DON'T BE A VICTIM OF

PHISHING

What is phishing? Phishing is a scam tactic fraudsters use to impersonate a person or business in order to obtain money or sensitive information from an unsuspecting victim.

How does it work? Scammers use public information sources such as websites, LinkedIn, or online directories to try to be as convincing as possible to the recipient. The messages aren't always flagged by spam filters, so human error is possible. In addition to posing as a company executive, fraudsters are also impersonating the IRS, USPS, Amazon, QuickBooks invoices, and more.

KNOW WHAT TO LOOK FOR

Fraudsters are betting that an employee will glance at an email from a higher-up, overlooking the typos in the email address and the body of the message, simply because it's coming "from" a person of authority. ***See the red flags***

The next message will likely involve a request to purchase gift cards and reply to them with the card numbers and even your cell phone number. ***Don't fall for it!***

KNOW WHAT TO DO NEXT

Verify legitimacy
Review for the red flags on this handout. Separately contact the actual person or source.

Forward to IT
Still unsure? Ask your tech team to check it out and to block the suspicious sender.

Delete the message
Don't reply or click links. Never send sensitive info such as cell phone or routing numbers.

Always be vigilant
Scam artists continue to get more creative... ***Don't let your guard down!***

Report fraud: If you realize after the fact that you may be a scam victim, come forward to try to remediate the situation, take protective measures, or involve the authorities if needed.

ALLOY SILVERSTEIN

SCAMMER

RED FLAGS

1 **URGENCY**
Scammers purposely utilize pressure and authority by posing to be an executive of a company. They typically want their request filled ASAP or EOD, while they have you "hooked."

2 **SUSPICIOUS DOMAIN**
Double check, even triple check, the domain of the email address. Slight variations of an email address are used intentionally. A gmail or other generic email domain can be another warning sign.

3 **TONE + TYPOS**
A big tell-tale for fraudsters tends to be spelling errors and poor grammar. Ask yourself, does the body of the message *sound* like the sender? Are their title and email signature correct?

4 **TOO VAGUE**
Phishing emails are often short and to the point, lacking context of the request. This can be a red flag, especially when received out of the blue.

5 **GIFT CARDS OR CRYPTO**
Whether pretending to be a CEO, CFO, or even the IRS, scammers' requests frequently involve purchasing gift cards, bitcoin, or demanding wire transfers.

6 **"OFF" FEELING**
Trust your gut! Weird time of day? Unexpected invoice? Not related to a project you've *ever* worked on before? Don't ignore your instincts.

PICK UP THE PHONE

...or walk down the hall or compose a fresh new email. The point is, you must ***independently verify*** the request with the "person" if you have *any* doubts at all—don't just reply to the email.