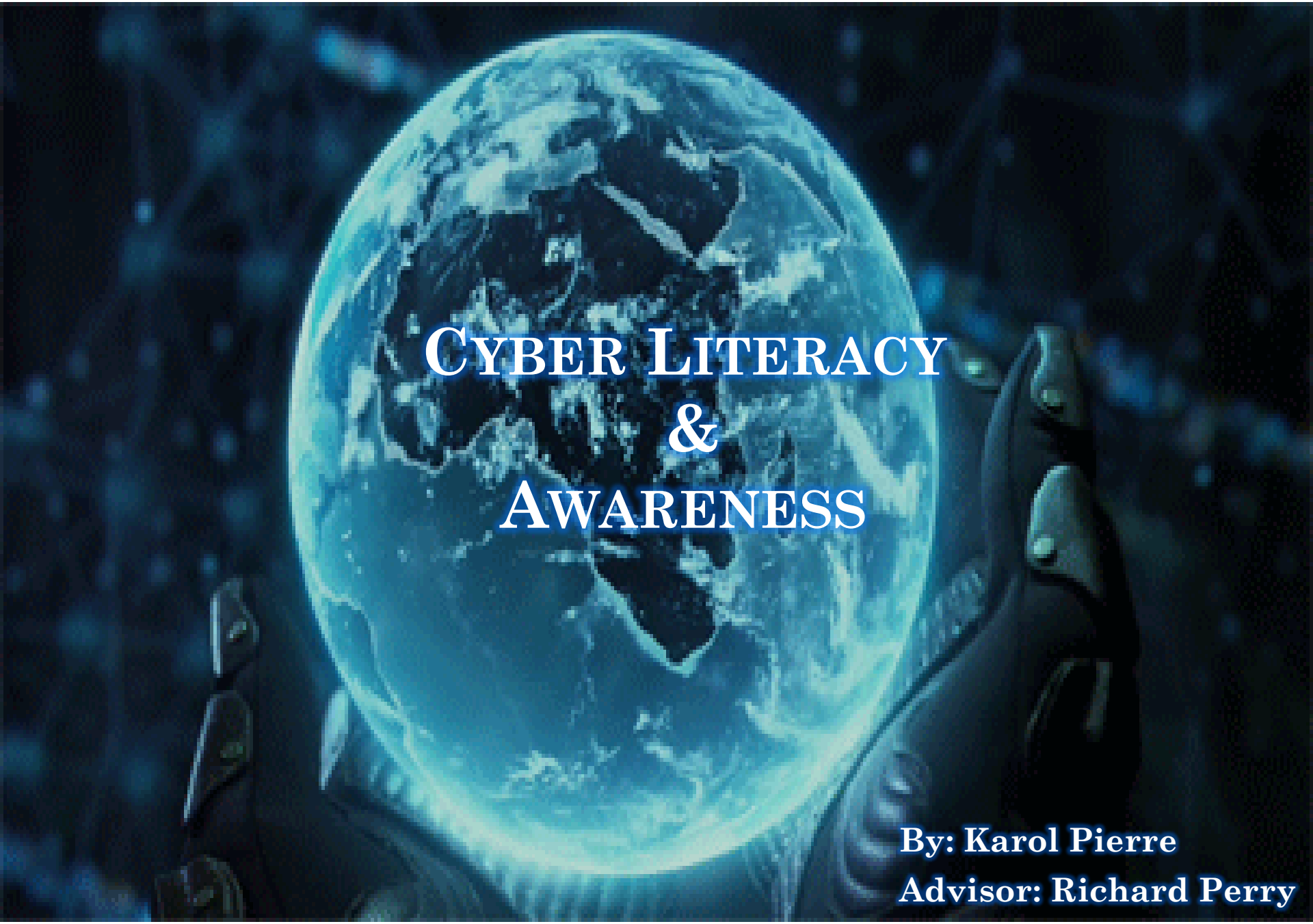

Cyber Literacy
&
Awareness
By: Karol Pierre
Advisor: Richard Perry

# TYPES OF ATTACKS




- **Attacker Techniques**
  - **Adware** : digital advertisments that automatically display when a user is online
  - **Scareware** : Victims are bombarded with false alarms and threats, prompting immediate action
  - **Pretexting** : Attacker gains trust by impersonating an official position (bank, tax-officials, police) , ask questions to confirm identity (actually stealing info)
  - **Phishing** : email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims
  - **Spear-phishing** : similar to phishing, but directed at a specific target and requires more time

# Phishing Example & Detection

From: Bank of America <crvdgi@comcast.net>
Subject: **Notification Irregular Activity**
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdgi@comcast.net

**Check the from for legit email**

Bank of America

**Online Banking Alert**

**Would be capitalized**

**Dear member:**

We detected unusual activity on your Bank of America debit card on **09/22/2014**.
For your protection, please verify this activity so you can continue making debit card transactions without interruption.
**Please sign in to** your account **at** https://www.bankofamerica.com
to review and verify your account activity, After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.
If you do not contact us, certain limitations may be placed on your debit card.

