Phishing and how to avoid

By: Abdelrahman Ahmed

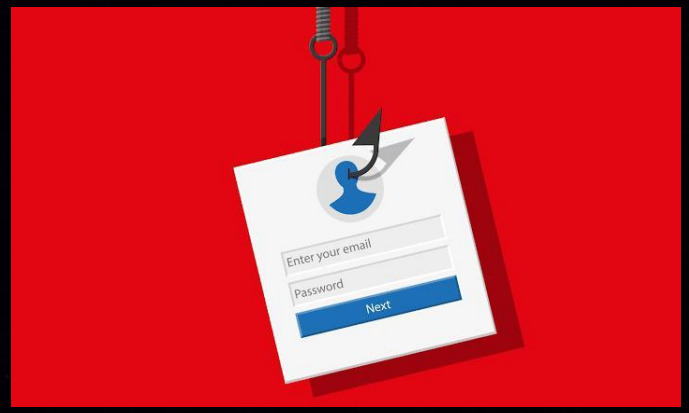
Code Alpha Project

What is Phishing ?

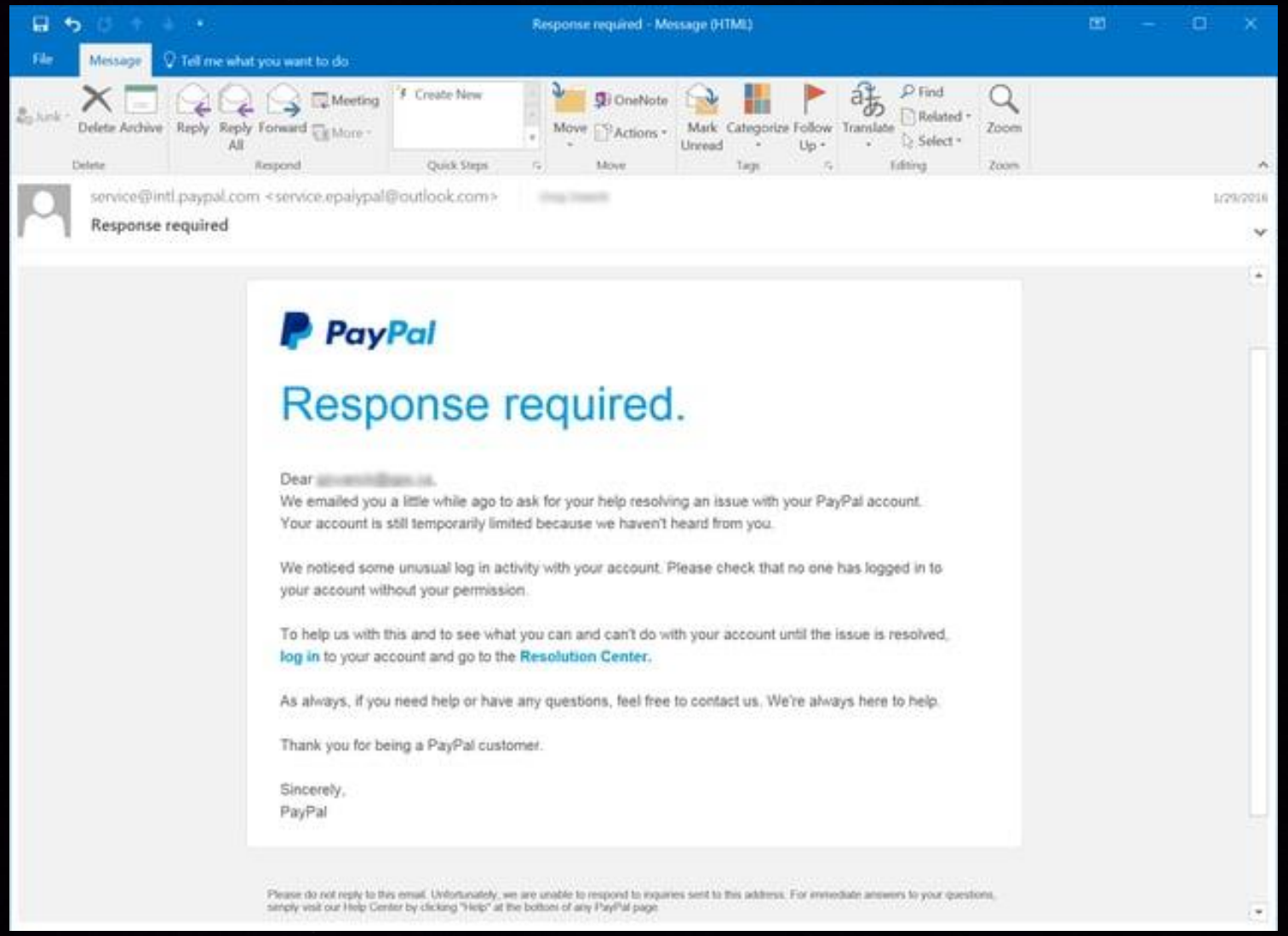
- A phishing attack is a type of cyberattack where an attacker tries to trick someone into giving away sensitive information — like passwords, credit card numbers, or login credentials — by pretending to be a trusted person or organization.
- **Example of a phishing attack:**
- An attacker sends an email that looks like it’s from your bank. The email says your account has a problem and asks you to click a link to log in. The link goes to a fake website that looks like the real bank site, and when you enter your username and password, the attacker steals them.

How to Recognize phishing attacks ?

- Check the sender’s address:
- Fake emails often come from strange or misspelled domains.
- Look for spelling and grammar mistakes:
- Official organizations rarely make language errors.
- Beware of urgent or threatening messages:
- Attackers try to make you act quickly without thinking.
- Hover over links before clicking:
- Check if the real URL matches the official website.
- Watch for generic greetings:
- Messages saying “Dear Customer” instead of your real name are suspicious.
- Avoid suspicious attachments or links:
- Don’t download or open files from unknown senders.



Real World Example



Some Social Engineering tatics

- Authority:
- Pretending to be a trusted person or organization (like a bank, manager, or IT admin).
- Curiosity:
- Using tempting or shocking subjects to make you click (e.g., “Confidential report attached” or “You’ve won a prize!”).
- Trust and Familiarity:
- Using names or details from your company, colleagues, or contacts to seem legitimate.
- Greed or Reward:
- Offering fake rewards, discounts, or gifts to lure victims into clicking links or giving info.
- Fear of Loss:
- Making you afraid of losing access, money, or opportunities if you don’t respond.
- Impersonation:
- Using look-alike domains or similar logos to mimic real websites or email addresses.
- Emotional Manipulation:
- Exploiting emotions like fear, curiosity, or sympathy to lower your guard.

Tatics to avoid failing victim

- Pause and think before you click
- Don’t act on urgent emails or messages immediately. Take a moment to verify.
- Verify the sender independently
- If an email or message asks for sensitive info, contact the organization using a phone number or website you know is official — don’t use the contact info in the message.
- Check links before clicking
- Hover over links (or long-press on mobile) to see the real URL. If it looks wrong or unfamiliar, don’t click it.
- Look for spelling, grammar, and tone
- Poor language, odd phrasing, or a surprising level of urgency are red flags.
- Never enter credentials from an email link
- Go to the service’s official website manually (type the URL or use a bookmarked link) and log in there.