https://www.crowdstrike.com/cybersecurity-101/ransomware/

How has the COVID-19 pandemic impacted the cybersecurity landscape?

Attackers are capitalizing on fear

- The U.S. Federal Trade Commission (FTC) received **1.4 million reports of identity theft in 2021,** double the number from 2019.
- **Since the start of the COVID-19 pandemic, there has been a 300% increase in the number of cybercrimes in the U.S.**
- In 2020, the Federal Bureau of Investigation's (FBI) Internet Crime Center (IC3) received a record-breaking 791,790 cybercrime complaints, with reported losses being responsible for some US $4.2 billion in losses.
- By 2025, there will be 55-75 billion connected devices. Of these, 75% will be connected to the Internet of Things (IoT).
- According to Symantec, in **2021 IoT devices** experienced an average of 5,200 attacks per month.

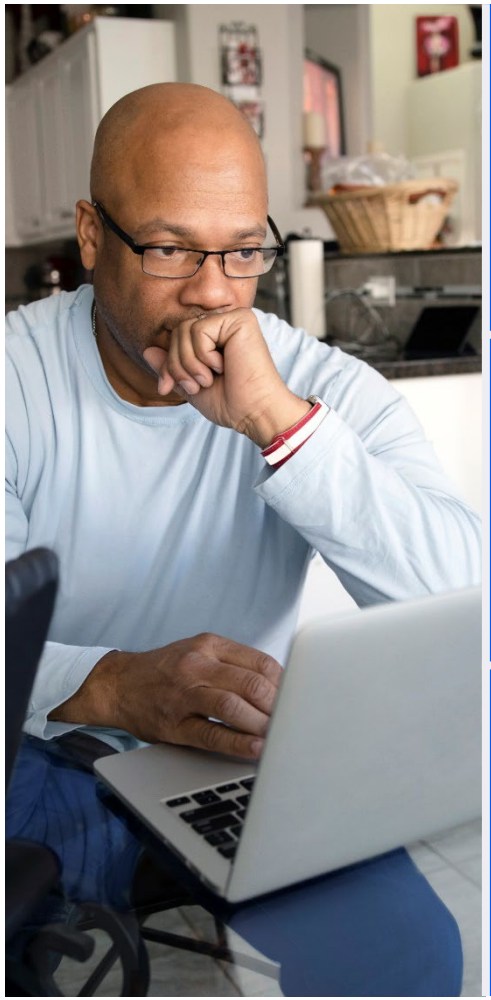
The cyber security attack surface has widened

Working from home poses unique opportunity for attackers

- Less-secure environment and connections at home
- Companies are moving quickly to respond to implications of the pandemic on their industry
- There may be less vigilance due to meeting business needs fast
- The lines are blurred between business and personal
- Employees just don’t know security policies

We often think about cybersecurity when we're physically present at work, but what kind of threats are present when working from HOME?

COVID-19 related work from home threats



Computing	• Business Email Compromise, impersonating company executives • Phishing emails related to Centers for Disease Control, World Health Organization, “new cases in your area,” charitable causes • Personal email use for official business • Unsecure connections and home Wi-Fi networks
Physical	• Leaving equipment outside employee’s control—overnight at family member’s house, etc. • Equipment not stored in a locked-down environment • Untrustworthy person in home • Printing and disposal of sensitive information
Voice	• Teleconferencing software security vulnerabilities • Zoombombing • Personal assistant devices always listening (Amazon Echo, Google Home, etc.) • Sensitive information discussed via third party tools

See end disclosures.

Real-life COVID scam examples

Dear Sir / Madam,

In response to the COVID-19 outbreak and resulting economic decline, many countries have responded with a consumer stimulus package to provide economic stability to individuals and families like yours.

See the attached consumer stimulus package document to find consumer relief measures issued in your country.

These economic benefits will allow you to take the necessary measures to limit person-to-person contact and slow the spread of COVID-19.

