



CITY OF  
FORT LAUDERDALE

 **CyberSmartFTL**

The logo for CyberSmartFTL, featuring the text "CyberSmartFTL" in a bold, blue font with a white outline. The text is integrated with a stylized circuit board design in orange and white, with lines extending from the letters and ending in small circles.

# What is Cybersecurity?

Protection of **data, devices** and **networks** from cyberattacks

What can be affected?

- Your **computer, account** and stored **information**.

How/why does this happen?

- Hackers using **social engineering**
  - Online manipulation tactics used for exploitation.

# Types of Cyber-Attacks?



CITY OF  
FORT  
LAUDERDALE



# Types of Malware and Cyber Threats



## Virus

A **malicious** program with the intent of harmfully **infecting** a computer.

### Found in

- Email attachments
- Attachable Media
- Random internet downloads



## Trojan Horse

**Malicious** code presenting itself as a **legit** software

- Requires user execution to be carried out
- Spies on users, steal data, gain remote access

# Types of Malware and Cyber Threats



## Phishing

*Fraudulent* messages that trick users into providing sensitive data.

### Spear Phishing

- Well planned phishing attempts
- Aiming to mask trusted sender

### Whaling

- Attacks targeting high level officials
- Due to their access



## Ransomware

Malware that prevents access into system or files

- Attackers **retain** control until **ransom** is paid
- System and data can become **permanently** unavailable if not resolved

# Types of Malware and Cyber Threats



## Scareware

Forces Pop-ups or siren noises through computer speakers

Usually links to some kind of ad site or payment site like Paypal



<https://www.ulm.edu/it/cybersecurity/dyk-scareware-20220518.html>

# Ransomware case studies



CITY OF  
FORT  
LAUDERDALE



What results when an exploit materializes?

## Ransomware case studies

# City of Atlanta 2018



### What happened?

- Malware caused **disruption** across city due to weak password
  - Affected utilities



### Impact

- 5 days to regain access to applications
- Online payments **disabled** for a week



### Cost

- 2.6 million spent
- Used for **emergency IT** contracts

What results when an exploit materializes?

## Ransomware case studies

# Colonial Pipeline 2021



COLONIAL PIPELINE CO.



### What happened?

- **Leaked** user password
- Causing **unethical** service access



### Impact

- 100GB of data **stolen**
- Forced pipeline shutdown
  - Lack of fuel across states.
- **Increased** attack



### Cost

- **\$4 million**
- Company paid **ransom**



CITY OF FORT LAUDERDALE

What results when an exploit materializes?

## Ransomware case studies

# City of Baltimore 2019



### What happened?

- Loss **access** to city computers and data
- Affected by **malware** (malicious software)



### Impact

- Failure to complete **operations** across departments
- Temporary city **email** disability



### Cost

- **\$18.2** million
- **Restoration**
- **Mitigation** effort
  - FBI, Microsoft, etc
- Revenue **Loss**



CITY OF  
FORT  
LAUDERDALE

# Recognizing Phishing Attempts

---

# Recognizing Phishing Attempts

- 🔗 Tone of **urgency, pressure** to act
  - 🔗 Past *due*, *overdue*, last chance
- 🔗 Subject lines that grasp **attention**
  - 🔗 Payment, change or update
- 🔗 Acting with **authority**
  - 🔗 Boss, coworker or contractor
- 🔗 **Requests** for personal/sensitive information
  - 🔗 *Random* demands



# Recognizing Phishing Attempts

## Mismatched email addresses

- Email doesn't match **sender name**

## Incorrect Website spelling

- Slight alteration in **ending**
  - @fortlauderdale.gov (right)
  - @fort1auderda1e.xyz (wrong)

## Generic greetings

- **Avoidance** of name
  - Hello Customer
  - Hello Sir or Madam

## Grammatical errors

- **Spelling** mistakes
- Poor sentence structure
- Incorrect punctuation usage



# Recognizing Phishing Attempts

## Website spoofing

- Sites that **mocks** the **look** of a legit site.

## Unexpected Attachments

- **Avoid** .iso, .exe, zip files and **unverified** office documents

## Confirm Links

- Hover over links to **confirm** where you are being **directed**.



Dear Employee,

This is a final notification regarding the dispatch of your recent printer order. Your Canon image CLASS MF465dw Monochrome Printer has been processed and is awaiting release from our warehouse. Please verify all shipping and payment details to avoid delivery delays.

