

WINDOWS & MAC

Laptop Security Checklist (Windows & Mac)

A lost or infected laptop is one of the most common ways small-business data leaks. Every item below uses settings already built into Windows and macOS.

Updates and protection

- ☐ Turn on automatic updates for the operating system, browser, and apps; restart when prompted
- ☐ Keep built-in protection on: Microsoft Defender on Windows, XProtect and Gatekeeper on Mac
- ☐ Turn on the built-in firewall (Windows Security, or System Settings > Network > Firewall on Mac)
- ☐ Remove software you no longer use, and replace a laptop that no longer receives security updates

Encryption and sign-in

- ☐ Turn on full-disk encryption: BitLocker or Device Encryption on Windows, FileVault on Mac
- ☐ Store the encryption recovery key somewhere safe, such as your password manager, not on the laptop
- ☐ Use a strong password or passphrase, plus Windows Hello or Touch ID for convenience
- ☐ Use a standard (non-administrator) account day to day; keep a separate admin account for installs
- ☐ Lock the screen automatically after 5 minutes or less, and lock it whenever you step away

Browsing and accounts

- ☐ Use a password manager and turn on multi-factor authentication (MFA) for email, banking, and work apps
- ☐ Keep separate browser profiles for work and personal use
- ☐ Install only a few browser extensions you trust; remove the rest
- ☐ Do not save company files in personal cloud storage or personal email

Backup and recovery

- ☐ Follow the 3-2-1 rule: 3 copies, on 2 different types of storage, 1 offline or off-site
- ☐ Test a restore at least twice a year
- ☐ Turn on Find My Device (Windows) or Find My (Mac) so a lost laptop can be located, locked, or erased
- ☐ Never leave the laptop visible in a car, and use a privacy screen when working in public

Sources and further reading

CISA: Secure Our World: <https://www.cisa.gov/secure-our-world>

NIST SP 800-114 Rev. 1: User's Guide to Telework and BYOD Security: <https://csrc.nist.gov/pubs/sp/800/114/r1/final>

Need help rolling this out across your team? Request a consultation at nexussecurityadvisors.com/get-started.