CSNP
CYBERSECURITY NON-PROFIT

Security Basics 101

Essential cybersecurity fundamentals every small business needs to know

CYBERSECURITY NON-PROFIT (CSNP)

WHY IT MATTERS

Cybersecurity: Your Business Lifeline

Cyberattacks aren't just a big business problem—60% of small businesses close within six months of a major breach. Your customer data, financial records, and reputation are all at risk.

The good news? Most attacks are preventable with basic security practices. This guide covers the essential knowledge every business owner and employee needs to stay protected.

43%

Small Businesses Attacked

Percentage targeted annually

$200K

Average Breach Cost

Financial impact per incident

COMMON THREATS

Know Your Enemy: Top Cybersecurity Threats

Phishing Attacks

Deceptive emails designed to steal credentials or install malware. The most common entry point for cybercriminals.

Ransomware

Malicious software that encrypts your files and demands payment. Can shut down operations for days or weeks.

Data Breaches

Unauthorized access to sensitive information. Can result from weak passwords, insider threats, or system vulnerabilities.

Social Engineering

Psychological manipulation tactics that trick employees into revealing confidential information or bypassing security.

PASSWORD SECURITY

Building a Fortress: Password Best Practices

01

Create Strong Passwords

Use at least 12 characters mixing uppercase, lowercase, numbers, and symbols. Avoid personal information and common words.

02

Never Reuse Passwords

Each account needs a unique password. If one is compromised, others remain safe.

03

Use a Password Manager

Store passwords securely and generate strong ones automatically. Recommended tools: Bitwarden, 1Password, LastPass.

04

Enable Multi-Factor Authentication

Add an extra layer requiring a code from your phone or authenticator app. Blocks 99% of automated attacks.

