CSNP

CYBERSECURITY NON-PROFIT

Incident Response Training

Essential guidance for recognizing and responding to security incidents effectively. Every employee plays a critical role in protecting our organization.

CYBERSECURITY NON-PROFIT

What is a Security Incident?

A security incident is any event that compromises the confidentiality, integrity, or availability of our information systems or data. These events can range from minor policy violations to major breaches that threaten organizational operations.

Understanding what constitutes an incident is the first step in protecting our organization and the communities we serve.

Common Types of Security Incidents

Phishing Attacks

Deceptive emails or messages attempting to steal credentials or distribute malware

Malware Infections

Viruses, ransomware, or spyware that compromise systems and data

Data Breaches

Unauthorized access to sensitive information or personal data

Unauthorized Access

Compromised accounts or systems accessed by unauthorized individuals

Lost Devices

Missing laptops, phones, or storage devices containing organizational data

Insider Threats

Intentional or accidental misuse of access by employees or contractors

Your Role in Incident Response

01

First Line of Defense

You are often the first to detect unusual activity or suspicious behavior

02

Rapid Reporter

Quick reporting enables faster containment and minimizes potential damage

03

Evidence Preserver

Your actions immediately after detection can preserve critical forensic evidence

04

Security Champion

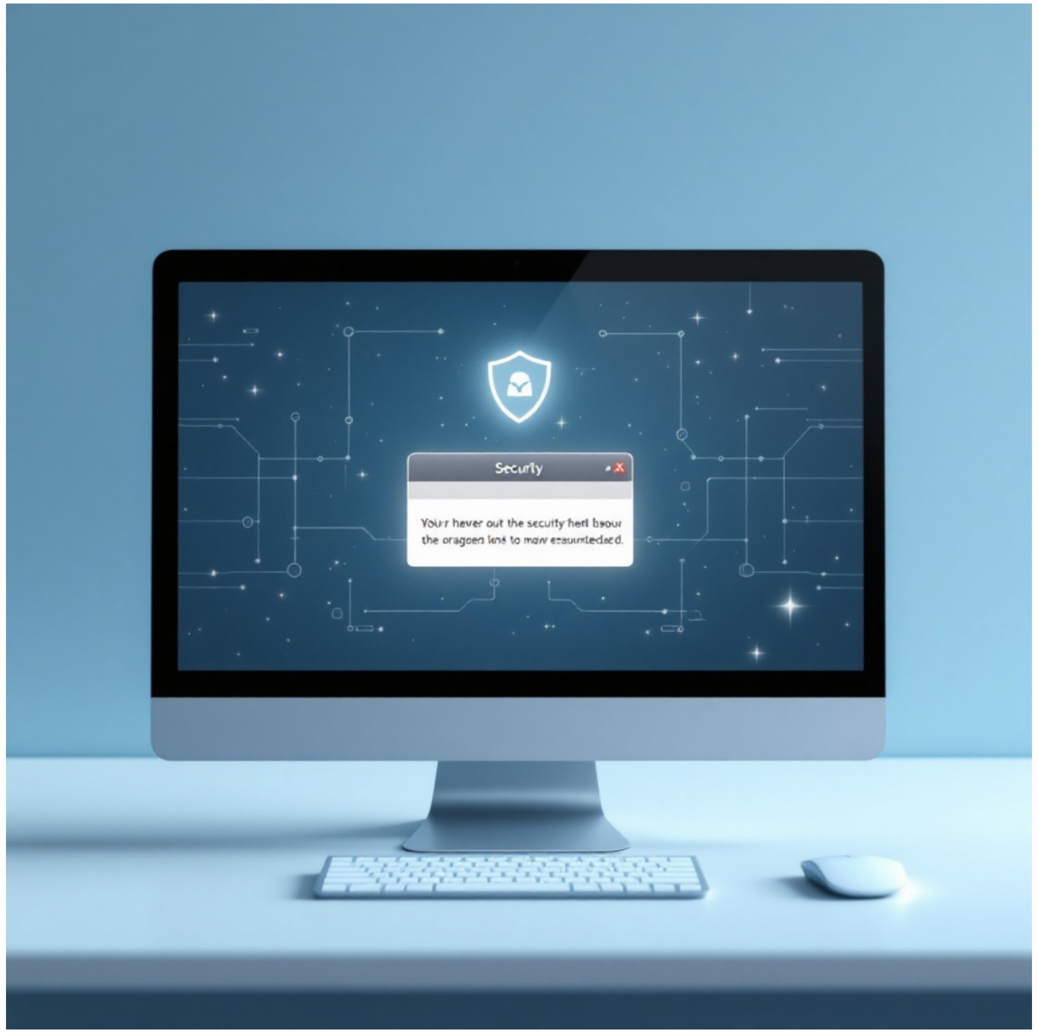
You help create a culture of security awareness throughout the organization

