Protecting Yourself in Today's Security Landscape

CTAO Fall 2024 Conference
October 11, 2024

Presenter:

Amber Buening,
SVP, Security Outreach Director

Huntington
Welcome.

Huntington
Welcome.

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.

What is Security Culture? And why should I care?

Huntington
Welcome.®

Sharing Our Security Culture

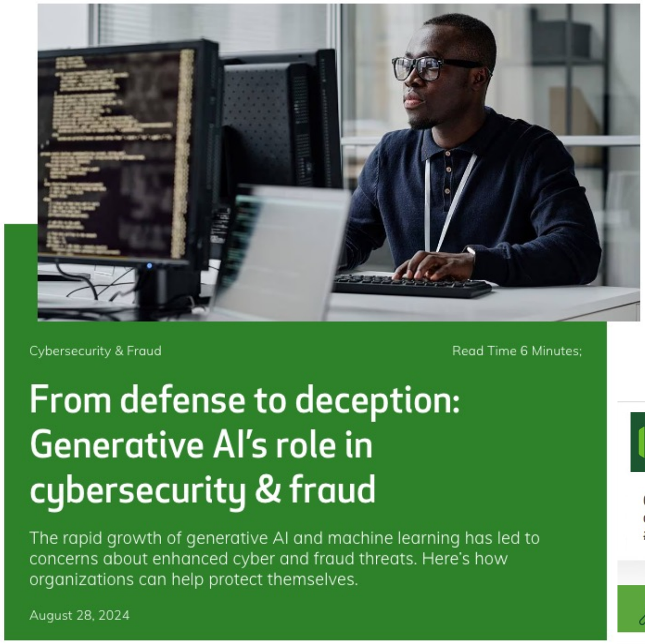
Huntington has a dedicated security culture. It includes **our attitude, perceptions, and beliefs about security**. It is driven by shifting behavior through best practices.

Sharing our security culture with our customers and the communities we serve is important to building comfort in their relationship with Huntington.

Be a hero.
Fight fraud.
FRAUDWEEK.COM
FRAUD
AWARENESS
WEEK
2024 OFFICIAL SUPPORTER
November 17–23, 2024

LEARN MORE: https://www.fraudweek.com/resources

Sharing our Security Culture

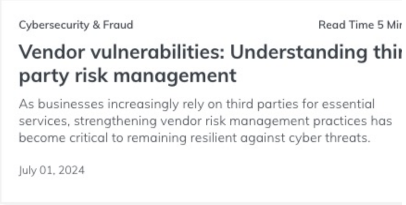


Cybersecurity & Fraud Read Time 6 Minutes;

From defense to deception: Generative AI's role in cybersecurity & fraud

The rapid growth of generative AI and machine learning has led to concerns about enhanced cyber and fraud threats. Here's how organizations can help protect themselves.

August 28, 2024



Cybersecurity & Fraud Read Time 5 Mi

Vendor vulnerabilities: Understanding thi party risk management

As businesses increasingly rely on third parties for essential services, strengthening vendor risk management practices has become critical to remaining resilient against cyber threats.

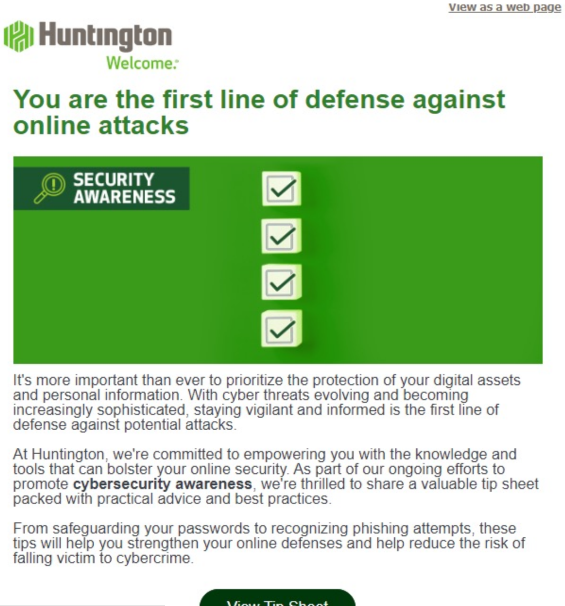
July 01, 2024

Cybersecurity & Fraud Read Time 3 Mi

How to help protect against the growing threat of ransomware

Ransomware losses reached $59.6 million last year. Learn how t help protect your organization against costly ransomware attack

June 04, 2024



View as a web page

Huntington Welcome.

You are the first line of defense against online attacks

It's more important than ever to prioritize the protection of your digital assets and personal information. With cyber threats evolving and becoming increasingly sophisticated, staying vigilant and informed is the first line of defense against potential attacks.

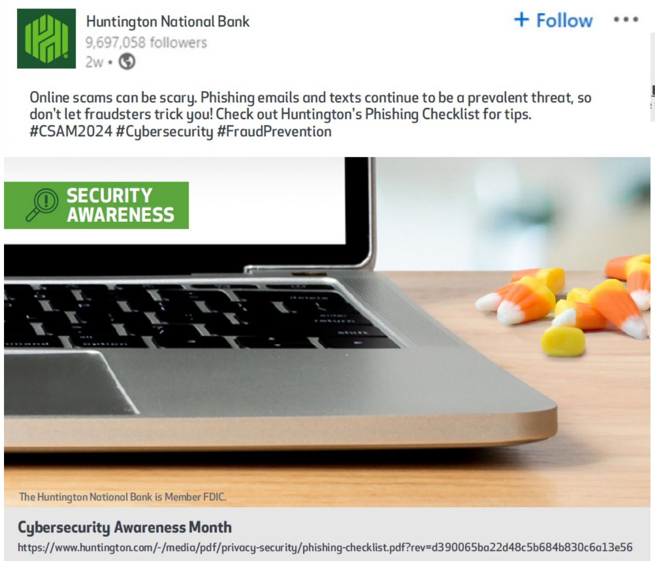
At Huntington, we're committed to empowering you with the knowledge and tools that can bolster your online security. As part of our ongoing efforts to promote **cybersecurity awareness**, we're thrilled to share a valuable tip sheet packed with practical advice and best practices.

From safeguarding your passwords to recognizing phishing attempts, these tips will help you strengthen your online defenses and help reduce the risk of falling victim to cybercrime.

View Tip Sheet

BANK & ATM LOCATOR

you print.



Huntington National Bank + Follow ...

