A Step Ahead:

Understanding Cyber Security Trends and Safeguarding Your Business

Presenters:

EVP Tim Held, Chief Information Security Officer

AVP Charles L. Bank, Manager of Information Security

March 8, 2022

Presentation Overview

- Speaker Introductions
- ISS at a Glace
- Navigating the Cyber Landscape
- Spear Phishing Attack
- Prevention strategies and response
- Q&A

Charles Banks – Manager, Security Briefing Center Ops

Assistant Vice President, U.S. Bank

Charles Banks is a member of Information Security Services at U.S. Bank, and as an Assistant-Vice President, manages **Security Briefing Center Operations**. He is responsible for both the day-to-day operations at these state-of-the-art security facilities, as well as the information and cyber security awareness education delivered in these briefing centers.

With a focus on internal and external constituent engagements that raise general user awareness of socially engineered and digitally delivered cyber threats, his team's mission is to change, or prevent, behaviors that result in digitally compromised, or lost data. His team hosts both virtual and on-site events in the **Cyber Security Fusion & Executive Briefing Centers** for both internal business lines and external clients of U.S. Bank.

Charles' team also cultivates and coordinates proactive community outreach and cybersecurity education partnerships. In addition to educating local communities about digital threats, and responsible, security minded cyber practices, the **Security Briefing Center Operations** team is a **STEM & STEAM** education driver. With the creation and delivery of content to regional elementary education, high school, and secondary education students, the team's goals are to develop the next generation of a diverse cybersecurity workforce and to highlight how U.S. Bank should be the employer of choice for careers in cyber security.

Charles has been with U.S. Bank for 13 years with a background in training, training design, communications, and cyber security awareness delivery. He joined the Cyber & Information Security team in 2015.

Tim Held – Chief Information Security Officer

Executive Vice President, U.S. Bank

Chief Information Security Officer, Tim Held, is responsible for leading a multidisciplinary information security team operating across the United States, Europe, and Asia, focusing on prevention, detection, and response. Among other things, Mr. Held is responsible for the Bank's cybersecurity architecture, engineering, security operations, incident response, data loss prevention, vulnerability assessment services, online fraud detection, security monitoring, insider threat, and cyber threat intelligence.

Mr. Held has over **20-years of information technology experience**, with 18 of those years focused on information security and risk management. His diverse background blends rich leadership experience with deep technical acumen.

Mr. Held currently sits on **seven Board of Director committees**;

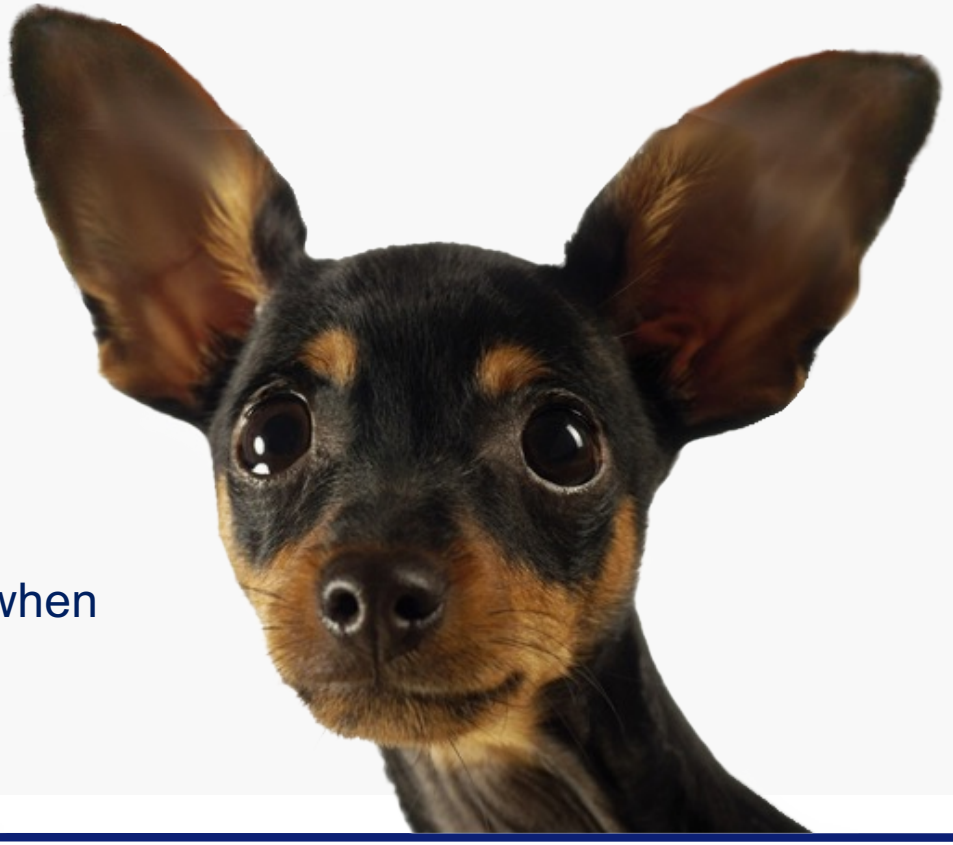
- The Financial Services Information Sharing and Analysis Center (FS-ISAC)
- Kohls Security Advisory
- CyberOhio Security Advisory
- National Technology Security Coalition (NTSC),
- Evanta Governing Board
- American Transaction Processors Coalition (ATPC) Cyber Council
- Fairfield Youth Basketball League

