CSNP

CYBERSECURITY NON-PROFIT

Remote Work Security Guide

Essential cybersecurity practices for protecting your business in the remote work era. A comprehensive guide from CSNP.

OVERVIEW

The Remote Work Security Landscape

Remote work has transformed how we do business, but it's also expanded the attack surface for cyber threats. Home networks, personal devices, and distributed teams create new vulnerabilities that require proactive security measures.

This guide provides practical, actionable steps to protect your organization's data and systems when employees work from anywhere. From network security to incident reporting, we'll cover everything you need to know.

68%

Remote workers

Percentage of employees working remotely at least part-time

3x

Higher risk

Increase in security incidents with remote work

FOUNDATION

Securing Your Home Network

Change Default Credentials

Replace your router's default username and password immediately. Use a strong, unique password with at least 16 characters combining letters, numbers, and symbols.

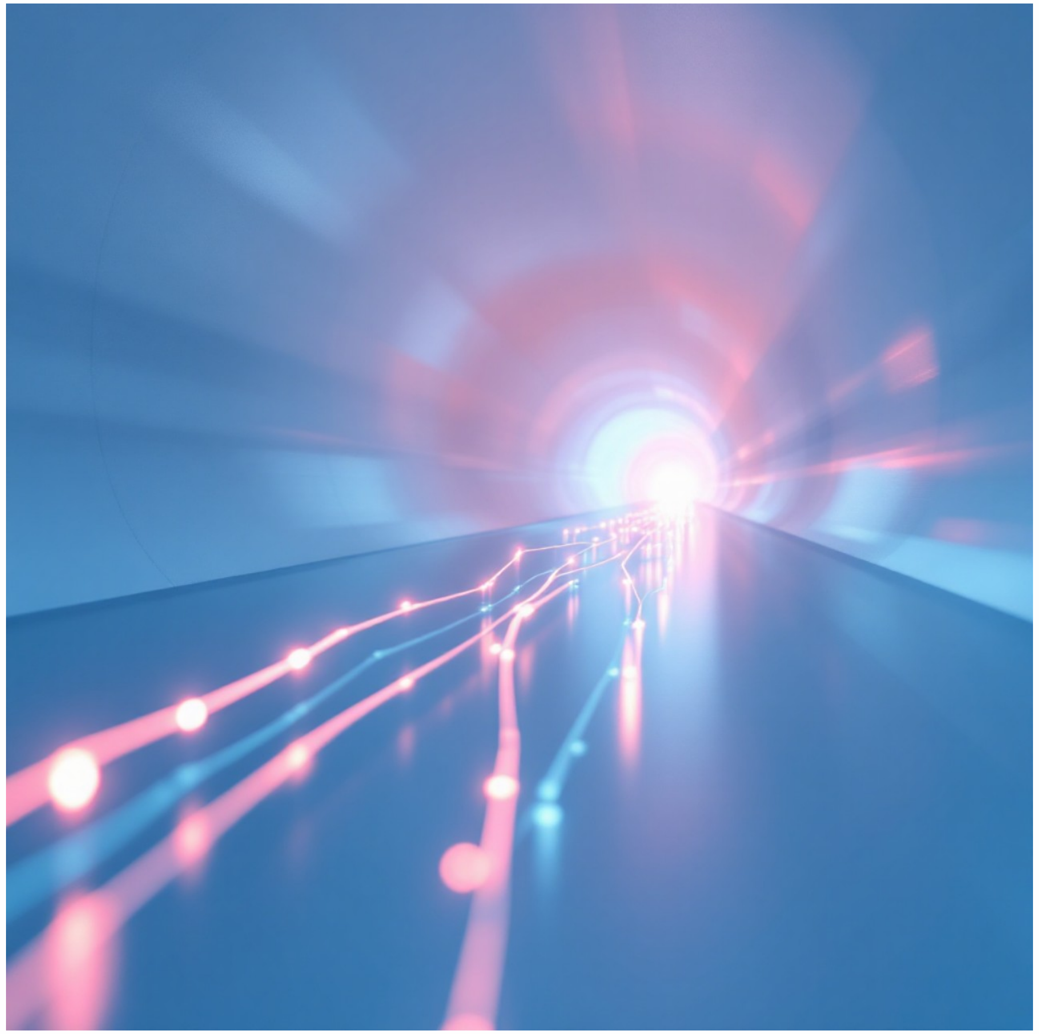
Enable WPA3 Encryption

Use WPA3 encryption if available, or WPA2 as a minimum. Avoid WEP and WPA, which are easily compromised. Update your router firmware regularly.

Create Separate Networks

Set up a dedicated network for work devices. Keep personal devices, smart home gadgets, and guest access on separate networks to limit exposure.

VPN: Your Secure Connection



Why VPNs Matter

A Virtual Private Network (VPN) encrypts your internet connection, protecting sensitive data from interception. It's essential for accessing company resources securely from home or public locations.