**Order Summary:**

- **Item:** Canon CLASS MF465dw Laser Printer
- **Quantity:** 1 Unit
- **Status:** Pending Address Confirmation
- **Scheduled Delivery Date:** July 12, 2025
- **Tracking ID:** [#CNMF465-FTL2025](#)

**To confirm your order or view the shipment details, please click the following link: [fortlauderdale.gov](https://fortlauderdale.gov)**

*Note:* Accessing the dispatch portal requires authentication of your billing email domain.

**Billing Details:**

- **Company:** City of Fort Lauderdale Department
- **Shipping Address:** 100 N. Andrews Avenue Fort Lauderdale, FL 33301
- **Invoice Amount:** \$389.99 USD
- **Payment Type:** ACH Verification Required

**⚠ URGENT:** Your account is currently unverified. Please complete the billing check by replying to this message with your company's financial contact information. Failure to confirm will result in shipment hold and service fee reassessment.

For technical support or to cancel the order, contact our customer care agent: [✉ Email: jasmine.rivera@edg-etechs-secure-mail.co](mailto:jasmine.rivera@edg-etechs-secure-mail.co) [📞 Phone: +1 \(954\) 944-0613](tel:+19549440613)

We appreciate your prompt attention to this matter and hope to continue serving your office automation needs.

Sincerely,

Dear Employee,

This is a final notification regarding the dispatch of your recent printer order. Your Canon image CLASS MF465dw Monochrome Printer has been processed and is awaiting release from our warehouse. Please verify all shipping and payment details to avoid delivery delays.

**Order Summary:**

- **Item:** Canon CLASS MF465dw Laser Printer
- **Quantity:** 1 Unit
- **Status:** Pending Address Confirmation
- **Scheduled Delivery Date:** July 12, 2025
- **Tracking ID:** #CNMF465-FTL2025

<https://www.getcybersafe.gc.ca/en/blogs/why-you-shouldnt-click-links-suspicious-messages>  
Ctrl+Click to follow link

To confirm your order or view the following link: [fortlauderdale.gov](https://www.fortlauderdale.gov) please click

Note: Accessing the dispatch portal requires authentication of your billing email domain.

**Billing Details:**

- **Company:** City of Fort Lauderdale Department
- **Shipping Address:** 100 N. Andrews Avenue Fort Lauderdale, FL 33301
- **Invoice Amount:** \$389.99 USD
- **Payment Type:** ACH Verification Required

**⚠ URGENT:** Your account is currently unverified. Please complete the billing check by replying to this message with your company's financial contact information. Failure to confirm will result in shipment hold and service fee reassessment.

For technical support or to cancel the order, contact our customer care agent: [Email: jasmine.rivera@edg-etechs-secure-mail.co](mailto:jasmine.rivera@edg-etechs-secure-mail.co) [Phone: +1 \(954\) 944-0613](tel:+19549440613)

We appreciate your prompt attention to this matter and hope to continue serving your office automation needs.

Sincerely,

Fw: [EXTERNAL:CAUTION!]- You have a refund coming

**From:** State Farm <statefarm@mail-company.net>  
**Sent:** Tuesday, July 8, 2025 3:17 PM  
**To:** Joseph DellaVecchia <JDellaVecchia@fortlauderdale.gov>  
**Subject:** [EXTERNAL:CAUTION!]- You have a refund coming

[::CAUTION!:] This email originated from *outside* The City of Fort Lauderdale.  
Do Not Reply, click links, or open attachments from an unknown or suspicious origin. Confirm the email address is from an expected source before taking action.  
Report any suspicious emails to [spamadmin@fortlauderdale.gov](mailto:spamadmin@fortlauderdale.gov)



Hello Joseph,

You have a \$51.58 refund coming.

To get your refund faster, **select your refund method within three business days**. You can choose the specific financial account where you want us to send the refund.

If you don't take action, we'll refund the money to your saved financial account.

[Select refund method](#)

Email intended for: [JDellaVecchia@fortlauderdale.gov](mailto:JDellaVecchia@fortlauderdale.gov)

You received this email because you have a State Farm policy/account or there is a policy/account for which you have legal authority to represent the named insured (eg, business entity, trust or estate); or you requested information from State Farm.

For your protection, do not include sensitive personal information such as credit/debit card number, financial account number, driver's license number, or health/medical information in an email. Call your State Farm agent or [State Farm customer service](#) to discuss sensitive information.

