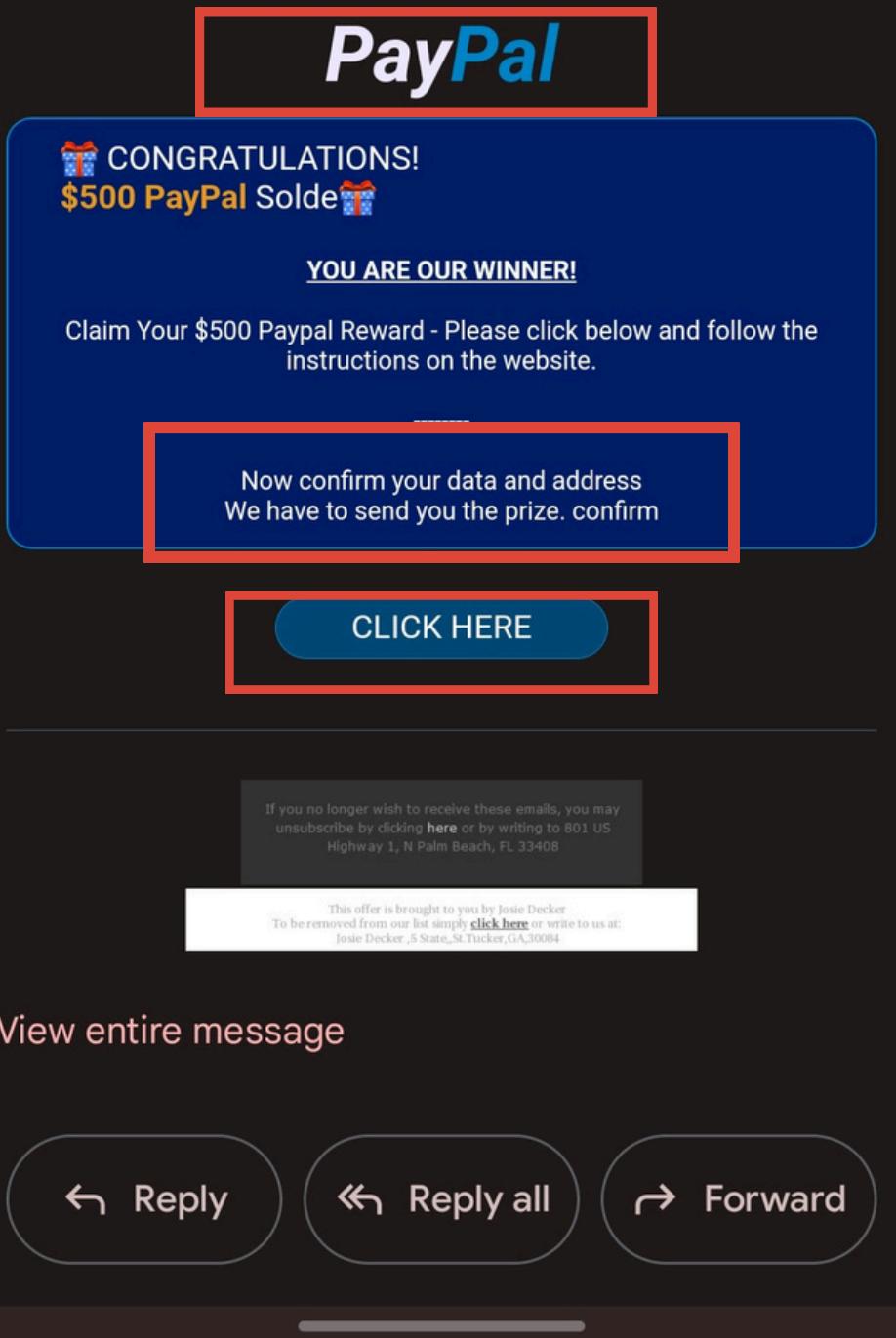




# PHISHING ATTACKS

**Phishing is a cyberattack where scammers attempt to steal personal information by disguising themselves as a trusted entity, like a bank or company. They often send fake emails, texts, or messages with links or attachments that lead to malicious websites or downloads.**