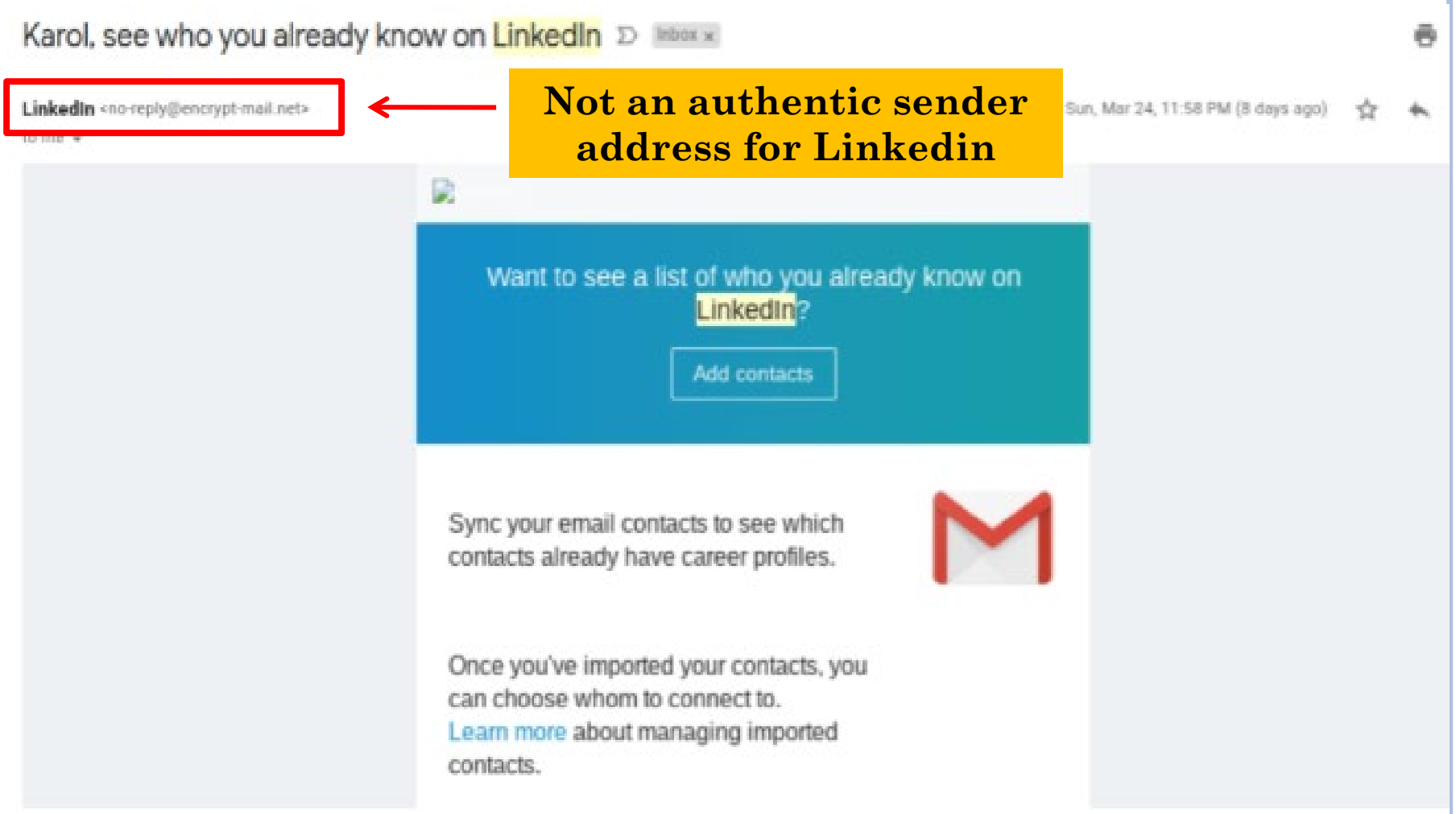
**Hover over link to verify whether link is authentic**