9,697,058 followers

2w •

Online scams can be scary. Phishing emails and texts continue to be a prevalent threat, so don't let fraudsters trick you! Check out Huntington's Phishing Checklist for tips. #CSAM2024 #Cybersecurity #FraudPrevention

Cybersecurity Awareness Month

https://www.huntington.com/-/media/pdf/privacy-security/phishing-checklist.pdf?rev=d390065ba22d48c5b684b830c6a13e56

LEARN MORE: https://www.huntington.com/Commercial/insights/cybersecurity

Public

The Security Landscape

Huntington Welcome.®

These days, cybercriminals and 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

- Authentication Attacks
- Denial of Service
- Exploited Vulnerabilities
- Fraud
- Insider Threat
- Human Error
- Malware (Ransomware)
- Social Engineering
- System Intrusion
- Web Application Attack

The root of most security threats in an increasingly digitized world have **common denominators:**

LACK OF CYBERSECURITY (BEST) PRACTICES

THE “HUMAN ELEMENT”

Sources: Verizon Data Breach Investigations Report; Splunk Top 50 Security

Cybercrime on the Rise

$12.5 BILLION IN LOSSES

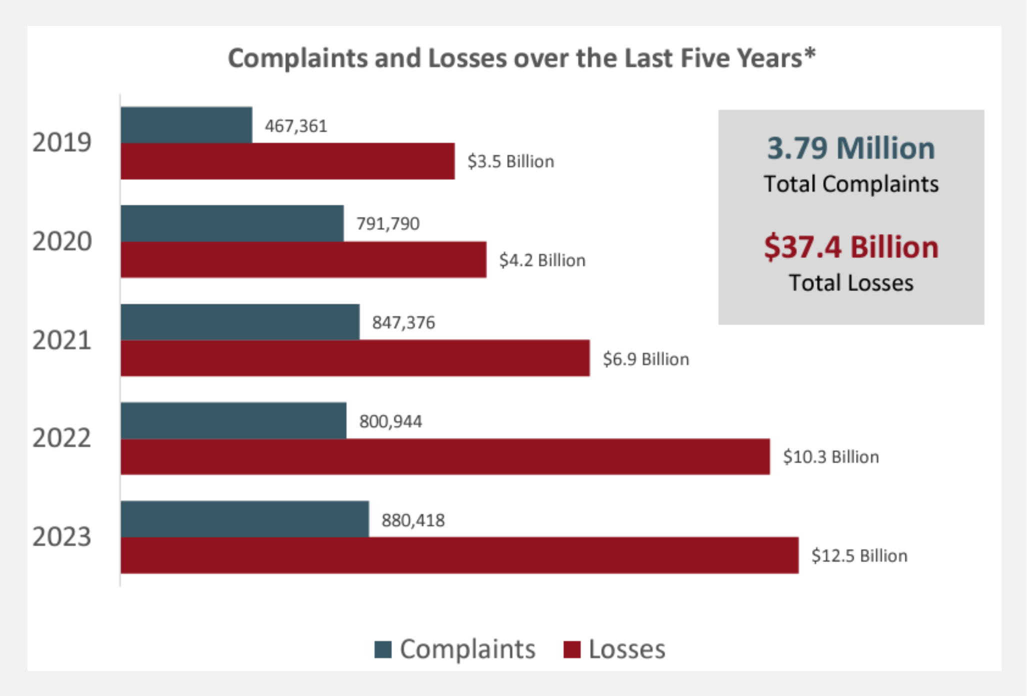
Investment Scams: $4.57 billion in losses *(38% increase from 2022)*

Business Email Compromise (BEC): $2.9 billion in losses

Imposter Scams: $1.3 billion in losses *(Government impersonation & Tech/Customer Support are most common)*

