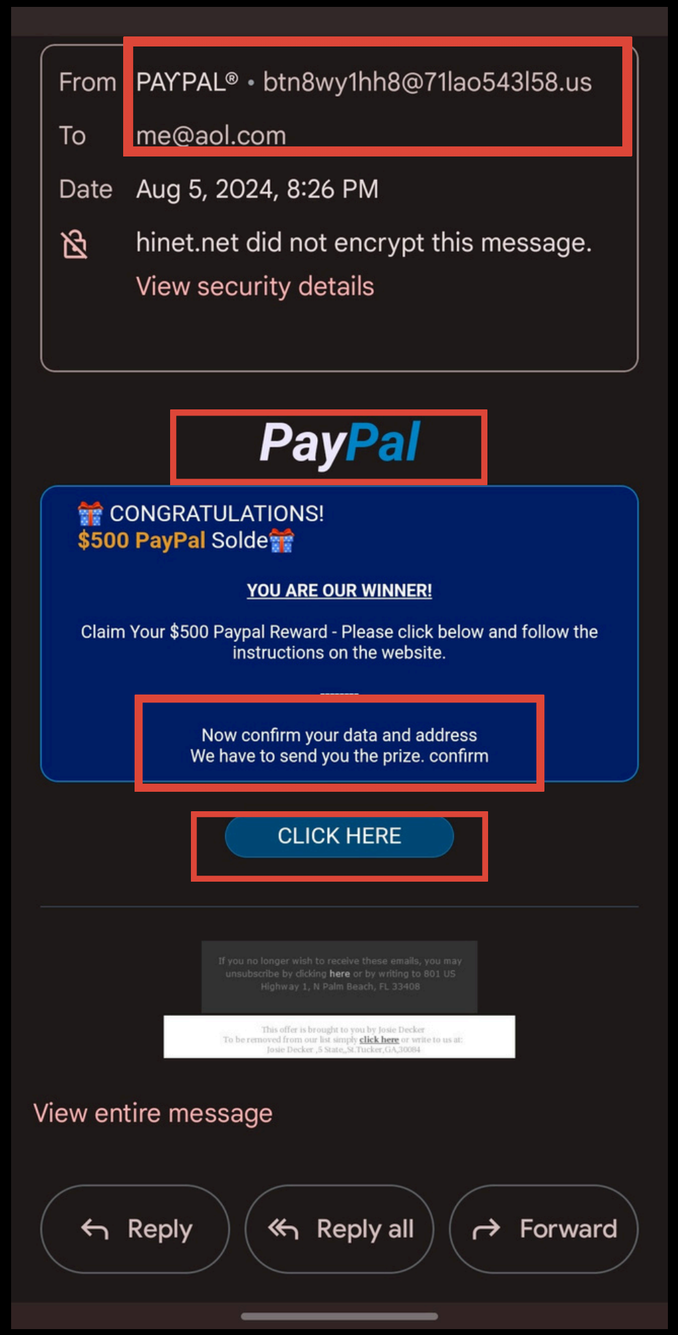
PHISHING ATTACKS

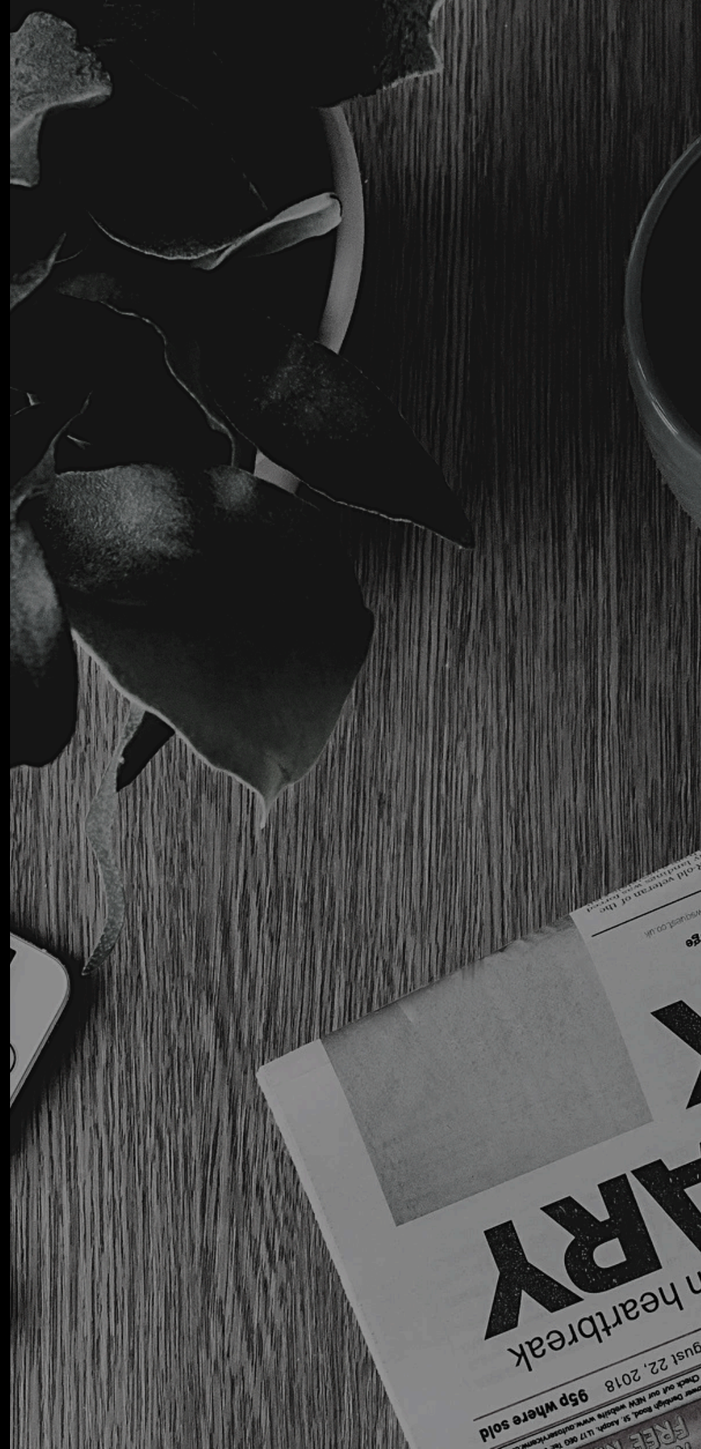
Phishing is a cyberattack where scammers attempt to steal personal information by disguising themselves as a trusted entity, like a bank or company. They often send fake emails, texts, or messages with links or attachments that lead to malicious websites or downloads.

