Phishing Awareness Training

Recognizing and Avoiding Cyber Threats

Learn how to identify, avoid, and report phishing attempts to protect yourself and your organization from one of the most common and successful cyber attack vectors.

What is Phishing?

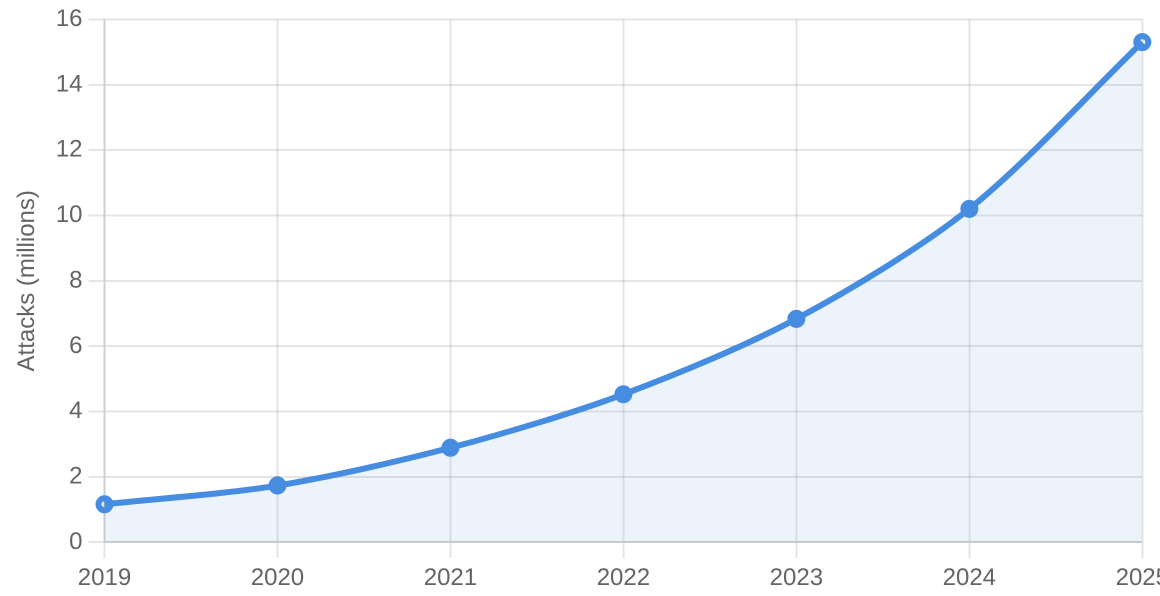
"Phishing is a type of social engineering attack where attackers disguise themselves as trusted entities to trick victims into revealing sensitive information or installing malware."

History: Evolved from simple AOL scams in the 1990s to today's sophisticated techniques targeting multiple platforms and using advanced technologies.

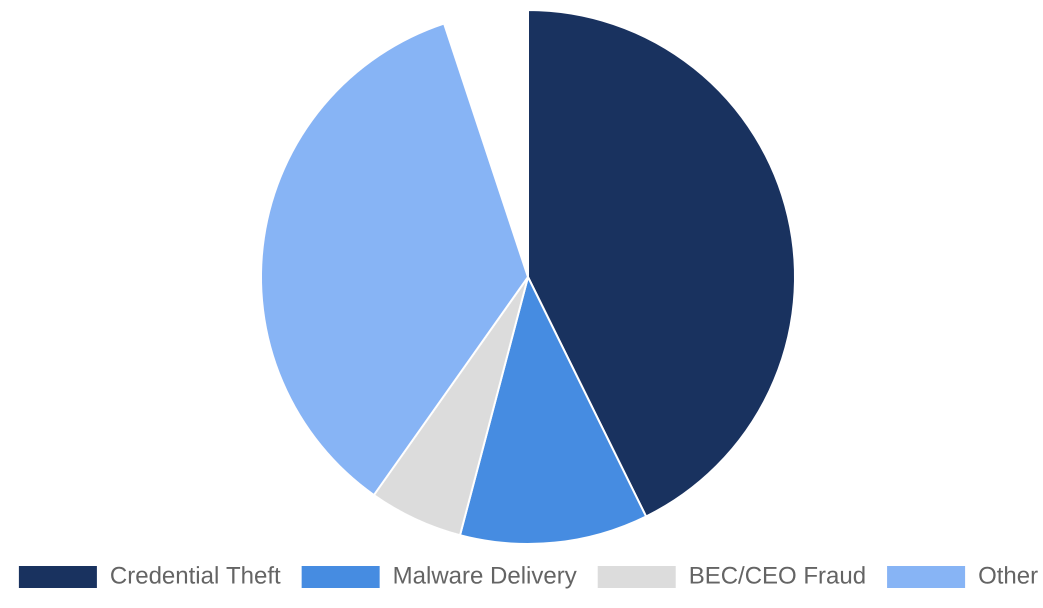
Impact: Phishing accounts for more than 80% of reported security incidents, with an average data breach cost of $4.65 million.

