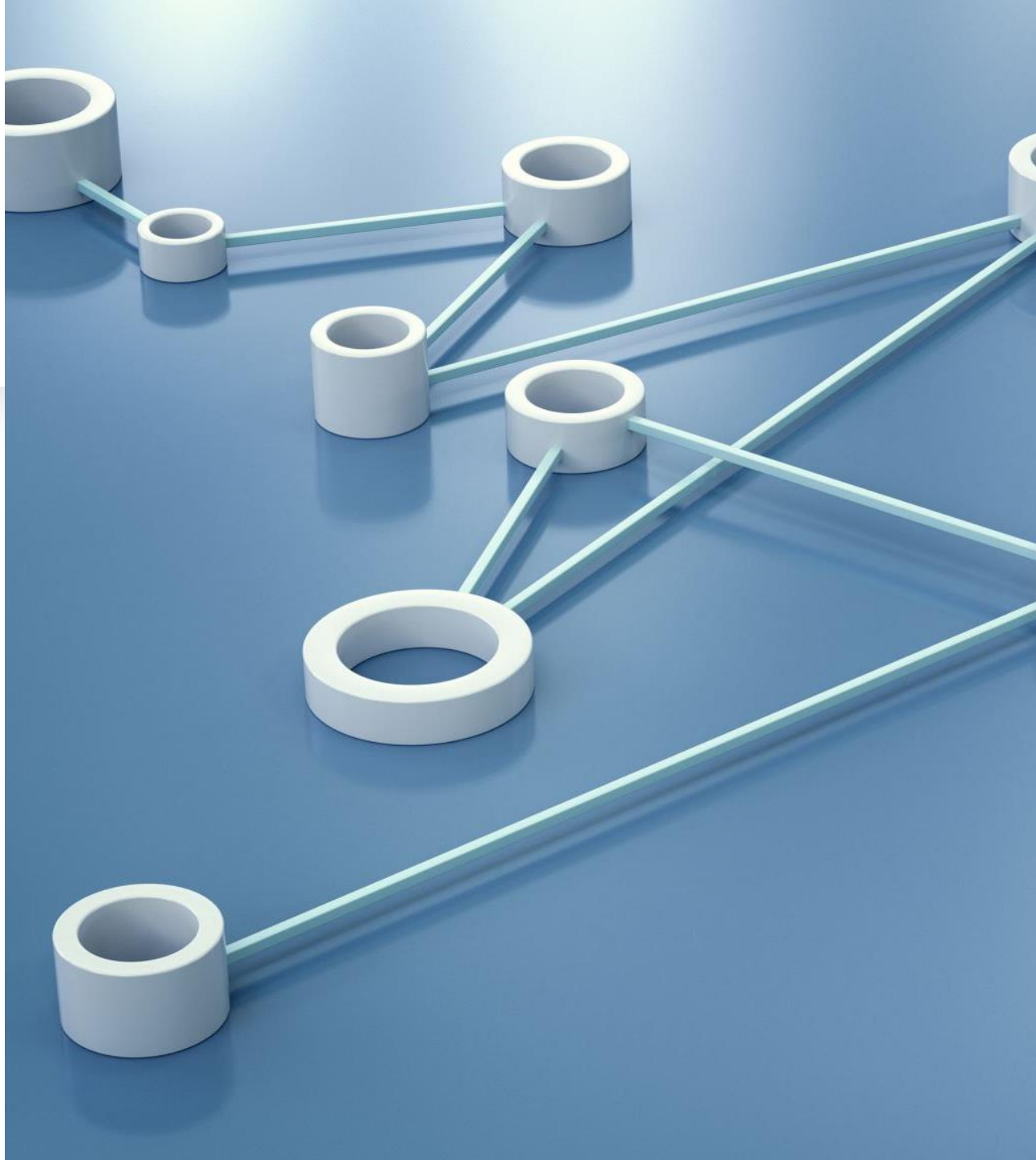
Phishing Awareness Training

Recognizing and Avoiding Online Threats

What is Phishing?

- Phishing is a cybercrime where attackers pose as legitimate entities to trick individuals into revealing sensitive information.
- Goal: To steal personal data, financial information, or gain unauthorized access to systems.
- Methods: Primarily through deceptive emails, websites, and social engineering tactics.