http://bit.do/ghsdfhgsd

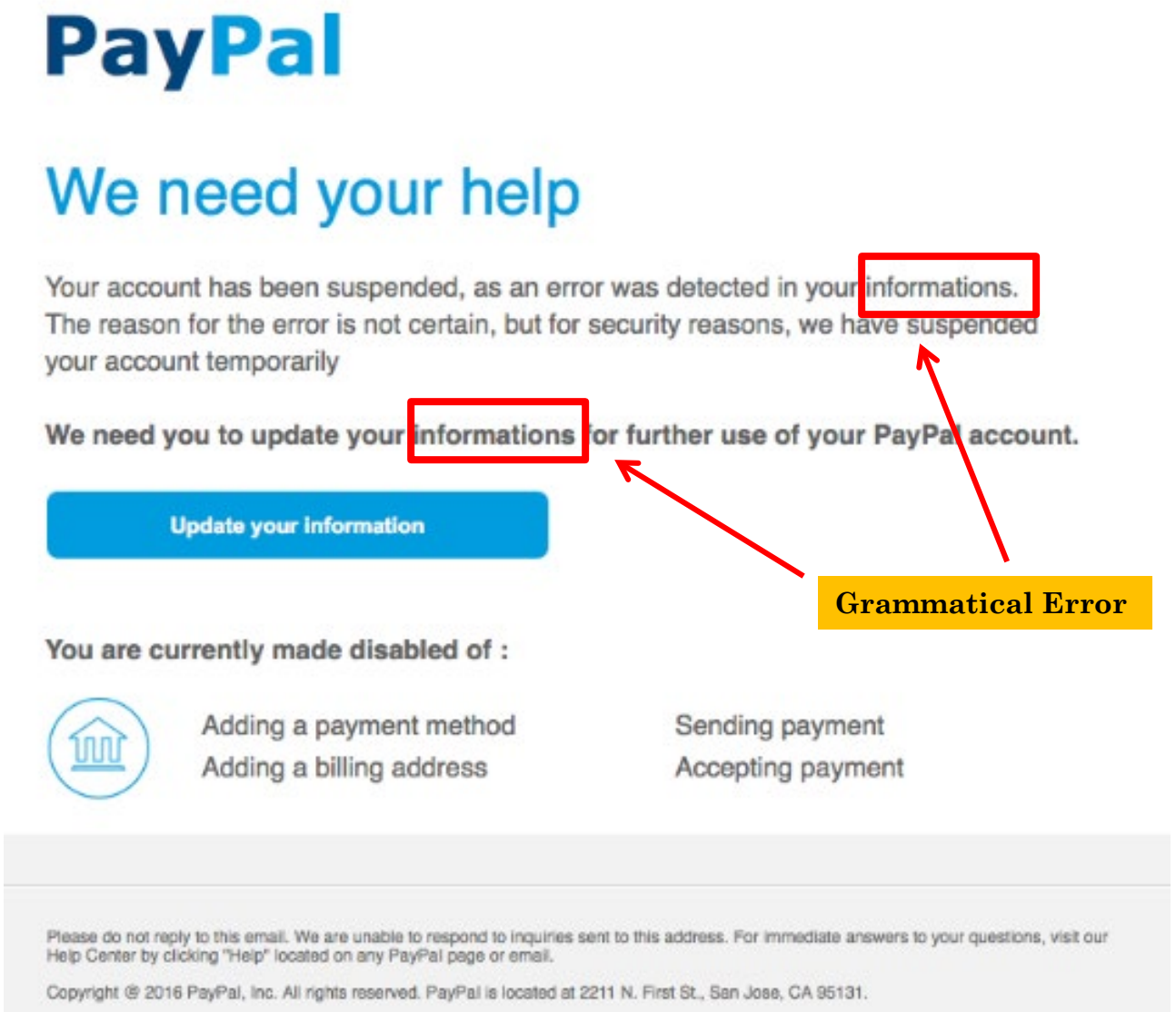
© 2014 Bank of Ame ts reserved.

