Creating Strong & Secure Passwords

mother
technologies

In 2022, over 24 billion passwords were exposed by hackers.

Passwords are vital in our digital world, safeguarding emails, banking, and systems from unauthorised access. With cyber threats evolving, prioritising password security is crucial. Here are our steps to creating a strong password:

Make Passwords Lengthy

Passwords should be at least 12 characters long. According to the National Institute of Standards and Technology, increasing password length is more effective for improving security than complexity. For instance, an eight-character password could be cracked in less than a day using the latest AI, and a password with fewer than 6 characters can be cracked in seconds.

Create Complex Passwords

m#P52s@ap$V!

Because of the prevalence of weak passwords like '123456,' over 80% of cyberbreaches that occur are related to stolen passwords. It's crucial to use a combination of uppercase and lowercase letters, numbers, and special characters in passwords. Avoid easily guessable information like names, birthdates, common words or repetition.

Different Passwords for Different Accounts

Using the same password for multiple accounts increases the risk because if one account is breached, hackers can potentially access all other accounts using the same password. Employ a password manager for generating and storing complex passwords for each account, enhancing security and reducing the impact of breaches.

Frequently Update your Passwords

Keeping passwords up to date is essential for preventing data breaches. Businesses should encourage employees to change passwords regularly, especially for important accounts like banking or customer files. This helps strengthen online security and protects against cyber threats. Refreshing passwords every few months is crucial for safeguarding assets and reputation from cyber criminals.

Enable 2FA

Two-factor authentication enhances security by requiring a second verification alongside your password, such as a code sent to your phone or email. Even if your password is compromised, access remains protected. Learn more about our 2FA service here.