Cybersecurity & Emerging Threats

July 26, 2022

Ohio Treasurer of State Webinar

Presenter: Amber Buening

SVP, Security Outreach Director

Huntington
Welcome.®

Huntington
Welcome.®

Agenda

- Threats & Trends
- Examples
- Best Practices
- Q&A
- Additional Resources

Huntington
Welcome:

Threats & Trends

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

- Account Take Over

- Compromised Credentials/Systems

- Exploited Vulnerabilities

- Human Error

- Insider Threat

- Malware/Ransomware

- Social Engineering

- Web Application Attack

Cyber Crimes on the Rise

2021 Report
- **BEC** ↑
- **Ransomware** ↑

The 2021 FBI IC3 (Internet Crime Center) report shows a continued rise in BEC and Ransomware threats over the last three years.

Last 3 Year Complaint Loss Comparison

By Victim Loss		▼ ▲ = Trend from previous Year	
Crime Type	2021	2020	2019
Advanced Fee	$98,694,137 ▲	$83,215,405 ▼	$100,602,297 ▲
BEC/EAC	$2,395,953,296 ▲	$1,866,642,107 ▲	$1,776,549,688 ▲
Civil Matter	$85,049,939 ▲	$24,915,958 ▲	$20,242,867 ▲
Confidence Fraud/Romance	$956,039,739 ▲	$600,249,821 ▲	$475,014,032 ▲
Corporate Data Breach	$151,568,225 ▲	$128,916,648 ▲	$53,398,278 ▼
Credit Card Fraud	$172,998,385 ▲	$129,820,792 ▲	$111,491,163 ▲
Crimes Against Children	$198,950 ▼	$660,044 ▼	$975,311 ▲
Denial of Service/TDoS	$217,981 ▼	$512,127 ▼	$7,598,198 ▲
Employment	$47,231,023 ▼	$62,314,015 ▲	$42,618,705 ▼
Extortion	$60,577,741 ▼	$70,935,939 ▼	$107,498,956 ▲
Gambling	$1,940,237 ▼	$3,961,508 ▲	$1,458,118 ▲
Government Impersonation	$142,643.253 ▲	$109,938,030 ▼	$124,292,606 ▲
Health Care Related	$7,042,942 ▼	$29,042,515 ▲	$1,128,838 ▼
Identity Theft	$278,267,918 ▲	$219,484,699 ▲	$160,305,789 ▲
Investment	$1,455,943,193 ▲	$336,469,000 ▲	$222,186,195 ▼
IPR/Copyright and Counterfeit	$16,365,011 ▲	$5,910,617 ▼	$10,293,307 ▼
Lottery/Sweepstakes/Inheritance	$71,289,089 ▲	$61,111,319 ▲	$48,642,332 ▼
Malware/Scareware/Virus	$5,596,889 ▼	$6,904,054 ▲	$2,009,119 ▼
Non-Payment/Non-Delivery	$337,493,071 ▲	$265,011,249 ▲	$196,563,497 ▲
Other	$75,837,524 ▼	$101,523,082 ▲	$66,223,160 ▲
Overpayment	$33,407,671 ▼	$51,039,922 ▼	$55,820,212 ▲
Personal Data Breach	$517,021,289 ▲	$194,473,055 ▲	$120,102,501 ▼
Phishing/Vishing/Smishing/Pharming	$44,213,707 ▼	$54,241,075 ▼	$57,836,379 ▲
Ransomware	$49,207,908 ▲	$29,157,405 ▲	$8,965,847 ▲

Huntington

Cyber Crime on the Rise

- **Everyone's a Target:** A company's size doesn't necessarily affect its ability to be targeted.

- **Common Denominators:** Lack of cybersecurity practices & technology + the 'human element' are at the root of most security threats.

  - **Verizon's 2022 Report** on data breaches found that **82% of incidents** involved **"the human element,"** whether through stolen credentials, malware, phishing attacks, or human error.

  - Phishing remains a low bar of entry for data breach and/or ransomware attacks, leading to network intrusion.

  - Once in, the bad actor can interrupt business operations, demand a ransom for hijacked data, or leak confidential records.

Sources: Verizon 2022 Data Breach Investigations Report [https://www.verizon.com/business/resources/reports/dbir/].

Impacts of Cyber Crimes

The average data breach cost in **2021** rose to **$4.24 million**. The highest figure recorded in 17 years.

Trust & Customer Confidence: Companies might recover financially from a data breach, but **reputational impacts** could persist.

Jul 6, 2022

CISA: NORTH KOREA-BACKED ACTORS USING MAUI RANSOMWARE

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].

BEC on the Rise

Based on FBI report data, some <u>progress has been made</u> in pursuing the fraudsters. But their data continues to show a rise in cybercrimes since the onset of the pandemic and a more virtual environment.