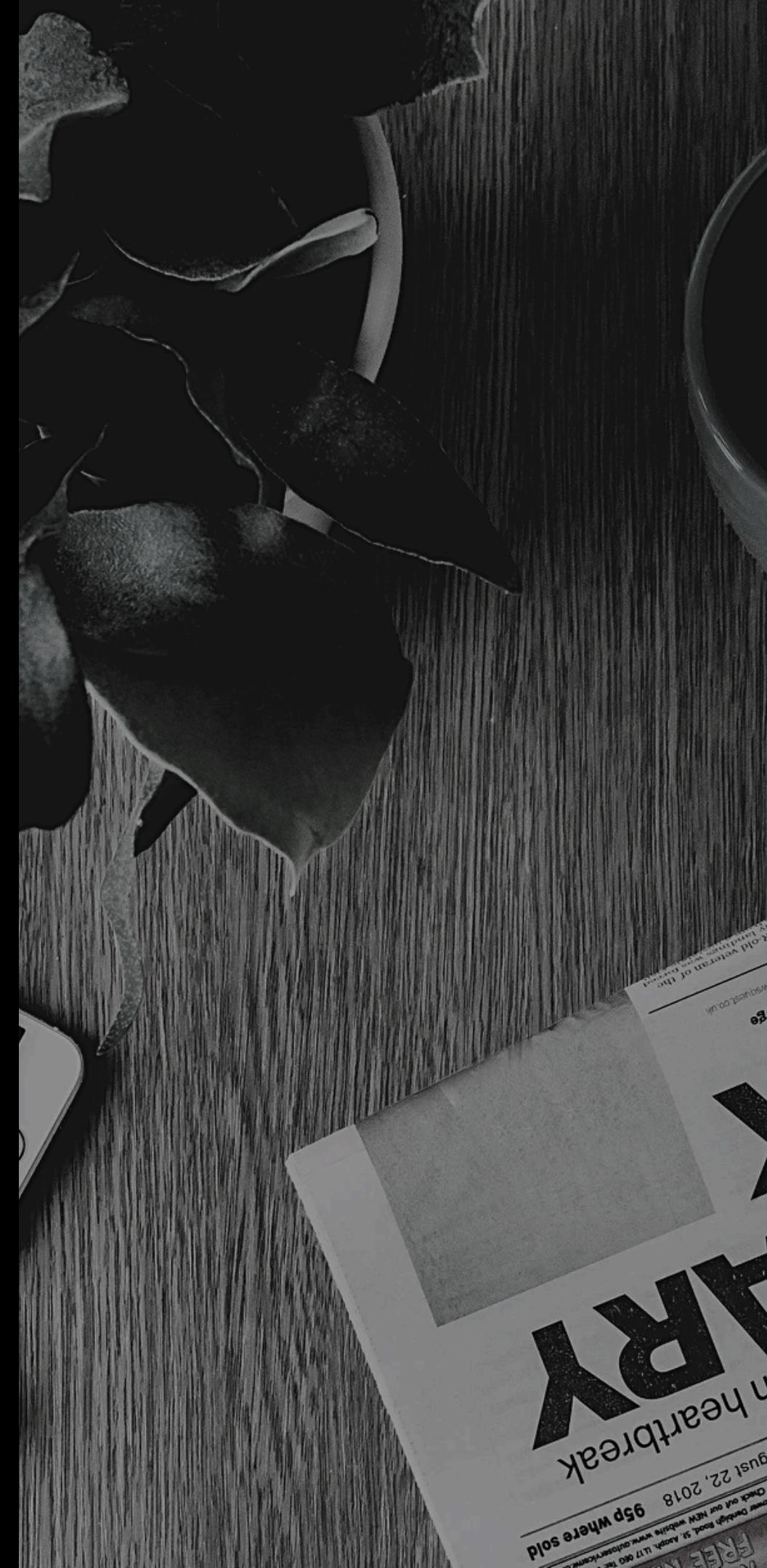
From PAYPAL® • btn8wy1hh8@71lao543l58.us  
To me@aol.com  
Date Aug 5, 2024, 8:26 PM  
hinet.net did not encrypt this message.  
[View security details](#)

