CSNP
CYBERSECURITY NON-PROFIT

Security Awareness Training

Essential cybersecurity knowledge for protecting your organization and personal data

CSNP TRAINING PROGRAM

Why Security Matters

95%

Human Error

Percentage of cybersecurity breaches caused by human mistakes

$4.45M

Average Cost

Average cost of a data breach in 2023

277

Days to Identify

Average time to identify and contain a breach

Every employee plays a critical role in protecting organizational data, client information, and business continuity. Security awareness isn't just IT's responsibility—it's everyone's.

Common Cyber Threats

Phishing

Deceptive emails designed to steal credentials or install malware

Malware

Malicious software including ransomware, spyware, and trojans

Social Engineering

Manipulation tactics to trick people into revealing sensitive information

Weak Passwords

Easy-to-guess credentials that provide unauthorized access

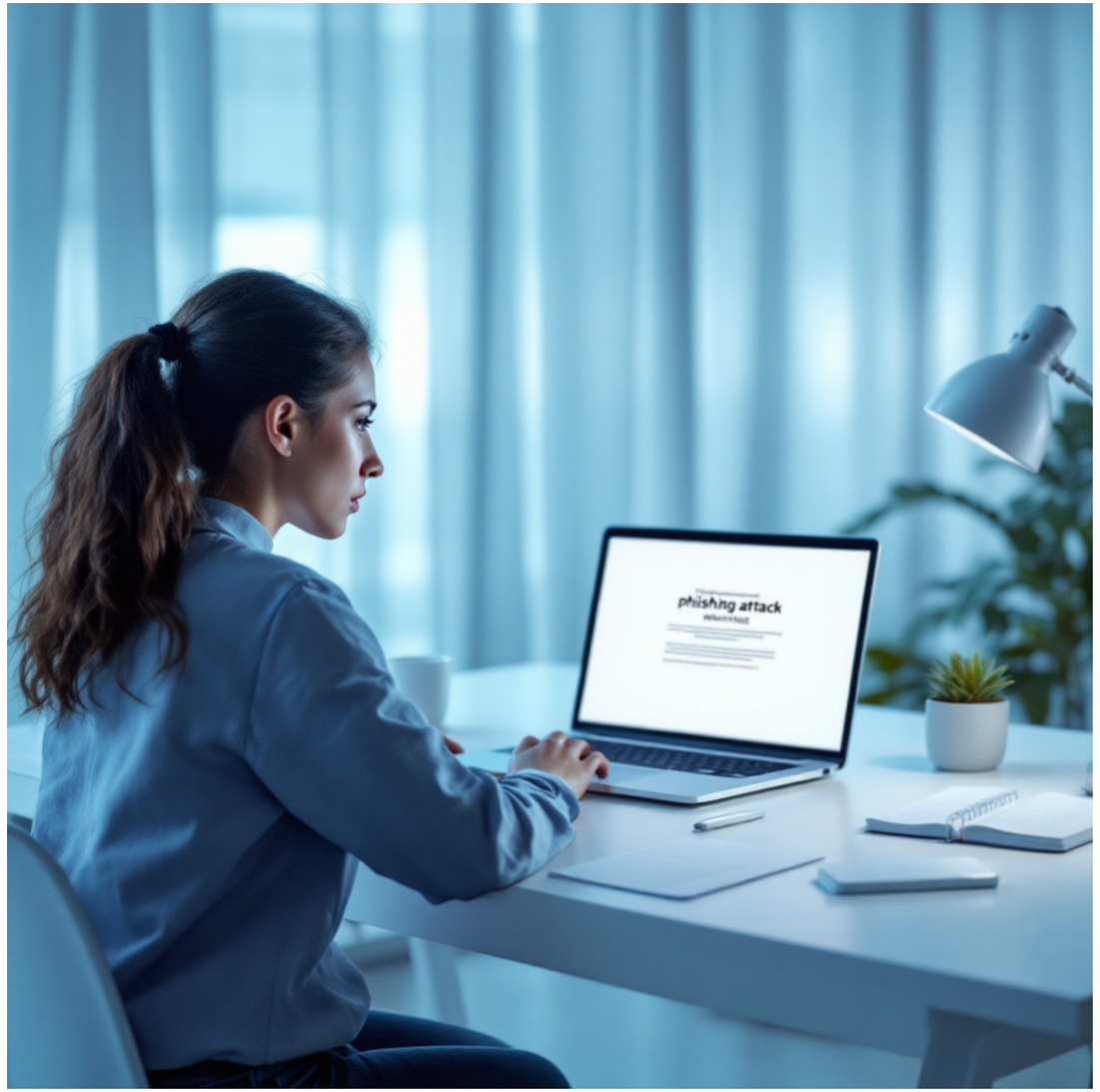
Understanding Phishing Attacks

What is Phishing?

Phishing is a fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity in electronic communications.

Common Tactics

- Urgent or threatening language
- Requests for personal information
- Suspicious links or attachments
- Too-good-to-be-true offers
- Impersonating trusted brands



Real Phishing Examples

1

Fake IT Department

> "Your password will expire in 24 hours. Click here to update immediately or your account will be locked."

