DETECTING A PHISHING EMAIL

10 Tips to Protect Your Organization

cyber claw
IT Security Solutions

1

CHECK THE SENDER

Expand the email address to make sure it appears legitimate.

2

HOVER BEFORE YOU CLICK

Verify the link address matches the description.

3

BE SKEPTICAL OF URGENCY

Phishing emails use urgency to bypass better judgment.

4

BE CAUTIOUS WITH ATTACHMENTS

An attacker can quickly install malware through intriguing attachment names.

5

CHECK THE SPELLING

Malicious emails are known for bad grammar and spelling.

6

CHECK THE EMAIL SIGNATURE

Most sincere senders include a full email signature that matches their address.

7

PROTECT PERSONAL INFORMATION

Legitimate companies rarely ask for personal information via email.

8

CHECK FOR VAGUE INTRODUCTIONS

"Valued customer" or similar intros are signals the email is from an outsider.

9

TRUST YOUR GUT

If something seems slightly off, make a call or report the email.

10

REPORT, REPORT, REPORT

Tech support and management would rather check suspicious emails than have the organization put at risk.

Over **90%** of malware received is by email

30% of phishing messages get opened by targeted users

Phishing accounts for over **90%** of data breaches

DoerenMayhew | doeren.com | 248.244.3000

Source of Statistics: Verizon 2018 Data Breach Report