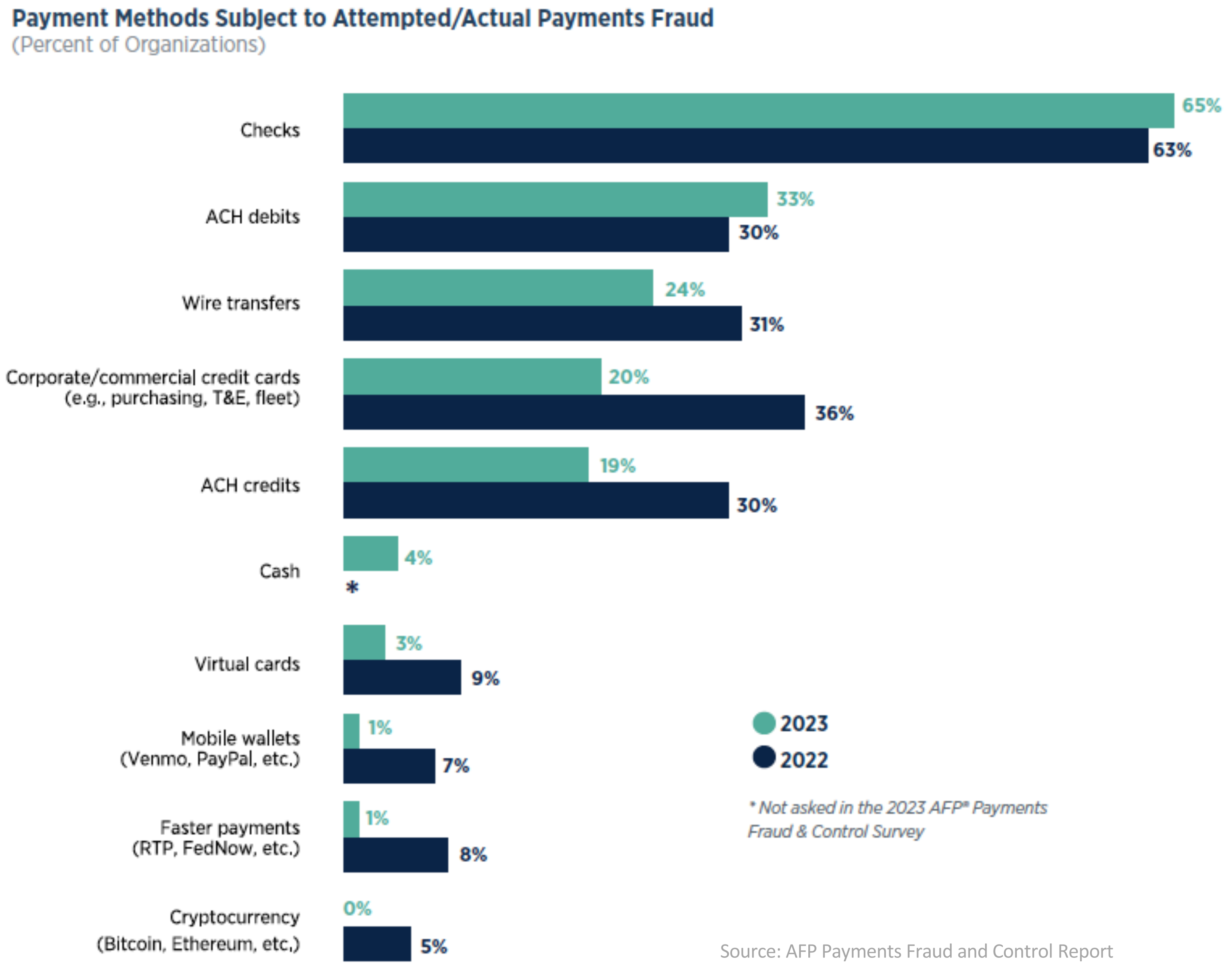
Ransomware: $59.6 million in losses

Elder Fraud: $3.4 billion in losses *(victims over the age of 60)*



Source: 2023 IC3 Annual Report

Common Fraud Scenarios



Not asked in the 2023 AFP® Payments Fraud & Control Survey

Source: AFP Payments Fraud and Control Report

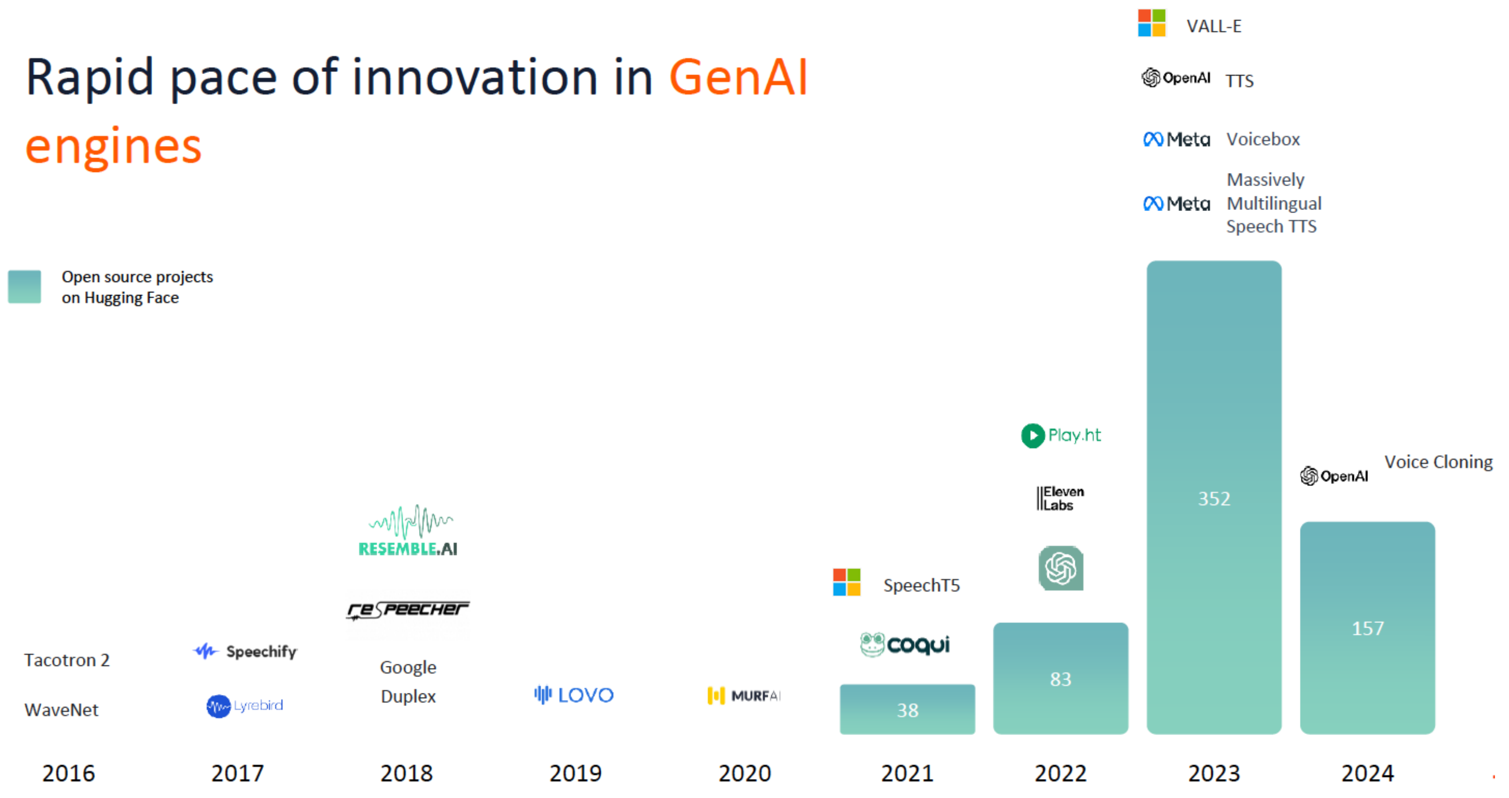
GenAI-Enabled Attacks

Huntington
Welcome.®

GenAI’s Role: The Double-Edged Sword

GenAI-Enabled Attacks: Evolving Complexity

Cyber criminals leverage GenAI to produce very sophisticated (human-like) social engineering attacks, voice/image exploits, enable malware development, and even create web apps.



Rapid pace of innovation in GenAI engines

1,265% increase in phishing email attacks since the launch of ChatGPT

Sources: PinDrop; SlashNext Security, The State of Phishing Report

GenAI-Enabled Attacks

Deepfakes attacks are becoming more sophisticated.

Recorded voice replay

Fraudster replays a voice recording or concatenate words from different recordings to formulate phrases.

Examples: portable devices, laptop, tablet, smartphone)

Speech synthesis

Fraudster uses a voice model and types text to generate spoken words that sound like an actual person.

Examples: ElevenLabs, ResembleAI, Vall-E

Automated voice chatbot

Fraudster uses an automated chat bot & voice model to sound like and interact like another real person

Examples: Google Duplex, DoNotPay

Voice conversion

Fraudster speaks into a device that changes their voice to the sound of another person using a model