Thanks and regards,

Dr. Tedros Adhanom Ghebreyesus

World Health Organization

World Health Organization

Avenue Appia 20

1211 Geneva 27

Switzerland

Social media post: **Malvertising**

Phishing email

COVID-19 Everything you need to know

JD • John DeFranco <[redacted]>

To: • [redacted]

How to Protect your friends from nCov 2019 FAQ

There are more than 75,000 infected COVID-19 cases all around the world!

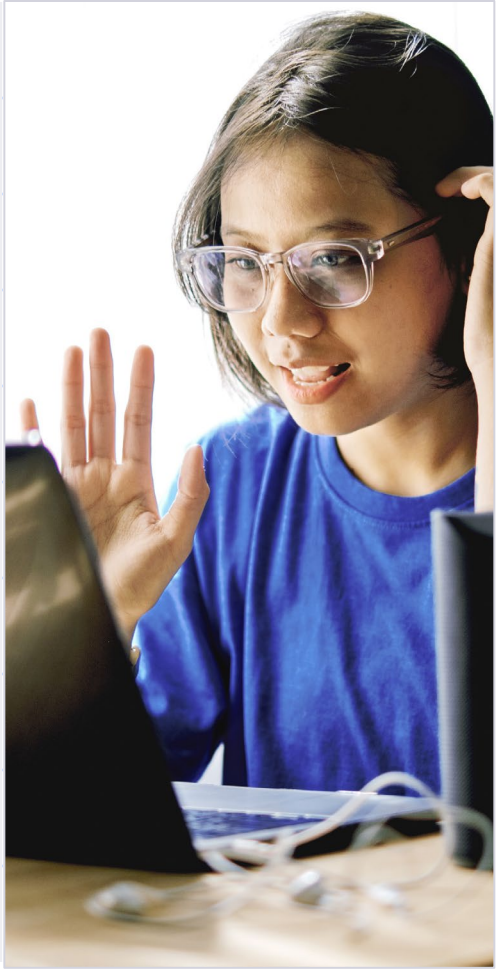
COVID-19-FAQ - uploaded with iCloud Drive.

Regards,
John DeFranco

As companies begin to solidify their return-to-office plans and transition into new working models, what can employees do to PROTECT themselves while working from home or in hybrid working models?

10 security tips for employees working from home

1	Pay close attention to email domains (internal and external)
2	**Make sure hardware, software and operating systems are current**
3	Take a second look at transactions; picking up phone is easiest
4	Don’t use personal email for business
5	Beware of printing and how documents are disposed
6	**Protect home Wi-Fi network**
7	Enhance your teleconferencing software security settings
8	**Use a VPN to connect to company network**
9	Don’t connect personal devices to work computers
10	**Don’t re-use passwords for work and personal**