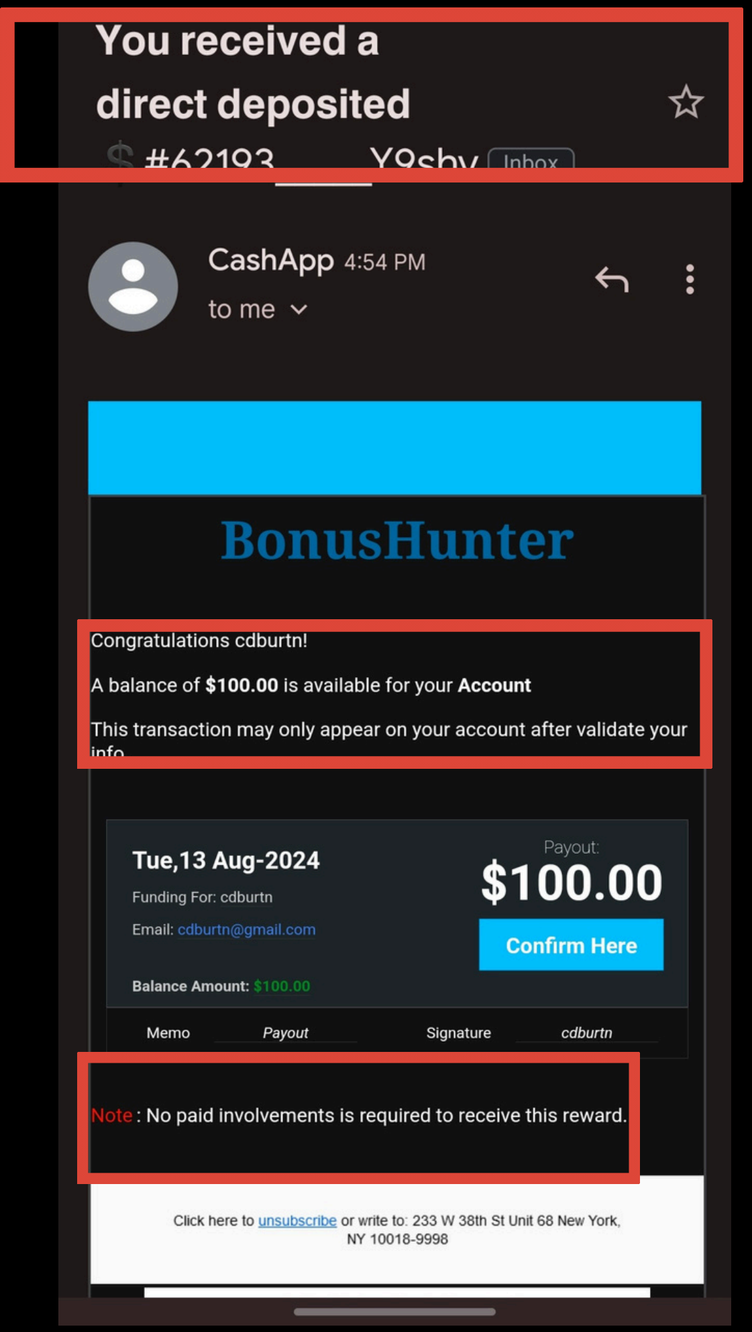


- *UNFAMILIAR OR SPOOFED SENDER ADDRESS: CHECK THE EMAIL ADDRESS CAREFULLY FOR SLIGHT VARIATIONS OR TYPOS.*

IN THIS CASE, EVEN THE RECIPIENT ADDRESS IS INCORRECT

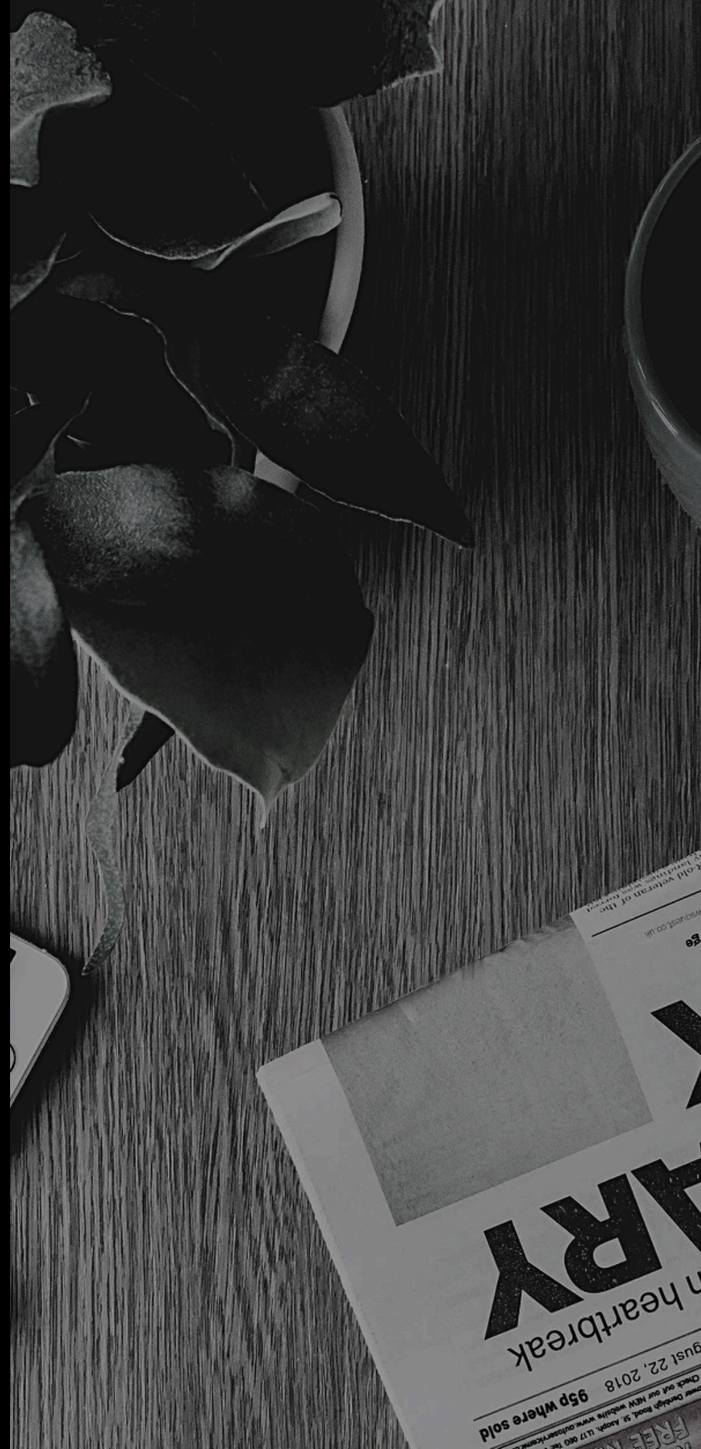
- *INCONSISTENT BRANDING OR DESIGN: LOOK FOR MISMATCHED LOGOS, FONTS, OR OVERALL APPEARANCE.*
- *LACK OF PERSONALIZATION: PHISHING EMAILS ARE OFTEN MASS-SENT, SO THEY MAY LACK DETAILS SPECIFIC TO YOU.*
- *OFFERS THAT SEEM TOO GOOD TO BE TRUE: BEWARE OF UNREALISTIC PROMISES LIKE LARGE CASH PRIZES OR EASY 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.*



