Protecting Yourself in Today's Cybersecurity & Fraud Landscape

County Treasures Association of Ohio Spring Conference

April 26, 2023

Presenter: **Amber Buening**, SVP, Security Outreach Director

Huntington
Welcome.®

Public

Investment, Insurance, and Non-Deposit Trust products are:
NOT A DEPOSIT • NOT FDIC INSURED • NOT GUARANTEED BY THE BANK • NOT INSURED BY ANY FEDERAL GOVERNMENT AGENCY • MAY LOSE VALUE

The Huntington National Bank is an Equal Housing Lender and Member FDIC.

This presentation is intended for educational purposes only and does not replace independent professional judgment. Statements of fact and opinions expressed are those of the individual participants and, unless expressly stated to the contrary, are not the opinion or position of Huntington National Bank or its affiliates. Huntington does not endorse or approve, and assumes no responsibility for, the content, accuracy of completeness of the information presented. Professional assistance must be consulted prior to acting on any of the content in this presentation.

Agenda

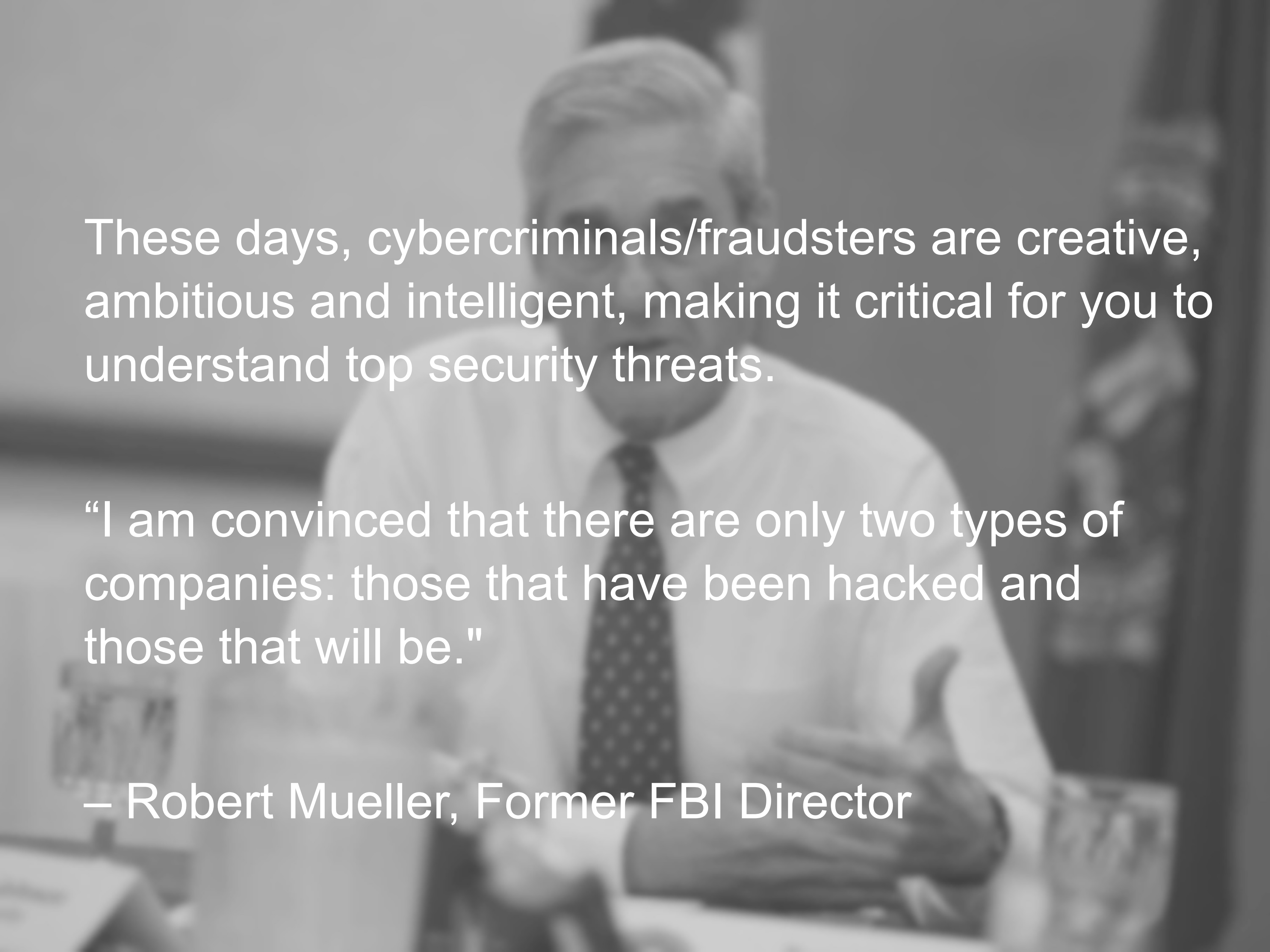
- Current Cybersecurity & Fraud Landscape
- Social Engineering & Fraud
- Best Practices
- Q&A
- Additional Resources