The Evolution of Phishing

1990s: Early phishing attacks via AOL messenger

2000s: Email phishing becomes widespread

2010s: Spear phishing and sophisticated social engineering tactics emerge

Present: Multi-channel attacks including SMS, voice, and social media

Common Types of Phishing Attacks

Email phishing: Mass-sent fraudulent emails

Spear phishing: Targeted attacks on specific individuals or organizations

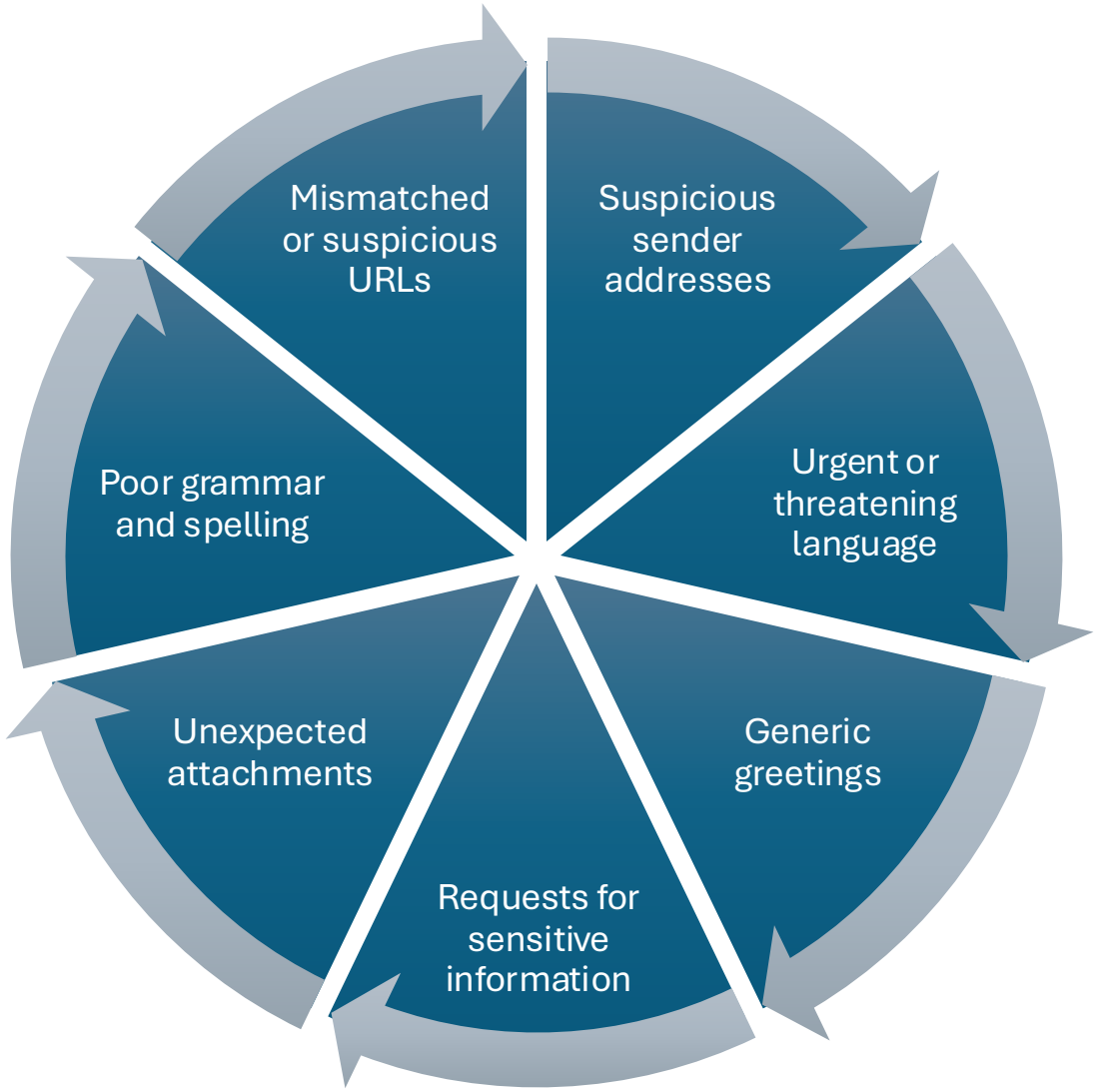
Whaling: Targeting high-profile executives

Smishing: Phishing via SMS or text messages

Vishing: Voice phishing over phone calls

Search engine phishing: Creating fake websites to appear in search results

Recognizing Phishing Emails



Identifying Fake Websites

Check	Check the URL carefully (look for slight misspellings)
Verify	Verify HTTPS and the padlock icon in the address bar
Be	Be wary of lookalike domains
Check	Check for poor design or unprofessional appearance
Verify	Verify site legitimacy through official channels or by directly typing the known URL

