Security — Complete End-User Guide

(Defender AV, phishing & safe email, device encryption, secure browsing & data handling, incident response)

> This manual helps you keep work data safe on Windows and macOS. It covers day-to-day security habits, how to use built-in protections (Microsoft Defender, Firewall, SmartScreen, FileVault/BitLocker), how to spot and report phishing, how to share files safely, and exactly what to do if something goes wrong. Admin-only notes are marked *(Admin)*.

---

0) What this covers

- Everyday security habits that prevent most incidents
- Running antivirus scans, handling detections, quarantines
- Ransomware protection (Controlled Folder Access), firewall basics
- Device encryption (BitLocker/FileVault) + recovery keys
- Safe email & messaging: phishing, business-email compromise, invoice fraud
- Safe file sharing (OneDrive/SharePoint), sensitivity labels, external guests
- Removable media (USB) and working on public or home networks
- What to do if you clicked a bad link, ran a suspicious file, or lost a device
- Escalation templates and paste-able responses (no links)

---

1) Core habits (90-second checklist)

- **Lock your device** when you step away (Windows: Win+L; macOS: Ctrl+Cmd+Q).

- **Use MFA** and keep two methods registered (Authenticator + phone or security key).
- **Update** OS and apps weekly; reboot at least twice a month.
- **Think before you click**: unexpected attachments, urgent money requests, password prompts → be skeptical.
- **Store work files in OneDrive/SharePoint**, not local Desktop—enables version history & restore.
- **Encrypt the device** (BitLocker/FileVault) and **encrypt USB** drives that hold work data.
- **Report suspected phishing** using the built-in Report button in Outlook (don't forward it).

---

2) Microsoft Defender (Windows) — AV, Firewall, SmartScreen

2.1 Open Windows Security

- **Start** → **Windows Security** (shield icon). Home shows **Virus & threat protection**, **Firewall & network protection**, **App & browser control**, **Device security**, **Device performance & health**.

2.2 Scans & updates

- **Quick scan**: Virus & threat protection → **Quick scan**.
- **Full scan**: **Scan options** → **Full scan** (thorough, takes longer).
- **Custom scan**: **Scan options** → **Custom** → pick a folder/drive.
- **Microsoft Defender Offline** (deep, before Windows loads): **Scan options** → **Microsoft Defender Offline scan** → **Scan now** (reboots; use if persistent malware is suspected).
- **Protection updates**: Virus & threat protection → **Protection updates** → **Check for updates**.

2.3 Quarantine & allowed list

- **Protection history** shows blocked items.
- If a file is quarantined, **do not restore** unless you are 100% sure it is safe and required. When in doubt, escalate.

2.4 Ransomware protection (Controlled Folder Access)

- Virus & threat protection → **Ransomware protection** → **Manage**.
- **Controlled Folder Access** can block untrusted apps from changing protected folders (Documents, Pictures, OneDrive).
- If a legitimate app is blocked, add it to **Allow an app through Controlled folder access** (or ask IT if centrally managed).

2.5 SmartScreen (safe web & downloads)

- App & browser control → **Reputation-based protection**: keep **Check apps and files**, **SmartScreen for Microsoft Edge**, and **Potentially unwanted app blocking On**.
- If you see a SmartScreen warning, stop and verify the source before proceeding.

2.6 Firewall (Windows)

- Firewall & network protection → confirm **Domain/Private/Public** firewalls are **On**.
- If an app needs network access, Windows may prompt to **Allow** on trusted networks. Choose **Private** (home/office), not **Public**, unless instructed.

(Admin): **Tamper protection** should be enabled to prevent Defender settings from being modified by malware or tools.

---

3) macOS protections (built-ins + common enterprise tools)

- **Gatekeeper** blocks unidentified apps by default. Right-click → **Open** only for trusted software.
- **XProtect/ MRT** (built-in) update silently; keep macOS current.
- **FileVault** for full-disk encryption (see §5.3).
- Many orgs deploy **Defender for Endpoint** or another EDR on macOS. If installed, follow the app's prompts for scans and updates.