Scale: 3.4 billion phishing emails are sent daily, with attacks increasing by more than 150% yearly since 2019.

Phishing Attack Growth Since 2019



Phishing Attack Distribution



Current Phishing Trends

QR Code Phishing (Quishing)

25% year-over-year increase. Exploits physical spaces like posters or fake business cards to direct victims to malicious websites.

AI-Generated Phishing

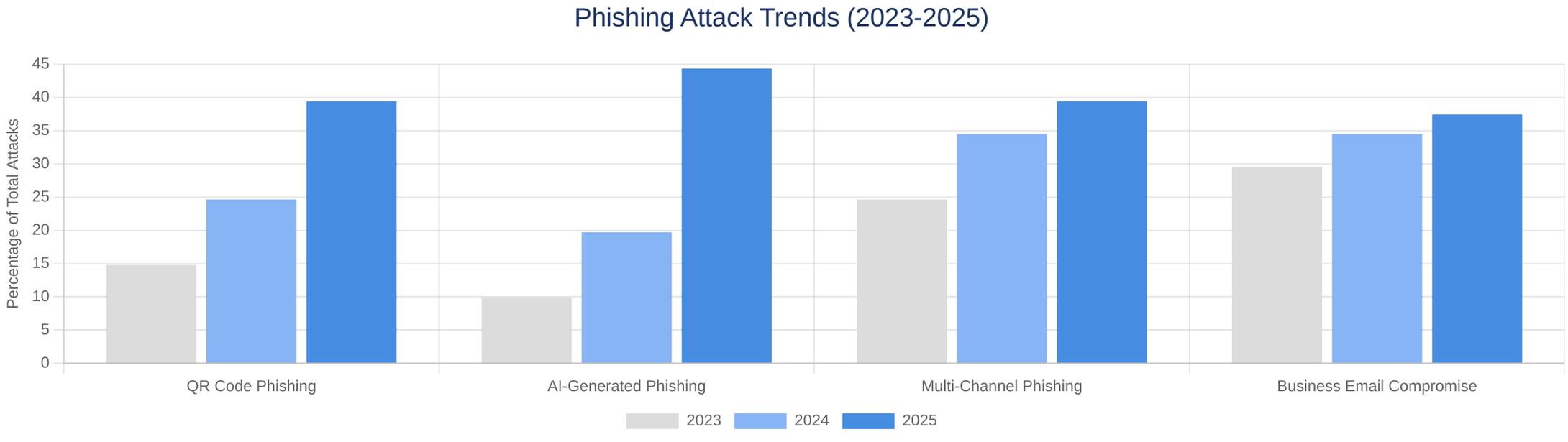
More convincing language with fewer grammatical errors. Personalized content based on public information and ability to mimic writing styles.

Multi-Channel Phishing

Attacks across email, SMS, social media, and messaging apps. Creates sense of legitimacy through multiple touchpoints.

Business Email Compromise

Targets executives and finance departments. Often requests wire transfers or sensitive information with sophisticated impersonation.



Common Types of Phishing Attacks

Email Phishing

Mass-distributed emails impersonating legitimate organizations, containing malicious links or attachments.

Spear Phishing

Targeted attacks using personal information, researched to appear highly relevant to the victim.