[Contact Us](#)

[Privacy Policy](#)

[Terms of Use](#)

[Manage Preferences](#)

*Like a good neighbor, State Farm is there.*



**From:** State Farm <statefarm@mail-company.net>

**Sent:** Tuesday, July 8, 2025 3:17 PM

**To:** Joseph DellaVecchia <JDellaVecchia@fortlauderdale.gov>

**Subject:** [EXTERNAL:CAUTION!]- You have a refund coming



**From:** State Farm <statefarm@mail-company.net>  
**Sent:** Tuesday, July 8, 2025 3:17 PM  
**To:** Joseph DellaVecchia <JDellaVecchia@fortlauderdale.gov>  
**Subject:** [EXTERNAL:CAUTION!]- You have a refund coming

[::CAUTION!:] This email originated from *outside* The City of Fort Lauderdale.  
Do Not Reply, click links, or open attachments from an unknown or suspicious origin. Confirm the email address is from an expected source before taking action.  
Report any suspicious emails to [spamadmin@fortlauderdale.gov](mailto:spamadmin@fortlauderdale.gov)



Hello Joseph,

You have a \$51.58 refund coming.

To get your refund faster, **select your refund method within three business days**. You can choose the specific financial account where you want us to send the refund.

If you don't take action, we'll refund the money to your saved financial account.

[Select refund method](#)

**From:** State Farm <statefarm@mail-company.net>  
**Sent:** Tuesday, July 8, 2025 3:17 PM  
**To:** Joseph DellaVecchia <JDellaVecchia@fortlauderdale.gov>  
**Subject:** [EXTERNAL:CAUTION!]- You have a refund coming

[::CAUTION!:] This email originated from *outside* The City of Fort Lauderdale.  
Do Not Reply, click links, or open attachments from an unknown or suspicious origin. Confirm the email address is from an expected source before taking action.  
Report any suspicious emails to spamadmin@fortlauderdale.gov



Hello Joseph,

You have a \$51.58 refund coming.

To get your refund faster, **select your refund method within three business days**. You can choose the specific financial account where you want us to send the refund.

If you don't take action, we'll refund the money to your saved financial account.

[Select refund method](#)

# Future Phishing Attempts?

## AI Writing



### What is AI's effect?

Creates **personalized** messages

Can build trust through **responses**

**Avoids** grammatical errors



### How to detect AI?

**Patterns** in punctuation or **sentence** structure

**Fluid** message

**Inconsistent** point of view

# Future Phishing Attempts Deepfake



## What is it

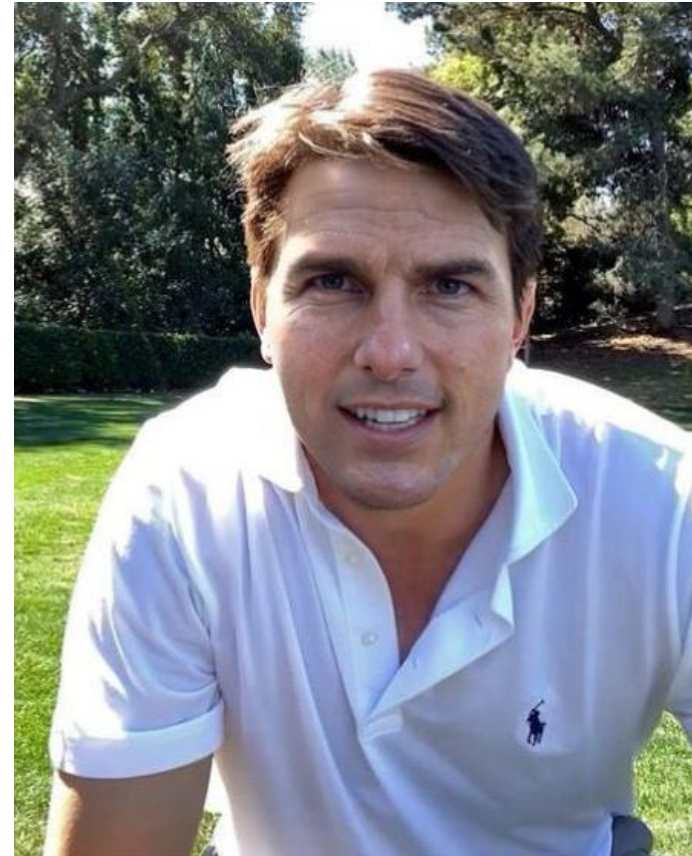
**Artificial** cloning of a human face or voice  
Impersonation of a **credible** person  
Applied to **videos** and **calls**