Recognizing Security Incidents

Warning Signs to Watch For

- Unexpected password reset requests or account lockouts
- Unusual system performance or unexplained crashes
- Suspicious emails requesting sensitive information
- Files appearing, disappearing, or being encrypted unexpectedly
- Pop-ups or alerts from unfamiliar security software
- Unusual network activity or slow internet connections
- Colleagues receiving strange emails from your account

Trust your instincts: If something feels wrong, report it immediately.


Securty
Yourr hever out the secutty herl bsour the oragoen lens to maw ezauntedacd.

Immediate Actions: What to Do

Stop and Assess

Pause what you're doing. Don't click further links or open suspicious attachments. Disconnect from the network if actively under attack.

Document Everything

Take screenshots, note the time, and record what happened. Write down any error messages or suspicious details you observed.

Report Immediately

Contact the security team right away. Minutes matter in incident response. Don't wait to see if it resolves itself.

Who to Contact

Security Operations Center (SOC)

Emergency Hotline: 1-800-555-CSNP (2767)

Email: security@csnp.org

Available: 24/7/365

During Business Hours

Contact your direct supervisor and the IT security team simultaneously

After Hours or Weekends

Use the emergency hotline - incidents don't wait for business hours

If Systems Are Down

Use personal devices to contact the security team via phone or personal email

Always provide: Your name, department, time of incident, description of what happened, and any affected systems or data.

Critical: What NOT to Do

Don't Investigate Alone

Avoid trying to "fix" the problem yourself. You may inadvertently destroy evidence or worsen the situation.

Don't Delete Anything

Never delete suspicious emails, files, or logs. These contain vital forensic information for investigation.

Don't Share Publicly

Avoid discussing the incident on social media or with unauthorized individuals. Loose talk helps attackers.

Don't Delay Reporting

Every minute counts. Don't wait to confirm suspicions - report immediately and let experts assess.

Preserving Evidence

Why Evidence Matters

Proper evidence preservation enables thorough investigation, helps identify the attack source, supports legal action if necessary, and prevents future incidents through lessons learned.

Best Practices

- Leave systems running if possible - don't restart
- Take photos or screenshots of your screen
- Preserve email headers and full messages
- Note file names, locations, and timestamps
- Don't touch or modify affected files

Communication Guidelines

1

Internal Communication

Only discuss the incident with authorized personnel. Use secure channels provided by the security team for updates.

2

External Communication

Never speak to media or external parties about incidents. Direct all inquiries to our designated communications officer.

3

Affected Parties

The security team will coordinate notification of affected individuals according to legal requirements and organizational policy.

Remember: Unauthorized disclosure can harm investigation efforts, violate legal obligations, and damage organizational reputation.

Post-Incident Support & Learning

Experiencing a security incident can be stressful. CSNP provides comprehensive support to help you through the process and emerge stronger.

Emotional Support

Counseling services available through our employee assistance program for anyone affected by an incident

Technical Training

Customized follow-up training to address specific vulnerabilities and strengthen security practices

Process Improvement

Lessons learned sessions to enhance organizational security posture and prevent recurrence

You will never be penalized for reporting a potential incident, even if it turns out to be a false alarm. We celebrate vigilance.

About CSNP

Making Cybersecurity Knowledge Accessible to Everyone

Through education, community, and practical resources, we empower organizations and individuals to protect themselves in our digital world.

Our Programs

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

Everything we offer is completely free.

Get Connected

Website: csnp.org

Resources: csnp.org/resources

Security Hotline: 1-800-555-CSNP