CSNP
CYBERSECURITY NON-PROFIT

Security Awareness Posters

A comprehensive collection of printable security posters designed to strengthen your organization's security culture. Display these throughout your office to keep security top-of-mind for all employees.

CSNP RESOURCES   FREE TO PRINT

Strong Passwords Save Accounts

Create Strong Passwords

- Use 12+ characters minimum
- Mix letters, numbers, symbols
- Avoid personal information
- Make each password unique

Use a Password Manager

- Securely stores all passwords
- Generates strong passwords
- Auto-fills login forms
- Syncs across devices

Enable Two-Factor Authentication

- Adds extra security layer
- Protects even if password leaks
- Use authenticator apps
- Enable on all critical accounts

Your password is the first line of defense. Never share it with anyone, and change it immediately if you suspect it's been compromised.

Don't Take the Bait: Spot Phishing

Warning Signs

- Urgent or threatening language
- Requests for personal information
- Suspicious sender addresses
- Unexpected attachments
- Grammar and spelling errors
- Links that don't match destinations

Stay Safe

- Verify sender identity independently
- Hover over links before clicking
- Never provide credentials via email
- Report suspicious messages
- When in doubt, contact IT
- Trust your instincts

> **Remember:** Legitimate organizations will never ask for passwords or sensitive data via email. If something feels off, it probably is.

Lock Your Screen

Step away? Lock it! Windows: Win+L | Mac: Cmd+Ctrl+Q. Set auto-lock after 5 minutes of inactivity.

Keep Your Desk Clear

Lock away sensitive documents at day's end. Shred what you don't need. No sticky notes with passwords!

Physical security is cybersecurity. Simple habits like locking your screen and maintaining a clean desk prevent unauthorized access and protect sensitive information. These small actions make a big difference in your organization's overall security posture.

See Something? Say Something!

01

Recognize Suspicious Activity

Unknown devices, unusual system behavior, unauthorized access attempts, unexpected requests for information, or anything that doesn't feel right.

02

Document What You Observed

Note the time, location, people involved, and specific details about the incident. Screenshots can be helpful if applicable.

03

Report Immediately

Contact your IT security team or designated security officer right away. Don't wait—early reporting can prevent breaches.

04

Follow Up

Stay available to provide additional information if needed. Your vigilance protects everyone in the organization.

You're not being paranoid—you're being prepared. Every report helps us improve security for everyone.

Social Engineering: The Human Hack

Social engineering attacks manipulate human psychology rather than exploiting technical vulnerabilities. Attackers use trust, authority, urgency, and fear to trick people into breaking security protocols.

