CSNP
CYBERSECURITY NON-PROFIT

Phishing Simulation Guide

A practical framework for running effective internal security awareness campaigns

CYBERSECURITY NON-PROFIT (CSNP)

Why Run Phishing Simulations

Identify Vulnerabilities

Discover which employees are most susceptible to phishing attacks before real threats strike your organization.

Build Awareness

Transform abstract security concepts into memorable learning experiences through realistic, safe practice scenarios.

Strengthen Defense

Create a human firewall by developing instinctive threat recognition across your entire team through regular training.

Measure Progress

Track improvement over time with concrete metrics that demonstrate the ROI of your security awareness investments.

Planning Your Campaign

Essential Preparation Steps

01

Secure Leadership Buy-In

Present business case and get executive approval

02

Define Clear Objectives

Set measurable goals and success criteria

03

Communicate Transparently

Inform staff about the program's educational purpose

04

Choose Your Platform

Select simulation tools that fit your budget

05

Schedule Strategically

Plan timing to avoid busy periods or major projects

Key Considerations

Legal & HR Alignment: Work with your legal and HR teams to ensure compliance with company policies and employment laws. Document consent procedures clearly.

Culture Matters: Frame simulations as learning opportunities, not "gotcha" moments. Foster psychological safety to encourage reporting of mistakes.

Resource Planning: Allocate time for campaign design, execution, analysis, and follow-up training. Budget for tools if needed.

Creating Realistic Scenarios

Effective phishing simulations mirror real-world attack patterns while remaining ethical and educational. Design scenarios that challenge your team without causing undue stress or embarrassment.

1

IT Department Requests

Password resets, system upgrades, or urgent security alerts from supposed IT staff

2

Executive Impersonation

Requests from C-suite executives for urgent wire transfers or sensitive information

3

Vendor Communications

Invoices, shipment notifications, or account issues from familiar business partners

4

HR Announcements

Benefits updates, policy changes, or required training with embedded malicious links

Email Template Examples

Password Expiration Alert

Subject: [URGENT] Your password expires in 24 hours

Your company password will expire tomorrow. Click here to reset it now and avoid account lockout. Failure to update will result in loss of system access.

Red flags: Urgency, generic greeting, suspicious link

Package Delivery Notice

Subject: Delivery Attempted - Action Required

We attempted to deliver your package but no one was available. Click to reschedule delivery or your package will be returned to sender within 48 hours.

Red flags: Unexpected delivery, time pressure, unfamiliar sender

CEO Urgent Request

Subject: Need this ASAP

I'm in meetings all day and need you to handle something confidential. Please purchase gift cards for a client event. Reply with confirmation once completed.

Red flags: Unusual request, pressure, requesting financial action via email

Landing Page Setup

When users click simulation links, redirect them to educational landing pages that explain what happened and why it matters.