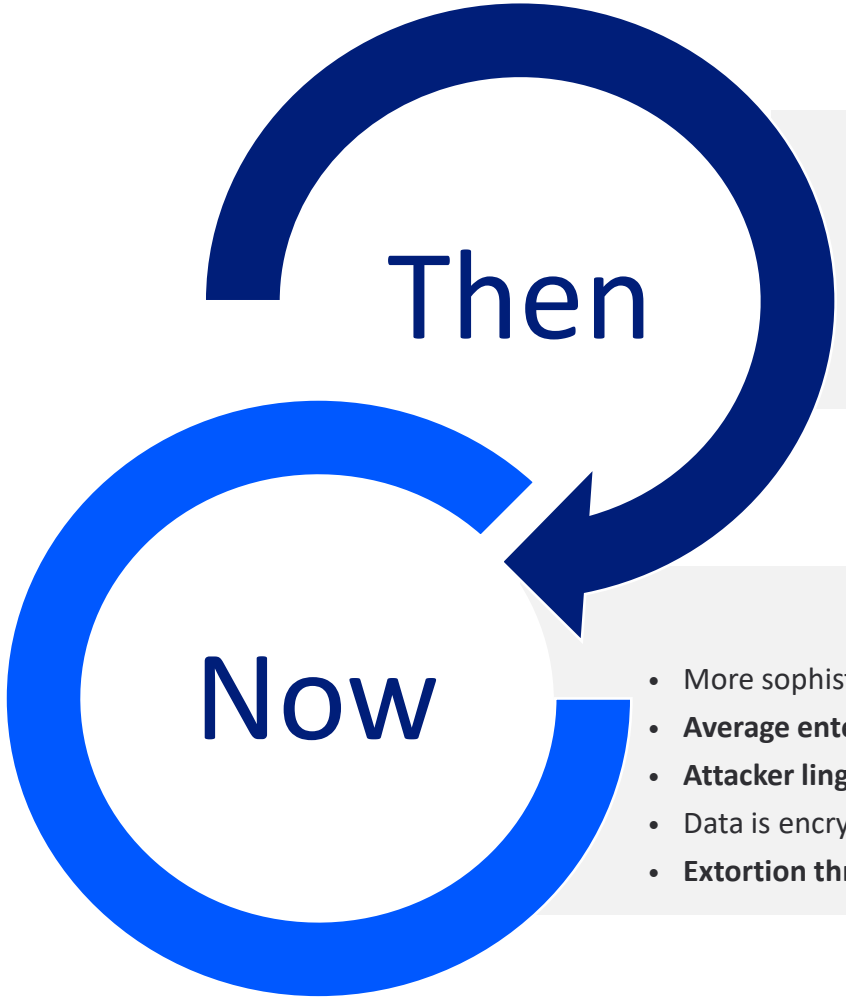
See end disclosures.

How Secure Is My Password?

Global ransomware attack volume increased by 151% LAST YEAR. How has ransomware evolved in the past couple of years?

Human-operated ransomware

Ransomware threat actors are getting more sophisticated. It's an old threat, with new tactics.



- Targeted individuals and smaller organizations
- Average enterprise ransom by end of 2018 - $7K
- Individual computers and/or systems infected
- Data encrypted (locked) until ransom paid

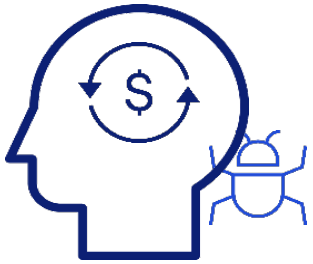
- More sophisticated—**targets large organizations**
- **Average enterprise ransom - $111K; larger enterprises $1MM+**
- **Attacker lingers in network searching for "crown jewels"**
- Data is encrypted AND exfiltrated (removed)
- **Extortion threats to disclose confidential information to public**

Sources: https://www.zdnet.com/article/ransomware-the-cost-of-rescuing-your-files-is-going-up-as-attackers-get-more-sophisticated/; https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

How does a ransomware attack WORK?

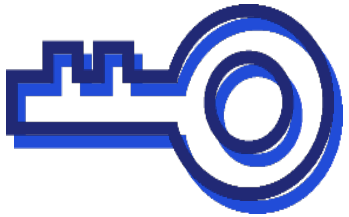
Anatomy of a ransomware attack

Adversaries use ransomware to monetize network access.



1 **Threat actor** infiltrates company by exploiting poor security practices

- Unpatched vulnerability
- Running unsupported software
- Unsecured accounts
- System misconfiguration
- Phishing, social engineering



2 **Threat actor** gains unauthorized, privileged access to network and identifies vulnerable systems to target

3 **Threat actor** encrypts identified target; demands payment in exchange to deliver access

- **Double extortion by exfiltrating data and threatening to go public**

Real-life ransom note

Maze support system

What's just happened?

If you see this page it means you have a vulnerability in your system.
This vulnerability was used to modify your valuable data in a way, which temporary disallow further usage of it.
Please upload DECRYPT-FILES.txt using the form below and start recovering your data.
If this file is recognized by our parser, you will be successfully authorized and provided with further instructions.

Please upload DECRYPT-FILES.txt

Browse... No file selected.

Guarantees?

We can recover your files, as our software is carefully designed to keep the integrity and safety of your files.

Don't be afraid and start recovering!

Antivirus corporations?

If you are waiting for a free solution to come, we must disappoint you.