Common Tactics

Pretexting: Creating fake scenarios to extract information

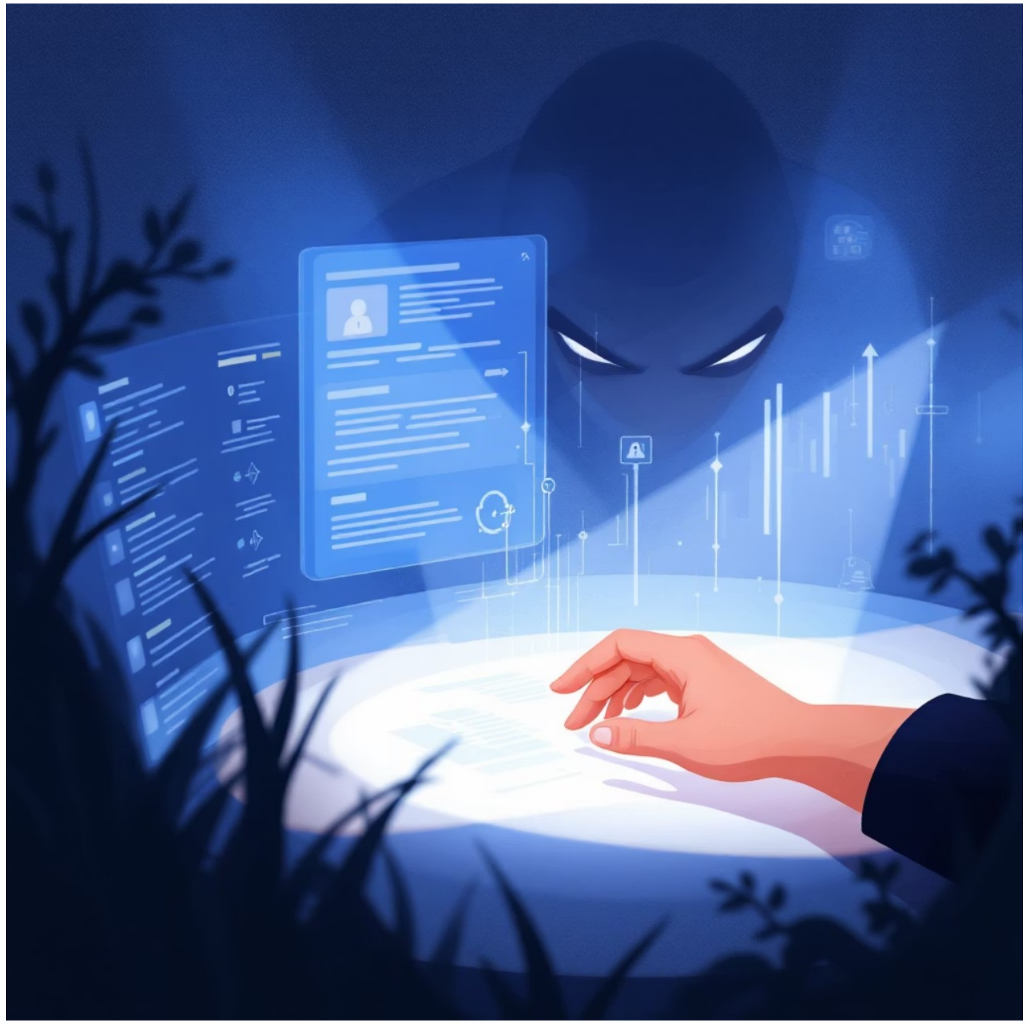
Baiting: Offering something enticing to deploy malware

Tailgating: Following authorized personnel into secure areas

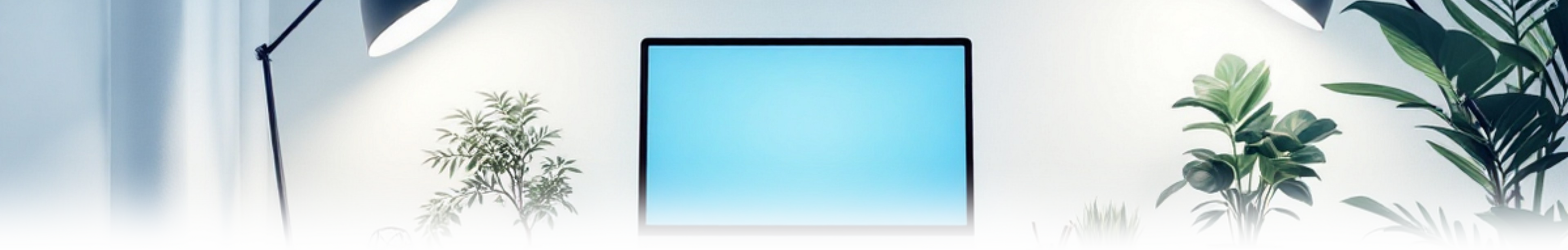
Impersonation: Posing as IT, executives, or vendors

Protect Yourself

- Verify identities through official channels
- Question unusual requests, even from "authority"
- Never bypass security procedures for convenience



> "The weakest link in security is always the human element."



Data Protection & Remote Work Security

1

Encrypt Sensitive Data

Use encryption for files containing personal information, financial data, or confidential business information. Enable full-disk encryption on all devices.

2

Secure Your Home Network

Change default router passwords, enable WPA3 encryption, keep firmware updated, and use a VPN when accessing company resources remotely.

3

Protect Company Devices

Never leave laptops unattended in public spaces. Use privacy screens in shared areas. Keep devices updated with latest security patches.

4

Be Mindful of Your Surroundings

Avoid discussing sensitive information in public. Be aware of shoulder surfers. Use headphones for confidential video calls.

Cybersecurity Non-Profit

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

Business & Non-Profit Security

Family Cybersecurity

Kids Safety

Senior Digital Safety

Women's Security

Parents & Educators

Everything We Offer Is Free

We believe cybersecurity education should be accessible to everyone, regardless of budget or technical expertise.

Visit csnp.org

Browse Resources