

Basic Digital Safety

Data backup is essential to protecting your important data. Here are some tips for protecting your data as well as the reasons it's crucial:

Prevent Data Loss:

- Cyberattacks, human mistake, and hardware malfunctions can all result in data loss.
- Frequent backups guarantee that you have a safety net in case of crises.

Benefits for Businesses:

- Reduce Downtime: Backups facilitate a business's speedy recovery from data loss.
- Save money by avoiding costly data recovery procedures by maintaining dependable backups.

Recommended Procedures:

- Safe Archive: Regularly backup critical files.
- Select Trustworthy Solutions: Employ reputable backup products or services.

Examine Restores: Remember, data backup is like an insurance policy for your digital life. Verify backups are working by occasionally restoring data 1. Start backing up now rather than waiting until it's too late! [1]



Keep Software Updated

Updating your software is essential to keeping your systems operating securely and efficiently. Frequent updates, such as firmware upgrades, software updates, and operating system patches, aid in addressing vulnerabilities and flaws that are found over time. You can guarantee that your devices have the newest security features and defences against potential dangers like malware and cyberattacks by keeping up with updates.

Furthermore, functional additions, UI improvements, and compatibility fixes are frequently included in software updates, which can improve the user experience overall. To keep your software secure and up to date, make it a practice to turn on automatic updates whenever it's feasible and to manually check for updates on a frequent basis. [2]



Turn on two-factor verification (2FA)

By adding an additional layer of security to your accounts, Two-Factor Authentication (2FA) requires a second form of verification in addition to your password. Once you've entered your password, you'll usually be asked to send in or get an SMS with a unique code that was produced on your smartphone using an authentication tool like Google Authenticator. This extra precaution guarantees that without the secondary code, unauthorised access is prevented even if your password is compromised. It is advised to use 2FA to secure sensitive data and important accounts since it lowers the possibility of unauthorised access and greatly improves account security. [3]



Strong Passwords

Strong passwords are at least 12 characters long and contain letters, numbers, and symbols. Your password should ideally be unintelligible as a word or phrase. Yes, you should give each internet account a different password. Seems difficult to recall? As we'll explain in a moment, using a password manager has never been simpler: many web browsers and phones come with password managers built in, and some even recommend using strong passwords. If not, we advise creating a password that is actually a "passphrase," which is a phrase with at least 12 characters. [4]