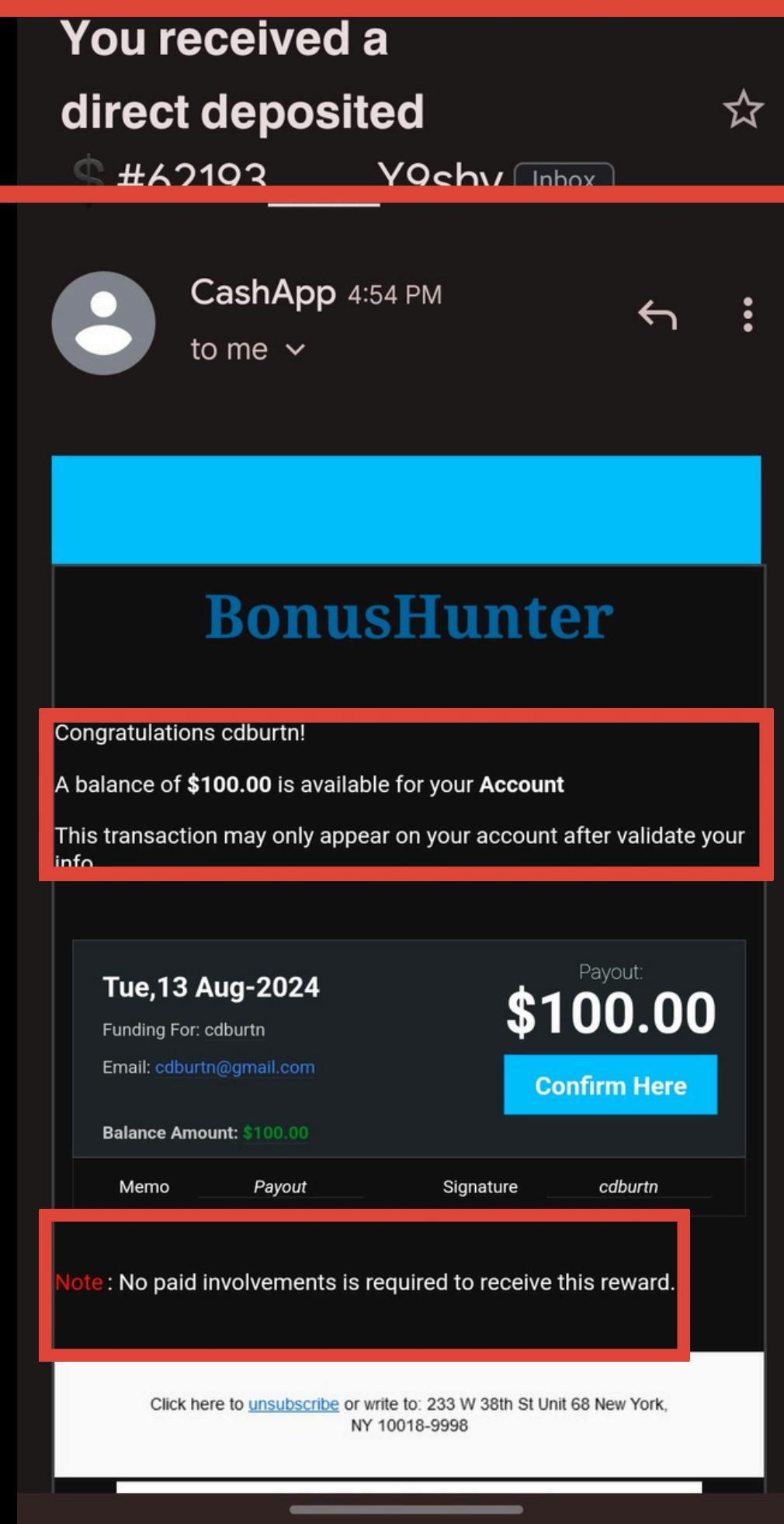


- UNFAMILIAR OR SPOOFED SENDER ADDRESS: CHECK THE EMAIL ADDRESS CAREFULLY FOR SLIGHT VARIATIONS OR TYPOS.

