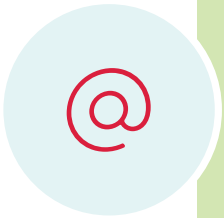
How to Spot a Phishing Email

10 TIPS

1 Use a Tool Like IDR to Identify Phishing Emails

Inbox Detection and Response is a great tool to identify malicious emails with just one click.



2 Examine the Email Address

Check for slight misspellings or unusual domains in the sender's email address.

3 Beware of Generic Greetings

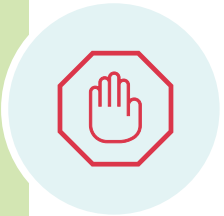
Phishing emails often start with "Dear Customer" rather than using your actual name.

4 Look for Spelling and Grammar Mistakes

Many phishing emails have typos or awkward phrasing.

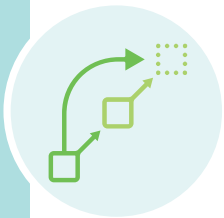
5 Check the Hyperlinks

Hover over any links without clicking. A mismatch between the link's description and its destination is suspicious.



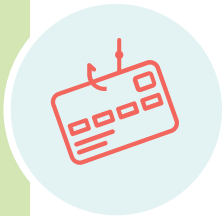
6 Unexpected Attachments are a Red Flag

Be wary of unsolicited attachments, especially if the email urges you to open them quickly.



7 Sense the Urgency

Emails pushing you to take immediate action, especially concerning account status or payments, should be approached with caution.



8 Requests for Personal Info are Suspicious

Legitimate organizations usually don't ask for sensitive data via email.

9 Analyze the Email's Tone

Phishing attempts may have an alarmist or overly casual tone that doesn't match the supposed sender's usual communications.

10 Verify Before Clicking

If an email claims to be from a known institution but seems off, contact that institution directly using trusted methods.

TPX

How to Protect Yourself Against Phishing

1 Strengthen your email security with Inbox Detection and Response

91% of all attacks begin with a phishing email. With TPx's Inbox Detection and Response, users can easily report potential phishing emails with one click.

91%

2 Train your staff to spot phishing emails with Cybersecurity Awareness Training

84% of U.S. organizations said security awareness training has reduced phishing failure rates. TPx offers a fully-managed program that includes randomized phishing simulation emails, as well as monthly training courses. Weekly tracking reports are delivered to you via email to stay in the loop of your staff's progress.

84%

3 Regularly back up your data. And don't forget about disaster recovery.

60% of SMBs that lose data will shut down within 6 months, yet 75% of small businesses don't have a written disaster recovery plan. With our Managed Backups & Disaster Recovery solution, your data is backed up both on-site and in a secure cloud location, providing extra security and redundancy. We also offer cloud-to-cloud backup to secure the data in the cloud.

60%

Other Measures to Strengthen Your Defenses

Advanced Threat Detection

Utilize cutting-edge technology and automated machine learning engines to detect and identify sophisticated ransomware and phishing attempts. Stay ahead of evolving threats and ensure timely response to potential attacks.

Endpoint Management & Security

Regularly updating software and operating systems is essential for addressing vulnerabilities that attackers may exploit. TPx can keep your important servers and workstations healthy and performing optimally.

Firewall and Network Security

Implement a next-gen firewall solution that monitors and filters incoming and outgoing network traffic. This helps prevent unauthorized access, blocks malicious connections, and fortifies your network against ransomware attacks and phishing attempts.

Security Advisory Services

We offer free ransomware evaluation — and a more comprehensive ransomware assessment (for a fee). This assessment focuses on the aspects of cybersecurity that have the highest value in defending your organization against ransomware attacks.

TPx