EMAIL SAFETY

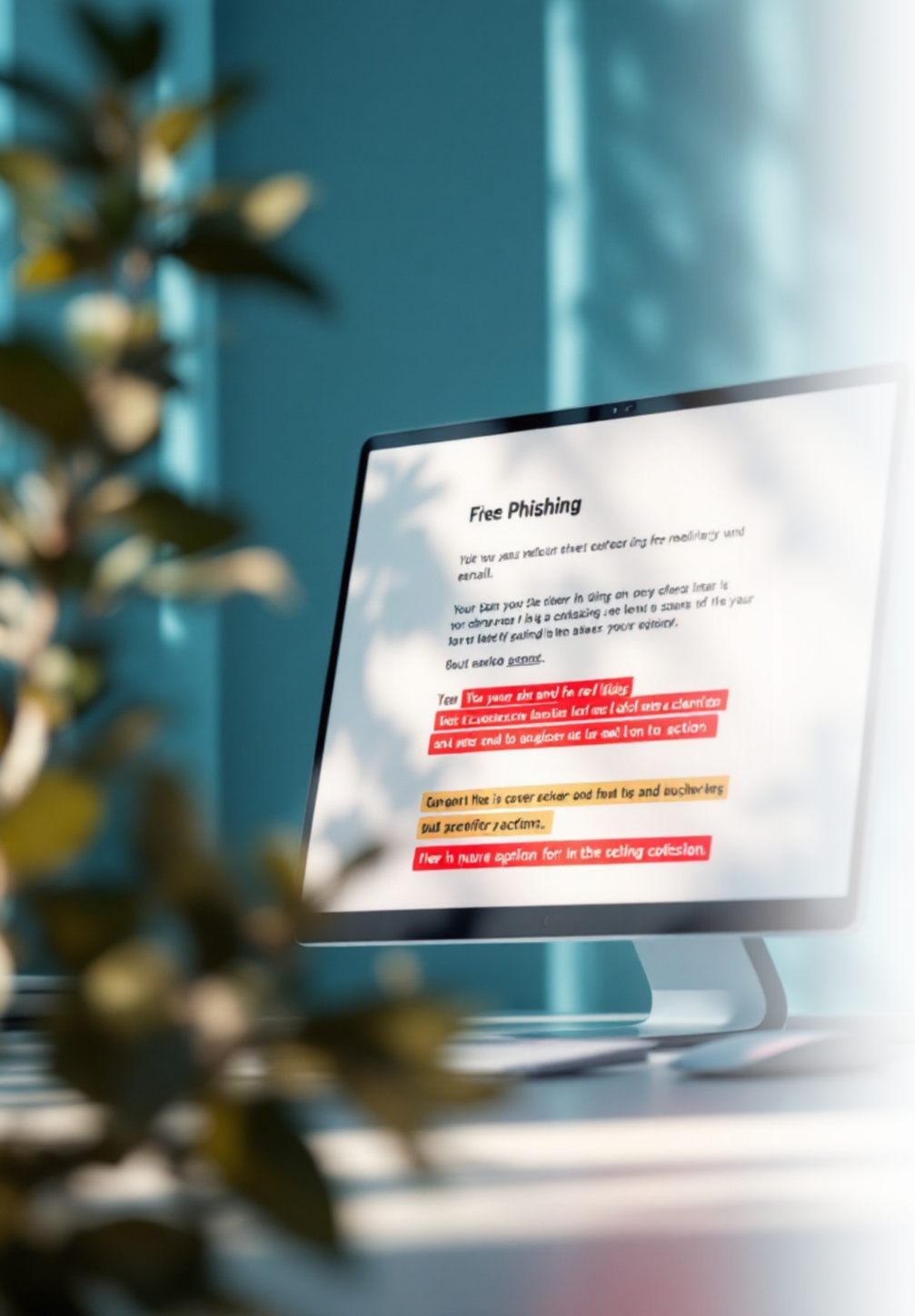
Email Security Essentials

Critical Email Habits

- Verify sender addresses carefully—look for subtle misspellings or unusual domains
- Never click links or download attachments from unknown sources
- Hover over links to preview URLs before clicking
- Use email encryption for sensitive information
- Be suspicious of urgent requests, especially involving money or credentials
- Report suspicious emails to your IT team immediately

Red Flag Warning

If an email creates a sense of urgency or fear, stop and verify through a separate channel. Scammers rely on emotional reactions.



PHISHING RECOGNITION

Spot the Phish: Recognition Guide

Urgent Language

"Your account will be suspended!" or "Immediate action required!" are classic phishing tactics.

Suspicious Links

URLs that don't match the company name or have odd spellings like "paypa1.com" instead of "paypal.com".

Poor Grammar

Professional companies proofread. Multiple errors signal a scam attempt.

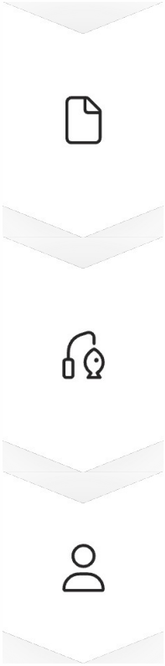
Generic Greetings

"Dear Customer" instead of your name suggests mass-distributed phishing.

SOCIAL ENGINEERING

Beyond Phishing: Social Engineering Tactics

Social engineering exploits human psychology rather than technical vulnerabilities. Attackers manipulate trust, authority, and fear to gain access to systems and information.



Pretexting

Creating a fabricated scenario to extract information. Example: Someone calls claiming to be from IT support and requests your password.

Baiting

Offering something enticing to get you to take action. Example: A USB drive labeled "Employee Salaries" left in your parking lot.

Tailgating

Following authorized personnel through secure doors or checkpoints by appearing legitimate or exploiting courtesy.

> **Defense Strategy:** Verify all requests through official channels. Never provide sensitive information based on a call, email, or in-person request alone.

MALWARE PROTECTION

Defending Against Malware

Essential Protection Layers

- **Install Antivirus Software**

  Use reputable solutions like Windows Defender, Malwarebytes, or Norton. Keep them updated and run regular scans.

- **Keep Systems Updated**

  Enable automatic updates for operating systems and applications. Patches fix security vulnerabilities.

- **Download Carefully**

  Only install software from official sources. Avoid pirated programs that often contain malware.

- **Use Browser Security**

  Enable pop-up blockers and safe browsing features. Consider security extensions like uBlock Origin.

NETWORK BASICS

Network Security Fundamentals

Secure Your Wi-Fi

Change default router passwords immediately. Use WPA3 encryption (or WPA2 minimum). Hide your network SSID if possible and create a separate guest network for visitors.

