Spotting the Phish

Protecting Yourself and the Company
Hadji Yono-Cruz Oct. 30 2024

What is Phishing?

- Definition: A cyberattack where attackers pose as legitimate entities to steal sensitive information.
- Types of Information Targeted:
  - Login credentials
  - Financial data
  - Personal details

Learn to Spot Phishing Emails

- **Key signs**
  - Suspicious sender address
  - Poor grammar or spelling
  - Urgent language (e.g., “Act now!”
  - Mismatched URLs
  - Unexpected attachments or links
  - Random prizes or rewards

Indicators from Simulation

From: MastercardsIT@mastercard.com
To: employee@email.com
Subject: Action Needed: Password Reset Required to Secure Account

Body:

Hello (insert name),

As part of the Mastercard commitment in preserving your security, we have detected unusual activity on your account. To ensure your information is secure, a password reset is required. Please complete the following steps within the next 24 hours to avoid any disruption to your account.

Reset your password now: https://mastercard-secure.com/reset-password

If you do not complete this action within the required time frame, your account may be temporarily locked as a security measure.

For questions and concerns, please contact our support team at support@mastercard.com

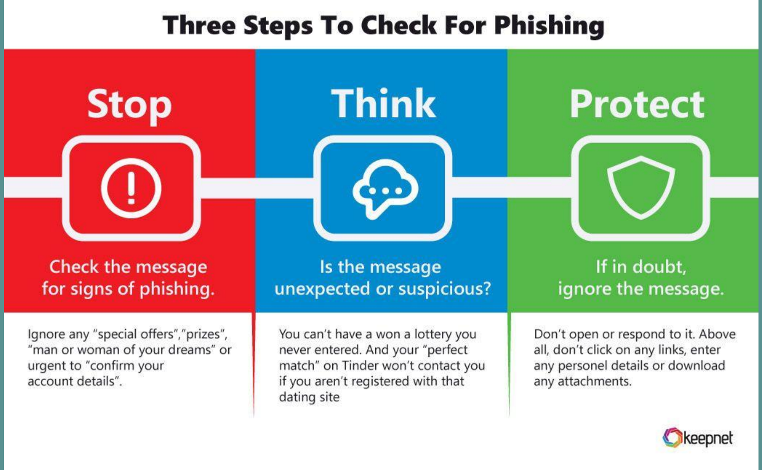
Thank you,

Mastercard IT Security Team
CONFIDENTIAL: This email is intended only for the person or entity which it is addressed and may contain confidential and/or privileged material. If you are not the named recipient for which this information is intended, please contact the sender and do not forward or distribute this email to any other than the intended recipient.

1. Action needed.
2. Required time frame to complete action.
3. Hover over hyperlinks to confirm URLs.

What to Do When You Suspect Phishing

- Steps to Take:
  - Do not click links or download attachments.
  - Verify the sender through trusted channels.
  - Report the email to IT/security.
  - Delete suspicious emails if confirmed unsafe.
  - Block or flag suspicious email.



Three Steps To Check For Phishing

Stop

Check the message for signs of phishing.

Ignore any "special offers","prizes", "man or woman of your dreams" or urgent to "confirm your account details".

Think

Is the message unexpected or suspicious?

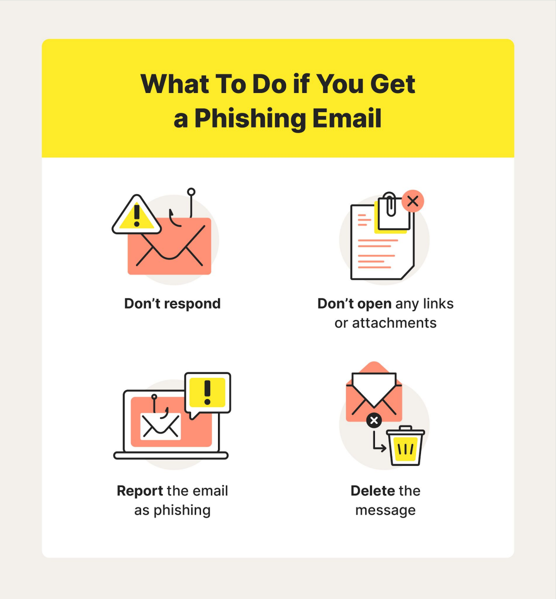
You can't have a won a lottery you never entered. And your "perfect match" on Tinder won't contact you if you aren't registered with that dating site

Protect

If in doubt, ignore the message.

Don't open or respond to it. Above all, don't click on any links, enter any personel details or download any attachments.

keepnet



What To Do if You Get a Phishing Email

Don't respond

Don't open any links or attachments

Report the email as phishing

Delete the message

Preventing Phishing Attacks

- **Best Practices**
  - Use strong, unique passwords
  - Enable multi-factor authentication (MFA)
  - Stay cautious with unsolicited messages.
  - Keep software updated
  - Go to trusted website instead of clicking links in email.

Think Before You Click!