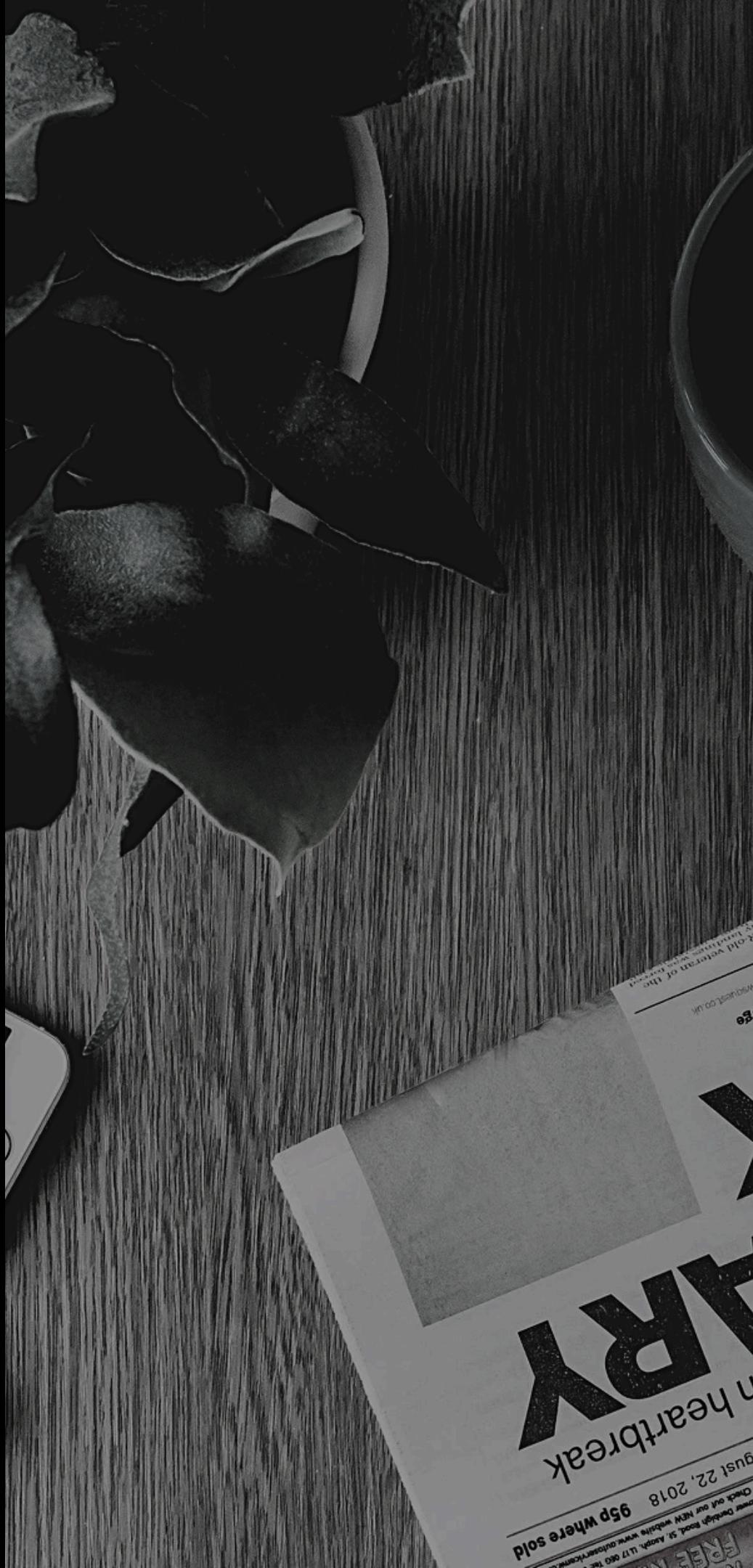
IN THIS CASE, EVEN THE RECIPIENT ADDRESS IS INCORRECT

- INCONSISTENT BRANDING OR DESIGN: LOOK FOR MISMATCHED LOGOS, FONTS, OR OVERALL APPEARANCE.
- LACK OF PERSONALIZATION: PHISHING EMAILS ARE OFTEN MASS-SENT, SO THEY MAY LACK DETAILS SPECIFIC TO YOU.
- OFFERS THAT SEEM TOO GOOD TO BE TRUE: BEWARE OF UNREALISTIC PROMISES LIKE LARGE CASH PRIZES OR EASY MONEY.
- REQUESTS FOR PERSONAL INFORMATION: LEGITIMATE BUSINESSES WON'T ASK FOR SENSITIVE DATA VIA EMAIL.
- SUSPICIOUS LINKS OR ATTACHMENTS: HOVER OVER LINKS TO CHECK THE URL; AVOID CLICKING OR DOWNLOADING UNEXPECTED FILES.