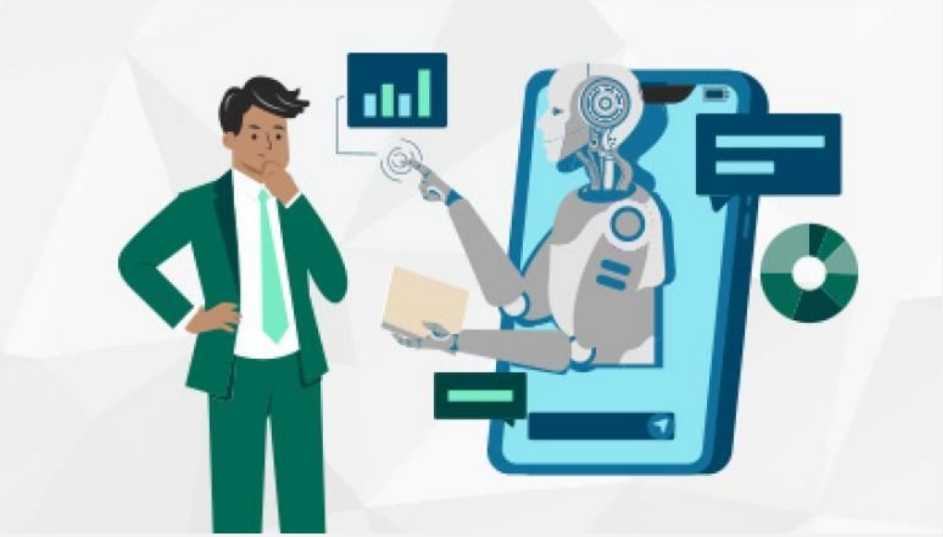
Examples: Respeecher

Low — Scale of Complexity — High

Source: PinDrop

GenAI-Enabled Attacks

Humans struggle to detect deepfakes, particularly in text and audio. How can you decern if you’re being 'played'? 🚩



- **Audio Clues:** Listen for choppy language, unusual pauses, lack of breathing, and strange sentence structures – all signs of voice cloning
- **Visual Clues:** Watch for unnatural movements, distorted proportions, lighting discrepancies, and inconsistencies that suggest the use of deepfake technology
- **BEC Red Flags**

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 and financial, technical, and security postures, recovery may not be feasible.

This also applies to individuals.

Why Is My Data Valuable & Where Does It Go?

Public

Social Engineering: Phishing, Smishing & Vishing

Huntington
Welcome.®

Phishing, Smishing & Vishing

Being able to identify and report suspicious emails is critical to prevent becoming a victim.

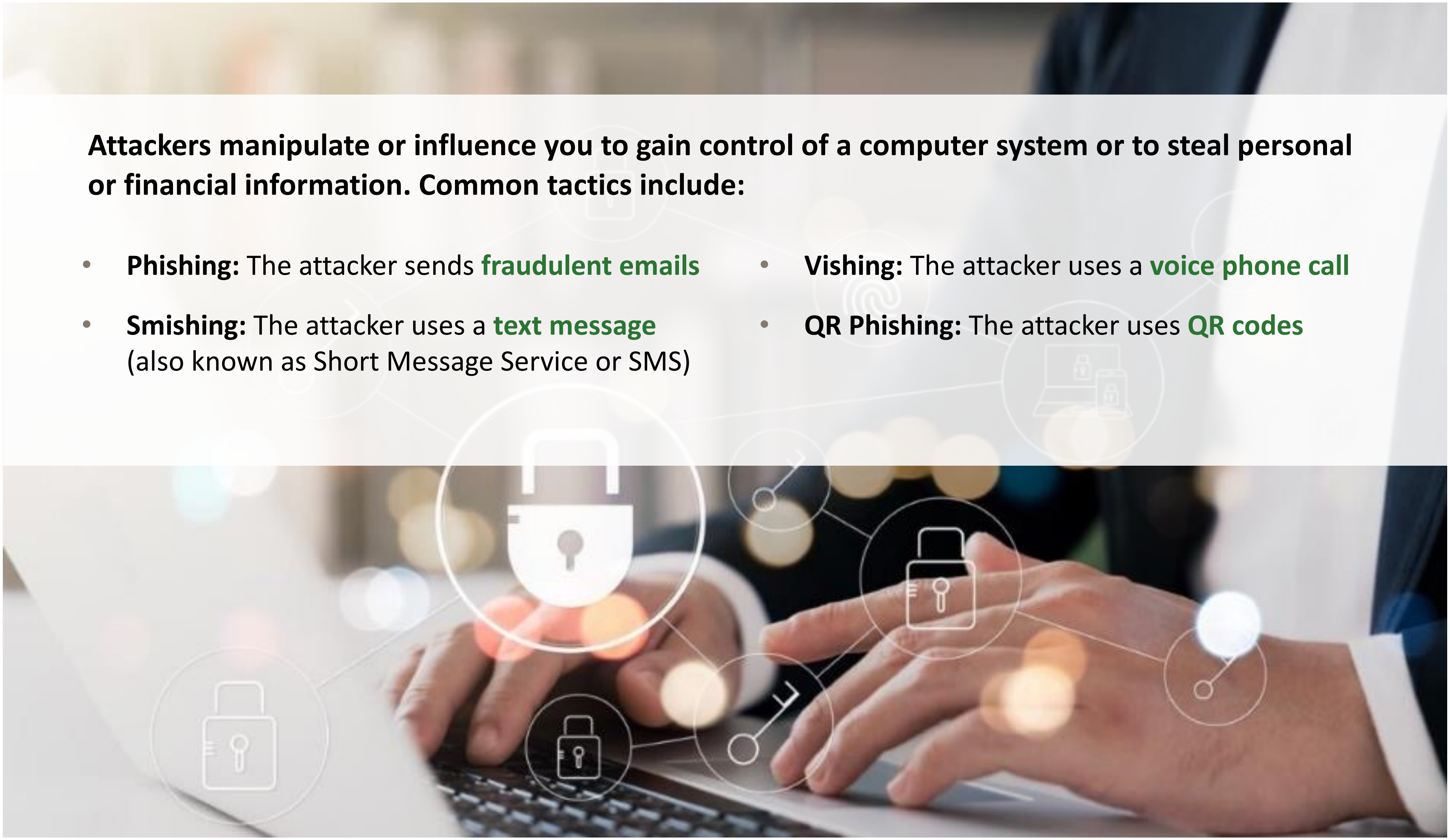
Remember: Huntington will never ask for confidential information such as username, password, personal identification number (PIN) or other information in a text message, email, or over the phone ***unless you call us*** about an issue, such as something to do with your account, first.

95%

OF DATA BREACHES STILL START WITH A PHISHING ATTACK

Source: World Economic Forum, The Global Risks Report, 17th Edition.