Huntington
Welcome.

The Cybersecurity & Fraud Landscape

Huntington

Welcome.®



These days, cybercriminals/fraudsters are creative, ambitious and intelligent, making it critical for you to understand top security threats.

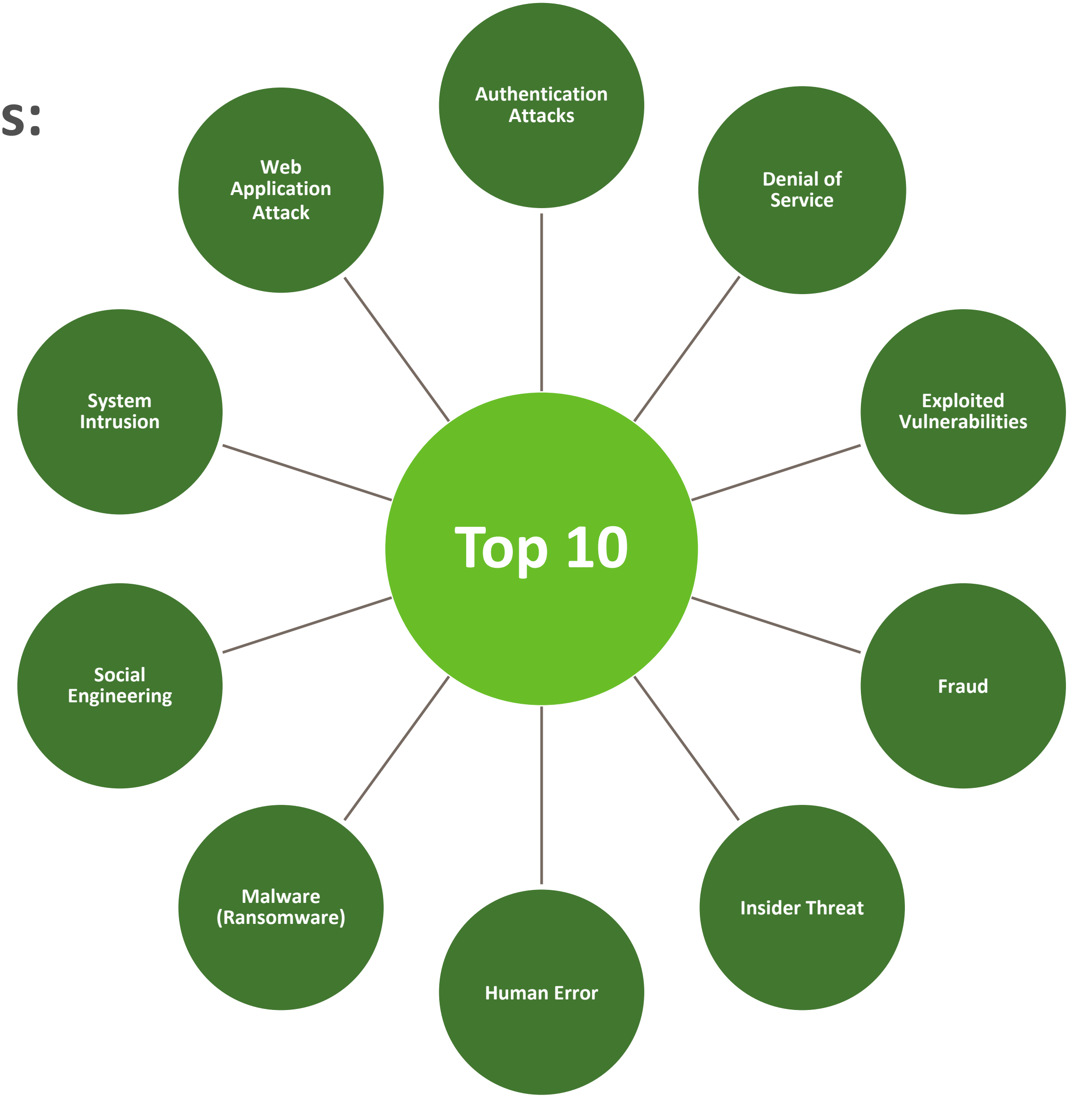
“I am convinced that there are only two types of companies: those that have been hacked and those that will be."

