



# TECHNICAL ASSISTANCE

POWERED BY THE ILLINOIS TOLLWAY

*Equipping Businesses for Success*

Administered by



Presented by Xavier John

April 14th 2025

# Cyber Security

An Overview



**TECHNICAL ASSISTANCE**

POWERED BY THE ILLINOIS TOLLWAY



# Agenda

- What is Cyber Security?
- The Importance of Cyber Security
- What are the Different Cyber Security Threats
- Examples of Hacks
- How to Reduce Risk of Cyber Security Attacks

# What is Cyber Security?

---

- Cyber Security refers to the practice of protecting devices and data from cyber attacks



**TECHNICAL ASSISTANCE**  
POWERED BY THE ILLINOIS TOLLWAY



# What is the Importance of Cyber Security?



**TECHNICAL ASSISTANCE**

POWERED BY THE ILLINOIS TOLLWAY





# The Importance of Cyber Security

- Cyber security is important for protecting sensitive data from theft or damage.
- It can protect companies' information by using many methods and technologies such as encryption, using access controls and providing company training.
- These methods when used together can improve the security of a company by enhancing employee awareness and providing an extra layer of protection.

# What are the Different Cyber Security Threats?

- Malware
- Ransomware Attacks
- Credential Stuffing & Brute Force Attacks
- Business Email Compromise (BEC)

# Malware (Malicious Software)

## What it is:

Software designed to disrupt, damage, or gain unauthorized access to a system.

## Examples:

- **Viruses** – Infects files and spreads when executed.
- **Worms** – Self-replicating malware that spreads across networks.
- **Trojan Horses** – Disguised as legitimate software but contains malicious code.
- **Ransomware** – Encrypts data and demands payment for decryption.
- **Spyware** – Secretly gathers information about users (keystrokes, credentials, etc.).

## How to protect against it:

- Use antivirus and anti-malware software.
- Keep systems and applications updated.
- Educate employees about phishing and suspicious downloads.





# Ransomware Attacks

## What it is:

A type of malware that encrypts data and demands a ransom in exchange for the decryption key.

## Notable Ransomware Attacks::

- **WannaCry (2017)** – Infected over 200,000 computers worldwide..
- **Ryuk** – Targets businesses and demands large ransoms.
- **LockBit** – A newer ransomware that spreads quickly and encrypts files.

## How to protect against it:

- Keep regular backups of critical data offline
- Use endpoint detection and response (EDR) solutions.
- Restrict user permissions and network access.



# Credential Stuffing & Brute Force Attacks

## What it is:

Cybercriminals try to gain unauthorized access by guessing or using stolen passwords

## How It Works:

- **Brute Force Attack** – Hackers use automated tools to try millions of password combinations.
- **Credential Stuffing** – Attackers use leaked username/password pairs from previous breaches.

## How to protect against it:

- Implement multi-factor authentication (MFA)
- Enforce strong password policies (long and complex passwords).
- Use account lockout features after multiple failed login attempts.



# Business Email Compromise (BEC)

## What it is:

Hackers impersonate executives or business partners to trick employees into transferring money or revealing confidential data.

## How it Works:

- Attackers spoof company emails and pretend to be the CEO/CFO.
- They urgently request wire transfers or sensitive financial data.
- The victim sends money or information, thinking the request is legitimate.

## How to protect against it:

- Verify sensitive email requests via phone or in person.
- Use email authentication protocols (SPF, DKIM, DMARC).
- Train employees to recognize social engineering tactics.



# Bonus: Deep Fakes

## What it is:

Hackers use AI-generated audio or video to impersonate executives or trusted partners and trick employees into taking harmful actions.

## How it Works:

- Attackers create realistic deepfake videos or voice recordings of executives (e.g., CEO, CFO).
- These deepfakes may instruct employees to urgently transfer money or share confidential data.
- Because the audio/video appears authentic, victims believe the request is legitimate and comply.