Our cryptography scheme is military grade. It will require decades to crack.

Start working with us and get your files back.

Price?

We understand that the customer cannot always pay the fee. We have discounts and price can be negotiated.

Source: https://news.sophos.com/en-us/2020/05/12/maze-ransomware-1-year-counting/

How do organizations get infected?

There are 3 ways the vast majority of organizations are compromised with ransomware attacks:

- Phishing attacks – users click on phishing emails and provide information or unknowingly install malware that allows the attacker into the environment.
- Exposed Remote Desktop Protocol (RDP) instances, which attackers brute force and/or purchase credentials on the Dark Web for.
- Insecurely configured Virtual Private Networks (VPNs) not utilizing best practices, such as Multifactor Authentication (MFA).

“Ask any security professional…

…and they will tell you that the weakest link in the security chain is the human who accepts a person or scenario at face value.”

***Linda Criddle**, Founder of iLookBothWays.com*

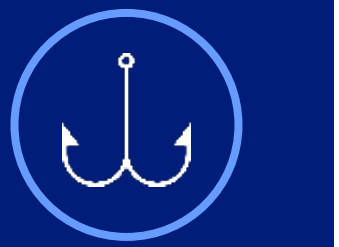
What is Social Engineering?

Name
Role Or Position
How long have you been an ACH participant?
Your Social Media Footprint

What is social engineering?

Social engineering is the use of deception to manipulate individuals into divulging sensitive information that may be used for fraudulent purposes. A combination of these tactics may be used.

The ultimate goal of these tactics is to induce individuals to reveal sensitive information for the attacker's personal gain.



Phishing
(vishing, phishing)

Deceptive emails, phone calls, SMS text messages

Pretexting

A fabricated pretext or scenario

Baiting

The promise of goods to entice victims

Quid Pro Quo

The promise of services to entice victims

Tailgating

Following closely behind an employee with the correct credentials

Source: tripwire: https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

Be on the alert to spot phishing

Things to look out for:

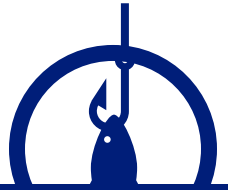
- “Phishy” company emails
- Requests for credentials or account information

Focused twists:

- “Spear phishing”
- Executives = “whales”
- Adding a telephone component

1. Phishing email

A fraudulent email is sent masquerading as legitimate.



2. Bait taken

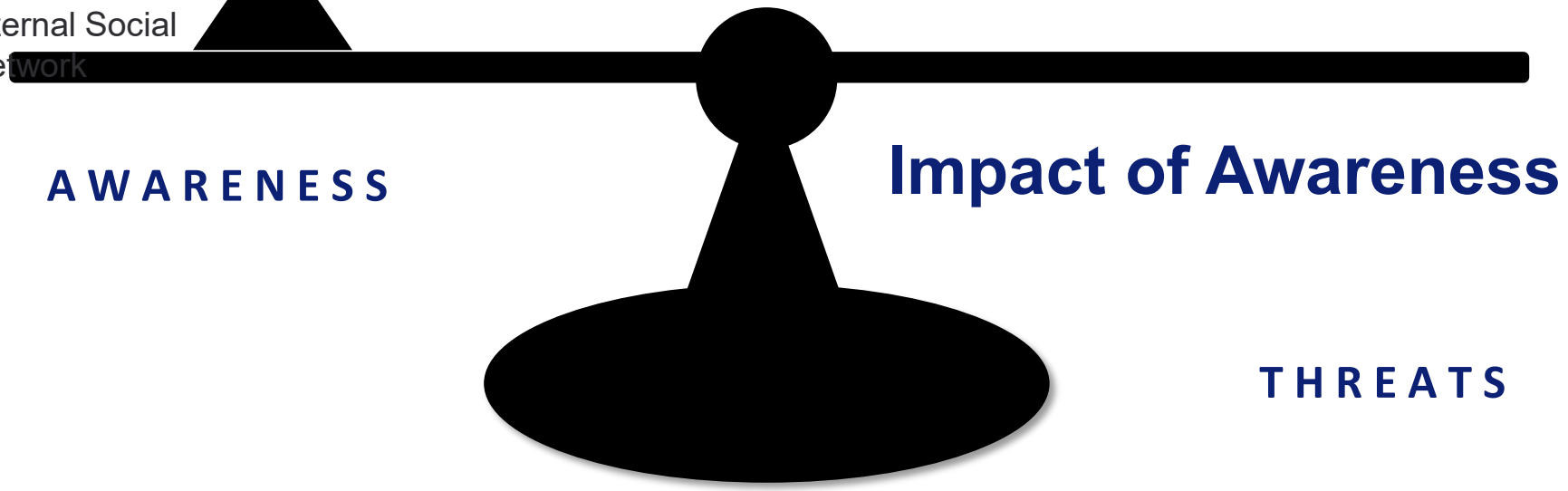
Phisher tries to acquire victim’s login credentials or account information.