Navigating the Cyber Risk Landscape

Our disclaimer

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

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



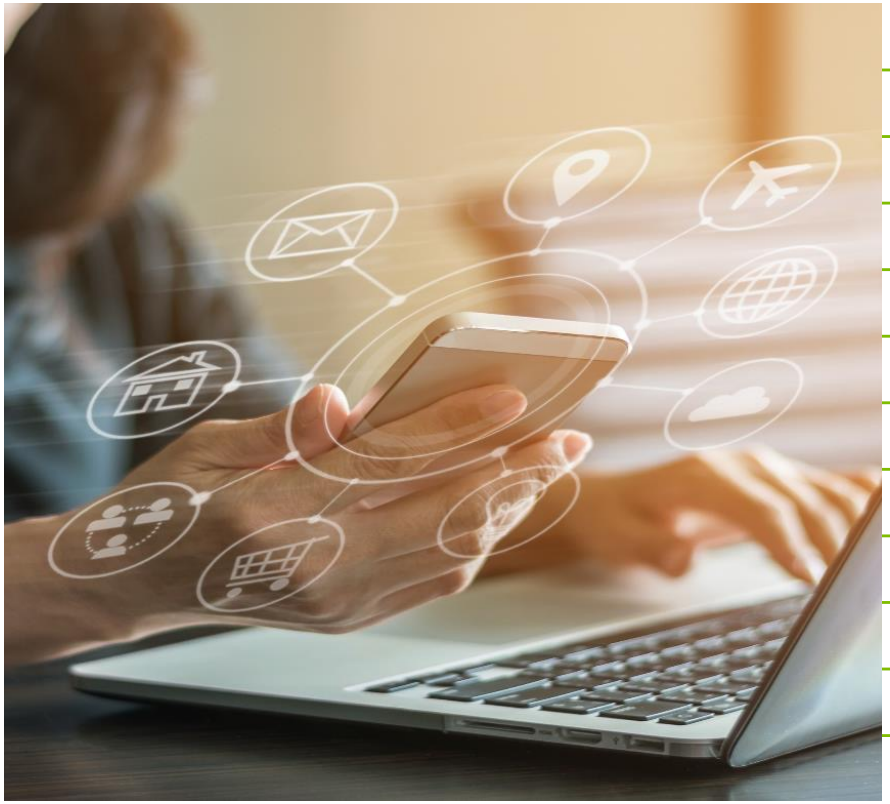
Cyber-physical “Internet of Things”