– Robert Mueller, Former FBI Director

Top Security Threats

Common Denominators:

Lack of cybersecurity practices and the ‘human element’ are at the root of most security threats in an increasingly digitized world.



Sources: Verizon 2022 Data Breach Investigations Report [https://www.verizon.com/business/resources/reports/dbir/]; Splunk Top 50 Security Threats [https://www.splunk.com].

Cybercrime on the Rise

2022 FBI IC3 Report

Total ↑ 800,944 complaints, exceeding $10.3 billion in losses

- **Phishing** ↑ 300,497 complaints, $52.1 million in losses
- **BEC** ↑ $2.7 billion in losses
- **Investment Scams** ↑ $3.31 billion in losses, *127% increase from 2021*

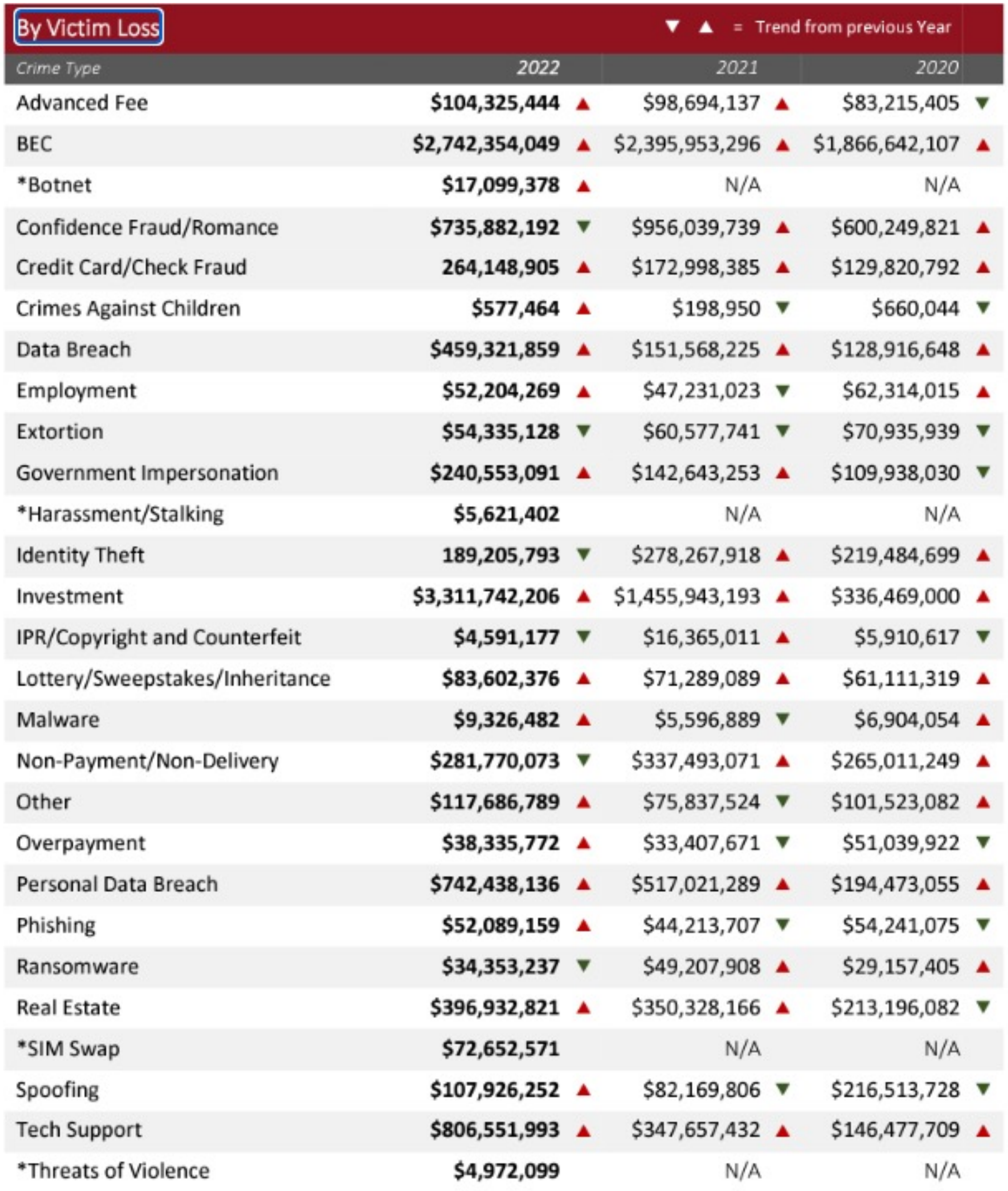
  Within those complaints, cryptocurrency investment fraud rose from $907 million in 2021 to $2.57 billion in 2022, an increase of 183%.

- **Ransomware** ↑$34.3 million in losses
- **Elder Fraud** ↑$3.1 billion in losses from victims over the age of 60

Sources: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Cybercrime on the Rise

FBI IC3 Complaint Loss Comparison (2020-2023)



By Victim Loss

▼ ▲ = Trend from previous Year

Crime Type	2022		2021		2020	
Advanced Fee	**$104,325,444**	▲	$98,694,137	▲	$83,215,405	▼
BEC	**$2,742,354,049**	▲	$2,395,953,296	▲	$1,866,642,107	▲
*Botnet	**$17,099,378**	▲	N/A		N/A	
Confidence Fraud/Romance	**$735,882,192**	▼	$956,039,739	▲	$600,249,821	▲