3. Credentials stolen

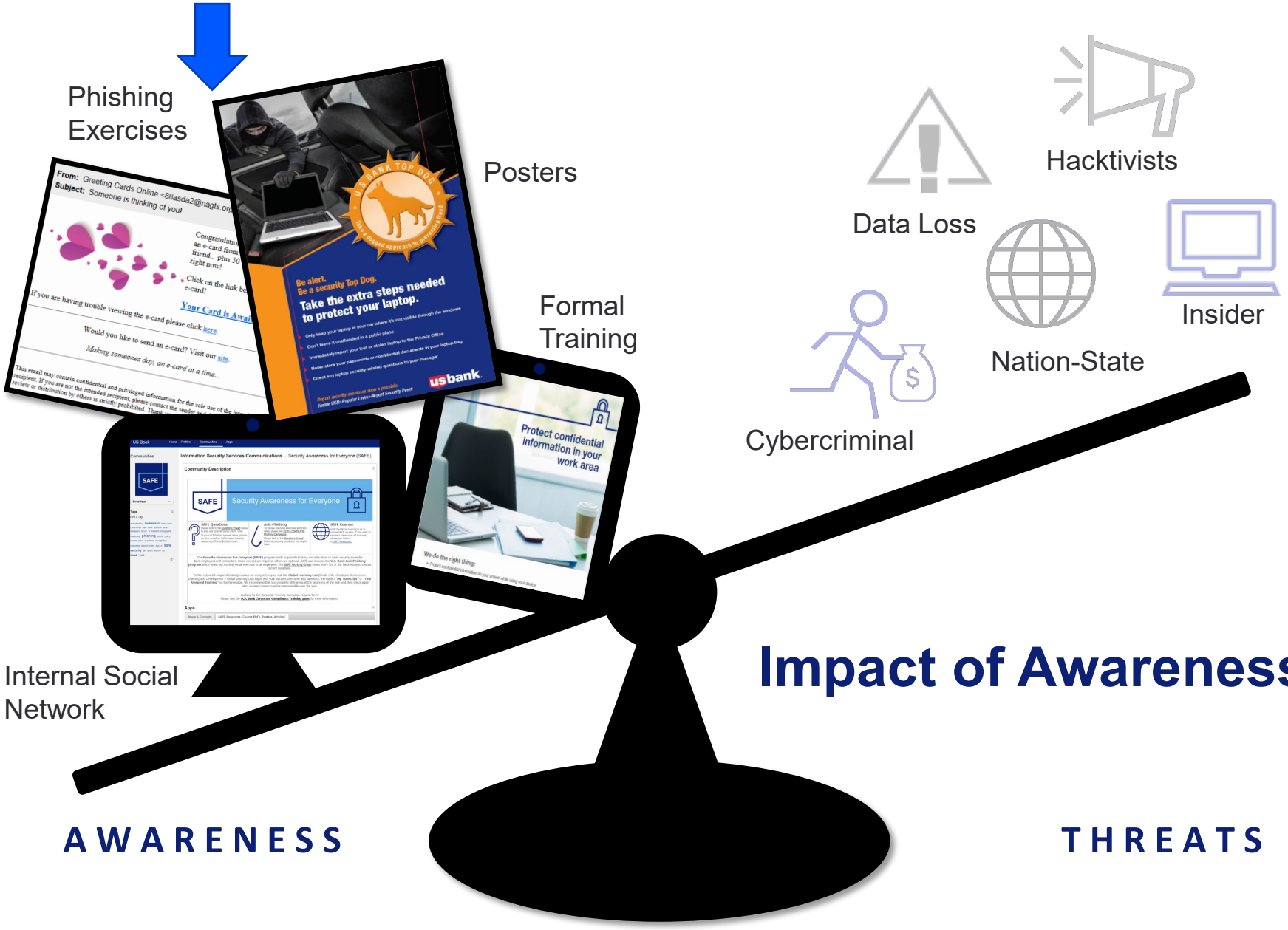
If successful, the phisher can use login credentials or account information for their purposes.