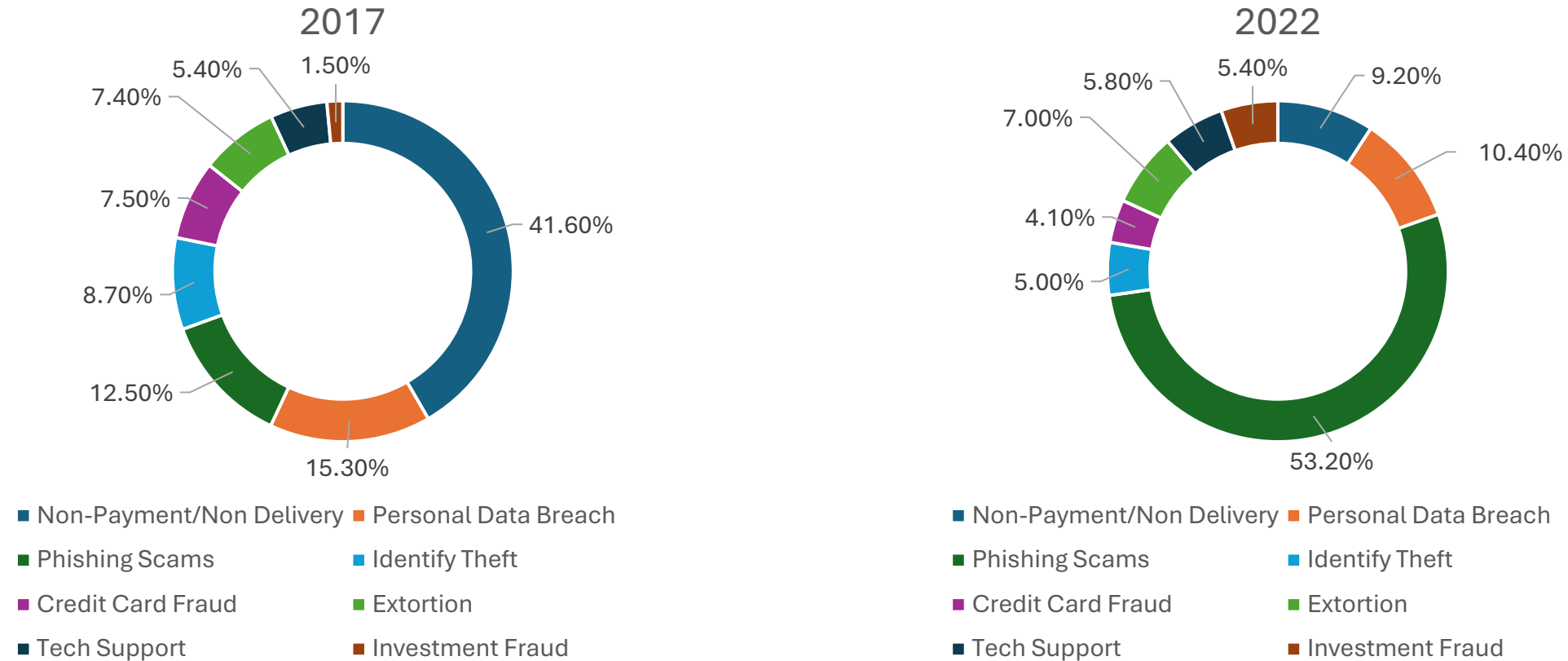
## How to Protect Against It:

- **Always verify** unusual or sensitive requests via a trusted second channel (e.g., phone or in person).
- **Educate employees** on the risks of deepfakes and how to spot inconsistencies (unnatural facial expressions, lip-sync errors, odd tone shifts).
- **Implement strict protocols** for approving financial transactions or sharing sensitive information.
- **Leverage deepfake detection tools** and stay informed on emerging threats.



# The Most Prevalent Forms of Cybercrime

The charts below show the share of worldwide cyber-attacks for the years 2017 and 2022



Sourced from "The Most Prevalent Forms of Cyber Crime" by Florian Zandt

# Examples of Cyber Security Hacks



# No One Is Immune



Illinois Department of Transportation

Dear Xavier John

This is a final notice regarding the verification of your organization's information. Please do confirm that the details provided below are correct and up-to-date:

**Important:** Failure to verify your information within the next 24 hours will result in the revocation of your license.

Click the secure verification link below to complete the process. This link will expire in 24 hours.

Your prompt attention to this matter is crucial. We urge you to act immediately to avoid any disruption in your services.

|                        |  |
|------------------------|--|
| Firm                   | AXSmodern Inc  |
| Address 1              | XXXXXXXXXXXXXXXXXXXXXXXXXXXX   |
| City                   | Chicago  |
| State                  | IL   |
| Zip Code               | 60616  |
| Contact                | Xavier John  |
| Fax                    |  |
| Phone                  | XXXXXXXXXXXX   |
| Email                  | xavier.john@axsmodern.com  |
| County                 | Cook   |
| District               | 1  |
| Airport Concessionaire | N  |
| Specialty              | NAICS Code: 518210 - Computing in Infrastructure Providers, Data Processing, Web Hosting, and Related Services (Specialty: Web hosting (excluding software publishing)); NAICS Code: 541511 - Custom Computer Programming Services (Specialty: Computer software analysis and design services, custom, Computer software programming services, custom, Software programming services, custom, custom computer, Web (i.e., Internet) page design services, custom); NAICS Code: 611420 - Computer Training (Specialty: Computer programming, software, and systems training, online (through a website or mobile application), Computer software training, Software application training) |
| NAICS                  | NAICS Code: 518210 - Computing in Infrastructure Providers, Data Processing, Web Hosting, and Related Services; NAICS Code: 541511 - Custom Computer Programming Services; NAICS Code: 611420 - Computer Training  |

