Keeping Your Devices Safe & Secure Guide

Contents

Overview

This guide provides security recommendations for staff members who use personal devices (computers, laptops, phones, and tablets) to access organizational systems and data. Following these guidelines will help protect both your personal information and organizational data from cyber threats.

Who Should Use This Guide

This guide is for staff members who:

- Access work email on personal devices
- Store work documents on personal devices
- Use personal devices to communicate about organizational matters
- Access any organizational systems from personal devices

---

1. Device Access Control

Access control is the practice of ensuring only authorized individuals can use your devices and access the information on them. Think of it as the locks and keys for your digital workspace. When you use personal devices for work, you're responsible for controlling who can access them both physically and digitally. Weak access controls are like leaving your office door unlocked when you leave: anyone walking by can enter and access everything inside. The measures in this section create strong barriers that prevent unauthorized access to your devices and the organizational data they contain.

1.1 Screen Lock Configuration

All devices used for work should be configured with automatic screen lock.

Recommendations:

- Set computers and laptops to lock after a maximum of 5 minutes of inactivity
- Set mobile devices to lock after a maximum of 2 minutes of inactivity
- Manually lock devices whenever leaving them unattended, even briefly
- Avoid leaving devices unattended in public or unsecured locations

Why this matters: An unlocked device allows anyone with physical access to view emails, documents, and systems. Screen locks are your first line of defense against unauthorized access.

1.2 Authentication Standards

All devices should require authentication to unlock.

For computers and laptops:

- Use passwords that are at least 12 characters long
- Include a mix of uppercase letters, lowercase letters, numbers, and symbols
- Create memorable phrases rather than random characters (e.g., "***BlueCoffee!Mountain29***")
- Avoid easily guessable information like birthdays, pet names, or common words alone

For mobile devices:

- Enable biometric authentication (fingerprint or face recognition) where available
- Set a backup PIN or password that meets the standards above
- Avoid simple patterns or PINs like "1234"

Why this matters: Weak passwords are easily guessed or cracked. Strong authentication prevents unauthorized access even if someone gains physical access to your device.

---

2. Software and System Updates

Software updates are one of the most critical yet often overlooked aspects of security. Every piece of software from your operating system to your web browser contains vulnerabilities, which are flaws that attackers can exploit to gain unauthorized access to your device. Software developers constantly discover and fix these vulnerabilities, releasing updates (also called "patches") to close these security gaps. When you delay or ignore updates, you're leaving known entry points open for attackers

2.1 Operating System Updates

Keep device operating systems current with the latest security patches.

Best practices:

- Enable automatic updates where possible
- Install critical security updates within one week of release
- Don't indefinitely postpone or ignore update notifications
- Plan updates during non-working hours to minimize disruption

Why this matters: Updates fix security vulnerabilities that hackers actively exploit. Outdated systems are the easiest targets for cyber attacks.

2.2 Application Updates

Keep all applications, especially web browsers and communication tools, up to date.

Best practices:

- Enable automatic updates for applications where available
- Regularly check for updates on applications that don't update automatically
- Uninstall applications you no longer use

Why this matters: Vulnerabilities in outdated applications provide entry points for malware and unauthorized access.

---

3. Malware Protection

Malware (malicious software) refers to any program designed to harm your device, steal your information, or use your computer for criminal purposes without your knowledge. This includes viruses, ransomware (which locks your files and demands payment), spyware (which monitors your activity), and trojans (which pretend to be legitimate software). Malware can steal passwords, record your keystrokes, access your camera and microphone, encrypt your files, use your device to attack others, or steal sensitive organizational data.

3.1 Antivirus and Anti-Malware Software

All computers should have active malware protection.

Recommendations:

- Enable and maintain built-in security software (Windows Defender for Windows, XProtect for Mac)
- Ensure real-time protection is active
- Don't disable security software, even temporarily
- If security software detects a threat, don't ignore the warning

Why this matters: Malware can steal data, monitor your activity, encrypt your files for ransom, or use your device to attack others.

3.2 Safe Software Installation Practices

Only install software from trusted sources.

Best practices:

- Download software only from official websites or app stores
- Verify you are on the legitimate website before downloading (check the URL carefully)

- Be suspicious of free versions of normally paid software
- Don't install software from email attachments or pop-up advertisements
- When prompted for permission to install software or make system changes, verify you intentionally initiated the action

Red flags indicating potentially malicious software:

- Pop-ups claiming your device is infected and offering immediate downloads
- Offers for free versions of expensive professional software
- Downloads from unfamiliar websites or file-sharing services
- Unsolicited email attachments claiming to be important software updates

---

4. Account Security

Your online accounts such as email, password managers, cloud storage, and work systems are gateways to your digital life and organizational resources. Each account you create is a potential entry point for attackers. If someone gains access to your email account, they can often reset passwords for your other accounts, effectively taking over your entire digital identity. Account security goes beyond just passwords; it involves creating unique credentials for each service, adding additional verification steps, and actively managing your accounts to detect unauthorized access.

4.1 Password Management

Each account should have a unique, strong password.

Recommendations:

- Never reuse passwords across multiple accounts
- Use a password manager to generate and store complex passwords
- Choose one strong master password for your password manager
- Enable multi-factor authentication on your password manager

Recommended password managers:

- Bitwarden (free, open source)
- 1Password
- LastPass

Why this matters: If one account is compromised and you reuse passwords, attackers can access all your accounts. Password managers make it practical to use unique passwords everywhere.

