**Analyze Phishing Email Sample.**

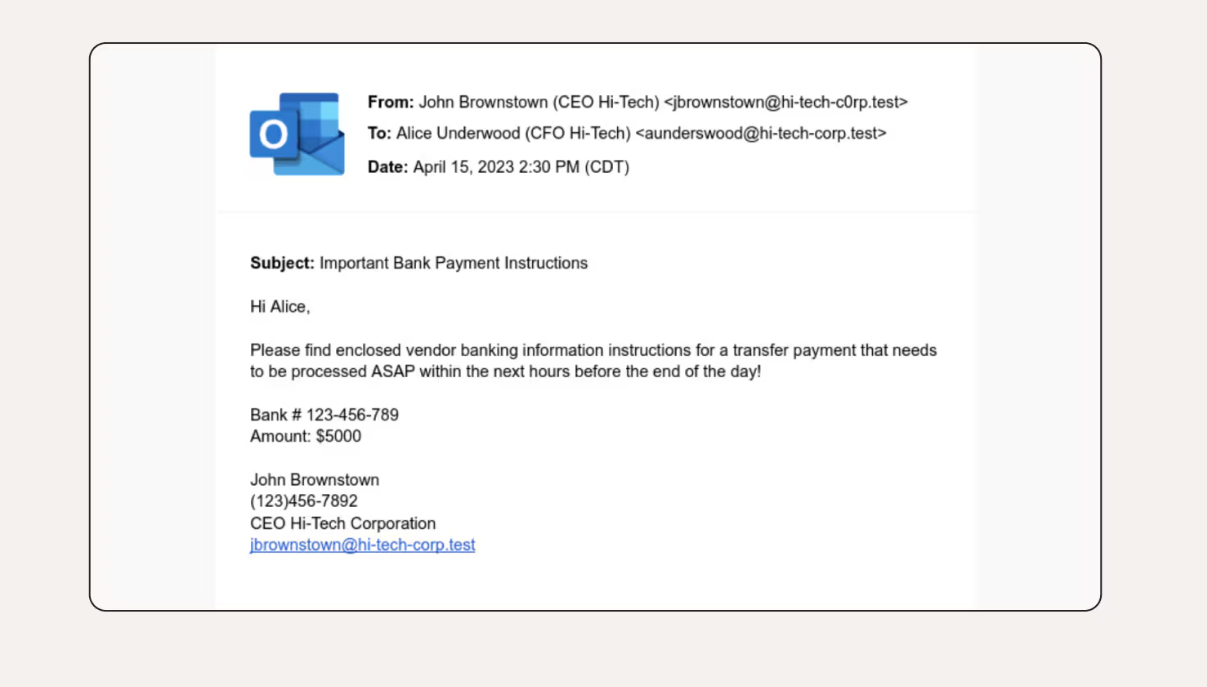
* **Familiarize yourself with phishing attacks**
* Phishing attacks use deceptive emails, texts, or calls to trick you into revealing sensitive information, like passwords or financial details, by pretending to be legitimate companies or people.
* These attacks exploit human psychology and can occur through various channels, including emails, text messages, and fake websites.
* **What is phishing?**
* Phishing is a type of cyberattack where attackers use social engineering to manipulate you into sharing personal or financial information.
* They do this by sending messages that appear to be from trusted sources, such as banks, popular websites, or even friends and family.
* These messages often contain links to fake websites, which are designed to steal your login credentials or other sensitive data**.**

* **Learn to spot phishing emails.**
* **Suspicious Sender Information**:
* Check the sender's email address for misspellings or unusual domains, even if the display name looks legitimate.
* **Generic Greetings**:
* Legitimate companies rarely use "Dear Customer" or other vague greetings in their communications.
* **Spelling and Grammar Errors**:
* Look for poor grammar, typos, and unnatural language, which are common in phishing emails.
* **Urgent or Threatening Tone**:
* Attackers often create a sense of urgency or fear to prompt you to act quickly without thinking.
* **Questionable Links and Attachments**:
* Never click on links or open attachments in unexpected messages. You can verify a link's legitimacy by hovering your mouse over it to see the actual URL.
* **Too-Good-To-Be-True Offers**:
* Be skeptical of offers that seem unreasonable or too good to be true.



* **Example of Phishing Email.**

****

* **Observations.**

1. The first thing to notice in this CEO phishing email example is the sender’s email doesn’t match the email in their email signature.
   * + Sender Mail Add- [jbrownstown@hi-tech-c0rp.test](mailto:jbrownstown@hi-tech-c0rp.test)
     + Email signature -[jbrownstown@hi-tech-corp.test](mailto:jbrownstown@hi-tech-corp.test)
2. The classic tactic of urgency is employed, giving the recipient little time to consider the request.

* *“Transfer payment that needs to be processed ASAP”.*

1. There are also grammatical errors and an unusual tone of voice—e.g., the CEO likely wouldn’t use formal language like “please find enclosed” to a CFO with whom he works closely.

* **How do we stop getting phished?**
* **Be Wary of Unsolicited Messages**:
* Exercise caution with any unsolicited communication that requests personal or financial information.
* **Verify Information Independently**:
* If you receive a suspicious message, do not use the contact information provided in the message. Instead, use a known phone number or website to contact the company directly and verify their request.
* **Use Strong Security Measures**:
* Enable two-factor authentication (2FA) for your accounts to add an extra layer of security.
* **Keep Software Updated**:
* Regularly update your antivirus software and other security software to protect against malware and other threats.
* **Stay Informed**:
* Education is a critical defense; stay knowledgeable about common phishing tactics