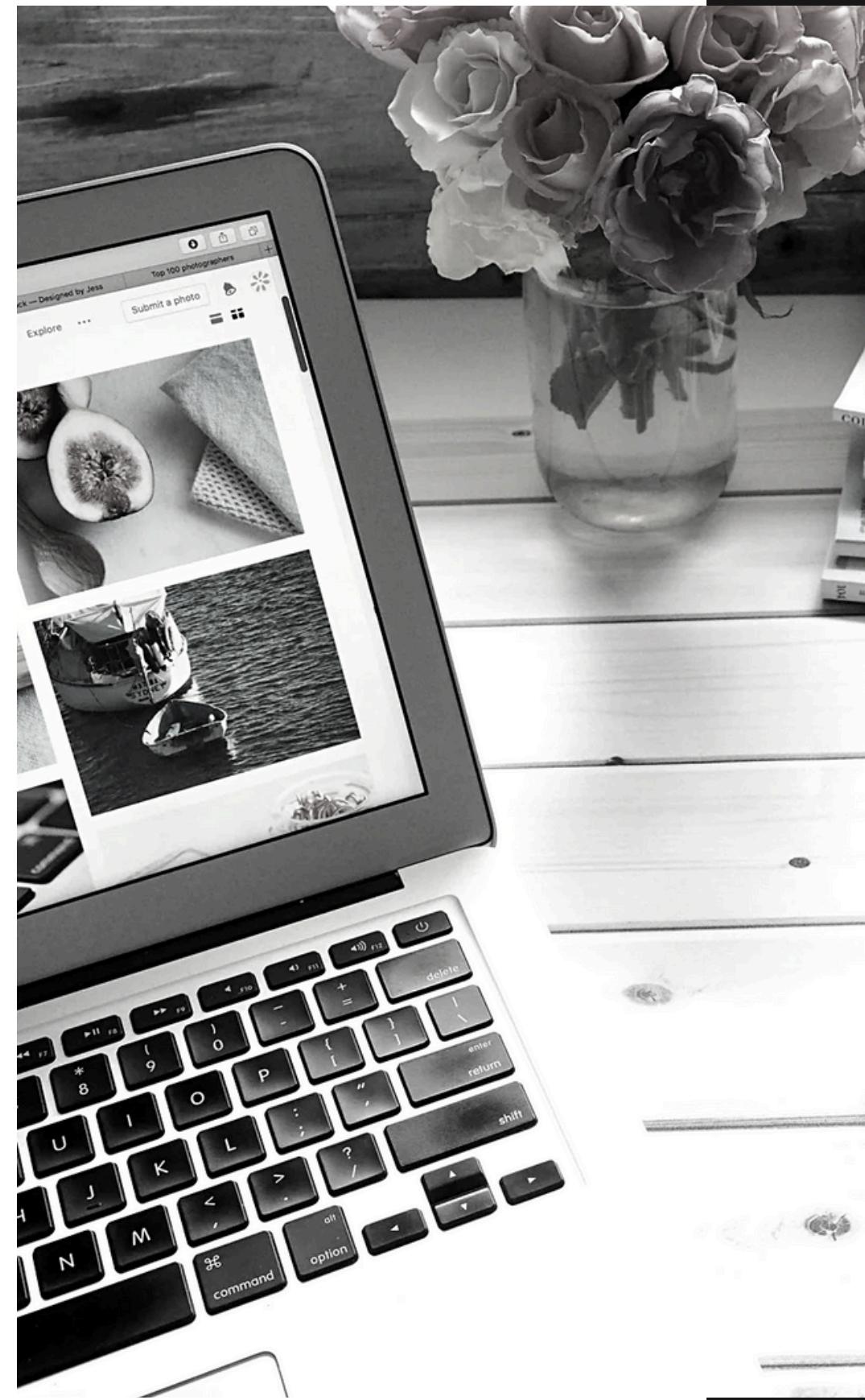




- POOR GRAMMAR OR SPELLING: COMMON IN PHISHING EMAILS DUE TO MASS DISTRIBUTION.
- GENERIC OR VAGUE CONTENT: LACKS SPECIFIC DETAILS ABOUT YOU OR YOUR ACCOUNT.



**PHISHING ATTACKS POSE SIGNIFICANT THREATS TO INDIVIDUALS AND ORGANIZATIONS. THESE CYBERATTACKS CAN LEAD TO SUBSTANTIAL FINANCIAL LOSSES THROUGH FRAUDULENT TRANSACTIONS, IDENTITY THEFT, AND ACCOUNT TAKEOVER. BEYOND MONETARY DAMAGES, PHISHING ATTACKS CAN COMPROMISE SENSITIVE DATA, DISRUPT BUSINESS OPERATIONS, AND ERODE TRUST IN COMPANIES. THE CONSEQUENCES CAN BE FAR-REACHING, AFFECTING INDIVIDUALS' PERSONAL LIVES AND ORGANIZATIONS' REPUTATIONS AND BOTTOM LINES.**



## **STEPS TO PROTECT YOURSELF FROM PHISHING ATTACKS**

- BE VIGILANT AND AWARE
- EDUCATE YOURSELF: UNDERSTAND THE TACTICS USED BY PHISHERS.
- BE SUSPICIOUS: APPROACH UNEXPECTED EMAILS OR MESSAGES WITH CAUTION.
- VERIFY SENDERS: DOUBLE-CHECK THE SENDER'S EMAIL ADDRESS FOR ANY DISCREPANCIES.
- HOVER OVER LINKS: CHECK THE ACTUAL URL BEFORE CLICKING.
- AVOID CLICKING ATTACHMENTS: UNLESS YOU'RE EXPECTING A FILE, AVOID OPENING ATTACHMENTS.
- TRUST YOUR INSTINCTS: IF SOMETHING FEELS OFF, IT PROBABLY IS.
- BE WARY OF URGENT REQUESTS: LEGITIMATE BUSINESSES RARELY DEMAND IMMEDIATE ACTION.
- VERIFY INFORMATION DIRECTLY: CONTACT THE COMPANY THROUGH A KNOWN PHONE NUMBER OR WEBSITE.
- USE CAUTION WITH PUBLIC WI-FI: AVOID ACCESSING SENSITIVE INFORMATION ON UNSECURED NETWORKS.

A black and white photograph of a person from the waist up. They are wearing a dark suit jacket over a light-colored shirt and a dark tie. Their hands are clasped together in front of them on a surface that appears to be a desk. The background is dark and out of focus.

**Good luck!**