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

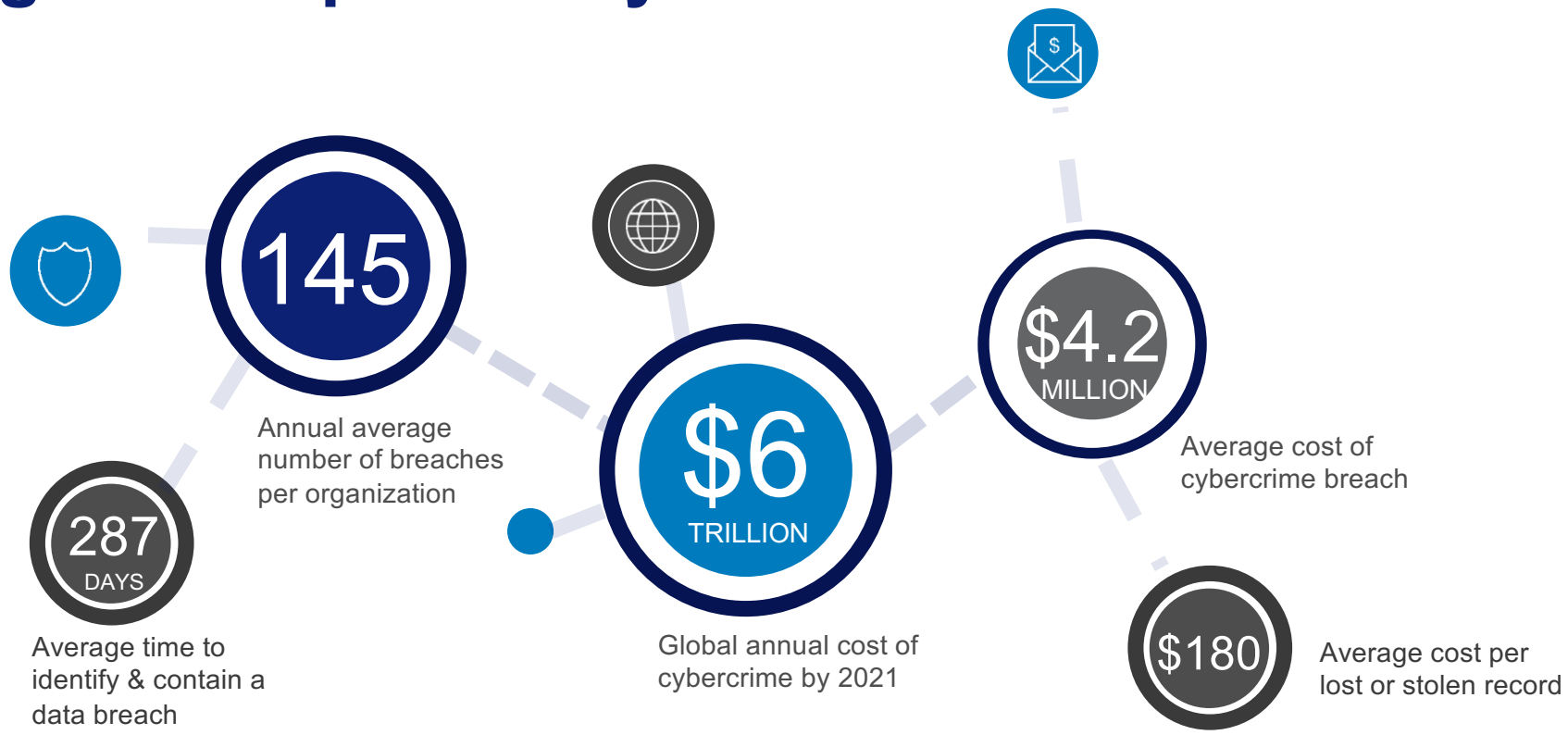
100K Teams users send messages

65K Instagram users share photos

856 Users host Zoom webinars

Source: July 2021, Data Never Sleeps 9.0.