Whaling

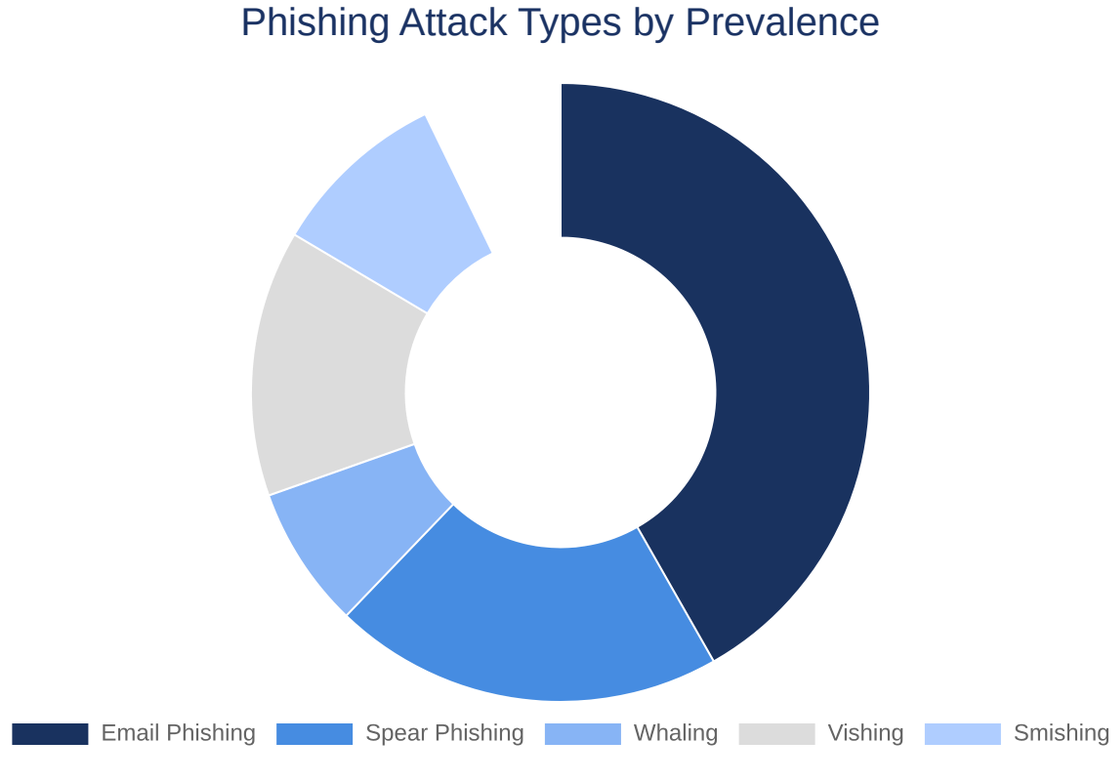
Targets high-profile executives or wealthy individuals, often involving significant financial fraud.

Vishing (Voice Phishing)

Phone calls impersonating trusted entities, often creating urgency to bypass security protocols.

Smishing (SMS Phishing)

Text messages with malicious links, exploiting limited URL visibility on mobile devices.