What can we do to PROTECT **ACH** participants from the threats of social engineering and ransomware?

Impact of Awareness



Impact of Awareness



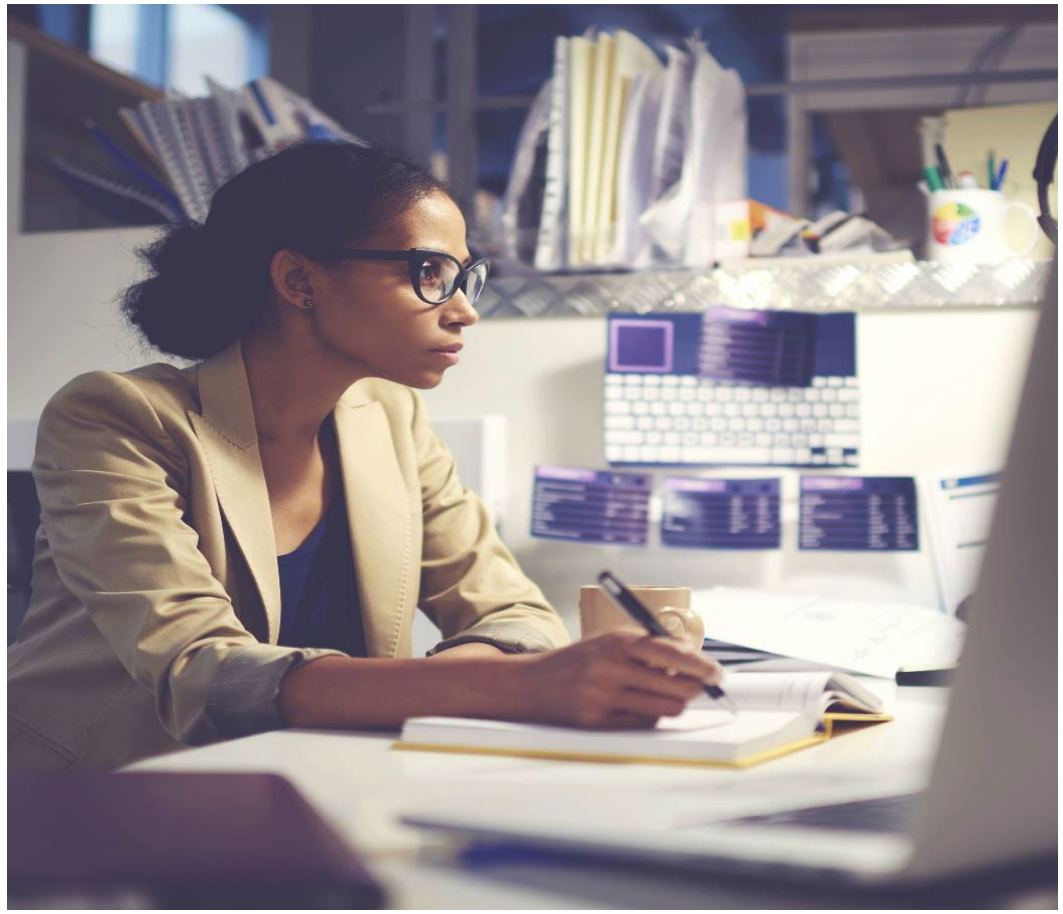
Anti-phishing programs

Phishing exercises help educate and train employees on how to recognize and respond to phishing threats.