Enable Firewalls

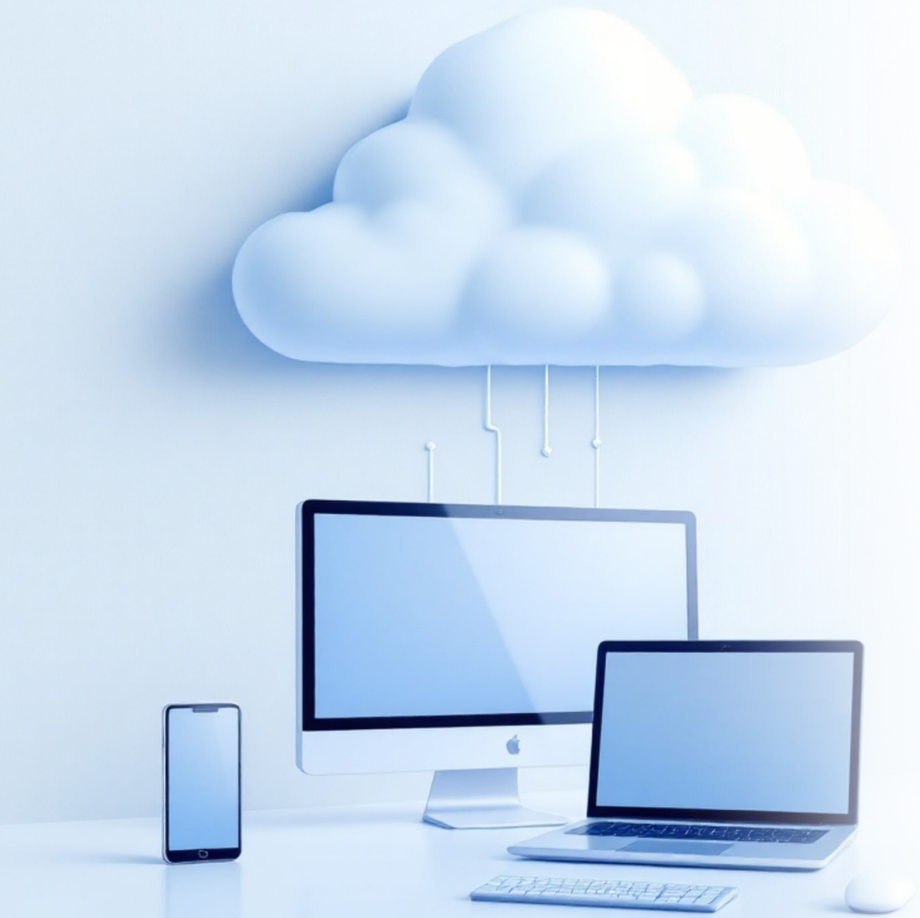
Activate both hardware (router) and software (computer) firewalls. They monitor and control incoming and outgoing network traffic based on security rules.

Use VPN for Remote Access

Virtual Private Networks encrypt internet connections, essential for remote workers accessing company resources. Never use public Wi-Fi without VPN protection.

Monitor Network Activity

Regularly review connected devices and access logs. Unusual activity may indicate a breach. Consider network monitoring tools for larger operations.



DATA BACKUP

The 3-2-1 Backup Rule

3 Copies

Keep three total copies of your data: the original plus two backups. This protects against single points of failure.

2 Different Media

Store backups on two different types of media (external hard drive, NAS device, cloud storage) to protect against media-specific failures.