$43 Billion

October 2013 – December 2021

$14B in the US

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

May 04, 2022

Alert Number
I-050422-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

Business Email Compromise: The $43 Billion Scam

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA I-091019-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to December 2021.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

2021: $2.4B in losses; 19,954 BEC complaints

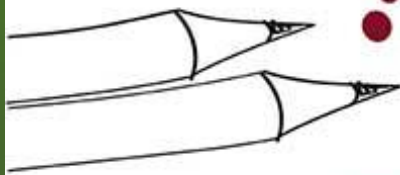Source: FBI Alert Number I-050422-PSA (https://www.ic3.gov/Media/Y2022/PSA220504)
extension://elhekieabhbkpmcefcoobjddigjcaadp/https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Examples

Huntington
Welcome.®

Social Engineering & Fraud

- **Phishing:** The attacker sends fraudulent **emails** with the intent of luring a user to click a link or open a document.

- **Vishing:** The attacker uses a *phone call* to attempt to gain money or information.

- **Smishing:** The attacker uses a *text message* to attempt to gain money or information.

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

- **Business Email Compromise (BEC):** The attacker/fraudster **spoofing a user's email address** to send fraudulent emails on their behalf.

Typical results of BEC are disclosure of sensitive and/or personal information or movement of funds.

Attacker Tactics

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

- Sense of urgency, including use of current crisis as topic or to increase urgency

- Timing, often near close of business on Friday

- Change in email tone

- Removal of addressees on the email chain (cc or other addresses)

- Less Common: Misspellings

Source: https://www.bankinfosecurity.com/bec-campaign-targets-hr-departments-report-a-13997; https://www.databreachtoday.com/ta505-apt-group-returns-new-techniques-report-a-13678

BEC Case Study: Invoicing, Electronic Payment

Construction Invoicing (St. Ambrose Catholic Parish)

1. Parish email server compromised

2. Fraudsters monitored communications

3. <u>Valid invoice</u> submitted to parish for payment

4. Fraudster spoofs message, as construction firm, to parish requesting a <u>change in payment wire instructions</u>

$1.75M LOST

Source: https://threatpost.com/bec-hack-cons-catholic-church/144212/
https://www.cleveland.com/crime/2019/04/email-hackers-steal-175-million-from-st-ambrose-catholic-parish-in-brunswick.html
https://www.news5cleveland.com/news/local-news/oh-cuyahoga/saint-ambrose-catholic-parish-victim-of-sophisticated-business-email-scheme-fbi-says

BEC Case Study: Invoicing, Electronic Payment

Local Government (Peterborough, New Hampshire)

1. Email impersonating local school district & local construction company demands $1.2M payment in July 2021

2. Investigation discovered other fraudulent payments

3. Secret Service investigation shows that the money was laundered through cryptocurrency

$2.3M LOST

Best Practices:
Actions You Can Take

It is nearly impossible to try to prevent every type of attack. Focusing on risk mitigation and management is key.

Security Best Practices for Your Business

1. **Create** an incident response and crisis response plan

2. **Be proactive** with cybersecurity awareness training

3. **Implement** detective and preventative measures in your environment;

4. **Create** well documented processes; Review/update

5. **Back up** important business data and information

6. **Implement** Identity and Access Management (IAM) policies

7. **Understand** the security posture of your IT environment

8. **Control** physical access to computers and network components

9. **Identify** and protect sensitive information

10. **Increase** information sharing and collection

11. **Act quickly** in the event of an incident

12. **Obtain &/or understand** your cyber insurance policy

Security Best Practices for You

1. Set strong, unique passwords or passphrases

2. Use two-factor authentication whenever you have that option

3. Install reliable anti-virus software on all your devices

4. Don't click suspicious links in texts or emails

5. Keep devices up-to-date

6. Delete unused apps from all devices

7. Be aware of your physical and virtual surroundings

8. Always confirm with a vendor or customer

Accounts & Passwords Tips

- **<u>Do NOT use the same username/password across accounts</u>**

- Do NOT share passwords or accounts

- Change passwords periodically

- Use a <u>password manager</u> – don't have to put sensitive accounts in password manager

- Use Two-Factor Authentication, where offered

Quick tip on security challenge questions – Fib!!!!

Social Media Tips

- Share too much personal information

- Be mindful of quizzes, add-on apps

- Not being mindful can result in your device infected with malware, catfishing, or home invasion.

Home Network

- Keep all devices on current OS versions

- Keep all applications up-to-date

- Ensure that you have antivirus software installed on your devices

- Only download applications from reputable app stores or websites

- Back up data (phones and computers)

- Dispose of old phones, computers, and media

- Securely store and appropriately destroy/shred sensitive information

- Update OS and Applications

- Only use apps from authoritative apps stores

- Limit application access (to data, photos, location, etc.)

- Backup your phone data

- Disable automatic Wi-Fi connections

- Be cautious of where you charge your phone in public using a USB cord

- Never leave your phone unattended and ensure you have an access pin or biometric in place to gain access

- Utilize caller ID to monitor robo calls, etc.

Electronic & Mobile Banking Security

Utilize:

- A known link to the bank's web services

- Your bank's app

- Remote Deposit Capture – Security of paper check

- Accounts Alerts

- Credit & Identity Monitoring Alerts

- Registered Devices

Q&A

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

Huntington

Welcome.

Thank you.