Cybersecurity Awareness: Understanding Email Threats

Different Types of Spear Phishing:

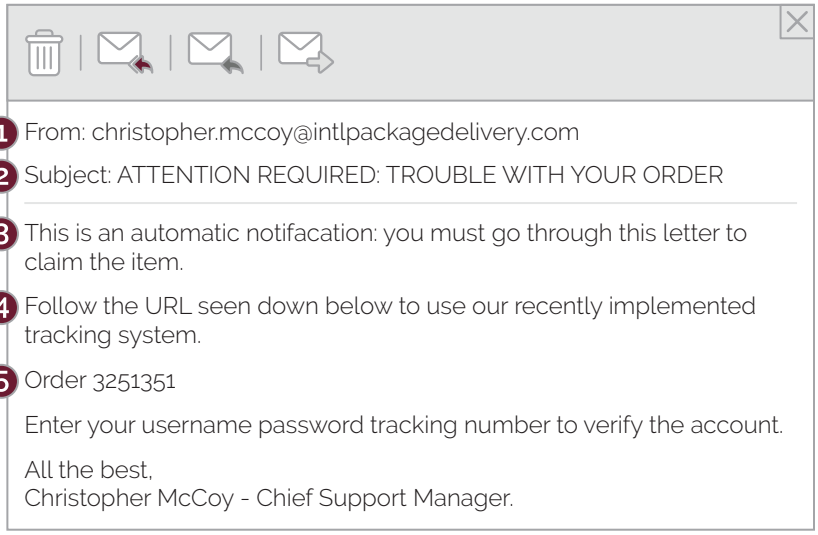
Click Only:
Prompt you to click on a malicious link

Credential:
Prompt you to enter your login usernames and passwords under the pretext of accessing a legitimate looking website

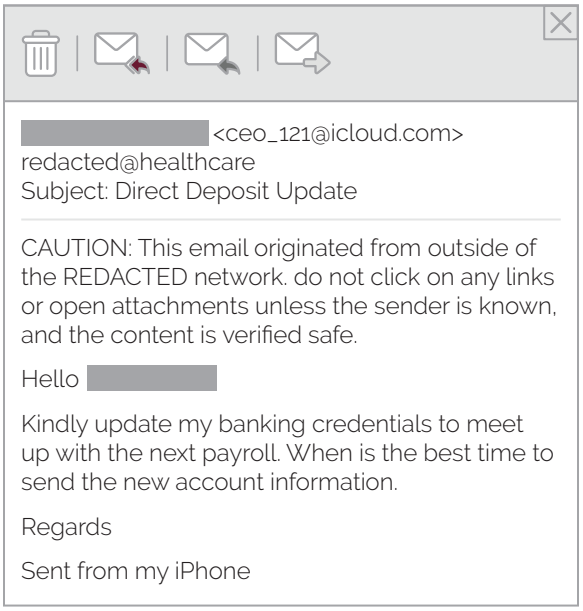
Attachment:
Prompt you to download an infected attachment

Warning Signs of a Phish

1. **Unknown Sender –**
   - Do you recognize this sender?
2. **Emotional Appeal –**
   - It appeals to urgency, fear or desire.
3. **Spelling/Grammatical Errors**
4. **URL Link –**
   - Urges to click a link or download attachments
5. **Solicits Sensitive Information –**
   - Like your password



There is a fourth type that has been added to the mix – **Business Email Compromise (BEC)**. These type of messages don't have any of the three elements mentioned above – but the threat actor is looking for you to interact with them. This type of email is easy to get through security gateways because there aren't any tactics or indicators that can be specific enough to block.