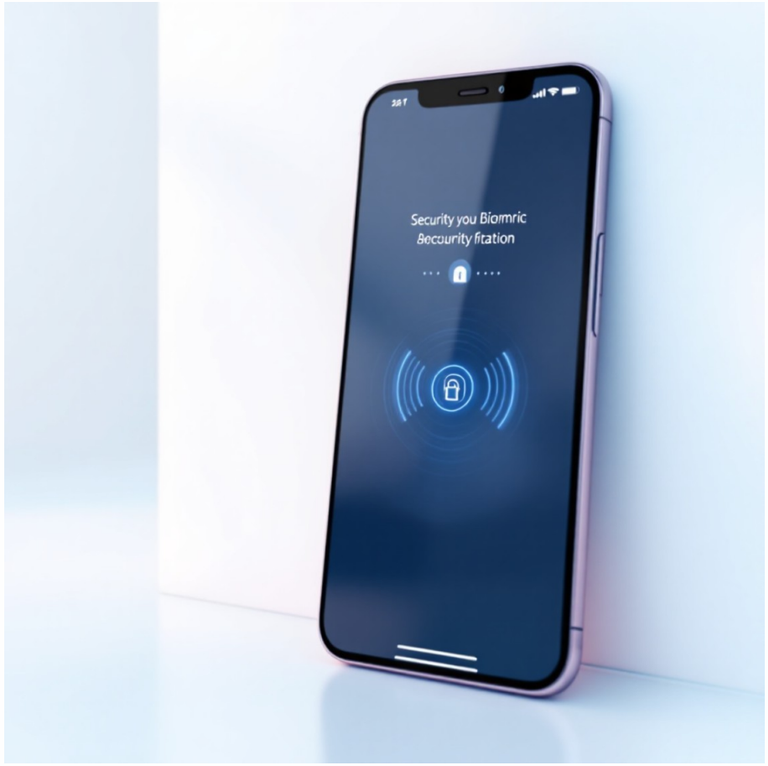
1 Offsite Copy

Keep at least one backup offsite or in the cloud. This protects against physical disasters like fire, flood, or theft.

Automate backups to run daily or weekly depending on how frequently your data changes. Test restoration regularly—a backup you can't restore is worthless. For critical business data, consider versioned backups that let you recover from ransomware attacks.

MOBILE SECURITY

Securing Mobile Devices



Mobile Device Protection

- Enable screen locks with strong PINs or biometric authentication
- Keep mobile OS and apps updated automatically
- Install apps only from official stores (Apple App Store, Google Play)
- Review app permissions—deny unnecessary access to contacts, location, or camera
- Enable remote wipe capability through Find My iPhone or Android Device Manager
- Avoid public charging stations (juice jacking risk) or use USB data blockers
- Use mobile security apps for additional protection

Lost Device Protocol: Immediately report lost or stolen devices to your IT team. Remote wipe if necessary to protect company data.

PHYSICAL SECURITY

Don't Forget Physical Security

Cybersecurity isn't just digital. Physical access to devices and facilities remains a critical vulnerability that's often overlooked.

Access Control

Implement keycard systems or biometric access for sensitive areas. Maintain visitor logs and escort guests. Never prop open secure doors.

Clean Desk Policy

Lock away sensitive documents at end of day. Use privacy screens on monitors. Shred confidential papers before disposal.

Surveillance

Install security cameras at entry points. Monitor and review footage regularly. Post clear signage about surveillance.

Device Security

Use cable locks for laptops in offices. Secure servers in locked rooms with limited access. Track all hardware inventory.

TRAINING

Your Team Is Your Strongest Defense

Building a Security Culture

95% of cybersecurity breaches involve human error. Your employees are both your greatest vulnerability and your most powerful defense.

Regular training transforms your team from potential weak points into active security participants who can identify and stop threats.

Training Program Essentials

- Conduct security awareness training quarterly
- Run simulated phishing exercises monthly
- Create clear, accessible security policies
- Establish easy reporting procedures for incidents
- Celebrate employees who identify threats
- Update training as new threats emerge

INCIDENT RESPONSE

When Something Goes Wrong: Incident Response

Despite best efforts, incidents happen. A quick, organized response minimizes damage and gets you back to business faster.

Identify & Contain

Recognize the incident immediately. Isolate affected systems from the network to prevent spread. Document everything you observe.

Notify Stakeholders

Alert your IT team, management, and if necessary, law enforcement. Don't delay—early notification enables faster response.

Investigate & Eradicate

Determine the attack vector and scope. Remove malware, close vulnerabilities, and ensure the threat is completely eliminated.

Recover & Review

Restore from clean backups. Monitor systems closely. Conduct a post-incident review to prevent future occurrences.

Create an incident response plan now with clear roles, contact information, and procedures. Don't wait for an emergency to figure out who does what.

Your Partner in Cybersecurity Education

> *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
- Parents & Educators Resources

Everything we offer is completely free.

Get Started Today

Visit our website for comprehensive guides, downloadable resources, training materials, and community support.

Visit CSNP.org | Browse Resources

Cybersecurity Non-Profit (CSNP) is dedicated to making digital safety accessible to individuals, families, and organizations of all sizes.