## How to detect it?

**Imperfection** on the face (blur, loss of facial hair)  
**Robotic** tone (monotone/lacks emotion)  
Inconsistent lighting  
**Irregular** actions (breathing, blinking, lip movements)

# Which Image is the **deepfake**?



# Detect the **deepfake**



# Detect the deepfake

Professor Mollick (PhD and MBA)



# Detect the deepfake

Professor Mollick (PhD and MBA)





ORIGINAL

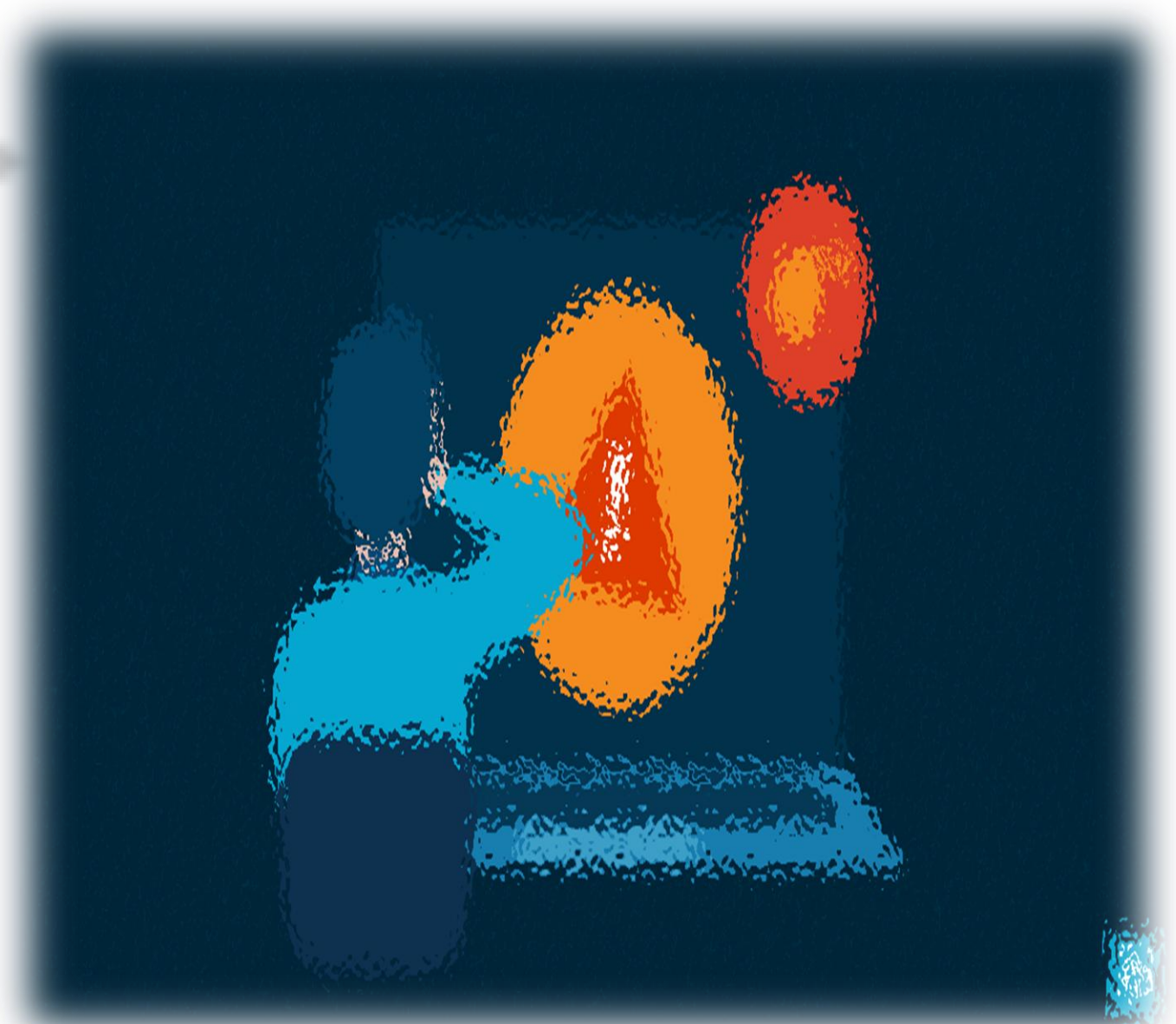


DEEPPFAKE

---

Why is all this important to you?