**CLICK HERE TO VERIFY.**

- *AXSModern recently experienced a phishing attempt. The email claimed to be from Illinois Department of Transportation, asking the viewer to secure verification by clicking a suspicious link*

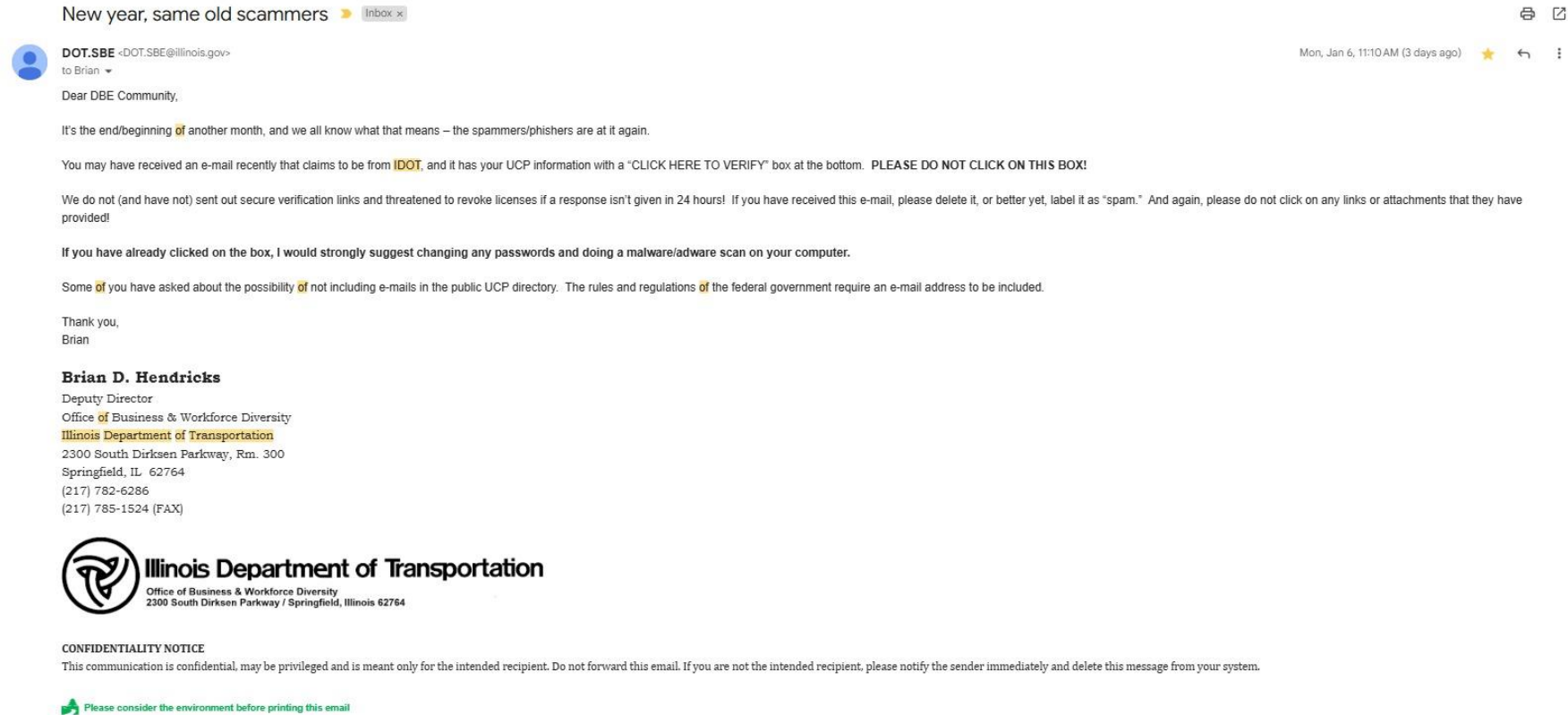


## TECHNICAL ASSISTANCE

POWERED BY THE ILLINOIS TOLLWAY




# No One Is Immune



- *IDOT quickly released an email informing its users of the phishing attempt.*

# No One Is Immune




Illinois Department of Transportation  
2025 Annual License holder and Contractor information verification  
Dear AXSmodern Inc  
Final Notice: Immediate Action Required for Information Verification

