Keeping your software up to date isn't just about getting the new features, it's a foundation of digital safety. A recent *Forbes* article highlighted how critical it can be to both **update and periodically restart** devices like cellphones, but also computers, tablets and other connected devices to flush out malware hiding in your phone's active memory that can lurk unnoticed by you. Analysts and security experts now warn that without the latest patch updates and periodic reboots, sophisticated spyware can remain active and evade detection, quietly stealing data or causing your device to act erratically or slow down its performance.

The main reasons to update are **security patches**. These are fixes released by software developers to close weak spots that bad guys can use to access your device. When vendors like Apple, Microsoft, or Google discover that their operating systems or applications have weak points, often identified after being reported by users, they push updates that repair those gaps. Ignoring these patches leaves devices exposed to known threats. Bad guys can reuse the same tactics repeatedly, knowing unpatched systems remain vulnerable. Cybersecurity research reinforces this point that delaying updates significantly increases the risk of compromise, and systems that stay current enjoy far fewer successful hacks.

But updates are about more than closing gaps. They often include **internal improvements** that make your device just run better. Many modern devices also incorporate new security software with updates such as extra protection that keep malware from running in the background that make it harder for malware to remain on your device. Without applying these updates, users miss out on these new defenses that can prevent attacks before they ever begin. When combined with regular device restarts, these updates ensure that any malicious code temporarily residing in system memory is cleared, reducing the chance attackers can maintain a foothold.

Another critical aspect is **system resilience against evolving threats**. Cyber attackers constantly refine their methods. a weak spot considered minor yesterday can become a spring-board for large-scale ransomware or spyware campaigns tomorrow. By updating software frequently, users bring their devices up to date with the latest threat intelligence, closing off those holes that cybercriminals are actively exploiting. Organizations that delay updates not only risk individual system breaches but could also cause a wider network breach that affects everyone.

Finally, there is a **behavioral and awareness dimension**. Many users delay updates because they find prompts inconvenient, fear new bugs, or simply aren't aware of the stakes. Yet, research shows that increasing awareness of the risks, especially highlighting how simple actions like updates and restarts block malware can significantly improve security. Making automatic updates the default and educating everyone about the real consequences of outdated software are essential steps in keeping you and your family safe from online predators.