elphasecure.com



# 7 steps to avoid being tricked by cybercriminals

Social engineering claims in the form of fraudulent instructions are on the rise. Here are 7 steps you can take to defend against email and voice phishing.

### Be cautious with high-risk requests

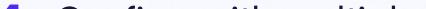
Always be vigilant when you receive email or phone instructions asking you to change banking information.

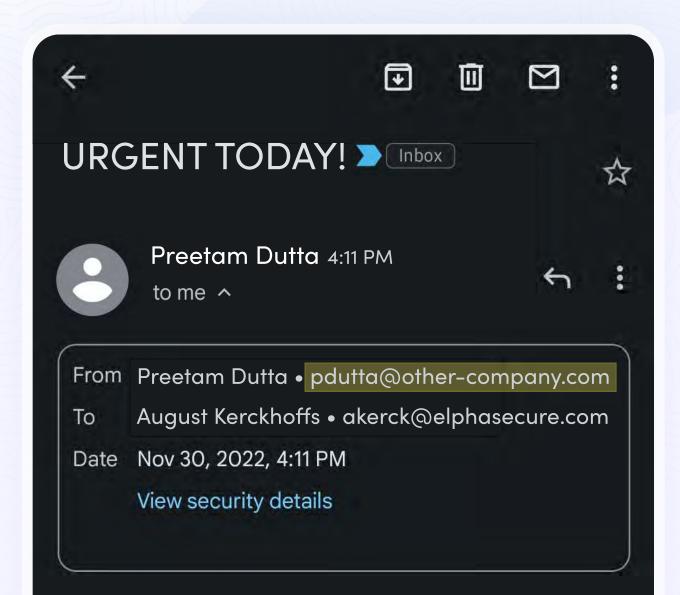
# Verify sender authenticity

Double-check the email address or phone number when receiving a request for banking information.

## Secondary communication methods

Use a second method to verify the request. Call a verified corporate number to confirm email requests.







#### Confirm with multiple people

By elevating high-risk requests to a second pair of eyes, such as a manager, you can limit your risk exposure.



#### Don't fall for pressure tactics

Look out for time-sensitive or hierarchical requests. Often our desire to be cooperative is emotionally manipulated.



### Look for Business Email Compromise

If a social engineering email is found, always investigate the potential for a email system compromise.

Use multi-factor authentication Implement multi-factor authentication (MFA) on all email accounts to mitigate Business Email Compromise.

Hi August,

I need you to run an urgent errand for me. Let me have a number i can text you on so i can text you what i need help with ASAP.

#### Thanks



Preetam K. Dutta, PhD **Chief Executive Officer** 

elphasecure.com

580 Fifth Avenue, Suite 820, New York, NY 10036



We recommend distributing this document to the appropriate individuals in your organization.

Insurance fused with security software for a complete defense. Have additional questions? Call (332) 242 6776 or visit elphasecure.com