**Grammatical Error:** *use of comma instead of period*

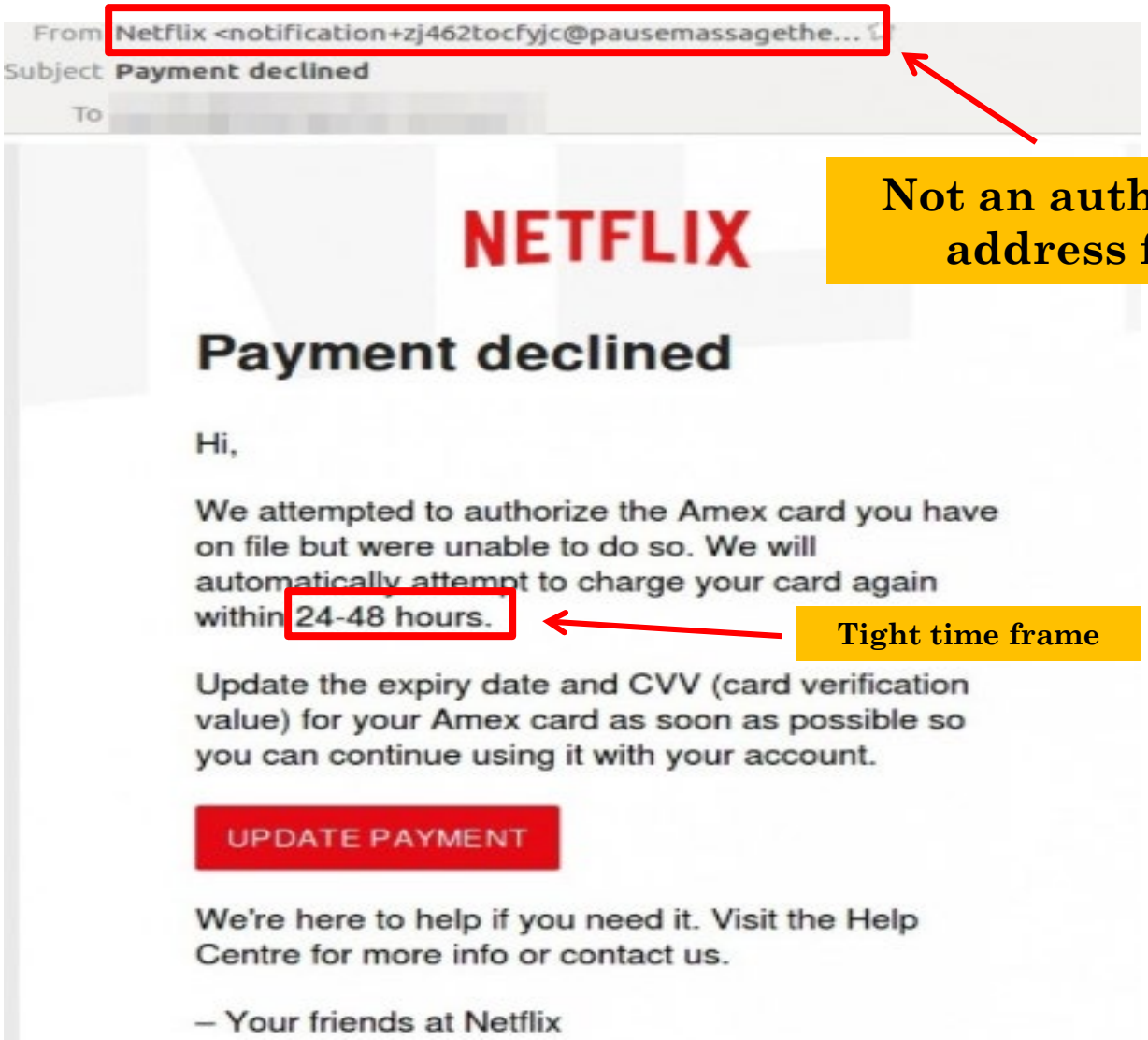
# Phishing Example & Detection



# Phishing Example & Detection



# Phishing Example & Detection




**Not an authentic sender address for Netflix**

**Tight time frame**

# Scareware Example & Detection




The goal is to alarm and convince you

# Adware Example & Detection




**Aims to lure user by using word "free"**

# IMPLICATIONS




- Identity Theft
- Theft of Credit Card Information
- Personal Data Exfiltration:
  - SSN, Insurance, and more
- Human Trafficking
- Blackmail
- Extortion



# Preventive Measures

- Don't Open emails and attachments from suspicious sources




- Be wary of tempting offers
- Secure Computing devices
  - Antivirus/Anti-malware, Firewall, email filters, passwords, multifactor authentication
- Slow down
  - Make sure to take your time
  - Read everything through




- Foreign offers are fake
- Beware of any download link

# Cited Works


- https://securityiq.infosecinstitute.com/Templates/index
- https://www.us-cert.gov/ncas/tips/ST04-014
- https://www.incapsula.com/web-application-security/social-engineering-attack.html
- https://towardsdatascience.com/applied-text-classification-on-email-spam-filtering-part-1-1861e1a83246