Social Engineering Tactics

- Impersonation of authority figures
- Creating a sense of urgency
- Exploiting fear or greed
- Pretexting (creating a fabricated scenario)
- Baiting with free offers or prizes

Best Practices for Avoiding Phishing

1. Use strong, unique passwords for each account
2. Enable two-factor authentication wherever possible
3. Keep software and systems updated
4. Use reputable anti-virus and anti-malware software
5. Be cautious with unexpected emails or messages
6. Verify requests through separate, known channels
7. Don't click on suspicious links or download unexpected attachments
8. Use email filters and spam blockers

What to Do If You Suspect Phishing

DON'T CLICK ANY LINKS OR DOWNLOAD ATTACHMENTS

REPORT THE SUSPICIOUS EMAIL TO YOUR IT OR SECURITY TEAM

DELETE THE EMAIL

IF YOU'VE ENTERED INFORMATION, CHANGE PASSWORDS IMMEDIATELY

MONITOR YOUR ACCOUNTS FOR ANY SUSPICIOUS ACTIVITY

Real-World Phishing Examples

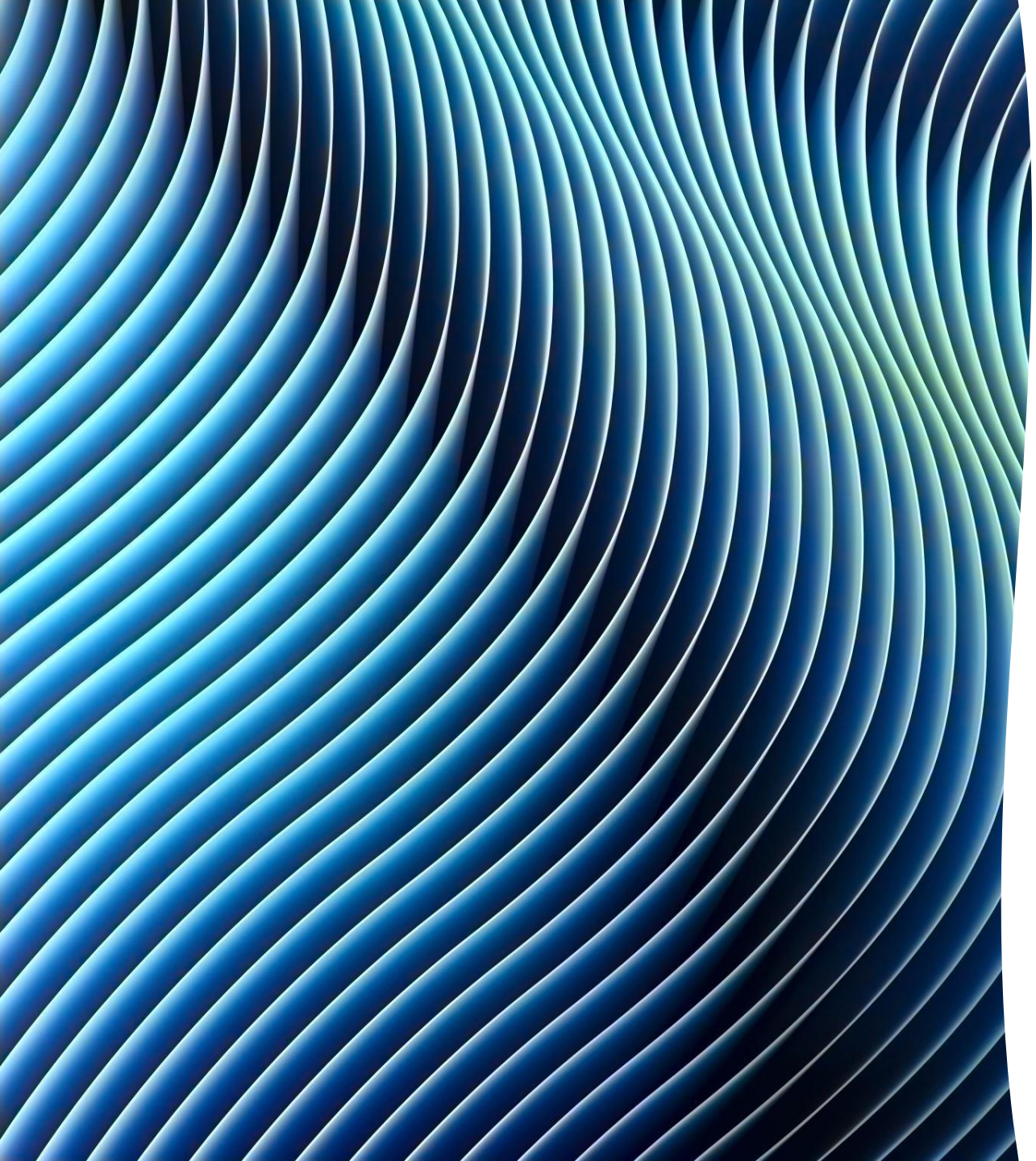
- Fake Bank Email (Wells Fargo)
- Source: Federal Trade Commission (FTC) https://consumer.ftc.gov/consumer-alerts/2020/03/scammers-spoofing-fbi-email-addresses
- Description: In this phishing attempt, scammers impersonated Wells Fargo bank, sending emails claiming that the recipient's account had been locked due to "unusual login attempts."