Social Engineering: How Fraudsters Deceive

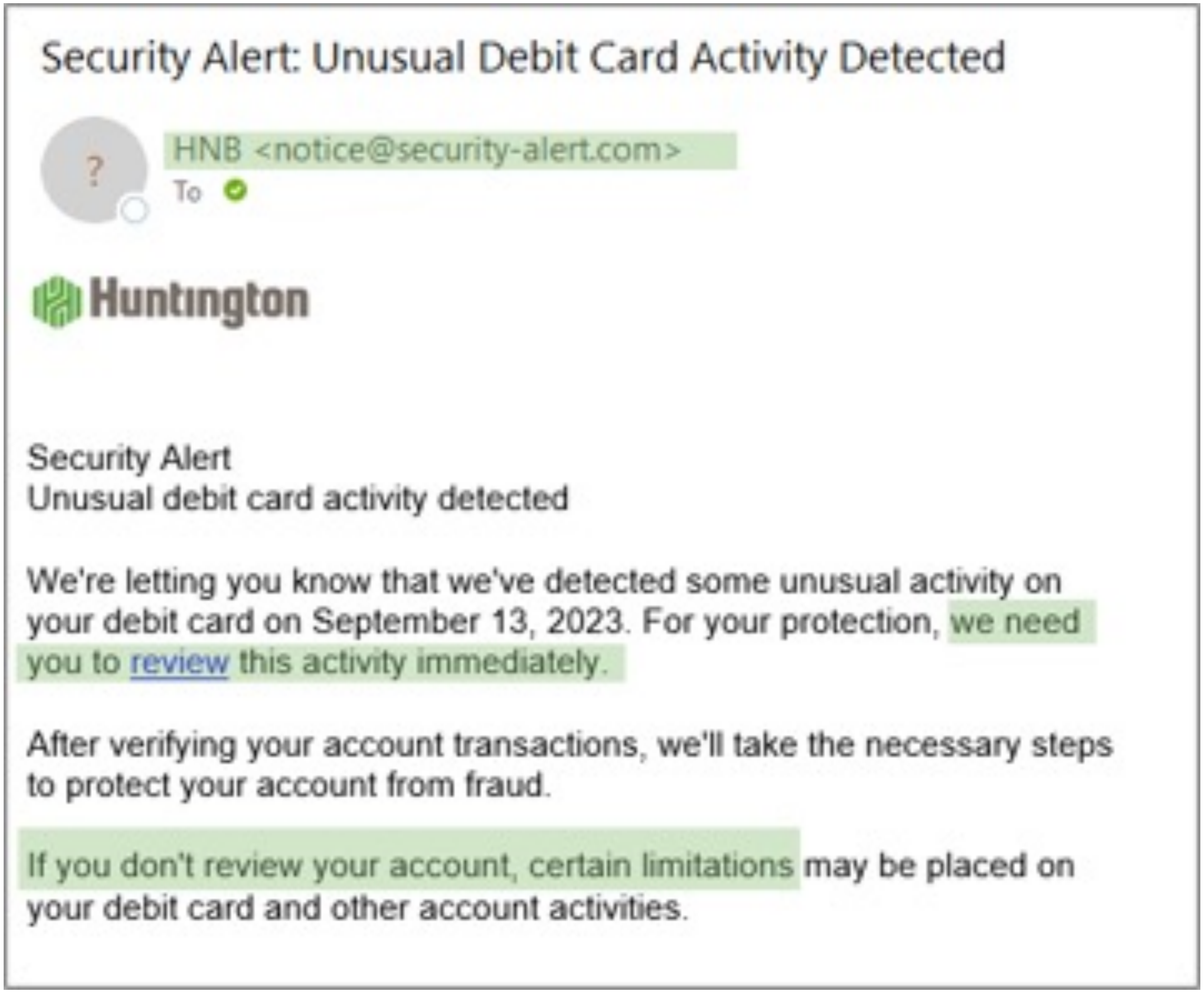


Attackers manipulate or influence you to gain control of a computer system or to steal personal or financial information. Common tactics include:

- **Phishing:** The attacker sends **fraudulent emails**
- **Smishing:** The attacker uses a **text message** (also known as Short Message Service or SMS)
- **Vishing:** The attacker uses a **voice phone call**
- **QR Phishing:** The attacker uses **QR codes**

LEARN MORE: https://www.huntington.com/Commercial/insights/social-engineering

Spot a Phish: Real or Fake?



Security Alert: Unusual Debit Card Activity Detected

HNB <notice@security-alert.com>
To

Huntington

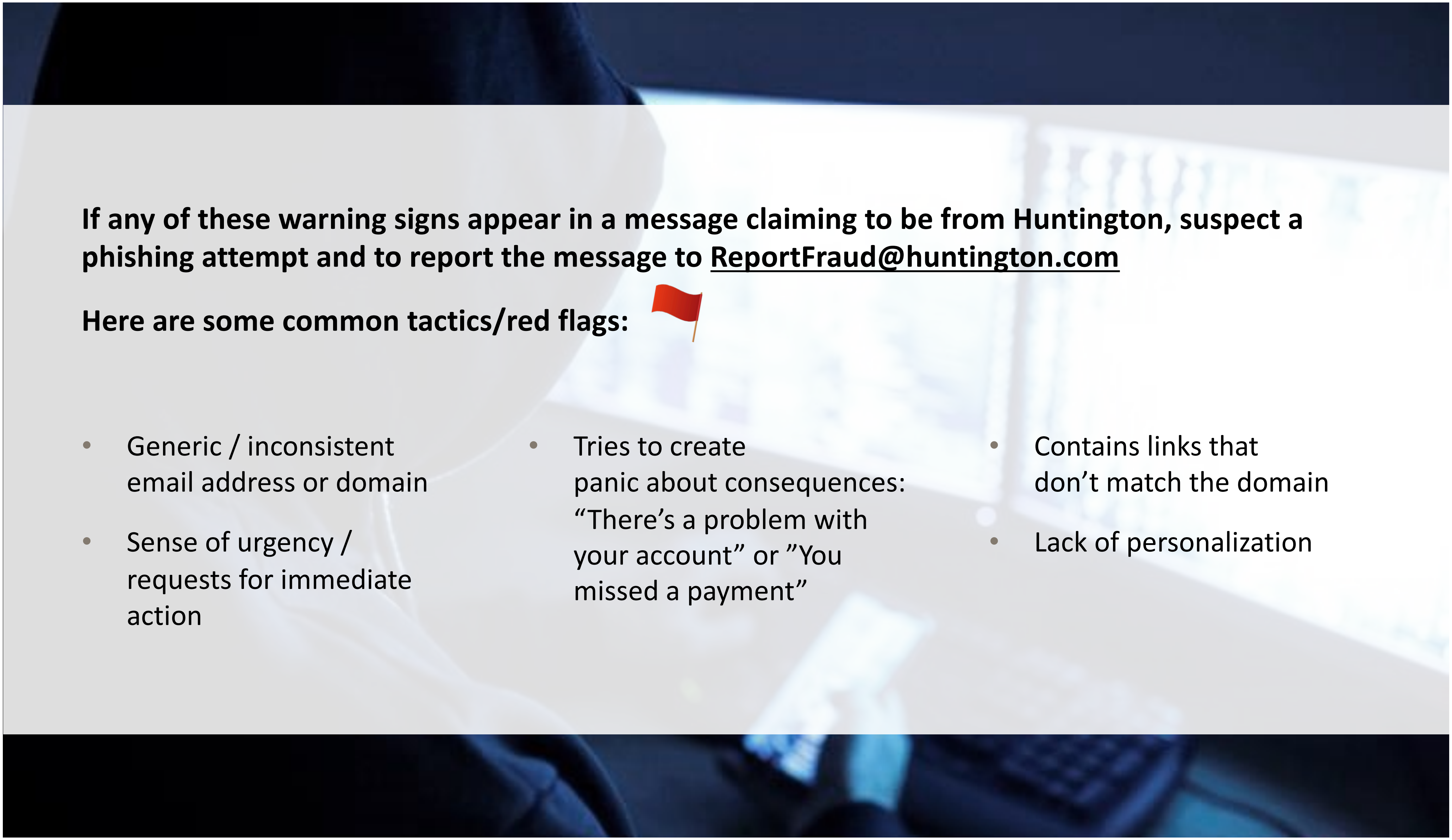
Security Alert
Unusual debit card activity detected

