# The Essential 8 Explained in Plain Language

The **Essential 8 (E8)** is a set of practical strategies from the Australian Cyber Security Centre (ACSC).  
They are designed to protect against the most common types of cyberattacks.

Below is a plain-language description of each strategy, with examples of how they apply in the real world.

## 1. Application Control

**What it means:** Only let approved programs run on your computers.  
**Why it matters:** Stops hackers from installing malicious software.  
**Example:** A ransomware program tries to run, but because it is not on the “approved” list, it is blocked.

## 2. Patch Applications

**What it means:** Keep software (like browsers, PDF readers, and apps) up to date with the latest fixes.  
**Why it matters:** Hackers often take advantage of old bugs in software.  
**Example:** A security update for Chrome is released. If you install it quickly, attackers cannot use that bug to break in.

## 3. Configure Microsoft Office Macros

**What it means:** Control or block macros (tiny programs that can run inside Office documents).  
**Why it matters:** Hackers often use Word or Excel files with hidden macros to deliver malware.  
**Example:** Someone emails you a spreadsheet with a malicious macro. Because macros from the internet are blocked, the attack fails.

## 4. User Application Hardening

**What it means:** Turn off risky features in common apps.  
**Why it matters:** Reduces the ways attackers can sneak in.  
**Example:** Blocking Flash, ads, or Java in your browser so attackers cannot exploit them.

## 5. Restrict Administrative Privileges

**What it means:** Only give admin (high-level) access to the people who really need it.  
**Why it matters:** If a hacker breaks into a normal user account, they should not get admin powers.  
**Example:** A hacker steals a staff member’s password. Because that account is not an admin, the attacker cannot take over the whole system.

## 6. Patch Operating Systems

**What it means:** Keep your operating systems (Windows, macOS, Linux) up to date with security patches.  
**Why it matters:** Old versions of operating systems are a common target for attackers.  
**Example:** Installing Windows updates regularly prevents attackers from exploiting known vulnerabilities.

## 7. Multi-Factor Authentication (MFA)

**What it means:** Require more than just a password to log in, such as a code on your phone or a biometric check.  
**Why it matters:** Even if a hacker steals your password, they still cannot get in.  
**Example:** A stolen password is useless because logging in also requires a one-time code sent to your mobile.

## 8. Regular Backups

**What it means:** Keep secure, recent copies of important data and test that you can restore them.  
**Why it matters:** Lets you recover quickly if data is stolen, corrupted, or held for ransom.  
**Example:** Ransomware encrypts your files, but you restore everything from yesterday’s backup and avoid paying.

## Key Message

The Essential 8 is not about perfection, it is about reducing risk.  
By raising maturity across these eight areas, you make it much harder for attackers to succeed.