Red flags: Urgency, suspicious link, IT departments don't request credentials via email

2

CEO Impersonation

> "This is urgent. I need you to purchase gift cards for a client meeting. Reply with confirmation ASAP."

Red flags: Unusual request, pressure tactics, asks for immediate action outside normal channels

3

Package Delivery Scam

> "Your package couldn't be delivered. Click to reschedule delivery and verify your address."

Red flags: Unexpected delivery, suspicious link, requests personal information

Password Security Fundamentals

Your First Line of Defense

Passwords protect access to sensitive systems, data, and communications. Weak passwords are like leaving your office door unlocked overnight.

The High Cost of Compromise

81% of data breaches involve weak or stolen passwords. Once compromised, attackers can access email, financial systems, and confidential information.

Password Best Practices

01

Use Strong, Unique Passwords

Create passwords with at least 12 characters combining uppercase, lowercase, numbers, and symbols. Never reuse passwords across accounts.

02

Enable Multi-Factor Authentication

Add an extra security layer requiring a second form of verification beyond your password, such as a code sent to your phone.

03

Use a Password Manager

Store passwords securely in encrypted password managers like Bitwarden, 1Password, or LastPass instead of writing them down or reusing them.

04

Change Compromised Passwords Immediately

If you suspect a password has been compromised or appears in a data breach, change it immediately and review account activity.

Social Engineering Tactics

What is Social Engineering?

Psychological manipulation techniques that exploit human trust and behavior to gain unauthorized access to information or systems.

Common Techniques

Pretexting: Creating false scenarios to extract information

Baiting: Offering something enticing to install malware

Tailgating: Following authorized persons into restricted areas

Quid pro quo: Offering services in exchange for information

Defense Strategy

Verify, verify, verify. Always confirm requests through official channels, especially for sensitive information or unusual requests. Trust your instincts—if something feels off, it probably is.

Physical Security Matters

Secure Workspaces

Lock doors and cabinets containing sensitive materials. Never prop open secured doors or share access codes with unauthorized individuals.

Visitor Management

Challenge unfamiliar people in secure areas. Ensure visitors sign in, wear badges, and are escorted when necessary.

Lock Your Screen

Always lock your computer when stepping away, even briefly. Use Windows Key + L or Command + Control + Q as quick shortcuts.

Protect Credentials

Never share access badges or passwords. Report lost or stolen badges immediately to security or IT.

Mobile Device Security

Enable Screen Locks

Use PIN, password, fingerprint, or face recognition on all devices

Keep Updated

Install security updates and patches promptly to fix vulnerabilities

Vet Applications

Only download apps from official stores and review permissions carefully

Enable Remote Wipe

Configure ability to remotely erase data if device is lost or stolen

Public WiFi Risks

The Dangers of Open Networks

Public WiFi networks at coffee shops, airports, and hotels are convenient but dangerous. Attackers can intercept unencrypted data, set up fake networks, or deploy man-in-the-middle attacks.

Safe Practices

- Avoid accessing sensitive accounts or financial information
- Use a VPN to encrypt your internet connection
- Verify network names with staff before connecting
- Disable automatic WiFi connections
- Use your mobile hotspot when possible
- Ensure websites use HTTPS encryption

Data Protection Principles

Classify Information

Understand what data is public, internal, confidential, or restricted. Handle each classification appropriately based on organizational policies.

Encrypt Sensitive Data

Use encryption for sensitive files, especially when storing on portable devices or transmitting via email or cloud services.

Minimize Data Collection

Only collect and retain data necessary for business purposes. Securely dispose of information when no longer needed.

Control Access

Implement least-privilege access—people should only access data required for their role. Review permissions regularly.

Clean Desk Policy

Clear Surfaces

Remove sensitive documents, notes, and removable media from desks when not in use

1

Secure Storage

2

Lock confidential materials in drawers or filing cabinets at end of day

Proper Disposal

3

Shred sensitive documents; never throw them in regular trash bins

Screen Privacy

4

Position monitors away from public view and use privacy screens when necessary

Why it matters: A clean desk policy prevents unauthorized access to sensitive information, protects client confidentiality, and demonstrates professional security practices.

Incident Reporting

Recognize the Incident

Suspicious emails, unexpected system behavior, lost devices, unauthorized access attempts, or potential data breaches

Stop and Contain

Disconnect from network if compromised, don't click suspicious links, preserve evidence, and prevent further damage

Report Immediately

Contact IT security team, provide detailed information about what happened, when, and what systems were affected

Document Everything

Record timeline of events, screenshots, error messages, and any actions taken for investigation purposes

Remote Work Security

Secure Your Home Network

Change default router passwords, enable WPA3 encryption, keep firmware updated, and use a separate network for work devices when possible.

Create a Private Workspace

Work in areas where screens aren't visible to family members or through windows. Be mindful of background visuals during video calls.