Clear Alert Message

Inform them this was a test in a non-punitive, supportive tone

Explain the Warning Signs

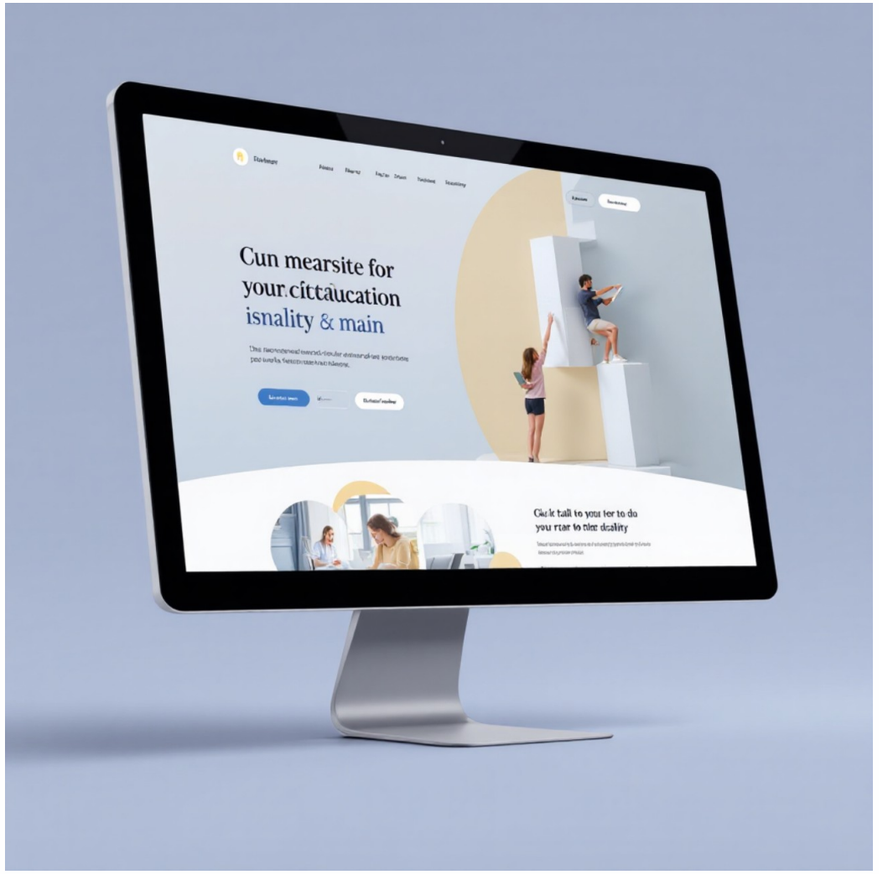
Point out specific red flags they should have noticed

Provide Actionable Tips

Offer concrete steps to identify future phishing attempts

Link to Resources

Direct them to additional training materials and reporting procedures



Best Practice: Keep landing pages positive and educational. Avoid shame or blame language. Emphasize that everyone can fall for sophisticated attacks, and learning to recognize them is a skill that improves with practice.

Measuring Campaign Results

23%	8%	12%	47
Click Rate	**Data Submission**	**Reporting Rate**	**Response Time**
Percentage of recipients who clicked the phishing link	Users who entered credentials or sensitive information	Employees who reported the suspicious email to IT	Average minutes until first click or report

Track these metrics over multiple campaigns to identify trends, high-risk departments, and the effectiveness of remediation training. Compare results against industry benchmarks and your own baseline to demonstrate improvement.

Remediation & Progressive Difficulty

Remediation Training

Employees who fail simulations should receive immediate, targeted education:

- Short microlearning modules (5-10 minutes)
- Interactive scenarios with real-world examples
- Clear guidance on reporting procedures
- Follow-up assessments to confirm understanding
- Supportive tone that encourages improvement

Make remediation convenient and accessible. Mandatory training should be scheduled during work hours and shouldn't feel like punishment.

Progressive Difficulty Levels

Level 1: Basic

Obvious spelling errors, generic greetings, suspicious sender domains

Level 2: Intermediate

Legitimate-looking senders, branded templates, contextually relevant

Level 3: Advanced

Sophisticated spoofing, personalized content, timely business context

Level 4: Expert

CEO fraud, vendor compromise scenarios, multi-stage attacks

Sample 12-Month Campaign Calendar

Q1: Foundation

Jan: Announce program & baseline simulation

Feb: Basic IT request scenario

Mar: Results review & training

Q2: Building Skills

Apr: Vendor impersonation

May: HR policy update

Jun: Mid-year assessment

Q3: Advanced

Jul: Executive fraud attempt

Aug: Multi-stage campaign

Sep: Department-specific scenarios

Q4: Mastery

Oct: Sophisticated spear-phishing

Nov: Holiday-themed attacks

Dec: Annual review & planning

Space campaigns 4-6 weeks apart to allow time for training and skill development. Vary timing and scenarios to prevent pattern recognition. Coordinate with your IT team to ensure simulations don't conflict with real security incidents or major projects.

Cybersecurity Non-Profit (CSNP)

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

Our Programs

Business & Non-Profit Security – Practical guidance for organizations

Family Cybersecurity – Protecting your household digital life

Kids Safety – Age-appropriate online safety education

Senior Digital Safety – Empowering older adults online

Women's Security – Specialized privacy and safety resources

Parents & Educators – Tools to teach digital citizenship

Everything we offer is completely free – because cybersecurity education should be accessible to everyone.

Visit csnp.org

Browse Resources