Credit Card/Check Fraud	**264,148,905**	▲	$172,998,385	▲	$129,820,792	▲
Crimes Against Children	**$577,464**	▲	$198,950	▼	$660,044	▼
Data Breach	**$459,321,859**	▲	$151,568,225	▲	$128,916,648	▲
Employment	**$52,204,269**	▲	$47,231,023	▼	$62,314,015	▲
Extortion	**$54,335,128**	▼	$60,577,741	▼	$70,935,939	▼
Government Impersonation	**$240,553,091**	▲	$142,643,253	▲	$109,938,030	▼
*Harassment/Stalking	**$5,621,402**		N/A		N/A	
Identity Theft	**189,205,793**	▼	$278,267,918	▲	$219,484,699	▲
Investment	**$3,311,742,206**	▲	$1,455,943,193	▲	$336,469,000	▲
IPR/Copyright and Counterfeit	**$4,591,177**	▼	$16,365,011	▲	$5,910,617	▼
Lottery/Sweepstakes/Inheritance	**$83,602,376**	▲	$71,289,089	▲	$61,111,319	▲
Malware	**$9,326,482**	▲	$5,596,889	▼	$6,904,054	▲
Non-Payment/Non-Delivery	**$281,770,073**	▼	$337,493,071	▲	$265,011,249	▲
Other	**$117,686,789**	▲	$75,837,524	▼	$101,523,082	▲
Overpayment	**$38,335,772**	▲	$33,407,671	▼	$51,039,922	▼
Personal Data Breach	**$742,438,136**	▲	$517,021,289	▲	$194,473,055	▲
Phishing	**$52,089,159**	▲	$44,213,707	▼	$54,241,075	▼
Ransomware	**$34,353,237**	▼	$49,207,908	▲	$29,157,405	▲
Real Estate	**$396,932,821**	▲	$350,328,166	▲	$213,196,082	▼
*SIM Swap	**$72,652,571**		N/A		N/A	
Spoofing	**$107,926,252**	▲	$82,169,806	▼	$216,513,728	▼
Tech Support	**$806,551,993**	▲	$347,657,432	▲	$146,477,709	▲
*Threats of Violence	**$4,972,099**		N/A		N/A	