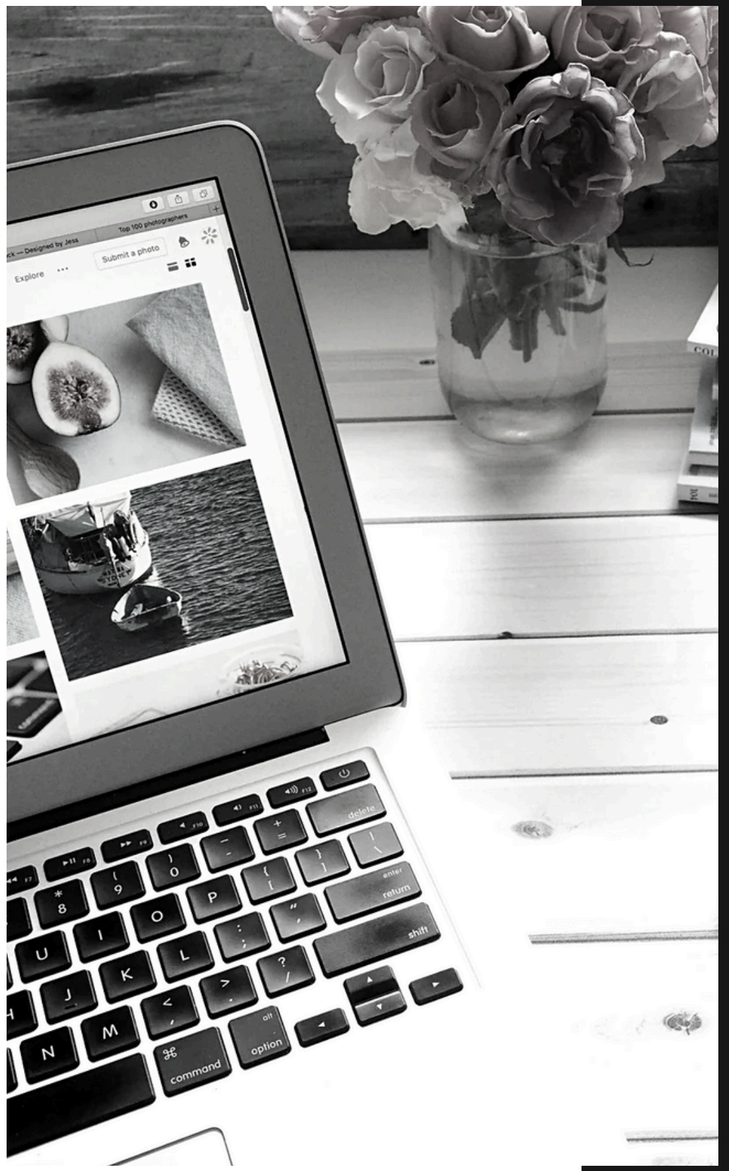


- POOR GRAMMAR OR SPELLING: COMMON IN PHISHING EMAILS DUE TO MASS DISTRIBUTION.

- 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.



Requirement #5: Protect all systems and networks from malicious software.

PCI Security Standards Council

Requirements and Testing Procedures		Guidance
5.4 Anti-phishing mechanisms protect users against phishing attacks.		
Defined Approach Requirements **5.4.1** Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks. **Customized Approach Objective** Mechanisms are in place to protect against and mitigate risk posed by phishing attacks. **Applicability Notes** The focus of this requirement is on protecting personnel with access to system components in-scope for PCI DSS. Meeting this requirement for technical and automated controls to detect and protect personnel against phishing is not the same as Requirement 12.6.3.1 for security awareness training. Meeting this requirement does not also meet the requirement for providing personnel with security awareness training, and vice versa. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**Defined Approach Testing Procedures** **5.4.1** Observe implemented processes and examine mechanisms to verify controls are in place to detect and protect personnel against phishing attacks.	**Purpose** Technical controls can limit the number of occasions personnel have to evaluate the veracity of a communication and can also limit the effects of individual responses to phishing. **Good Practice** When developing anti-phishing controls, entities are encouraged to consider a combination of approaches. For example, using anti-spoofing controls such as Domain-based Message Authentication, Reporting & Conformance (DMARC), Sender Policy Framework (SPF), and Domain Keys Identified Mail (DKIM) will help stop phishers from spoofing the entity's domain and impersonating personnel. The deployment of technologies for blocking phishing emails and malware before they reach personnel, such as link scrubbers and server-side anti-malware, can reduce incidents and decrease the time required by personnel to check and report phishing attacks. Additionally, training personnel to recognize and report phishing emails can allow similar emails to be identified and permit them to be removed before being opened. It is recommended (but not required) that anti-phishing controls are applied across an entity's entire organization. *(continued on next page)*

Requirement #12: Support information security with organizational policies and programs.

PCI Security Standards Council

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Educating personnel on how to detect, react to, and report potential phishing and related attacks and social engineering attempts is essential to minimizing the probability of successful attacks. **Good Practice** An effective security awareness program should include examples of phishing emails and periodic testing to determine the prevalence of personnel reporting such attacks. Training material an entity can consider for this topic include: • How to identify phishing and other social engineering attacks. • How to react to suspected phishing and social engineering. • Where and how to report suspected phishing and social engineering activity. An emphasis on reporting allows the organization to reward positive behavior, to optimize technical defenses (see Requirement 5.4.1), and to take immediate action to remove similar phishing emails that evaded technical defenses from recipient inboxes.
12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of cardholder data and/or sensitive authentication data, including but not limited to: • Phishing and related attacks. • Social engineering.	**12.6.3.1** Examine security awareness training content to verify it includes all elements specified in this requirement.	
Customized Approach Objective		
Personnel are knowledgeable about their own human vulnerabilities and how threat actors will attempt to exploit such vulnerabilities. Personnel are able to access assistance and guidance when required.		
Applicability Notes		
See Requirement 5.4.1 for guidance on the difference between technical and automated controls to detect and protect users from phishing attacks, and this requirement for providing users security awareness training about phishing and social engineering. These are two separate and distinct requirements, and one is not met by implementing controls required by the other one. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

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.