Business Email Compromise (BEC) Scams:

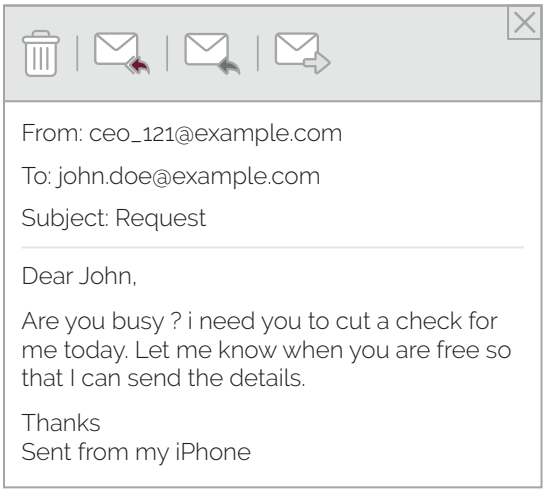
Traditionally impersonate executives or vendors/suppliers to solicit wire transfers or checks using emails

Evolved into Payroll Diversion Scams - appear to come from ANY employee to Finance or Human Resources

Payroll Diversion - Evolved BEC Scams

- Since threat actors have realized that emails from execs might garner more scrutiny, they are now pretending to be regular employees
- Emails are typically sent to Human Resources/Finance – anyone handling payroll
- These emails are typically focused around payroll requests
- Threat actors request a change to the payroll routing information – replace legit information with their bank information to route deposits into their accounts

Business Email Compromise Examples



From: ceo_121@example.com

To: john.doe@example.com

Subject: Request

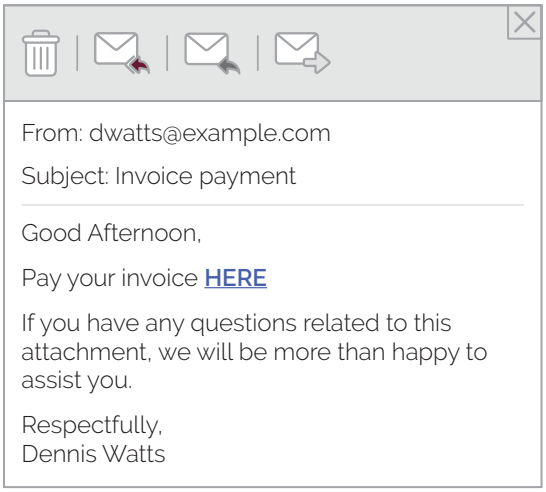
Dear John,

Are you busy ? i need you to cut a check for me today. Let me know when you are free so that I can send the details.

Thanks
Sent from my iPhone

CEO Fraud

- Threat actors have either spoofed or hacked an executive's email address and are attempting to exploit authority
- Email appears to come from the CEO of the company – a respected title that invokes the sense of urgency and importance
- Request from the CEO can "represent" urgency or an emergency
- Email has several typos
- Is this typical of how the CEO communicates? Is this a typical request from the CEO? Do they often send such requests from their phone?



From: dwatts@example.com

Subject: Invoice payment

Good Afternoon,

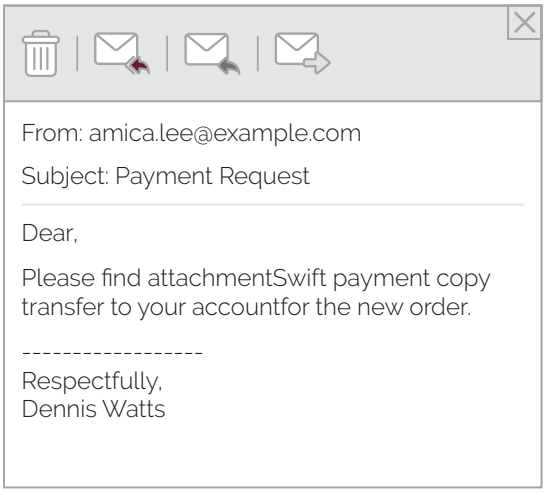
Pay your invoice HERE

If you have any questions related to this attachment, we will be more than happy to assist you.

Respectfully,
Dennis Watts

Bogus Invoice Email

- This appears to come from a vendor asking for payment of an invoice – typically a fake invoice
- The message contains a new location where you are instructed to wire the money



From: amica.lee@example.com

Subject: Payment Request

Dear,

Please find attachmentSwift payment copy transfer to your accountfor the new order.

Respectfully,
Dennis Watts

Payment Request Email

- Typically these emails might come from a hacked employee email address and might request payments from vendors in their address book
- Note the sender name is different from the signed name on the email
- There are grammatical errors/ no spacing
- There is no context to the payment request