4.2 Multi-Factor Authentication (MFA)

Enable multi-factor authentication on all accounts that support it.

Priority accounts for MFA:

- Work email (strongly recommended)
- Personal email accounts
- Password manager
- Banking and financial accounts
- Any account with access to sensitive information

Best practices:

- Use authenticator apps (Microsoft Authenticator, Google Authenticator, Authy) rather than SMS when possible
- Save backup codes in a secure location when setting up MFA
- Never share authentication codes with anyone

Why this matters: MFA requires both your password and a code from your phone. Even if someone steals your password, they cannot access your account without the second factor.

---

5. Mobile Device Security

We use mobile devices for email, messaging, document editing, photography, banking, and accessing organizational systems. Yet mobile devices face unique security challenges: they're easily lost or stolen, used in public places where screens can be observed, connected to various networks throughout the day, and often less protected than computers. A lost phone without proper security can provide immediate access to your email, messages, stored passwords, and potentially organizational systems. Mobile devices are also increasingly targeted by attackers because users tend to be less cautious on phones than on computers, downloading apps without scrutiny and clicking links in messages without the same level of skepticism they'd apply on a desktop

5.1 Mobile Device Configuration

Mobile devices benefit from specific security configurations.

Recommendations:

- Enable device encryption (enabled by default on most modern devices)
- Activate "Find My Device" features (Find My iPhone, Find My Device for Android)
- Only install applications from official app stores (Apple App Store, Google Play Store)
- Review and limit app permissions regularly
- Disable unnecessary features like Bluetooth when not in use

Why this matters: Mobile devices are easily lost or stolen. Proper configuration enables remote lock and wipe capabilities and limits potential damage.

5.2 Mobile Device Usage

Practice secure mobile device habits.

Best practices:

- Never leave devices unattended in public locations
- Be aware of your surroundings when viewing sensitive information
- Don't allow others to use your work-configured device
- Report lost or stolen devices immediately to your supervisor

---

6. Physical Security

Digital security often focuses on technical measures like passwords and encryption, but physical security protecting your devices from physical theft or unauthorized access is equally important. All the encryption and strong passwords in the world won't help if someone steals your unlocked laptop or inserts a malicious USB drive while you're away from your desk. Physical access to a device, even for a few seconds, can allow someone to install malware, copy data, or compromise your system in ways that bypass your digital security measures. Devices are also valuable targets for theft simply for their resale value, but the real damage from a stolen work device is the potential exposure of organizational data and systems

6.1 Device Physical Security

Protect devices from theft and unauthorized physical access.

Best practices:

- Never leave devices visible in vehicles
- Use laptop locks in semi-public spaces when available
- Store devices securely when not in use
- Be aware that USB devices can be used to install malware in seconds
- Don't allow untrusted individuals physical access to unlocked devices

Why this matters: Physical access to a device can bypass many security controls. Theft of devices can result in data breaches even with strong passwords.

Remember: *Reporting incidents quickly helps minimize potential damage. There is no penalty for reporting suspected issues, it's always better to report something that turns out to be harmless than to ignore a real threat.*

7. Protecting Your Connection with VPN

When you connect your device to the internet whether at a cafe, hotel, airport, or even some home networks, your data travels across networks you don't control. On unsecured or public networks, attackers can position themselves between your device and the internet, intercepting everything you send and receive: passwords, emails, documents, and browsing activity. This is especially dangerous on public Wi-Fi where dozens of strangers share the same network. A Virtual Private Network (VPN) creates an encrypted tunnel between your device and the internet, making your data unreadable to anyone trying to intercept it. Think of it as sending your communications through a secure, locked pipe that no one else can see into, rather than shouting across an open room.

7.1 Using a VPN

Use a VPN whenever connecting to networks outside your control.

When to use a VPN:

- Any public Wi-Fi (cafes, airports, hotels, libraries)
- Shared networks in co-working spaces
- Any network where you're unsure of the security
- When accessing sensitive work systems or data from any location

Choosing a VPN:

- Use a reputable VPN service (examples: NordVPN, ExpressVPN, ProtonVPN)
- Avoid free VPN services, which may sell your data or inject advertisements
- Look for VPNs with a clear privacy policy and no-logs commitment
- Consider VPNs recommended by trusted technology publications

Best practices:

- Install the VPN application on all devices you use for work
- Connect to the VPN before accessing any work systems or sensitive data
- Keep your VPN application updated
- Don't disconnect the VPN while working on sensitive tasks

Why this matters: Without a VPN, anyone on the same network can potentially intercept your communications. VPNs protect your device by encrypting all data leaving and entering it, regardless of network security.

Quick Reference: Essential Security Actions

- Lock your screen every time you step away
- Think before clicking links or opening attachments
- Be aware of your physical surroundings when working
- Install any pending security updates
- Back up important work files
- Check that security software is active
- Review account security settings
- Remove applications you no longer use
- Verify MFA is enabled on critical accounts

When in doubt:

- Don't click
- Don't install
- Don't share
- Ask someone

Glossary

Authenticator App: A mobile application that generates time-based codes for multi-factor authentication

Biometric Authentication: Using fingerprints, face recognition, or other physical characteristics to verify identity

Encryption: Converting data into a code to prevent unauthorized access

Malware: Malicious software designed to damage devices or steal information

Multi-Factor Authentication (MFA): Requiring two or more forms of verification to access an account

Phishing: Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity

VPN (Virtual Private Network): A service that encrypts your internet connection and hides your online activity