PHISHING AWARENESS TRAINING

Recognizing and Preventing Online Threats

Start Now →

WHAT IS PHISHING?

Definition of Phishing

A cyberattack where scammers trick users into revealing sensitive information.

Common targets: Emails, websites, social media messages.

WHY IS PHISHING DANGEROUS?

- Can lead to identity theft.
- Financial loss and fraud.
- Data breaches in organizations.
- Loss of personal and business reputation.

COMMON TYPES OF PHISHING ATTACKS

Email Phishing

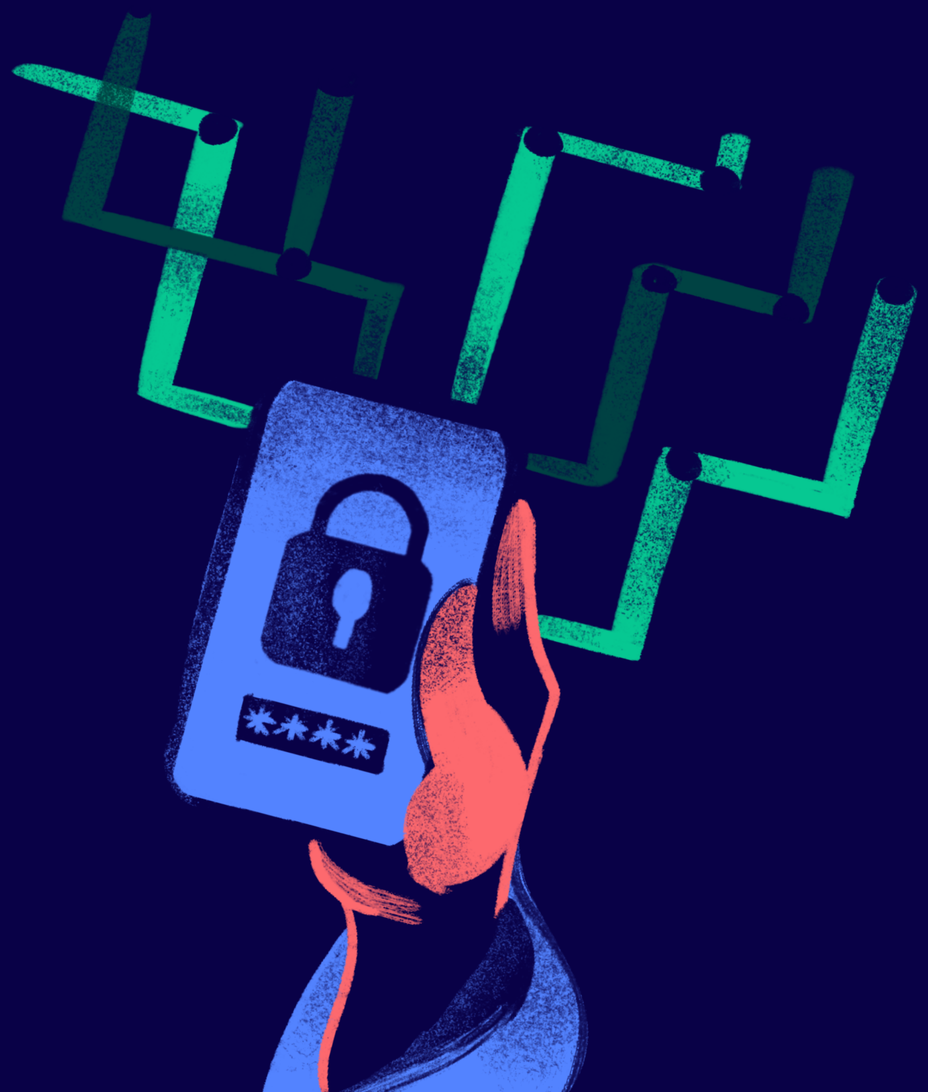
Fake emails pretending to be from legitimate sources.

Spear Phishing

Targeted attacks on specific individuals or organizations.

Whaling

High-profile attacks on executives or decision-makers.



HOW TO RECOGNIZE PHISHING EMAILS

- Urgent or threatening language.
- Suspicious email addresses.
- Unexpected attachments or links.
- Requests for personal information.
- Spelling and grammar errors.

HOW TO PROTECT YOURSELF

- ✅ Verify email senders before clicking links.
- ✅ Hover over links to check the real URL.
- ✅ Use multi-factor authentication (MFA).
- ✅ Report suspicious emails to IT/security teams.
- ✅ Keep software and antivirus updated.

WHAT TO DO IF YOU GET PHISHED?

- Do not click any links or download attachments.
- Change your passwords immediately.
- Report the phishing attempt to IT/security.
- Monitor your accounts for suspicious activity.

Phishing Awareness Training

THANK YOU FOR ATTENTION

See You Next →