CSNP
CYBERSECURITY NON-PROFIT

# Phishing Defense Guide

Essential strategies to protect your organization from phishing attacks and social engineering threats

CYBERSECURITY NON-PROFIT (CSNP)

# Understanding Phishing Attacks

Phishing is a cybercrime where attackers impersonate legitimate organizations to steal sensitive information, credentials, or money. These attacks exploit human psychology rather than technical vulnerabilities, making them one of the most dangerous and prevalent cyber threats facing organizations today.

Attackers craft convincing messages that create urgency, fear, or curiosity to bypass rational decision-making. Understanding how these attacks work is the first step in building a robust defense.

**91%**

### Cyberattacks

Begin with phishing emails

**$4.9M**

### Average Cost

Per data breach incident

# Types of Phishing Attacks

### Email Phishing

Mass emails impersonating trusted brands, containing malicious links or attachments designed to steal credentials or install malware.

### SMS Phishing (Smishing)

Text messages with urgent requests or fake alerts, often claiming account issues or delivery problems to trick recipients into clicking links.

### Voice Phishing (Vishing)

Phone calls from scammers posing as tech support, banks, or government agencies, pressuring victims to share sensitive information.

### Spear Phishing

Highly targeted attacks using personalized information about specific individuals or organizations to increase credibility and success rates.

# Red Flags: Spotting Phishing Attempts

### Urgent or threatening language

Messages creating panic like "Account will be closed!" or "Immediate action required!" are designed to bypass careful thinking.

### Suspicious sender addresses

Look closely at email domains. "support@amaz0n.com" or "paypal-security@gmail.com" are red flags indicating impersonation.

### Generic greetings

"Dear Customer" instead of your name suggests mass phishing. Legitimate companies usually personalize communications.

### Unexpected attachments or links

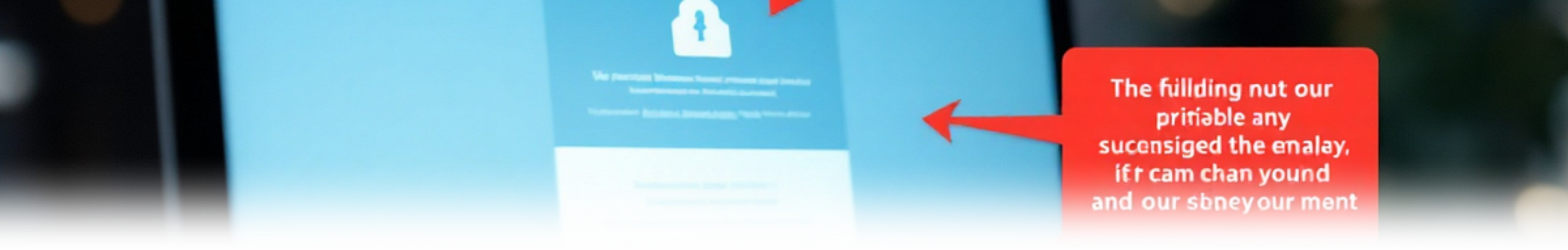
Unsolicited files or links, especially from unknown senders, may contain malware or lead to fake login pages.

### Requests for sensitive information

Legitimate organizations never ask for passwords, Social Security numbers, or credit card details via email or text.

### Poor grammar and spelling

Professional organizations proofread their communications. Multiple errors often indicate scam attempts.



# Anatomy of a Phishing Email

### Real Example Analysis

Examining actual phishing attempts helps train your eye to spot deception techniques used by attackers.

### Fake sender address

Domain doesn't match the company claimed (e.g., "security-team@verify-account-now.com" instead of official domain)

### Generic greeting

"Dear User" instead of your actual name shows this is a mass attack, not legitimate personalized communication

### Urgent threat

"Your account will be suspended in 24 hours" creates artificial panic to force quick, unthinking action

### Suspicious link

Hovering reveals the URL doesn't match the claimed destination—leads to a fake lookalike website

# Technical Defense Strategies

## Email Security

- Deploy email filtering and anti-spam solutions
- Enable SPF, DKIM, and DMARC authentication
- Configure advanced threat protection
- Block executable attachments (.exe, .scr)
- Implement link scanning and sandboxing

## Endpoint Protection

- Install and maintain antivirus/anti-malware
- Keep all software and systems updated
- Enable automatic security patches
- Use endpoint detection and response (EDR)

## Access Controls

- Implement multi-factor authentication (MFA)
- Enforce strong password policies
- Use password managers organization-wide
- Apply principle of least privilege access
- Monitor for suspicious login attempts

## Network Security

- Deploy web filtering and DNS protection
- Segment networks to limit breach impact
- Monitor outbound traffic for data theft
- Use VPNs for remote access

# Employee Training & Awareness

Technology alone cannot stop phishing—your employees are your strongest defense when properly trained. Regular education and simulated phishing exercises build organizational resilience.

01

## Conduct regular security awareness training

Quarterly sessions covering latest threats, real examples, and defense techniques keep security top-of-mind.

02

## Run simulated phishing campaigns

Test employee readiness with safe, controlled phishing tests to identify vulnerabilities and reinforce learning.

03

## Create clear reporting procedures

Establish simple, quick methods for employees to report suspicious messages without fear of punishment.

04

## Share threat intelligence updates

Regularly communicate new phishing trends and tactics targeting your industry or organization.

05

## Celebrate security victories

Recognize employees who identify and report threats to build a positive security culture.

# Incident Response: When Phishing Succeeds

1

### Immediate Containment

Isolate affected systems from the network. Disable compromised accounts. Change passwords immediately.

2

### Assess the Damage

Determine what information was accessed or stolen. Check for malware installation. Review system logs for unauthorized access.

3

### Notify Stakeholders

Alert IT security team, management, and affected individuals. Report to relevant authorities if required by law.

4

### Remediate & Recover

Remove malware, restore from clean backups, patch vulnerabilities. Implement additional security controls.

5

### Learn & Improve

Conduct post-incident review. Update security policies. Provide additional training to prevent recurrence.

# Your Phishing Defense Checklist

## Essential Protections

- Email filtering and authentication enabled
- Multi-factor authentication deployed
- Antivirus and endpoint protection active
- Regular software updates and patches
- Web filtering and DNS protection
- Quarterly security awareness training
- Simulated phishing tests conducted
- Clear incident reporting process
- Incident response plan documented
- Regular security policy reviews
- Password manager for all employees
- Network segmentation implemented

**Download the complete checklist:** Visit csnp.org/resources for printable security assessment tools and implementation guides.

# About Cybersecurity Non-Profit (CSNP)

> Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.

## Our Programs

### Business & Non-Profit Security

Protecting organizations of all sizes

### Family Cybersecurity

Keeping households safe online

### Kids Safety

Digital citizenship for young learners

### Senior Digital Safety

Protecting older adults from scams

### Women's Security

Privacy and safety education

### Parents & Educators

Tools to teach digital safety

---

**Everything we offer is completely free.** Access our full library of guides, training materials, and resources at **csnp.org/resources**

Visit CSNP.org

Browse Resources