We're letting you know that we've detected some unusual activity on your debit card on September 13, 2023. For your protection, we need you to review this activity immediately.

After verifying your account transactions, we'll take the necessary steps to protect your account from fraud.

If you don't review your account, certain limitations may be placed on your debit card and other account activities.

Criminal / Fraudster Tactics



If any of these warning signs appear in a message claiming to be from Huntington, suspect a phishing attempt and to report the message to ReportFraud@huntington.com

Here are some common tactics/red flags: 🚩

- Generic / inconsistent email address or domain
- Sense of urgency / requests for immediate action
- Tries to create panic about consequences: “There’s a problem with your account” or ”You missed a payment”
- Contains links that don’t match the domain
- Lack of personalization

LEARN MORE: https://www.huntington.com/Commercial/insights/social-engineering

Business Email Compromise (BEC)

Huntington
Welcome.®

Business Email Compromise (BEC)

BEC is one of the most financially damaging online crimes.

$2.9B

in losses due to BEC in 2023

Using common messaging tactics/attack methods, cybercriminals **convince an email recipient that a message is coming from a legitimate and trusted source.**

Cybercriminals **exploit our reliance on email** to conduct business — both personally and professionally.

Learn More: Huntington.com: Preventing BEC Scams

Source: FBI’s Internet Crime Complaint Center (IC3)

BEC Common Attack Scenarios

Supplier Account Change

A seemingly legit “supplier” requests funds to be wired to a new account; It may be framed as a rush because “your account is past due”

Fraudulent Invoice

Fraudster posing as a company/government entity requests payment for products, services, taxes or other fees

Executive Transaction Request

A seemingly real request from an Executive asking for a time sensitive transaction (often immediate funds transfer); They state it’s a highly confidential transaction

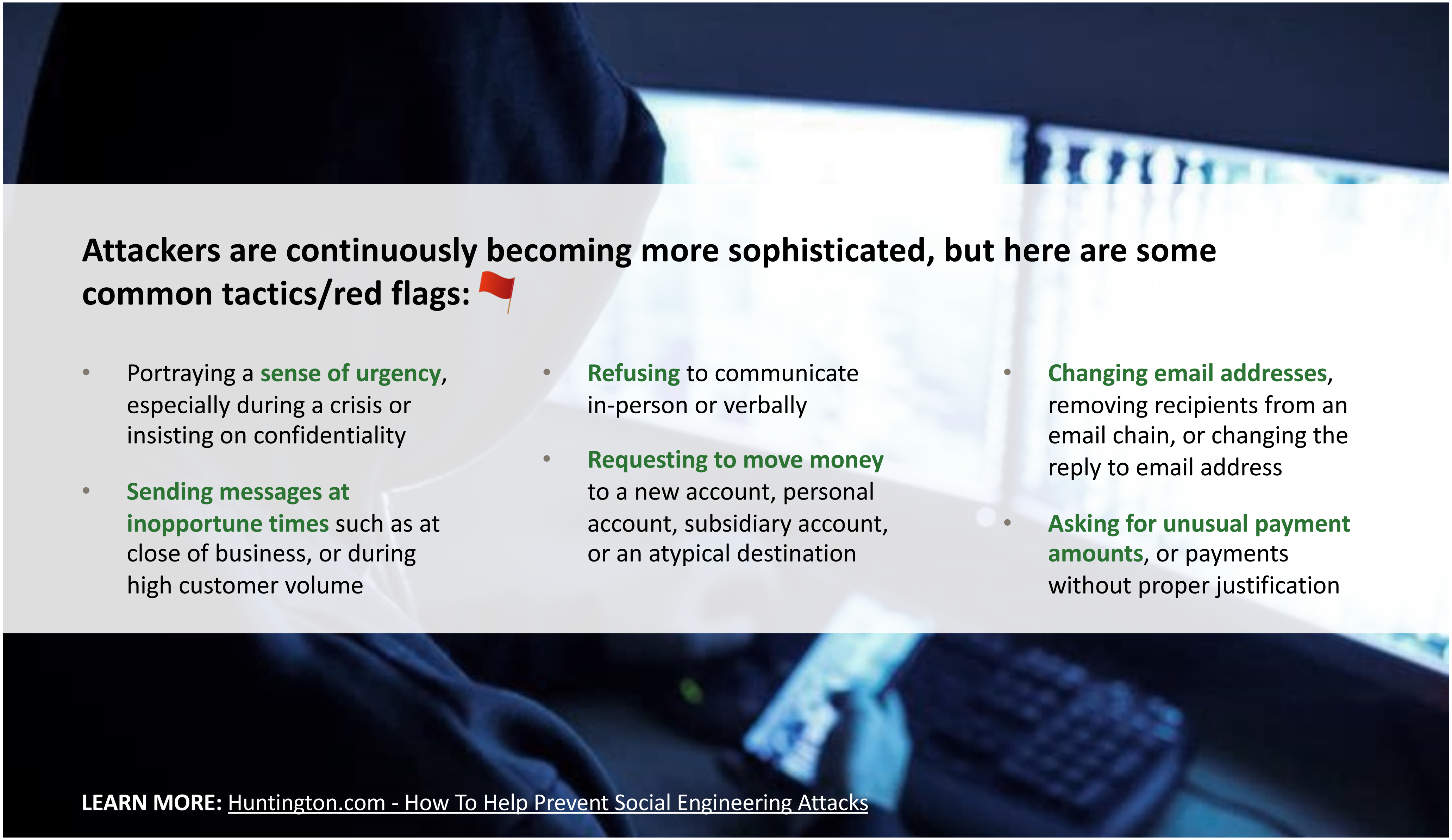
Executive Data Request

A seemingly real request from an Executive asking for HR, Payroll or Audit department and/or access to employees earning statements, tax records, or other personal information

