

Understanding Phishing Threats

- **Introduction:** Phishing is a cyber attack where attackers impersonate legitimate entities to steal sensitive information.
- **Target Teams:** HR and Marketing have shown higher susceptibility in recent phishing campaigns.



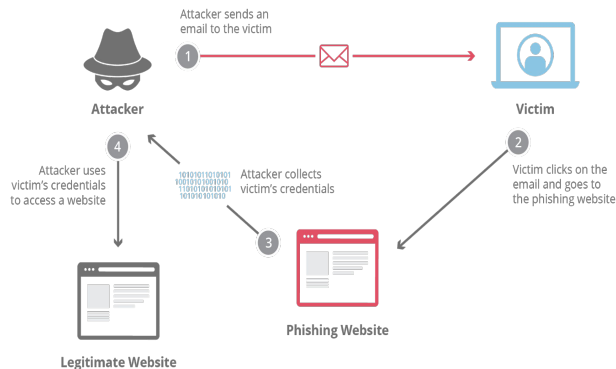
Even if you think the email is legitimate, if it is not something you are expecting it is a good idea to contact the person you believe to be the sender "out-of-band," or by another method than clicking "reply" or any links in the email. For example, call a phone number you know belongs to the institution or person or go directly to their website by typing in the URL.

What is phishing?

Definition: Phishing is a fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity in electronic communications.

Common Tactics:

- **Deceptive Emails:** Fake emails that look legitimate.
- **Malicious Links:** Links that lead to fake websites.
- **Urgent Requests:** Messages creating a sense of urgency to provoke hasty actions.



Learn to spot phishing emails



Signs of Phishing Emails:

- **Unusual Sender Address:** Email addresses that don't match the claimed sender.
- **Generic Greetings:** "Dear Customer" instead of your name.
- **Suspicious Links:** Hover over links to check the actual URL before clicking.
- **Spelling and Grammar Mistakes:** Poorly written emails can be a red flag.

SPAM EMAIL

SPOT THE DIFFERENCE

there are 6 differences between the fake and real one, can you spot them?

FAKE	REAL
<p>From: support@microsoft.co.uk Sent: 16/01/2023 11:44 To: Bob Smith <Bob.Smith@company.com> Subject: Urgent Action Needed!</p>  <p>Microsoft Account</p> <p>Verify your account</p> <p>We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.</p> <p>To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.</p> <p>http://account.live.com/ResetPassword.aspx</p> <p>Thanks, The Microsoft Team</p>	<p>From: support@microsoft.co.uk Sent: 16/01/2023 11:44 To: Bob Smith <Bob.Smith@company.com> Subject: Unusual Sign In Activity</p>  <p>Microsoft Account</p> <p>Verify your account</p> <p>We detected some unusual activity about a recent sign in for your Microsoft account bo*****@company.com. you might be signing in from a new location app or device.</p> <p>To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.</p> <p>Review recent activity</p> <p>Thanks, The Microsoft Team</p>

How do we stop getting phished?

- **Verify Requests:** Always verify requests for sensitive information through a known contact method.
- **Use strong Passwords:** Implement strong, unique passwords for different accounts.
- **Enable Two-Factor Authentication (2FA):** Adds an extra layer of security.
- **Report Suspicious Emails:** Notify your IT department of any suspicious emails.

Don't Get Hooked!

3 rules to avoid phishing cybersecurity attacks

- 1 Stop and think before clicking any links or attachments.
- 2 If things look "phishy," verify with the sender through a different medium.
- 3 "When in doubt, throw it out."
You are the last line of defense.