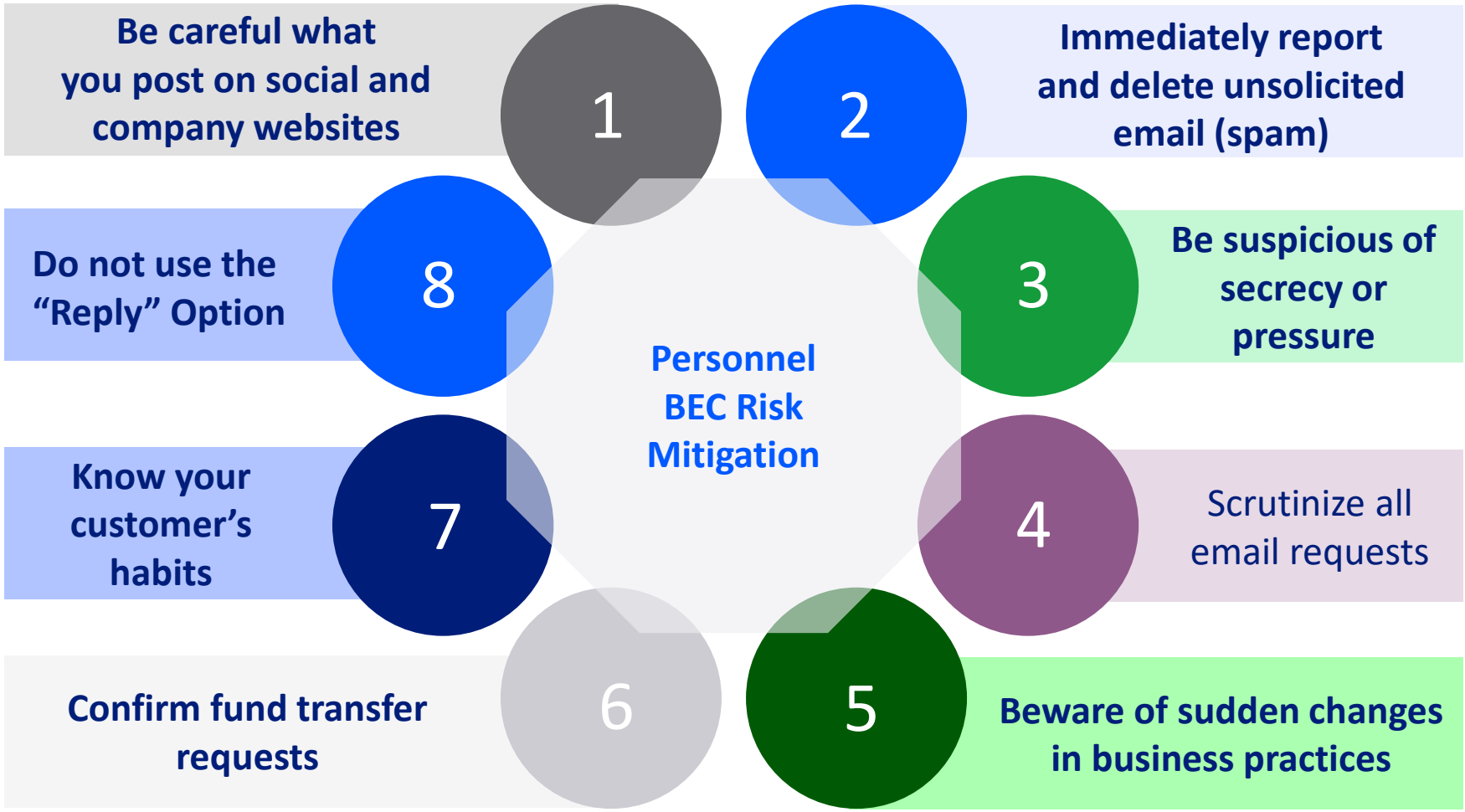
Educate Employees on how to spot phishing emails.