Sources: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Impacts of Cyber Crimes

- **Confidence & Trust:** Companies might recover financially from a data breach or security incident, but **reputational impacts** could persist. For individuals, trust in their providers or own ability can be lost.

- **Challenging Recovery or No Recovery:** Depending on a company's size financial, technical and security posture, recovery may not be feasible. This applies to individuals.

Sources: IBM Cost of a Data Breach Report 2021 [https://www.ibm.com/security/data-breach];
Duo Decipher News [https://duo.com/decipher/cisa-north-korea-backed-actors-using-maui-ransomware].

Social Engineering & Fraud

Huntington
Welcome.®

Understanding BEC

Business Email Compromise (BEC) is one of the most financially damaging online crimes.

- Cybercriminals exploit our reliance on email to conduct business — both personally and professionally – by **spoofing an email address** to send fraudulent emails.
- Cybercriminals convince an email recipient that a message is coming from a legitimate and **trusted** source.
- Messages often request the recipient to send funds through wire transfers, gift cards, Zelle, or other online person to person payment platforms.
- Typical results of BEC are disclosure of sensitive and/or personal information or movement of funds.

BEC Case Study: Invoicing, Wire Fraud

Source: https://vimeo.com/328296038?embedded=true&source=vimeo_logo&owner=23214550

Criminal/Fraudster Tactics

While attackers have become more sophisticated in their tactics (ex. target development), here are some common tactics/red flags:

- Portraying a sense of urgency, especially during a crisis or insisting on confidentiality
- Sending messages at inopportune times such as at close of business, or during high customer volume
- Changing email addresses, removing recipients from an email chain, or changing the reply to email address
- Containing poor formatting, unusual tone, and uncommon misspellings
- Refusing to communicate in-person or verbally
- Requesting to move money to a new account, personal account, subsidiary account, or an atypical destination
- Asking for unusual payment amounts, or payments without proper justification

Social Engineering

Social engineering attacks attempt to elicit sensitive information or influence the victim to perform an action.

- **Phishing:** The attacker sends fraudulent **emails** with the intent of luring a user to click a link or open a document.
- **Smishing:** The attacker uses a ***text message*** to attempt to gain money or information.
- **Vishing:** The attacker uses a ***phone call*** to attempt to gain money or information.
- **Whaling:** The attacker uses a ***form of phishing attack*** designed to socially engineer a very high-value target, such as a CEO.

Typical results of phishing, smishing, vishing, and whaling are system compromise (ex. malware) or credentials (ex. username).

Poll Question

Huntington

- **How confident are you in your ability to identify a phishing e-mail or a malicious link?**
  - Not Confident
  - Neutral
  - Confident
  - Very Confident

Public

Email Account Takeover

Often confused with BEC where an email appears to come from a trust source, in an email account takeover (EAC) attack the message does come from a trusted source by compromising, gaining access to legitimate email mailboxes.

