Phishing Awareness Training

How to Recognize, Prevent, and Respond to Phishing Attacks

Hassan Ahmed Malik

23%

Hackers use phishing scams to try to steal your identity or money by sending official-looking email asking for sensitive personal information. 23% of people open phishing email.

What is Phishing?

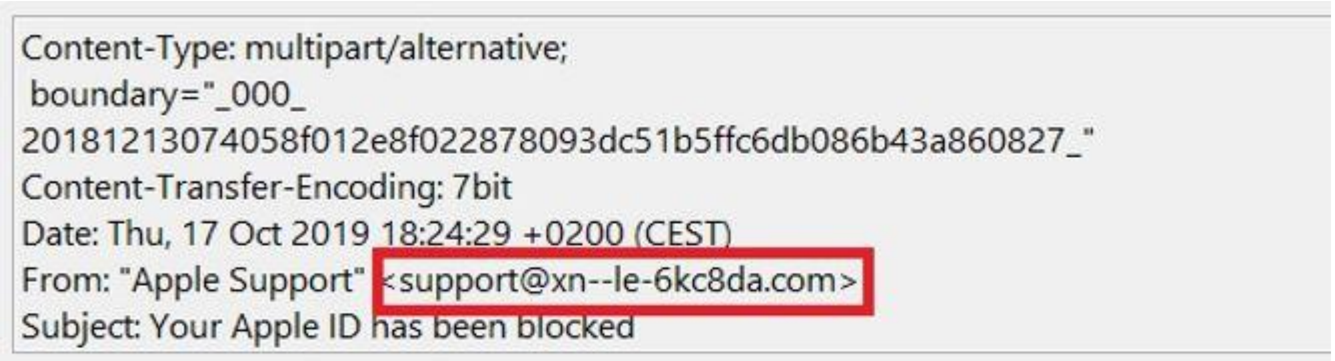
Definition: Fraudulent attempt to steal sensitive information by impersonating trusted entities

Common attack types: Spear phishing, business email compromise, clone phishing

Recent example: Scammers used fake Google Forms to steal crypto funds via convincing alerts

How to Recognize Phishing Attempts

Check the sender address; Look for typos or spoofed domains (e.g. “paypai.com” instead of paypal.com)



```
Content-Type: multipart/alternative;
 boundary="_000_
20181213074058f012e8f022878093dc51b5ffc6db086b43a860827_"
Content-Transfer-Encoding: 7bit
Date: Thu, 17 Oct 2019 18:24:29 +0200 (CEST)
From: "Apple Support" <support@xn--le-6kc8da.com>
Subject: Your Apple ID has been blocked
```

Watch for suspicious language: Poor grammar, unexpected urgency, strange requests

Hover over links to preview URL; Don’t click if domain doesn't match display text

Hover over links to preview URL; Don’t click if domain doesn't match display text

Social Engineering Attempts

Impersonation: Attackers pretend to be executives (CEO fraud), vendors, colleagues

Urgency and pressure: “you must act now,” “limited time,” “payment overdue”

Friendly tone or **personalized detail** to lower suspicion (“We know you’re new…” etc.)

Use of **official branding** or logos to appear legitimate

Best Practices and Prevention Steps

Verify before you act: call the person using a known number, confirm via separate channel

Use email authentication tech: DKIM, SPF, DMARC help filter spoofed messages

Regular phishing simulations and training: ongoing training reduces risk and improves detection

Report attempts immediately: don’t blame victims—promote a supportive culture where mistakes are shared and learned from

Stay updated on tactics: phishing attacks evolve—be alert to new scams and red flags

Quiz — Test Your Phishing Knowledge

What is a common red flag in phishing emails?
A. A generic greeting like "Dear Customer"
B. An attachment file you requested
C. Proper spelling and grammar
D. An email from your personal contact

When hovering over a hyperlink in an email, you notice the URL is different from the displayed text. This indicates:
A. A secure affiliate link
B. A genuine redirect
C. URL mismatch or spoofing
D. A shortened URL from a trusted brand

A sense of urgency (“Your account will be closed in 24 hours unless…”) is used to:
A. Inform politely
B. Trick users via social engineering
C. Offer a discount
D. Confirm identity