Red Flags:

- Urgent language creating panic ("Your account has been locked!")
- Generic greeting ("Dear Valued Customer")
- Request to click a link to "verify" account details
- Threat of account closure if not acted upon quickly
- Subtle errors in the bank's logo or formatting

Social Media Account "Verification" Message (Instagram)

- Source: Instagram Help Center https://help.instagram.com/416988132142112
- Description: This phishing attempt targets Instagram users, claiming their account needs verification to avoid being disabled. The message often appears to come from "Instagram Support" or a similar official-sounding name.

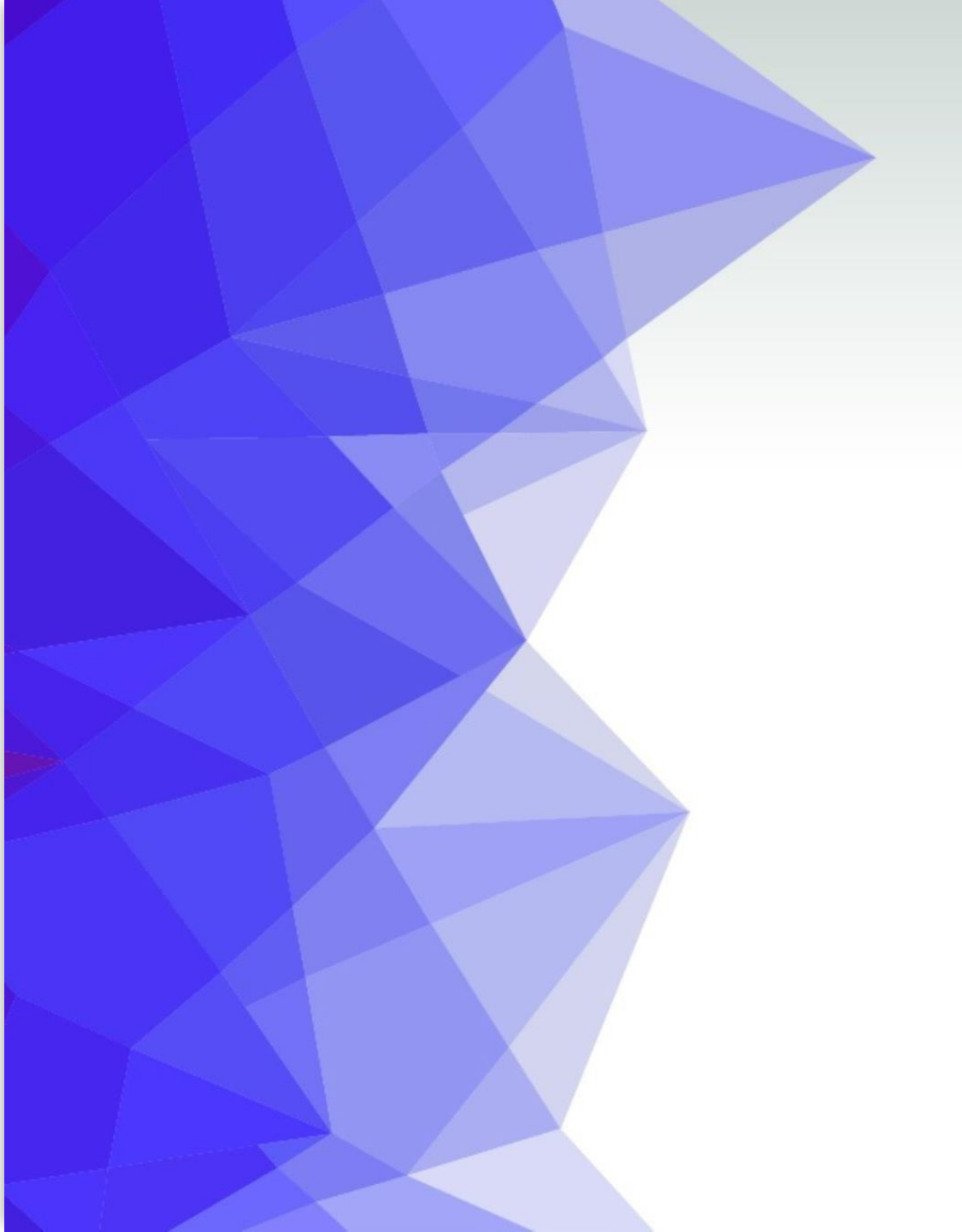


Red Flags:

- Unsolicited message about account verification
- Link to a fake Instagram login page
- Pressure to act quickly to avoid account suspension
- Use of Instagram's logo and color scheme to appear legitimate
- Sent as a direct message rather than through official channels

