LastPass

The Best Defense Against Social Engineering? A Password Manager

Businesses forecast phishing to be the biggest social engineering threat to businesses in 2024.[1]

81%

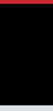
of businesses have seen an increase in phishing.[1]

Staying one step ahead of the bad actors is crucial to your organization's security.

Social engineering preys on human vulnerability through psychological manipulation.

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:

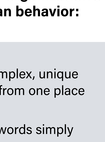


Use complex passwords

Password managers generate and store strong passwords for each account, reducing the need to use simple, guessable passwords. The harder to crack means the harder to phish.

Never reuse passwords

Unique passwords help prevent unauthorized access even if one set of credentials is compromised in a social engineering attack.



Stay away from fraudulent sites

A password manager restricts password entry to verified sites by autofilling credentials. If the password manager doesn't autofill, that may be a sign you're dealing with a phishing attempt.

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 organization's reliance on human behavior:

Manage complex, unique passwords from one place

Share passwords simply and safely

Go passwordless – as you're ready for it

With over 1 billion sites secured, millions of users, and 100,000 Business customers, LastPass makes online security simple.

Contact Us

Source:
[1] Combatting SocialEngineering, 2024, LastPass