The global impact of cybercrime

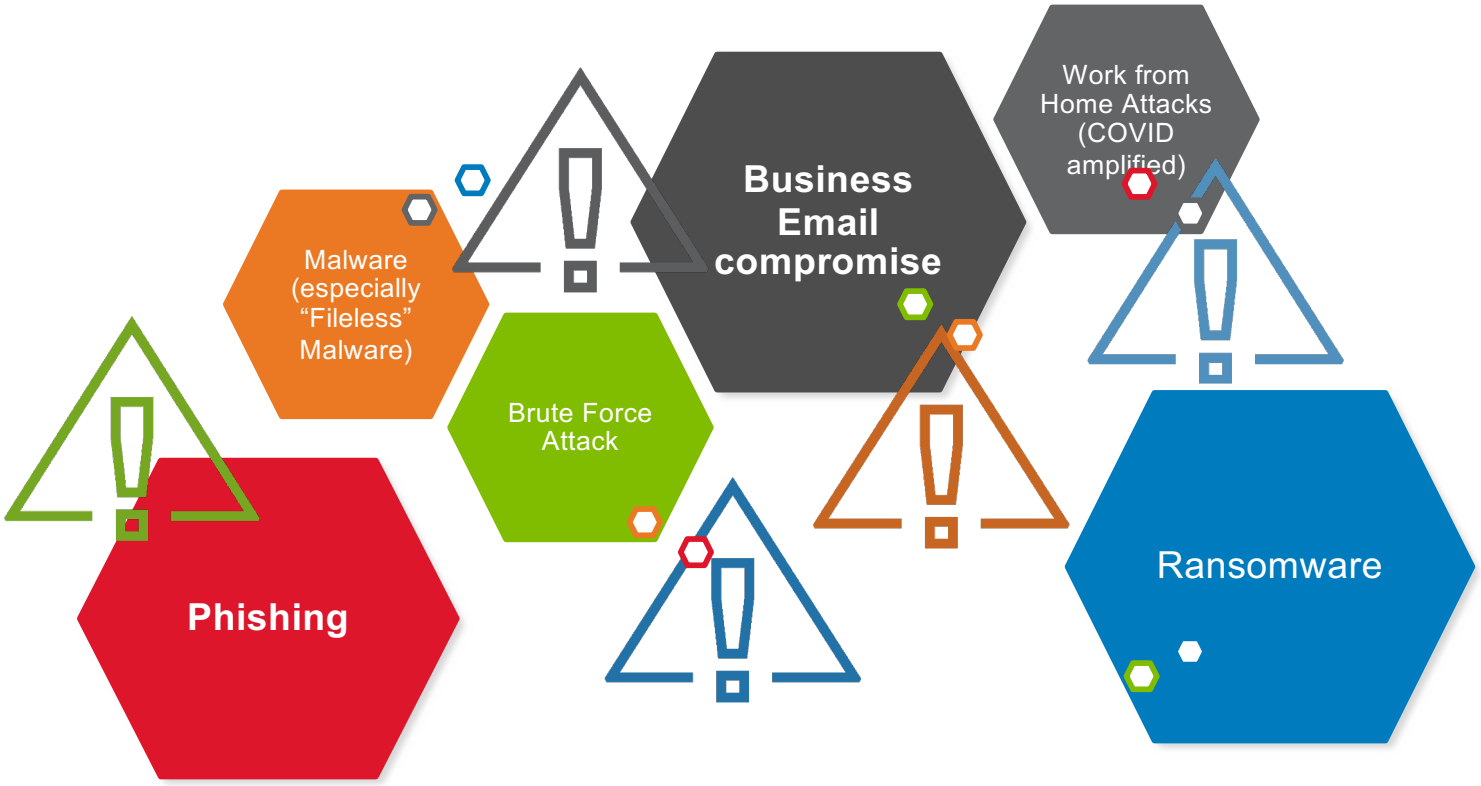


Source: Accenture - https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50
The Herjavec Group - https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Rapidly evolving threats — Current Landscape

Theft + Disruption + Destruction

Top cybersecurity threats in 2021



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

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.