This is a final notice regarding the verification of your organization's information. Please confirm that the details provided below are correct and up to date:  
Important: Failure to verify your information within the next 24 hours will result in the revocation of your license.  
Click the secure verification link below to complete the process. This link will expire in 24 hours.  
Your prompt attention to this matter is crucial. We urge you to act immediately to avoid any disruption in your services.

|          |  |
|----------|--|
| Firm     | AXSmodern Inc  |
| Address1 | 2111 South Wabash Ave. #1407   |
| Address2 |  |
| City     | Chicago  |
| State    | IL   |
| Zip      | 60616  |
| Contact  | Xavier John  |
| Fax      |  |
| Phone    | (773) 858-0411   |
| Email    | <a href="mailto:xavier.john@axsmodern.com">xavier.john@axsmodern.com</a> |
| County   | Cook   |

CLICK HERE TO UPDATE AND VERIFY YOUR INFORMATION.

...ital and privileged, and is not for the purpose of providing legal advice. Unless you are the intended addressee (or authorized to receive for the intended addressee), you may not use, copy, disclose, or forward th  
ved this message in error, please advise the sender by reply email and delete the message.  
© Copyright 2024. All Rights Reserved.



- This is another phishing attempt on AXSModern. Notice that it is very similar to the previous one*

# No One Is Immune



- The Change Healthcare ransomware attack exposed sensitive data of over 100 million Americans, causing widespread disruptions to healthcare services. This breach is among the largest in U.S. healthcare history.



- In 2024, AT&T suffered two major data breaches. In July, hackers stole phone numbers and call records of 110 million customers via AT&T's account with Snowflake. Earlier in March, 73 million customer records were leaked online, putting millions at risk of account hijacks.

# No One Is Immune



- Evolve Bank & Trust suffered a major cyberattack, exposing the personal data of at least 7.6 million people, including Social Security numbers, bank account details, and contact information.



- Cencora, a major U.S. pharmaceutical company, suffered a cyberattack in February 2024, exposing sensitive data including patient names, birthdates, health diagnoses, and medications.

# How to Reduce Risk of a Cyber Attack?



**TECHNICAL ASSISTANCE**

POWERED BY THE ILLINOIS TOLLWAY





# How to Reduce Risk?

| Method               | Example/Use Case   |
|----------------------|--|
| Employee Training    | Employees will be able to recognise and identify methods such as social engineering and phishing. Hence, they will know how to avoid them              |
| Use Strong Passwords | Even if other parts of your system is compromised, passwords are the final defence between hackers and your company's data.                            |
| Use Encryption       | Even if data is stolen, it would be unreadable and cannot be used. It also ensures that only authorised personnel would have access to sensitive data. |

# How to Reduce Risk?

| Method                                 | Example/Use Case   |
|--|--|
| Enable Access Controls and Permissions | Only authorised persons would have access to certain data based on their position. This limits the risk of compromised accounts, as only higher tier accounts would have access to more sensitive data                 |
| Regular Data Back Ups                  | If a company suffers from a cyber-attack, data may be lost, tampered with, or damaged. Regular back ups lessens the impact of data loss, ensuring that productivity is maintained.                                     |
| Software Updates                       | Hackers can exploit security vulnerabilities in outdated software. Regular updates addresses these security issues.  |
| Organizational Environment             | Microsoft Dataverse as a service provides several security features such as access controls, encryption and secure file sharing. Companies that use this service would have their data stored securely in one location |

# Risks of Not taking Cyber Security Seriously

| Risk  | Example/Statistics  |
|---|---|
| <b>Data breaches</b> which may lead to legal ramifications if clients' personal data is compromised   | <p>There was a 67% increase in data breaches between 2014 and 2019.</p> <p>In 2017, around 143 million consumers were impacted by a cyberattack on Equifax resulting in a financial toll exceeding \$4 billion for the company.</p> |
| <b>Ransoms Payments</b> due to the impact of a ransomware attack  | 81% of organizations were affected by ransomware at least once in 2023.   |
| <b>Loss of Credibility</b> as a result of legal ramifications and client distrust   | 59% of consumers are likely to avoid companies that suffered from a cyberattack in the past year.   |
| <b>Disruption to Operations</b> due to shifting of resources in containing the breach. This leads to a drop in productivity and therefore, financial loss | The global average cost of a data breach in 2023 was \$4.45 million, a 15% increase over three years  |

# Thank You

## **Any questions?**

You can find us at

- [Xavier@ICUTechAssist.net](mailto:Xavier@ICUTechAssist.net)