Phishing Awareness Training

CREATED BY: GAGANDEEP KAUR

Understanding Phishing

- **Definition**: A type of cyber-attack that attempts to steal sensitive information (e.g., passwords, credit card numbers) by pretending to be a legitimate source.

- **Purpose of Phishing Attacks**:
- To steal credentials
- To spread malware
- To commit identity theft

Common Phishing Techniques

Email Phishing: Fake emails that look like they're from legitimate companies or people.

Spear Phishing: Targeted phishing attacks aimed at specific individuals or organizations.

Whaling: Phishing attacks that target high-profile individuals like executives.

Clone Phishing: Creating a copy of a legitimate email to exploit the trust of the receiver.

Vishing (Voice Phishing): Phishing attacks conducted through phone calls.

Smishing (SMS Phishing): Phishing attacks conducted through SMS messages.

Recognizing Signs

- **Signs of a Phishing Email**:
- Suspicious sender addresses
- Urgent or threatening language
- Spelling and grammar errors
- Fake logos or branding
- Unusual attachments or links

Recognizing Signs

- **Phishing Websites**:
- Poor design or slightly modified URLs (e.g., google.com vs. goog1e.com)
- Requests for sensitive information
- Secure connection (HTTPS) absence or inconsistencies

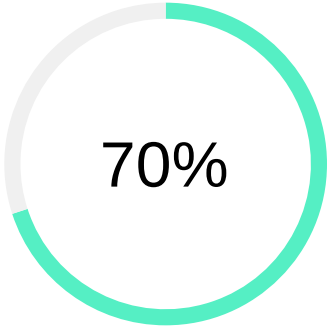
Protective Measures

- **Email Safety Tips**:
- Verify the sender before clicking any links.
- Avoid opening attachments from unknown senders.
- Use email filtering and anti-phishing tools.

- **Website Safety**:
- Check URLs for HTTPS and valid certificates.
- Don’t enter sensitive information on suspicious websites.

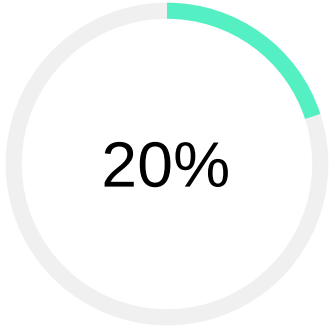
- **General Best Practices**:
- Use two-factor authentication (2FA).
- Regularly update software to patch vulnerabilities.
- Train employees and individuals on recognizing phishing.

Phishing Statistics



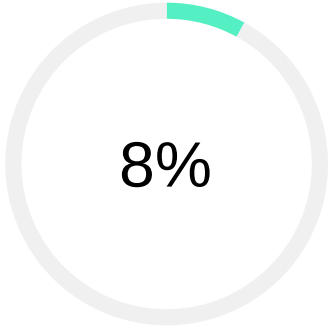
EMAIL PHISHING

Consists of 70% of reported phishing attempts, targeting users through deceptive emails.



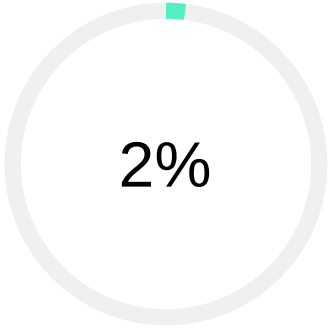
WEBSITE SPOOFING

Accounts for 20% of phishing, leading users to fraudulent sites.



SPEAR PHISHING

Targets specific individuals or companies, accounting for 8% of cases.



WHALING

Involves high-profile targets, making up 2% of phishing attacks.

What to do if you fall victim?

Immediate Actions:
•Disconnect from the network.
•Change passwords.
•Contact your IT department or service provider.

Reporting Phishing:
•Report the phishing email to the IT/security team.
•Forward suspicious emails to anti-phishing organizations

Thank You