---

4) Email & Messaging Safety (Outlook, Teams, mobile mail)

4.1 Spotting phishing & fraud

- **Mismatched sender** (display name shows a colleague, but the actual address is off by a character).
- **Urgent payment/gift card request**, secrecy, or threats.
- **Login page** that looks right but the address bar is wrong.
- **Unexpected invoice/attachment** (ZIP, HTML, ISO, macros).
- **"You won a prize"** or **password expires now** with a link.

4.2 What to do with suspicious email

- In Outlook: select message → **Report phishing** (or **Report junk**).
- **Do not reply**, **do not click links**, **do not open attachments**.
- If you already clicked, go to **§8 Immediate actions**.

4.3 Attachments & macros

- Prefer **OneDrive/SharePoint links** instead of sending files.

- Do **not** enable Office macros unless you are certain they're required and safe.

4.4 External mail markers

- Many orgs tag external messages with a banner. Treat these with extra caution before sharing internal info.

---

5) Device Encryption & Keys

5.1 Why encrypt?

- If a laptop or drive is lost or stolen, encryption protects data at rest. Encryption is required for devices that handle company data.

5.2 Windows — BitLocker

- **Check status**: Start → type **BitLocker** → **Manage BitLocker**.
- **Enable** (if available): **Turn on BitLocker** for the system drive; choose where to back up your **recovery key** (follow company policy: usually your work account/AD).
- **USB drives (BitLocker To Go)**: right-click the USB drive in File Explorer → **Turn on BitLocker** → set a strong password.
- **Recovery**: If a BitLocker screen appears at boot, you'll need the **recovery key**. Check your account recovery portal or contact IT.

(Admin): enforce backup of recovery keys to the directory and use **TPM + PIN** for high-risk roles.

5.3 macOS — FileVault

- **Enable**: **System Settings** → **Privacy & Security** → **FileVault** → **Turn On**.
- Store the **recovery key** securely (per policy) or let your management tool escrow it.
- On next login, FileVault begins encrypting; keep the Mac on AC power.

---

6) Safe File Sharing & Data Handling (OneDrive/SharePoint)

6.1 Use the right home

- **Personal drafts** → your **OneDrive**.
- **Team/department content** → the team's **SharePoint** library (or the Files tab in Teams).

6.2 Sharing links correctly

- Share with **People in your organization** by default; grant **Specific people** only as needed.
- Choose **Can edit** vs **Can view** consciously; avoid "anyone" links unless policy allows.
- Set **expiration** on external links where permitted.
- **Stop sharing** or **Manage access** to revoke old links when the project ends.

6.3 Sensitivity labels (if present)

- Apply labels like **Public / Internal / Confidential / Highly Confidential** to emails and files. Labels may watermark, encrypt, or restrict forwarding/printing automatically.

6.4 Version history & restore

- Use **Version History** on files to undo mistakes. For widespread damage (accidental deletes/ransomware), use **Restore your OneDrive** to roll back to a good point.

---

7) Removable Media (USB) & External Devices

- **Avoid unknown USB** devices; they can deliver malware.

- **Encrypt** any USB that stores work files (BitLocker To Go on Windows; encrypted DMG/third-party or management policy on macOS).
- **Scan** new media with antivirus before opening files.
- Disable **autorun** behaviors; open files intentionally, not automatically.

---

8) Something went wrong? Immediate actions (decision tree)

8.1 I clicked a suspicious link or opened a risky attachment

1. **Disconnect** from the internet (turn off Wi-Fi / unplug Ethernet) if you see unusual behavior.
2. **Do not reboot** repeatedly if ransomware is suspected; note any on-screen messages.
3. Run a **Quick scan** in Defender; if anything is found, follow with a **Full scan** or **Offline scan**.
4. **Report** the incident to IT immediately with details (see §11).
5. If you entered credentials on a fake page, **change your password** right away and review sign-in attempts.
6. If a corporate card or finance process is involved, **notify Finance** to hold payments.