Use Company-Approved Tools

Only use authorized software, cloud services, and communication platforms. Don't use personal accounts for work purposes.

Maintain Device Security

Keep work and personal activities separate, use VPN for company network access, and ensure anti-virus software is active and updated.

KNOWLEDGE CHECK

Security Awareness Quiz

Test your knowledge with these scenarios. Think carefully about the best response in each situation.

Question 1

You receive an urgent email from your "CEO" requesting an immediate wire transfer. The email address looks slightly off. What should you do?

Question 2

A visitor says they're from IT and need your password to "fix your computer remotely." What's the appropriate response?

Question 3

You find a USB drive labeled "Salary Information" in the parking lot. What should you do with it?

KNOWLEDGE CHECK

Quiz Answers

1

Verify Through Official Channels

Correct action: Never act on urgent financial requests via email alone. Contact the CEO directly using a known phone number or communication method. This is a classic CEO fraud phishing attempt.

2

Refuse and Report

Correct action: IT departments never ask for passwords. Politely refuse, verify their identity with your IT department, and report the incident immediately. This is social engineering.

3

Don't Plug It In

Correct action: Turn it in to security without connecting it to any computer. This could be a "baiting" attack with malware designed to infect systems when plugged in.

Key Takeaways

Security is Everyone's Responsibility

Every employee is a critical line of defense. Your awareness and actions protect the entire organization from cyber threats and data breaches.

Stay Vigilant and Skeptical

Question unusual requests, verify identities, think before clicking, and trust your instincts. When in doubt, report it.

Follow Best Practices Consistently

Strong passwords, locked screens, secure devices, and proper data handling should become automatic habits in your daily workflow.

Report Incidents Immediately

Quick reporting enables fast response, minimizes damage, and protects others. No incident is too small to report.

Additional Resources

Continuous Learning

Cybersecurity threats evolve constantly. Stay informed and refresh your knowledge regularly through these resources:

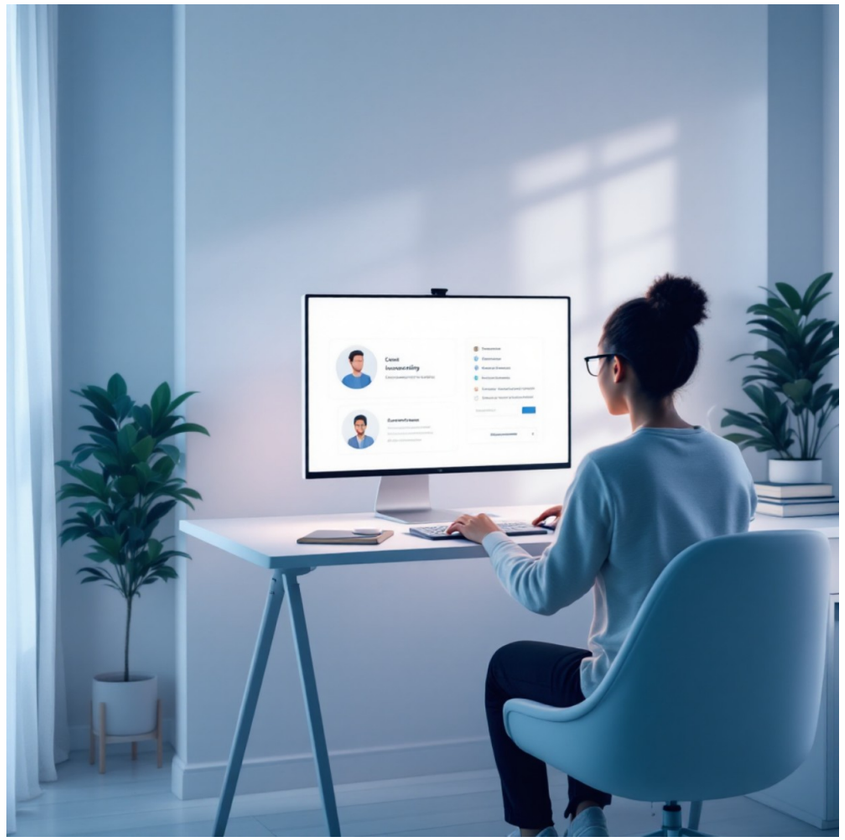
CSNP Resource Library: csnp.org/resources

Training Materials: Interactive modules and guides

Security Updates: Monthly threat briefings

Quick Reference Guides: Downloadable checklists

IT Support: Contact your security team anytime



Remember: This training is just the beginning. Apply these principles daily, stay curious about emerging threats, and never hesitate to ask questions or report concerns.

About CSNP

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

Our Programs

- Business & Non-Profit Security
- Family Cybersecurity
- Kids Safety Online
- Senior Digital Safety
- Women's Security Awareness
- Resources for Parents & Educators

Everything is Free

All CSNP training, resources, and support materials are provided at no cost. We believe cybersecurity education should be accessible to organizations and individuals of all sizes.

Get Started Today

Website: csnp.org

Resources: csnp.org/resources

Join our community and access comprehensive cybersecurity education tailored to your needs.