Fake Package Delivery Notification (FedEx)

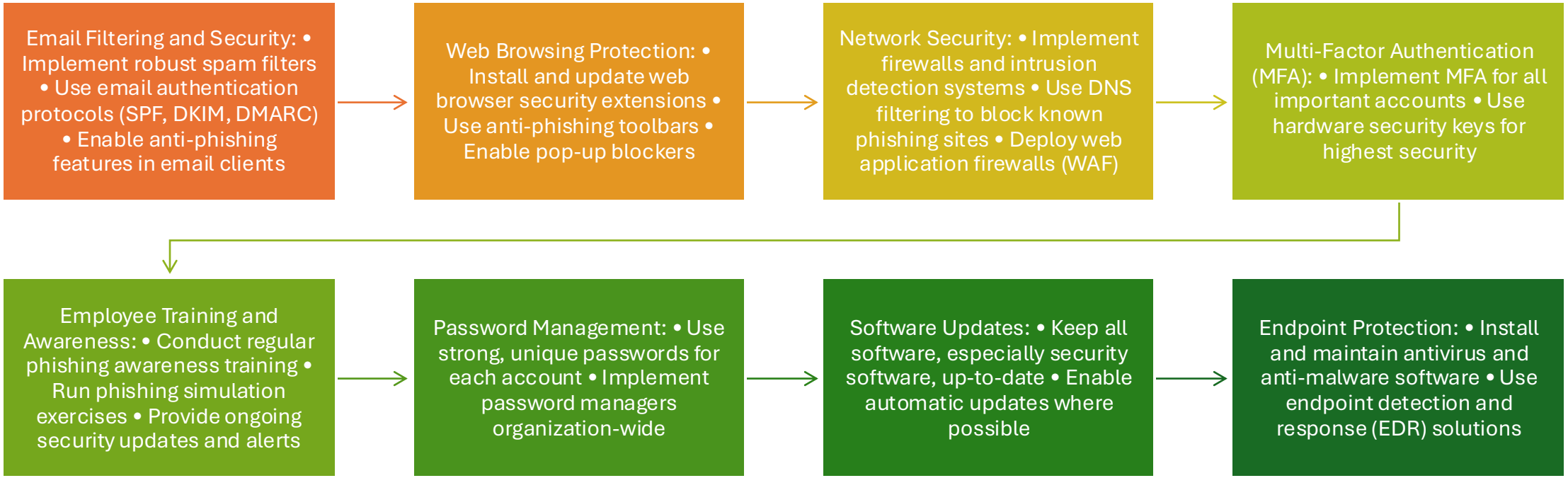
- Source: FedEx Security Alert https://www.fedex.com/en-us/trust-center/fraud-awareness.html
- Description: This phishing scam involves an email or text message claiming to be from FedEx, stating that a package couldn't be delivered due to an incorrect address or unpaid customs fees.



Red Flags

- Unexpected delivery notification
- Request to open an attachment to see delivery details
- Pressure to respond quickly to avoid return shipping fees
- Generic sender email address not matching official FedEx domains
- Poor grammar or spelling errors

Countermeasures For Phishing



Conclusion

Phishing is a prevalent and evolving threat

Always verify unexpected requests for information

Check email addresses, URLs, and website security

Report suspicious activities promptly

Continuous learning and awareness are crucial

Thank You