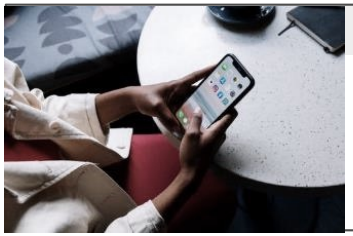
Cybersecurity Strategies

The World of Information Security

Technology trends and environmental factors influencing how we approach our work

ATTACK COMPLEXITY

- Ransomware evolves with collaboration, extortion, bigger targets and bigger ransoms
- Denial of Service extortion



TRANSFORMATION

- Security decentralization
- Customer-facing staff shifting to engagements with external ecosystems to support client preferences

WORKFORCE

- New forms of digital computing require new skill sets
- Demand outpaces availability

THIRD-PARTY

- Geopolitical concerns of shift to non-U.S. cybersecurity firms
- Increase in supply chain compromise attacks

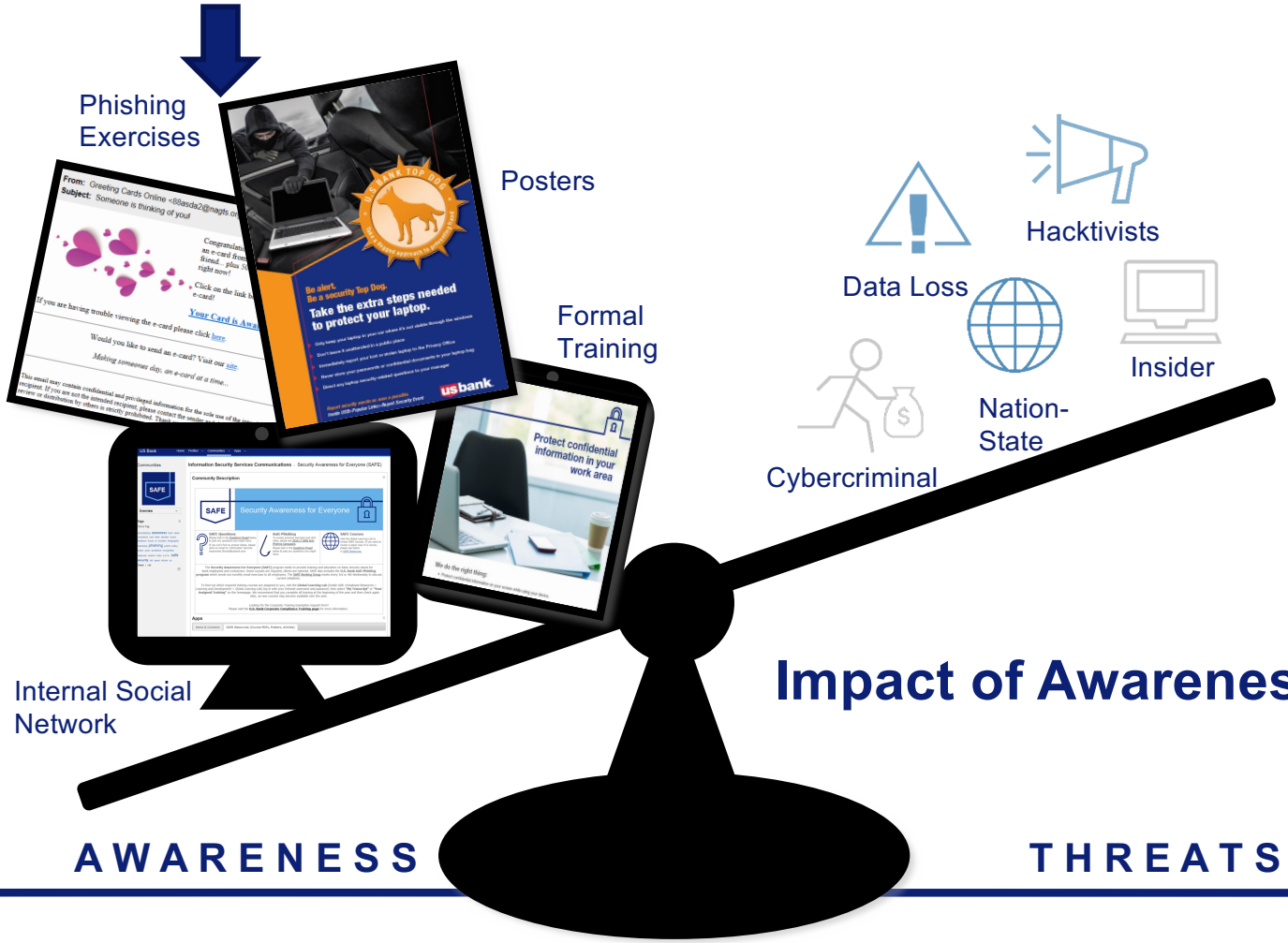
CLIMATE

- Climate-driven disruptions impacting availability

COVID-19 PANDEMIC

- Increase in cyber crime as personal income method
- Increased insider threats with work from home


