The Best Defense Against Social Engineering?
A Password Manager

Education and training can only go so far. The best tool you can give your employees to prevent social engineering? A password manager.

A password manager ensures that your employees:

- Stay away from fraudulent sites
- Use complex passwords
- Never reuse passwords
- Equipping your employees with a password manager is key to the integrity and safety of your business's data in the face of the growing threat of social engineering.

You can reduce your organisation's reliance on human behaviour:

- Manage complex, unique passwords from one place
- Share passwords simply and securely
- Go passwordless – it's really easy to do!

With over 1 billion sites secured, millions of users, and trusted Business customers, LastPass makes online security simple.

Use complex passwords
A password manager generates strong passwords and stores them securely, preventing you from having to remember them. The password manager only populates the login.

Never reuse passwords
Unique passwords are harder to crack and harder to engineer.

Equipping your employees with a password manager is key to the integrity and safety of your business's data in the face of the growing threat of social engineering.

You can reduce your organisation's reliance on human behaviour:

- Manage complex, unique passwords from one place
- Share passwords simply and securely
- Go passwordless – it's really easy to do!

With over 1 billion sites secured, millions of users, and trusted Business customers, LastPass makes online security simple.

Source: (1) Combatting Social Engineering, 2024, LastPass