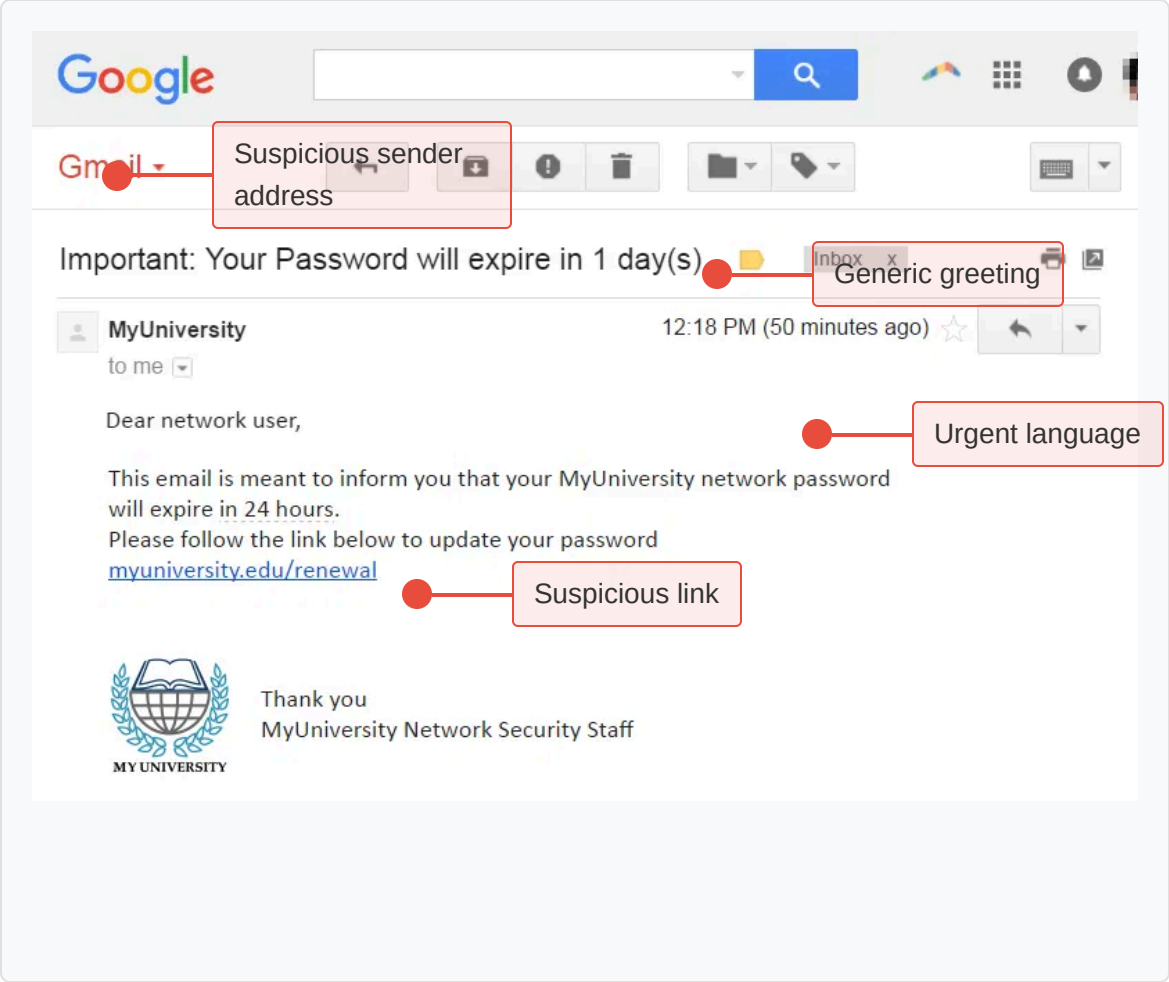


Anatomy of a Phishing Email

Red Flags to Look For:

- Mismatched or suspicious sender email addresses
- Generic greetings ("Dear User" instead of your name)
- Spelling and grammar errors
- Urgent or threatening language
- Requests for sensitive information
- Suspicious attachments or links
- Offers that seem too good to be true

Example of a Phishing Email:



Phishing Websites

How to Identify Fake Websites:

URL Inspection

- Check for misspellings or unusual domains
- Hover over links before clicking
- Be suspicious of URLs with random strings of characters
- Verify the domain matches the expected organization

Security Indicators

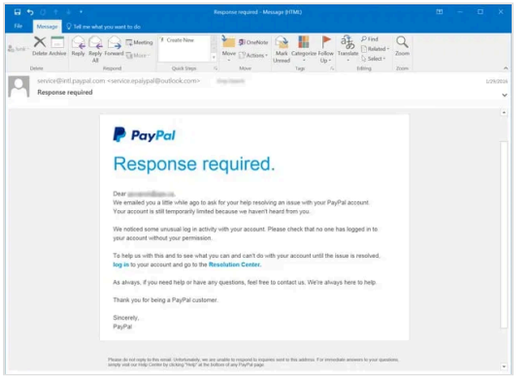
- Look for HTTPS and the padlock icon (but don't rely solely on these)
- Check for valid security certificates
- Be aware that phishing sites can also use HTTPS

Visual Cues

- Poor design, low-quality images, or inconsistent branding
- Unusual pop-ups requesting personal information
- Misaligned elements or unprofessional appearance