01

Use Company-Approved VPN

Always connect through your organization's VPN before accessing company systems or data.

02

Enable Auto-Connect

Configure your VPN to connect automatically when accessing work resources.

03

Verify Connection Status

Check that your VPN is active before handling sensitive information.

Device Security Essentials

1

Keep Systems Updated

Enable automatic updates for your operating system, applications, and security software. Updates patch vulnerabilities that attackers exploit.

2

Install Antivirus Protection

Use enterprise-grade antivirus software on all work devices. Ensure real-time scanning is enabled and definitions are current.

3

Enable Full Disk Encryption

Encrypt your hard drive using BitLocker (Windows) or FileVault (Mac) to protect data if your device is lost or stolen.

4

Use Strong Authentication

Enable multi-factor authentication (MFA) on all accounts. Use biometrics and password managers for added security.

5

Lock Devices Automatically

Set devices to lock after 5 minutes of inactivity. Use strong passwords or PINs, never simple codes like 1234.

VIRTUAL MEETINGS

Video Conferencing Security

- **Use Waiting Rooms**

  Enable waiting rooms to control who joins your meetings. Verify participants before admitting them.

- **Require Meeting Passwords**

  Always password-protect meetings and share credentials through secure channels, never in public posts.

- **Control Screen Sharing**

  Restrict screen sharing to hosts only or approved participants. Close sensitive documents before sharing.

- **Disable Recording by Default**

  Only record when necessary and with all participants' knowledge and consent.

- **Update Video Apps Regularly**

  Keep Zoom, Teams, and other platforms current to protect against known vulnerabilities.

Cloud Storage and File Sharing

Use Approved Platforms

Only store work files on company-approved cloud services. Avoid personal Dropbox, Google Drive, or other unauthorized platforms for business data.

Control Sharing Permissions

Review sharing settings carefully. Use specific email addresses instead of "anyone with link" options. Set expiration dates for shared access.

Encrypt Sensitive Files

Encrypt confidential documents before uploading. Use password protection for spreadsheets and documents containing sensitive information.

Pro Tip: Regularly audit your shared files and folders. Remove access for former employees or collaborators who no longer need it.

Physical Security at Home

Position Screens Carefully

Place your monitor away from windows and doors. Use privacy screens to prevent shoulder surfing. Be mindful of what's visible during video calls.

Secure Your Workspace

Lock devices when stepping away, even briefly. Store laptops and documents in locked drawers or cabinets when not in use. Shred sensitive papers.

Control Physical Access

Establish a dedicated workspace with limited access. Keep work devices separate from family computers and tablets to maintain security boundaries.

SHARED SPACES

Managing Family and Shared Environments

Educate Family Members

Explain the importance of work security to household members. Set clear boundaries about not touching work devices or entering during calls.

Keep Kids Away from Work Tech

Never let children use work laptops or devices. Accidental deletions, malware from games, or inadvertent data exposure are serious risks.

Use Separate User Accounts

If sharing a device is unavoidable, create separate user accounts with different credentials. Never share passwords with family.

Reporting Security Incidents Remotely

1 **Recognize the Incident**

Suspicious emails, unexpected system behavior, lost devices, or potential data breaches require immediate action.

2 **Disconnect If Needed**

If you suspect active malware or unauthorized access, disconnect from the network immediately to contain the threat.

3 **Document Everything**

Take screenshots, note times, and record what happened. Preserve evidence but don't investigate further yourself.

4 **Contact IT Security**

Report to your security team immediately using your incident response hotline or email. Don't wait or try to fix it yourself.

5 **Follow Instructions**

Your security team will guide response steps. Complete any required forms and cooperate fully with the investigation.

Emergency Contact: Keep your IT security team's contact information readily accessible, including after-hours numbers for urgent situations.

QUICK REFERENCE

Daily Remote Work Security Checklist

Before You Start Working

- Connect to company VPN
- Verify antivirus is running and updated
- Check for system updates
- Ensure workspace is private and secure
- Lock doors if handling sensitive data

During Your Workday

- Lock screen when stepping away
- Verify recipients before sending sensitive emails
- Use secure file sharing platforms only
- Keep work and personal activities separate
- Be cautious with unsolicited messages or links

End of Day

- Log out of all work applications
- Store devices in secure location
- Clear workspace of sensitive documents
- Disconnect VPN
- Report any suspicious activity to IT

About CSNP

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

Our Programs

- **Business & Non-Profit Security**

  Practical guides for organizations of all sizes

- **Family Cybersecurity**

  Protecting your household in the digital age

- **Kids Safety**

  Age-appropriate online safety education

- **Senior Digital Safety**

  Empowering older adults with security knowledge

- **Women's Security**

  Addressing unique privacy and safety concerns

- **Parents & Educators**

  Resources for teaching cybersecurity

Everything We Offer Is Free

We believe cybersecurity education should be accessible to everyone, regardless of budget or technical expertise. All our resources, guides, and programs are completely free.

Visit csnp.org Browse Resources