Specific Payment Methods

Fraudsters often request funds sent by wire transfers, gift cards, Zelle, or other online payment platforms

Business Email Compromise (BEC)



Attackers are continuously becoming more sophisticated, but 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
- **Refusing** to communicate in-person or verbally
- **Requesting to move money** to a new account, personal account, subsidiary account, or an atypical destination
- **Changing email addresses**, removing recipients from an email chain, or changing the reply to email address
- **Asking for unusual payment amounts**, or payments without proper justification

LEARN MORE: Huntington.com - How To Help Prevent Social Engineering Attacks

Protecting Against BEC

Monitor Payment Methods & Changes

- **Businesses don’t change their banks often. Be mindful of payment institution and payment type changes**
- Avoid using paper checks by using ACH or other electronic payment methods when possible

Follow Established Protocols

- Use dual authentication/approvers
- **Verify the customer’s contact information has not recently changed if you receive a change notification**
- Properly verify vendor payment updates
- Never call phone numbers or reply to email addresses sent in suspicious emails or texts
- Confirm any notifications of new payment information with a known contact at the vendor

Treat Emails With Caution

- **Use a secure email solution, monitor message change notifications**
- Avoid clicking suspicious links and report them promptly

Act Quickly

- **Trust your instincts. If something feels off, it probably is**
- In the event of an incident, move fast to promptly report it to the appropriate team or organization

Huntington BEC Webinar

Huntington

The Rising Threat of Business Email Compromise & Other Fraud Schemes

LEARN MORE: Huntington Webinar Recording

Ransomware

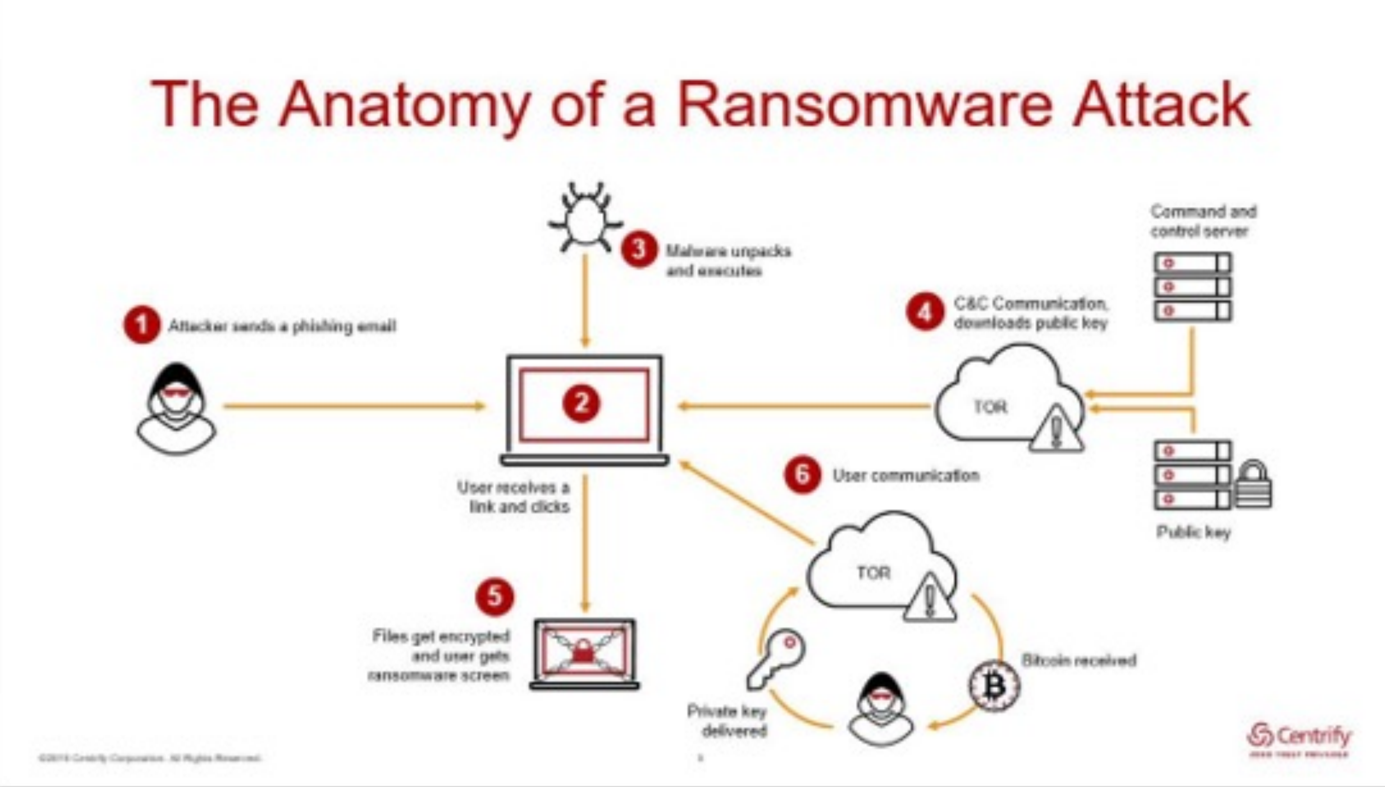
Huntington
Welcome.®

Ransomware

A NEW TARGET EVERY

14

SECONDS



The Anatomy of a Ransomware Attack

1 Attacker sends a phishing email
2
3 Malware unpacks and executes
4 C&C Communication, downloads public key
Command and control server
TOR
Public key
User receives a link and clicks
6 User communication
TOR
5 Files get encrypted and user gets ransomware screen
Private key delivered
Bitcoin received
Centrify
©2019 Centrify Corporation. All Rights Reserved.

Learn More: Huntington.com: Protect Your Organization Against Ransomware

Source: Cybersecurity & Infrastructure Security Agency (CISA)

Ransomware in the Public Sector

Cybercriminals often target public entities because of potential access to large amounts of funds and data. It’s important to be aware of how your organizations may be targeted.