- 74% of incidents caused by **human error**
  - **Minor** mistakes can have **costly** effects



---

# Phishing Repercussions

- ❖ Financial Loss
- ❖ Loss of personal data
- ❖ Identity theft



---

# What to do if you fall victim?

- **CHANGE YOUR PASSWORDS IMMEDIATELY**
- Sign out of all related accounts on all devices
- Call your financial institution and report fraud
- Run antivirus scan ( Norton, Malwarebytes, AVG )
- Check your computer for extra users ( I can send out a guide )
- Put a freeze on your credit (Calling Experian, TransUnion, and Equifax )
- In terms of Ransomware or persistent Scareware, "reimage" or have the computer professionally wiped





CITY OF  
FORT  
LAUDERDALE

# Quick Tips

# Quick Tips

- ⚠ Stay vigilant, think before you:
  - ⚠ **Click** links and attachments
  - ⚠ **Respond** to emails and phone calls
- ⚠ Use **strong** password: alphanumeric, upper and lowercase, special symbols
- ⚠ Keep software **updated**, stay connected to **VPN**, clear (browser) **cookies**
- ⚠ Pay attention to **red** flags: Grammatical errors, general greeting, tone of urgency, request for personal information or login credentials
- ⚠ Utilize Multi-Factor Authentication (**MFA**)
- ⚠ **Back-up** data

# Quick Tips: QR Codes

- Always be wary of randomly placed QR codes
- If they are associated with a business, you can always ask for the original document ( like an application or a menu )
- If the QR code is only, you can hover your mouse over to see where it links to





CITY OF  
FORT LAUDERDALE

---

**Any Questions?**

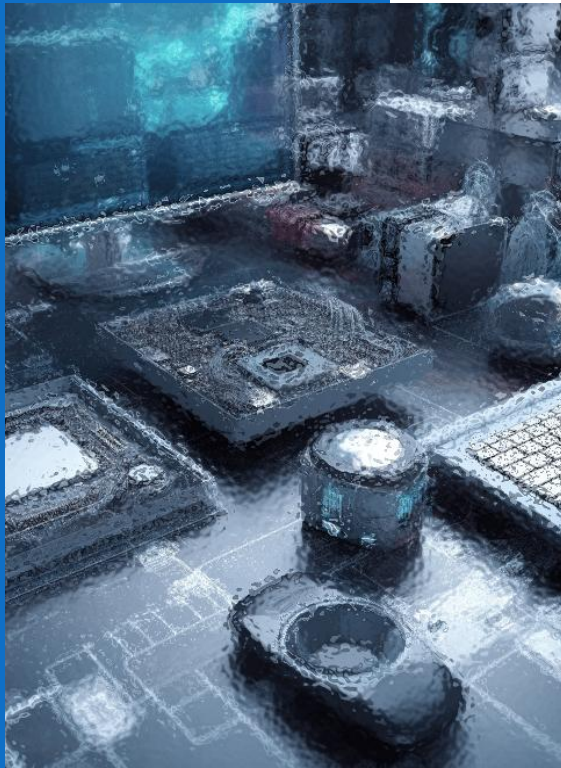


CITY OF  
FORT LAUDERDALE

---

**Thank You!**

# References



[74% Data Breaches Are Due to Human Error | Infosec](#)

[What is Domain Spoofing? Learn How to Stop This Cyber Threat](#)

[How AI is Used in Social Engineering Attacks | Advanced Cyber Threats & Protection Strategies - Web Asha Technologies](#)

[Overview < Detect DeepFakes: How to counteract misinformation created by AI — MIT Media Lab](#)

[4 Ways to Detect and Verify AI-generated Deepfake Audio](#)

[Atlanta Ransomware Case Study | Avast Business](#)

[Cyber Case Study: City of Atlanta Ransomware Incident - CoverLink Insurance - Ohio Insurance Agency](#)

[A Review of Colonial Pipeline Ransomware Attack](#)

[Colonial Pipeline attack: Everything you need to know | ZDNET](#)

[The Curious Case of the Baltimore Ransomware Attack: What You Need to Know](#)

[A Timeline of the Baltimore City Ransomware Attack | Cyware](#)

[wisdompress.co.in/wp-content/uploads/2023/10/Modern-Administrative-Techniques.pdf#page=85](#)

[What is a Trojan Horse Virus? \(Unmasking Hidden Threats\)](#)

[What is Ransomware? | Ransomware protection](#)

[What Is a Trojan Horse? Trojan Virus and Malware Explained | Fortinet](#)

[What is Malware? And its Types - GeeksforGeeks](#)