Phishing Exercises
Posters
Formal Training
Internal Social Network
Hacktivists
Data Loss
Insider
Nation-State
Cybercriminal
AWARENESS
Impact of Awareness
THREATS


Phishing Exercises
Posters
Formal Training
Internal Social Network
Hacktivists
Data Loss
Insider
Nation-State
Cybercriminal
Impact of Awareness
AWARENESS
THREATS


The largest areas of Cyber Security compromise are caused by a lack of security minded HUMAN BEHAVIORS.
Which Cyber Security exploit takes advantage of this the most?

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

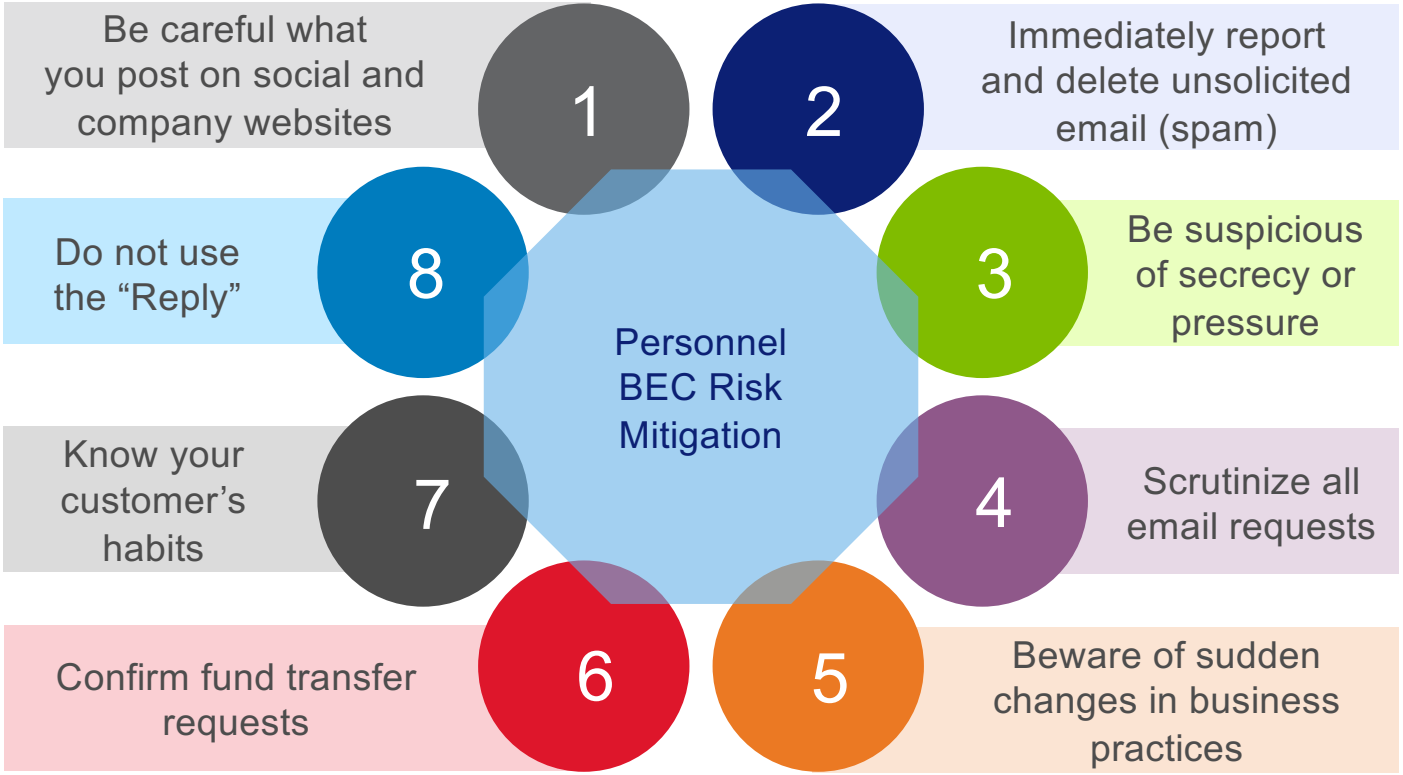
If successful, the phisher can use login credentials or account information for their purposes.