RESOURCES

Stop Ransomware Training & Information

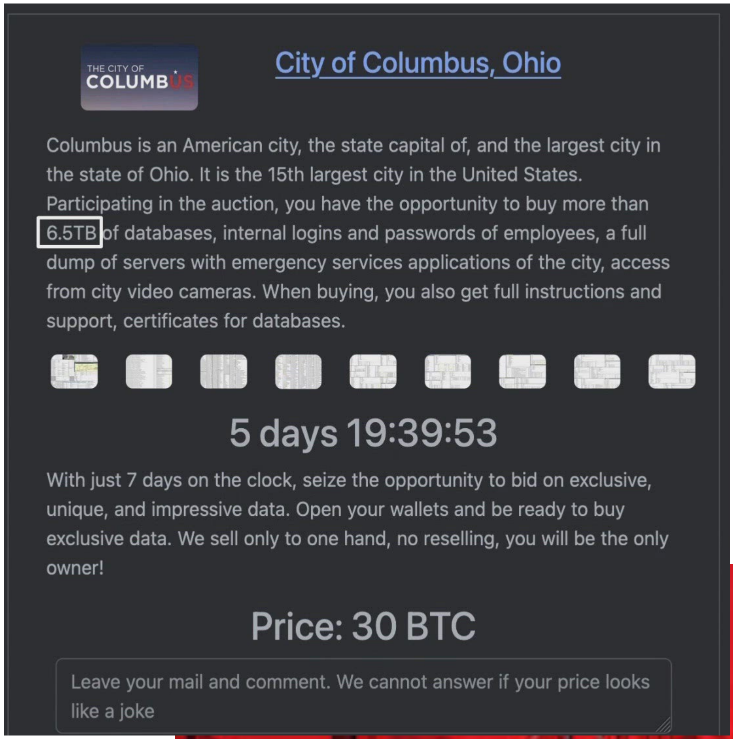
https://www.cisa.gov/stopransomware/resources

Ransomware Response for Victims

https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

File a Complaint with FBI Internet Crime Complaint Center (IC3)

https://www.ic3.gov/



City of Columbus, Ohio

Columbus is an American city, the state capital of, and the largest city in the state of Ohio. It is the 15th largest city in the United States. Participating in the auction, you have the opportunity to buy more than 6.5TB of databases, internal logins and passwords of employees, a full dump of servers with emergency services applications of the city, access from city video cameras. When buying, you also get full instructions and support, certificates for databases.

5 days 19:39:53

With just 7 days on the clock, seize the opportunity to bid on exclusive, unique, and impressive data. Open your wallets and be ready to buy exclusive data. We sell only to one hand, no reselling, you will be the only owner!

Price: 30 BTC

Leave your mail and comment. We cannot answer if your price looks like a joke

Enabling Security Culture by Changing Our Behaviors

Huntington
Welcome.®

Reporting Fraud

Timely reporting of fraud attempts or events helps law enforcement agencies investigate and prosecute offenders, contributing to the overall deterrence of fraudulent schemes.

WAYS TO REPORT

Local Law Enforcement

Internet Crime Complaint Center (IC3)

Federal Trade Commission (FTC)

Call Huntington at (800) 480-2265 immediately if money has been exchanged.

Security Best Practices: GenAI-Enabled Threats

In today's digital world, it's **important to follow security best practices** professionally and personally.

- **Consider enhancing verification processes** through multiple factor authentication (MFA), biometric verifications, and similar methods
- **Educate employees & contacts** about the threat of AI-enabled scams, including how to spot potential attempts
- **Implement an incident response plan**, which can assist in mitigating damages and analyzing breaches to prevent future incidents
- **Keep systems and applications updated** to help avoid vulnerability exploitation

Learn More: Huntington.com: AI-Enabled Threats

Enabling Security Culture by Changing Our Behaviors

Huntington
Welcome.®

Cyber Resiliency

No organization is immune from cybersecurity and fraud threats or weather-related crises, but proactive planning could help avoid costly disruptions.

Having an IT resiliency plan is critical to address cybersecurity and business continuity needs, incident response plans, and disaster recovery procedures.

Cyber resiliency is a concept that describes an organization's ability to:

- minimize the impact of an adverse cyber event
- restore their operational systems to maintain a business continuity

Average **hourly cost** of server downtime **exceeds $300,000** for 91% of surveyed businesses

Source: Information Technology Intelligence Consulting.
"IITC 2022 Global Server Hardware, Server OS Security Report."

Security Best Practices: GenAI-Enabled Threats

In today's digital world, it's **important to follow security best practices** professionally and personally.

- **Consider enhancing verification processes** through multiple factor authentication (MFA), biometric verifications, and similar methods
- **Educate employees & contacts** about the threat of AI-enabled scams, including how to spot potential attempts
- **Implement an incident response plan**, which can assist in mitigating damages and analyzing breaches to prevent future incidents
- **Keep systems and applications updated** to help avoid vulnerability exploitation

Learn More: Huntington.com: AI-Enabled Threats

Security Best Practices

In today's digital world, it's **important to follow security best practices** professionally and personally.

- **Use strong passwords** and practice good 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 & 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
- **For remote work,** use a Virtual Private Network (VPN), secure your home router, separate work & personal devices

Security Best Practices Checklist

PRIORITIZE INCIDENT RESPONSE PLANNING THAT INCLUDES DATA RECOVERY

- ❑ Create or strengthen an incident and crisis response plan.
- ❑ Maintain an accurate inventory of your organization’s assets (IT equipment, data, and systems).
- ❑ Perform automatic and continual backups of business data and information.
- ❑ Create and enforce corporate policies for systems or areas where personally identifiable information (PII) and other sensitive data are held.
- ❑ Add additional layers of protection for critical data.
- ❑ Review and update your cyber liability insurance policy.

Security Best Practices Checklist

MANAGE VULNERABILITIES

❑ Conduct an annual assessment of vulnerabilities in your IT environment.

❑ Keep all computer operating systems and applications updated with the latest security patches.

❑ Subscribe to CISA’s Known Exploited Vulnerabilities Catalog.

❑ Ensure your organization’s antivirus, malware protection, and email security software are active and the most updated version available.

❑ Address unknown insider threat risk through enforcement security controls for (remote) workers.

Security Best Practices Checklist

IMPLEMENT MEASURES TO PROTECT AGAINST COMMON CYBERTHREATS

- □ Employ identity and access management (IAM) policies.
- □ Implement role-based access control (RBAC) and restrict third-party access.
- □ Reduce or eliminate vulnerable connection methods into your network.
- □ Require permission for USB or remote drive access.
- □ Control physical access to computers and network components.
- □ Train employees to look for BIMI in their email provider.
- □ Add an external email banner.
- □ Assess your website and social media to determine whether they share too much information.

Security Best Practices Checklist

BEGIN DEVELOPING OR DEEPENING 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.

Want to learn more about security best practices?

Please check out these additional Huntington and partner resources!

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 Security

https://www.huntington.com/Privacy-Security

Huntington Insights

https://www.huntington.com/Commercial/insights/cybersecurity

Have I Been Pwned

https://haveibeenpwned.com/

Identity Theft Resource Center

https://www.idtheftcenter.org/

Thank you.