Familiarize yourself with phishing attacks

Phishing attacks are a significant threat in the workplace.
Teams identified as most at risk:

- **Customer Support**: Regularly handles sensitive customer information.
- **Finance Teams**: Common targets for stealing financial credentials.

What is phishing?

Phishing is an attempt to trick users into providing sensitive information such as passwords or financial details through deceptive emails or messages.

Attackers often impersonate trusted institutions, using urgent messages to get employees to click on malicious links or share personal data.

This can lead to compromised accounts, data breaches, or financial loss.

Learn to spot phishing emails

Common tactics used by attackers include:

- **Suspicious email addresses**: Look out for slight misspellings or unfamiliar domains.
- **Urgent language**: Messages pressuring you to act quickly (e.g., "Immediate action required").
- **Fake links**: Hover over links before clicking to check the real destination.
- **Unexpected attachments**: Be cautious of unfamiliar files that could contain malware.

How do we stop getting phished?

Verify the sender: Always double-check the email address before responding or clicking any links.

Be cautious with links: Hover over links to ensure they lead to legitimate websites.

Never share sensitive information: Legitimate companies will never ask for personal data via email.

Report phishing attempts: If you receive a suspicious email, report it to your IT department.

Stay informed: Regularly review security best practices and participate in phishing awareness training.