Familiarize yourself with phishing attacks

1. Train employees on phishing tactics.
2. Run phishing simulations to test responses.
3. Create an easy reporting process for suspicious emails.
4. Focus on high-risk roles (like finance or HR).5. Encourage team collaboration on security updates.

What is phishing?

Phishing is a type of cyber attack where attackers impersonate legitimate organizations or individuals to trick people into providing sensitive information, such as usernames, passwords, or financial details. This is often done through fake emails, messages, or websites that look authentic.

Key Points to Understand:

Common Techniques: Attackers may send emails that appear to come from trusted sources, such as banks or company executives, urging recipients to click on links or download attachments.

2. Red Flags: Look for signs like poor grammar, unfamiliar sender addresses, urgent requests, or unexpected attachments, which can indicate a phishing attempt.

3. Consequences: Falling for a phishing scam can lead to data breaches, financial loss, or identity theft, affecting both the individual and the organization.

4. Prevention: Always verify the sender's identity, hover over links to check their destination, and avoid sharing sensitive information through email. Use multi-factor authentication for added security.

Learn to spot phishing emails

An effective way to illustrate the tactics used in phishing emails is to create a series of side-by-side comparisons: legitimate emails next to phishing emails. This visual contrast can help highlight key differences and make it easier to spot potential scams.

To spot phishing emails, focus on these key tactics:

1.Impersonation: Fake email addresses and generic greetings (e.g., "Dear Customer").

2. Urgency/Fear: Warnings about immediate action or account closure.

3. Suspicious Links: Hover over links to check if they lead to legitimate websites.

4. Grammar/Spelling Errors: Phishing emails often have mistakes in the message.

5. Fake Attachments: Be cautious with unexpected files, which may contain malware.A side-by-side comparison of phishing vs. real emails with highlights on these red flags is an effective way to visualize the tactics.

How do we stop getting phished?

To stop getting phished:

1,Be skeptical of unsolicited emails.

2. Check email addresses for slight changes.

3. Hover over links before clicking.

4. Avoid unverified attachments.

5. Use strong spam filters.

6. Enable multi-factor authentication (MFA).

7. Keep software updated.

8. Stay informed about phishing tactics.

9. Report phishing emails.Stay vigilant by watching for red flags and following these protective steps.