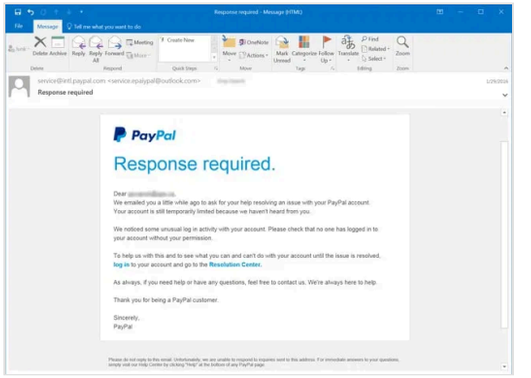
Legitimate vs. Phishing Website:

Legitimate Website



Notice: Correct domain, professional design, secure connection (HTTPS), no suspicious elements.

Phishing Website



Red Flags: Misspelled domain (faceb00k.com), poor quality logo, suspicious form fields, missing security indicators.

Social Engineering Tactics

> *"Social engineering is the psychological manipulation of people into performing actions or divulging confidential information."*

Common Manipulation Techniques:

Authority

Impersonating figures of authority like executives, IT staff, or government officials to gain compliance.

Urgency

Creating time pressure to force quick decisions without proper verification or thought.

Scarcity

Limiting availability to encourage action, such as "limited time offer" or "act now before it's gone."

Familiarity

Exploiting trust in known entities by impersonating colleagues, friends, or trusted brands.

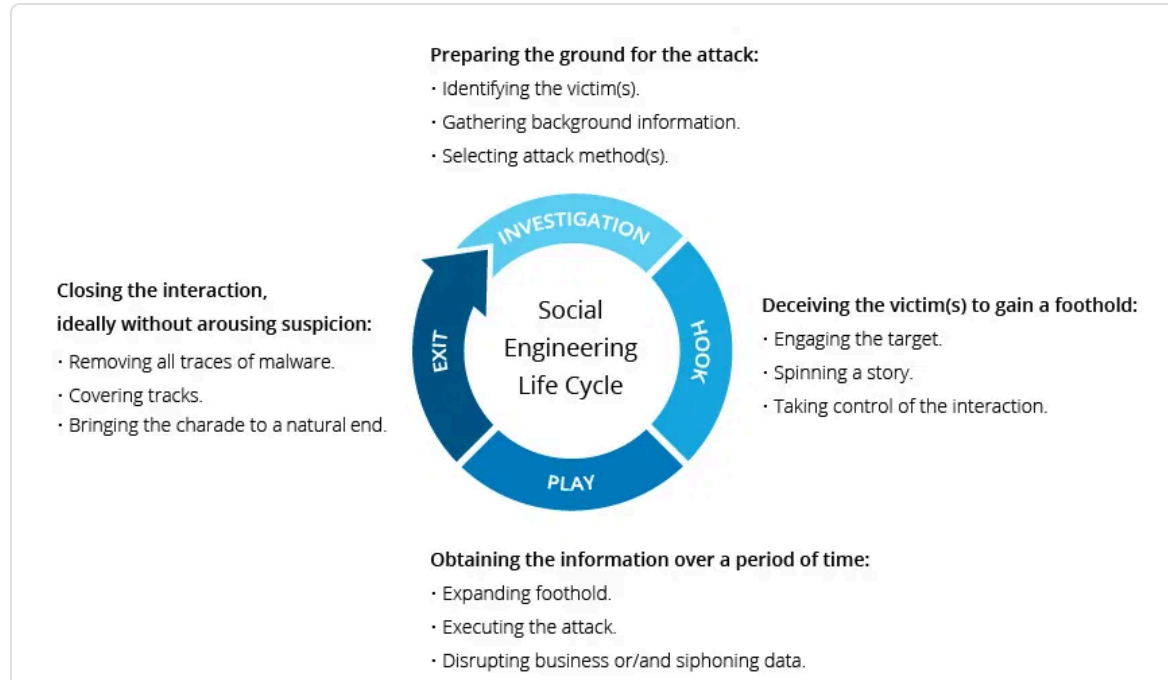
Fear

Using threats or warnings to provoke action, such as account suspension or legal consequences.

Curiosity

Enticing victims with intriguing content that encourages them to click links or open attachments.