The “Executive Masquerade”

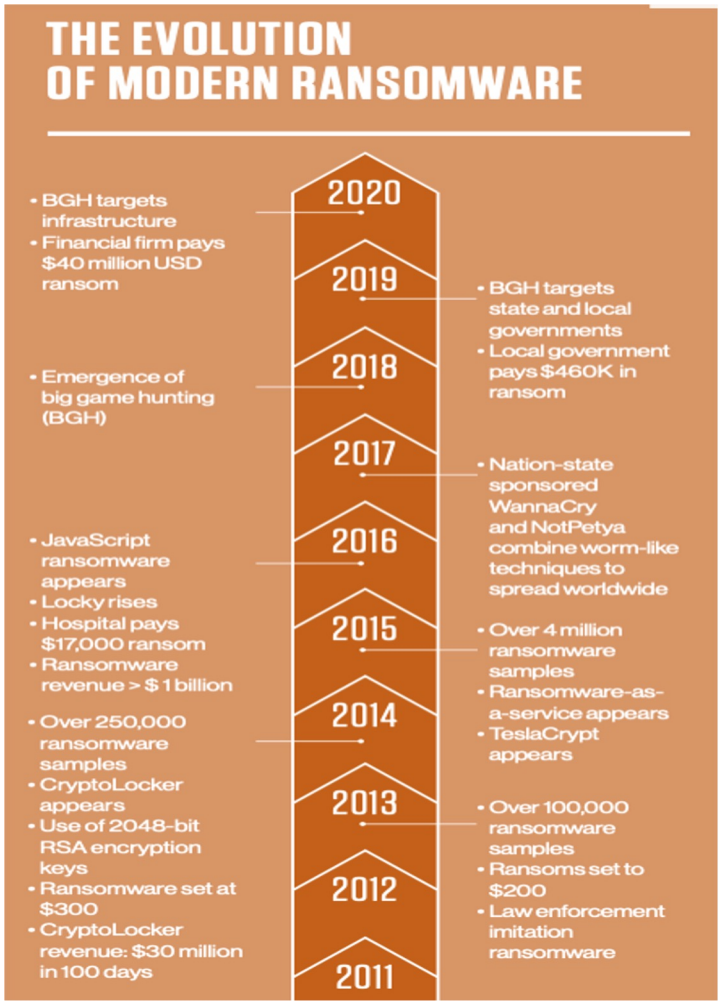
Spoof	Masquerade	Funds Transferred
• The email accounts of high-level business executives (Chief Financial Officer, Chief Technology Officer, etc.) are compromised. • The account may be spoofed or hacked.	• A request for a wire transfer from the spoofed account is made to a second employee responsible for processing requests. • In some instances, the request is sent directly to the financial institution with instructions to urgently send funds to bank “X” for reason “Y.”	• The victimized employee processes the fraudulent request. • The fraudster receives the wire transfer.

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

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



Evolution of Ransomware

- **Ransomware** has been around since 1989, but the current evolution of commoditized ransomware, known as “Big Game Hunting” emerged in 2018.

- **Big Game Hunting** (BGH) is conducted by organized groups partner with each other to gain access to a company’s environment, expand their foothold into the environment, deploy the ransomware, then negotiate and collect payment from the victim organizations.

Image Source: https://www.crowdstrike.com/wp-content/uploads/2021/01/history-of-ransomware-timeline.png/

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**

Questions?

Thank You

Disclaimer

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.