

Workplace Cybersecurity Guide

Essential digital safety strategies for professional women navigating today's connected workplace



Your Digital Workspace Matters

Why This Guide?

In today's digital workplace, your online security directly impacts your professional reputation, career advancement, and personal safety. Cyber threats don't discriminate, but knowledge empowers you to protect yourself.

This guide provides practical, actionable strategies you can implement immediately—no technical expertise required.

What You'll Learn

- Email security best practices
- Password management essentials
- Remote work protection
- Professional boundary setting
- Harassment prevention and reporting
- Career protection strategies

Email Security Fundamentals



Spot Phishing Attempts

Be skeptical of urgent requests, unexpected attachments, or messages asking for credentials. Verify sender addresses carefully —phishers often use look-alike domains.

Protect Sensitive Information

Never share passwords, financial data, or personal details via email. Use encrypted channels for confidential communications and verify recipients before sending.

Enable Two-Factor Authentication

Add an extra security layer to your email accounts. Even if someone obtains your password, they won't access your account without the second verification step.

Password Management Excellence

Create Strong Passwords

Use 12+ characters combining uppercase, lowercase, numbers, and symbols. Avoid personal information like birthdays or names.

Example: "Sunrise!2024@Coffee" is stronger than "password123"

Use a Password Manager

Tools like 1Password, LastPass, or Bitwarden generate and store complex passwords securely. You only need to remember one master password.

This prevents password reuse—the #1 security risk.

Regular Updates

Change passwords every 90 days for critical accounts. Update immediately if you suspect a breach or receive security alerts from services you use.



Remote Work Security Essentials

01

Secure Your Home Network

Change default router passwords, enable WPA3 encryption, and create a separate guest network for non-work devices.

02

Use VPN Connections

Always connect through your company VPN when accessing work resources remotely. Public Wi-Fi should never be used without VPN protection.

03

Secure Your Physical Space

Position screens away from windows and use privacy filters. Lock devices when stepping away and ensure confidential calls occur in private spaces.

04

Update Regularly

Enable automatic updates for operating systems and applications. Outdated software contains known vulnerabilities that attackers exploit.



Protecting Colleague Privacy



Respect Digital Boundaries

Don't share colleagues' personal contact information without permission. Avoid forwarding internal communications outside your organization, even to trusted friends.



Secure Group Communications

Use BCC when emailing groups to protect email addresses. Be mindful of what you share in group chats—screenshots can be taken and shared without context.



Meeting Etiquette

Ask permission before recording video calls. Be aware of what's visible in your background and respect others' privacy by not capturing their home environments without consent.



Setting Professional Boundaries Online



Separate Personal and Professional

Maintain distinct social media profiles for work and personal life. Review privacy settings regularly and limit work connections' access to personal content.



Establish Communication Hours

Set clear expectations about your availability outside work hours. Use email scheduling features and status indicators to reinforce boundaries without guilt.



Know When to Say No

You're not obligated to connect with colleagues on personal social media or share your personal phone number. Professional boundaries protect your wellbeing and prevent potential harassment.



Remember: Setting boundaries isn't unprofessional—it's essential self-care that enables sustainable career success.

Recognizing and Preventing Online Harassment

Warning Signs

- Persistent unwanted messages or friend requests
- Comments about your appearance unrelated to work
- Requests to move conversations to personal channels
- Sharing of your personal information without consent
- Inappropriate images or messages
- Monitoring or commenting on your online activity

Immediate Actions

- Document everything—save screenshots with dates
- Block the individual on all platforms
- Report to your supervisor or HR immediately
- Preserve evidence before it's deleted
- Don't engage or respond to harassment
- Review and tighten privacy settings

Reporting Procedures and Career Protection

Document the Incident

Record dates, times, and specifics of each occurrence. Screenshot messages and save emails in a secure location outside your work systems.

1

Know Your Rights

Familiarize yourself with company policies and legal protections. Retaliation for reporting harassment is illegal in most jurisdictions.

2

3

4

Report Internally

Follow your company's reporting procedures. Contact HR, your manager, or use anonymous reporting channels if available.

Seek External Support

If internal processes fail, contact external resources like EEOC, legal counsel, or professional advocacy organizations.

Protecting Your Career

Maintain backups of your work achievements and positive feedback in personal storage. Keep your professional network active and document your contributions regularly. These practices protect you regardless of workplace challenges and support future opportunities.

Cybersecurity Non-Profit (CSNP)

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

All Programs Are Free

We believe everyone deserves access to cybersecurity education. Our programs, resources, and support are completely free—no barriers, no costs.

Connect With Us

Website: csnp.org

Free Resources: csnp.org/resources

Join our community and access guides, workshops, and support for your digital safety journey.