Encourage Correct Behavior to report suspicious emails.

Create Awareness around phishing and information security risks.



Mitigate risk with personnel policies



Sources: 2017 FBI PSA: https://www.ic3.gov/media/2017/170504.aspx;
U.S. Bank Financial IQ – Minimize Risk: https://financialiq.usbank.com/index/improve-your-operations/minimize-risk.html

Protect your business from ransomware

Stay Current
Patch your software and operating systems

Create redundancy
Create file, system and data **back-ups**

Train
Teach employees to recognize **spear phishing** and to **browse safely**

Decide
Executives must decide before attack to pay or not pay; **FBI suggests to not pay**

To pay or not to pay

Best Practice: companies develop a ransomware position prior to an incident.

	PAY the ransom	DON'T pay the ransom
PROS	• Legitimate option if backups were compromised somehow • May protect our customers and reputation if compromised data causes substantial harm • Potentially easier recovery (not guaranteed)	• Aligned with official FBI stance • May discourage criminal enterprises • May deter repeat attacks
CONS	• Recovery of encrypted data not guaranteed • Become a future target; larger ransoms • Emboldens criminals to continue and funds future activity • Potential enforcement action under regulatory advisory; severity lessoned if due diligence is followed[1]	• May take longer time to recover • If backups are compromised, potential for greater harm to customers, operations and reputation

[1]U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments"

To avoid cyberattacks

Cybersecurity & Infrastructure Security Agency (CISA), the Federal Bureau of Investigations and National Security Agency encourage the cybersecurity community to adopt a *heightened state of awareness* and to conduct *proactive threat hunting.*

1	**Be prepared.** Confirm reporting processes and minimize personnel gaps in IT/OT security coverage. Create, maintain, and exercise a cyber incident response plan, resilience plan, and continuity of operations plan so that critical functions and operations can be kept running if technology systems are disrupted or need to be taken offline.
2	**Enhance your organization's cyber posture.** Follow best practices for identity and access management, protective controls and architecture, and vulnerability and configuration management.
3	**Increase organizational vigilance.** Stay current on reporting on this threat. **Subscribe** to CISA's **mailing list and feeds** to receive notifications when CISA releases information about a security topic or threat.

Source: 2022 – Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure. See end disclosures.

Key takeaways

- Ransomware has grown into a multibillion-dollar industry
- Cyber criminals are often sanctioned by regimes outside of U.S. law enforcement's reach (Russia, North Korea, Iran, et.al.)
- Executives must develop a ransomware position **prior** to an incident

"We certainly view it as one of the most serious cybercriminal problems we face right now."

Herbert Stapleton
Cyber Division Section Chief, FBI

Lay groundwork for a more secure future

Engage U.S. Bank security specialists

Utilize available resources

Visit our Financial IQ site

Discuss best practices and ways U.S. Bank can assist

U.S. Bank Resources	Partnerships and Information Sharing	Publications
• "Protect Yourself Online" Course • Financial IQ Articles • Online Security Tips	• Global Cyber Alliance • National Council of Information Sharing & Analysis Centers • InfraGard • Staysafeonline.org	• Ransomware Best Practices • Stop Ransomware Toolkit • 2021 Verizon Data Breach Investigations Report

Above links active in presentation mode. Addresses available in the speaker notes.

Closing thoughts?

Cybersecurity disclaimers

These websites, and the services provided, are under the exclusive control of the respective third-party provider. These links are provided as a courtesy and do not imply, suggest, or constitute any sponsorship, endorsement, or approval of any third party or any affiliation with any such third party. Further, we make no warranties or representations whatsoever with regard to any third-party website, merchandise, or service, and we are not responsible or liable to you for any damages, losses, or injuries of any kind arising out of your use of any third-party website.

This information has been obtained from sources believed to be reliable, but we cannot guarantee its accuracy or completeness.

usbank®