8.2 My browser suddenly downloaded a file I didn't want

- **Don't open it.** Delete it from **Downloads**.
- Run a **Quick scan**.
- Clear the browser's **Downloads list** and **cache**.

8.3 Defender detected and removed something

- Leave the item **quarantined**.
- Capture the **Protection history** details and **time**; send to IT if requested.
- If the detection keeps reappearing, escalate (could be persistence).

8.4 Lost or stolen device

- Notify IT **immediately** with last known location/time.
- If MDM is enabled, we can **wipe** or **lock** it remotely.
- Change your **password** and revoke any **app sessions**.

---

9) Working Safely on Home/Public Networks

- **Home Wi-Fi**: use WPA2/WPA3 with a strong passphrase; change default router passwords; keep firmware updated.
- **Public Wi-Fi**: treat as untrusted; avoid accessing sensitive data without VPN; always lock your screen.
- **Captive portals** (airports/hotels): complete the portal before starting VPN.
- Prefer **Ethernet** or a strong 5 GHz/6 GHz connection for calls.

---

10) Common Problems & Self-Service Fixes

10.1 “Defender is off” / can’t start

- Open **Windows Security** → if disabled by policy, contact IT. If locally off, click **Turn on** for Real-time protection. Reboot if required.

10.2 Repeated “threat blocked” pop-ups

- Open **Protection history** → note the **process** and **file path**.
- Run a **Full scan**.
- Check **Startup apps** (Task Manager) for unknown items; disable suspicious entries.
- If it persists, run **Microsoft Defender Offline** and escalate with logs.

10.3 Can’t open an encrypted email/file

- Make sure you’re **signed in** with your work account.
- If sensitivity label says **do not forward**, you need the right rights; request access from the owner.

10.4 BitLocker recovery at boot

- Retrieve the **recovery key** from your account portal or helpdesk.
- After access, avoid BIOS changes or disk moves that re-trigger recovery without notifying IT.

10.5 FileVault asking for recovery key

- Enter your **account password** if it’s bound to FileVault, else use the **escrowed recovery key** from IT.

10.6 “This site/file is blocked by SmartScreen/IT policy”

- It’s blocked for safety. If you have a business justification, submit a **whitelist request** with URL, reason, and business impact.

---

11) Escalation Checklist (what IT needs to help fast)

- **Who/where**: your name, department, location/time zone, callback number.

- **Device**: Windows/macOS version, device model, on VPN or not.
- **What happened**: exact **time**, what you clicked/opened, any prompts or warnings.
- **Symptoms**: pop-ups, encryption notes, unusual files, browser redirects.
- **Screenshots**: of warnings/detections/URLs.
- **Defender details**: Protection history entry (name, path, action taken).
- **Network**: home/office/public; SSID if Wi-Fi.
- **Actions taken**: disconnected network, scans run (quick/full/offline), password changed.

---

12) Paste-able Responses (no links)

Report suspected phishing

> Select the message → click **Report phishing** in Outlook. Don't reply or click links. We'll analyze and block similar messages.

Run a full AV scan (Windows)

> Open **Windows Security → Virus & threat protection → Scan options → Full scan**. Keep the PC on power until it finishes.

Ransomware protection tip

> Turn on **Controlled Folder Access** in Windows Security to block untrusted apps from changing your Documents/OneDrive. Add legit apps to the allow list if they're blocked.

Enable disk encryption

> Windows: open **Manage BitLocker** and turn it on; save the recovery key per policy.
> macOS: **System Settings → Privacy & Security → FileVault → Turn On**.

If you clicked a bad link

> Disconnect from the internet, run a **Quick then Full scan**, **change your password**, and **open a ticket** with the time and details.

USB policy

Use only approved USB devices. Encrypt any USB that stores work files. Scan before opening.

---

13) Final Notes

- Security is a **layered habit**: updates + MFA + encryption + careful sharing + healthy skepticism.
- When something feels off, **stop and report**—fast reporting prevents small issues from becoming incidents.
- Keep this manual alongside your **Outlook**, **VPN**, and **OneDrive/SharePoint** guides so users can handle email, remote access, and data protection end-to-end.