CICADA | RESOURCES

DEVICES | 30 MIN | ESSENTIAL | UPDATED NOVEMBER 2026

Encrypt laptops and phones

Turn a stolen laptop from a data breach into a hardware problem. Usually free, already installed, and often switched off.

The short version

- ✓ Encryption protects data at rest if a device is lost or stolen.
- ✓ BitLocker is built into Windows; FileVault into macOS.
- ✓ Store recovery keys somewhere you can reach if the device dies.
- ✓ Encryption is not a backup and doesn't stop malware running.

Check what's already on

Windows: Settings → Privacy & security → Device encryption, or search for BitLocker. Windows 11 Home often has device encryption; Pro has full BitLocker. **macOS:** System Settings → Privacy & Security → FileVault. **iPhone/Android:** a screen lock passcode encrypts the device by default on modern versions; confirm it's set.

If encryption is off, turn it on when the device is plugged in and you have time for it to finish. It can take a while on a full disk.

Handle recovery keys properly

When you enable encryption, a recovery key is created. If you lose it and the device fails, the data is gone. Store keys in the password manager's secure notes, escrow them in your device management platform, or print them and keep them in a safe. Don't leave them on the same laptop.

For BitLocker in a business, back the key to Entra ID / Active Directory or your management tool so IT can recover it.

Don't confuse encryption with the rest

Encryption protects a powered-off device. It doesn't stop a phishing email, ransomware running while you're logged in, or a backup failing. Pair it with screen locks, remote wipe, automatic updates and tested backups.

> **LOST DEVICE CHECKLIST**
>
> Report it, remote-wipe it, change the passwords for accounts signed in on it, revoke sessions, and check for unusual activity. If it held personal data, assess whether it's a reportable breach.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.

Action checklist

- [ ] Encryption enabled on every laptop
- [ ] Screen lock enabled on every phone
- [ ] Recovery keys stored outside the device
- [ ] Remote wipe enabled and tested
- [ ] Lost-device procedure written down
- [ ] Asset list records serial numbers

0 of 6 done