Real-World Example:



In this example, attackers combine multiple techniques: authority (impersonating a bank), urgency (account suspension), fear (financial loss), and a call to action that leads to credential theft.

Best Practices to Avoid Phishing

Email Security

- ✓ Verify sender addresses carefully
- ✓ Don't click on suspicious links or attachments
- ✓ Be skeptical of urgent requests, especially involving money or credentials
- ✓ Contact the purported sender through a known, legitimate channel when in doubt

Website Verification

- ✓ Type URLs directly instead of clicking links
- ✓ Use bookmarks for frequently visited sensitive sites
- ✓ Verify site security certificates
- ✓ Check for HTTPS but remember it's not a guarantee of legitimacy

Additional Protection

- ✓ Enable multi-factor authentication wherever possible
- ✓ Use a password manager for unique, complex passwords
- ✓ Keep software and systems updated
- ✓ Use email filtering and anti-phishing tools

Effectiveness of Security Measures

Remember the S.T.O.P. Method:

Stop and think before clicking or responding
Think about whether the message seems legitimate
Observe the sender, content, and links for red flags
Protect yourself by verifying through official channels

What to Do If You Suspect Phishing

Immediate Steps

1. Don't click any links or download attachments
2. Don't reply to the message
3. If you've clicked a link or provided information, disconnect from the network
4. Change compromised passwords immediately

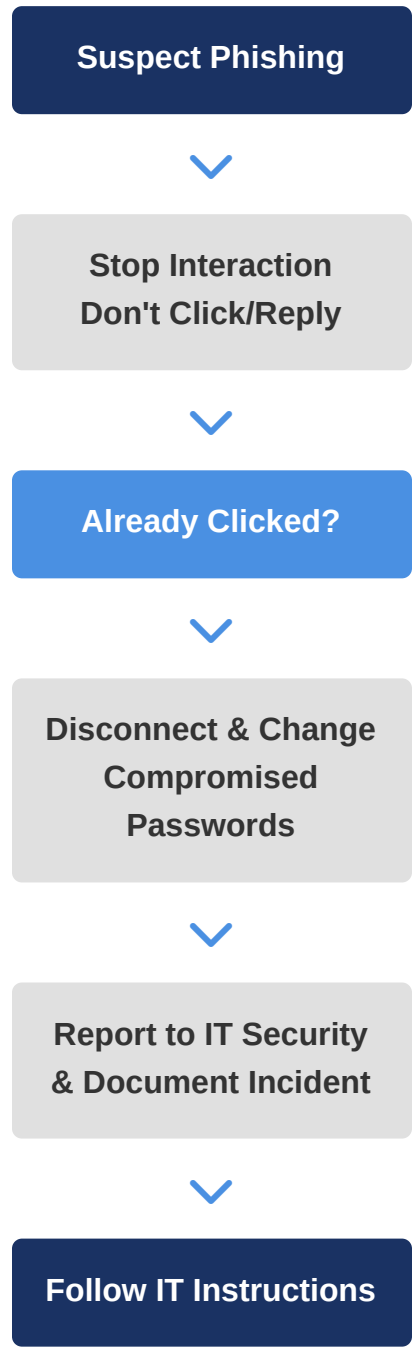
Reporting Procedures

1. Forward suspicious emails to IT security team
2. Use the "Report Phishing" button in email client if available
3. Document the incident with screenshots
4. Report to the organization being impersonated

Contact Information:

- IT Security: security@company.com
- Security Helpdesk: 555-123-4567
- Internal Security Portal: security.company-intranet.com

Phishing Incident Response Flowchart



Summary and Key Takeaways

Remember:

- Phishing attacks are constantly evolving - stay vigilant and keep learning about new techniques.
- Always verify before trusting - check sender addresses, inspect URLs, and be skeptical of urgent requests.
- When in doubt, reach out through official channels - never use contact information provided in suspicious messages.
- Report suspicious activities immediately - your vigilance helps protect the entire organization.

Resources:

Internal Security Portal

Access security guides, reporting tools, and latest phishing alerts.

Advanced Security Training

Sign up for additional training modules on cybersecurity best practices.

Phishing Simulation Program

Practice identifying phishing attempts in a safe environment.

Questions? Let's discuss how to apply these practices in your daily work.