Common tactics include phishing and malware but can include:

- **Baiting:** The attacker exploits the victims' curiosity. [Physical] storage media (cd or USB) containing malware in strategic locations providing the attacker remote network access.
- **Pretexting:** The attacker impersonates someone familiar to or of interest to the victim then creates an opportunity to engage the victim to obtain sensitive information.
- **Quid Pro Quo:** The attacker offers something with the expectation of obtaining some advantage or benefit, such as initial access or **credentials**, as a result.

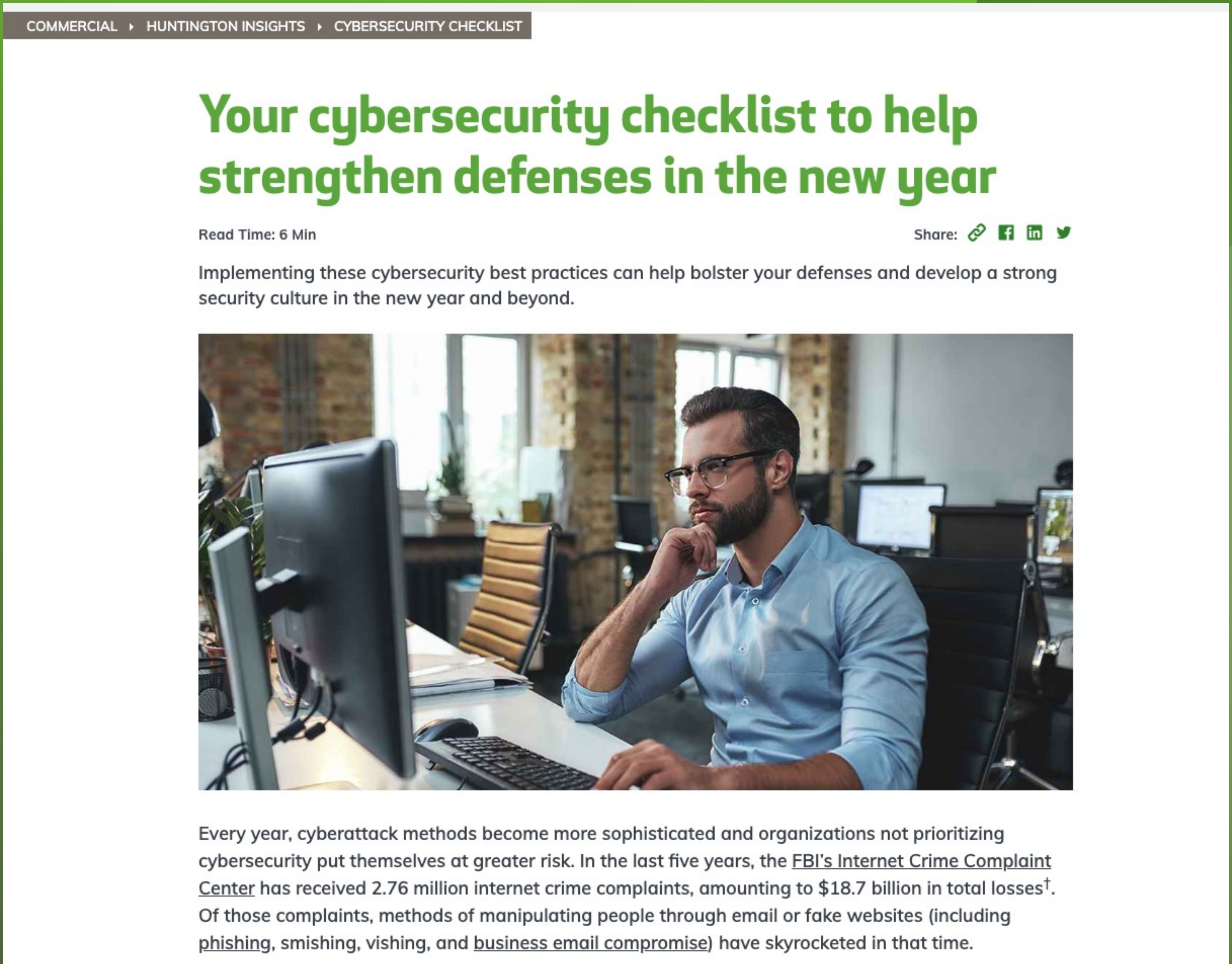
Source: Flashpoint October 2022 Intelligence Report – Social Engineering Tactics.

