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.

1 Be cautious with high-risk requests

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

2 Verify sender authenticity

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

3 Secondary communication methods

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

4 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.

5 Don’t fall for pressure tactics

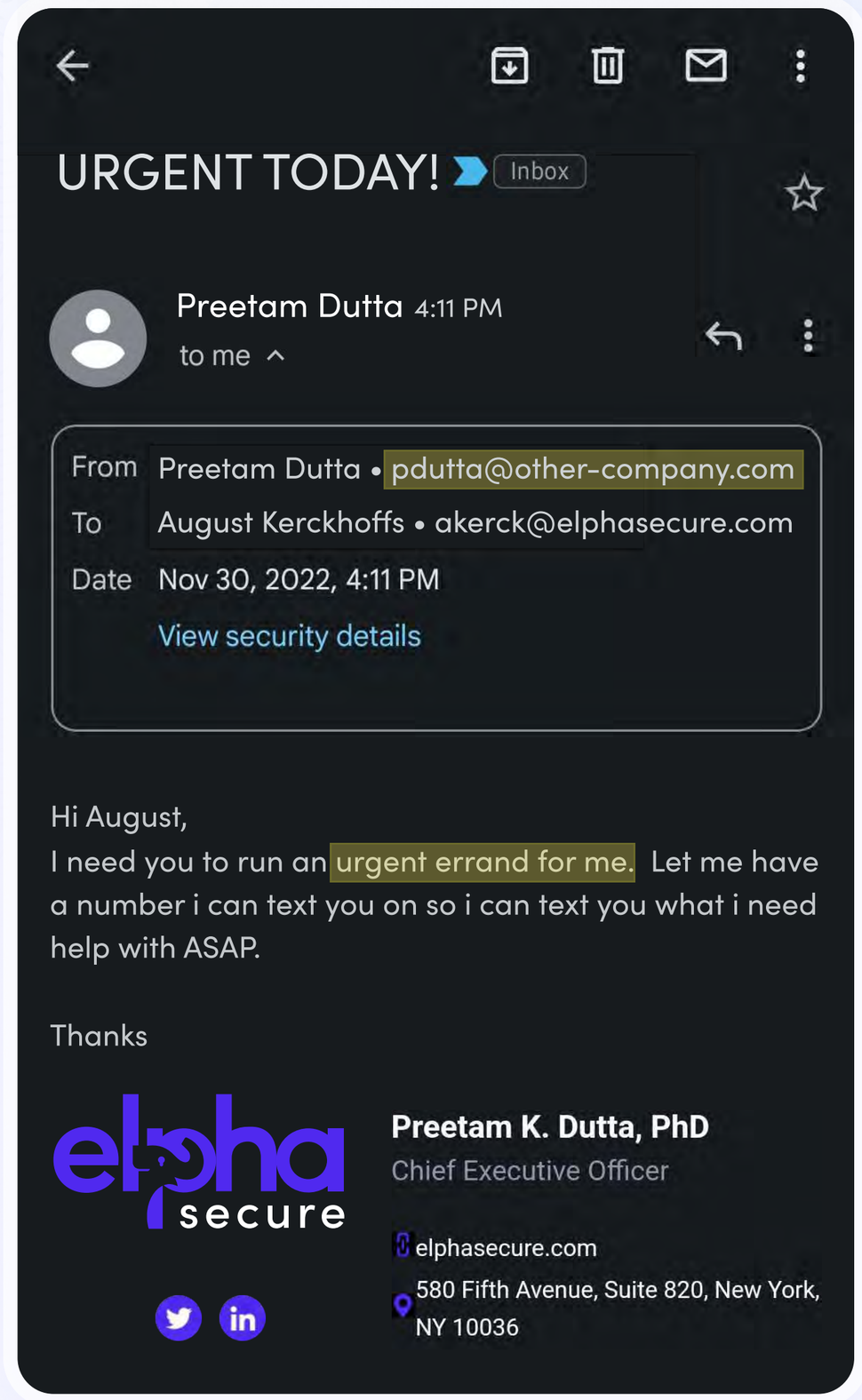
Look out for time-sensitive or hierarchical requests. Often our desire to be cooperative is emotionally manipulated.

6 Look for Business Email Compromise

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

7 Use multi-factor authentication

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



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