Best Practices: Enable Security Culture by Changing Our Behaviors

Huntington
Welcome.®

What is Security Culture?

Security culture is your (or your company's) attitude, perceptions and beliefs about cybersecurity. It is driven by shifting behavior through best practices.



Your cybersecurity checklist to help strengthen defenses in the new year

Read Time: 6 Min

Implementing these cybersecurity best practices can help bolster your defenses and develop a strong security culture in the new year and beyond.

Every year, cyberattack methods become more sophisticated and organizations not prioritizing cybersecurity put themselves at greater risk. In the last five years, the FBI's Internet Crime Complaint Center has received 2.76 million internet crime complaints, amounting to $18.7 billion in total losses†. Of those complaints, methods of manipulating people through email or fake websites (including phishing, smishing, vishing, and business email compromise) have skyrocketed in that time.

Source: https://www.huntington.com/Commercial/insights/cybersecurity/annual-cybersecurity-checklist

Source: https://www.huntington.com/Commercial/insights/cybersecurity/annual-cybersecurity-checklist

Protecting Against BEC Attacks

- Follow established processes and protocols for remittance processing
- Understand your responsibilities and liabilities
- Treat emails with caution, avoid clicking suspicious links and report them promptly
- Never call phone numbers or email addresses sent in emails or texts
- Verify that the customer's contact information has not recently changed
- Act quickly in the event of an incident and promptly report it to the appropriate team or organization
- Avoid using paper checks by using ACH or other electronic payment methods when possible
- Accept electronic deposits or utilize remote deposit capture, safeguard remotely deposited items and shred them once they clear
- Get a second opinion; if something feels off, it probably is

Security Best Practices

Between remote work and the internet of things, it's more important than ever to utilize these best practices professionally and personally:

- **Practice password hygiene:** strong passwords, password management
- **Use multi-factor authentication** (MFA) on online accounts
- **Don't click suspicious links**, report them
- **Encrypt & keep devices up-to-date** including software & apps
- **Be proactive** with cybersecurity awareness training
- **Identify and protect** sensitive information
- **Back up** important data
- **Control physical access** to computers and network components
- **Act quickly** in the event of an incident
- **Use access control**, such as role-based access control (RBAC)
- **Obtain &/or understand** your cyber insurance policy
- **Remote Work:** use a Virtual Private Network (VPN), secure your home router, separate work & personal devices

Develop or Deepen a Strong Security Culture

- Implement a year-round cybersecurity training program for employees.
- Plan regular communications to inform employees about common threats, such as phishing scams, and best practices for protecting against them.
- Remind employees about general cybersecurity hygiene.
- Set up multiple channels for employees to report suspicious behavior or cybersecurity incidents.
- Make sure employees can easily find contact information for your organization’s cybersecurity team.

Q&A

Huntington
Welcome.®

Additional Resources

- Cybersecurity & Infrastructure Security Agency: https://www.cisa.gov/publication/cisa-cybersecurity-awareness-program-toolkit
- National Cybersecurity Alliance: https://staysafeonline.org/resources/
- STOP. THINK. CONNECT. https://www.stopthinkconnect.org/
- Huntington: https://www.huntington.com/Privacy-Security
- Have I Been Pwned: https://haveibeenpwned.com/
- Identity Theft Resource Center: https://www.idtheftcenter.org/

Huntington
Welcome.

Thank you.