LastPass

Ihre beste Verteidigung gegen Social Engineering? Ein Passwort-Manager!

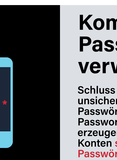
Phishing wird auch 2024 die größte Social-Engineering-Bedrohung für Unternehmen bleiben.[1]

81%

der Unternehmen erlebten im vergangenen Jahr eine Zunahme von Phishing.[1]

Entscheidend für die Sicherheit Ihres Unternehmens: Angreifern einen Schritt voraus zu sein.

Social Engineering baut darauf, dass Menschen anfällig für psychologische Manipulation sind.



Leider reichen Aufklärung und Schulung alleine nicht. Der beste Schutz Ihrer Mitarbeiter gegen Social Engineering? Ein Passwort-Manager.

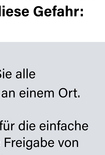
Ein Passwort-Manager sorgt dafür, dass Ihre Mitarbeiter ...

Komplexe Passwörter verwenden

Schluss mit einfachen, unsicheren Passwörtern: Passwort-Manager erzeugen für alle Konten starke Passwörter und verwahren sie sicher. Starke Passwörter schützen besser gegen Phishing.

Niemals Passwörter wieder-verwenden

Für jedes Konto ein eigenes Passwort: So können Social-Engineering-Angreifer mit einem gestohlenen Passwort nicht in weitere Konten eindringen.



Betrügerische Websites vermeiden

Auf legitimen Websites sorgt ein Passwort-Manager für die automatische Eingabe von Zugangsdaten. Unterbleibt sie, könnte es sich bei der betreffenden Website um eine Phishing-Site handeln.

Social Engineering ist eine wachsende Gefahr. Schützen Sie Ihr Unternehmen und die Integrität Ihrer Daten: Statten Sie Ihre Mitarbeiter mit einem Passwort-Manager aus.

Menschen können Fehler machen. Entschärfen Sie diese Gefahr:

Verwalten Sie alle Passwörter an einem Ort.

Sorgen Sie für die einfache und sichere Freigabe von Passwörtern.

Führen Sie Ihr Unternehmen in eine passwortlose Zukunft.

Mit mehr als einer Milliarde abgesicherter Websites, Millionen Nutzern und 100.000 Geschäftskunden macht LastPass die Onlinesicherheit einfach.

LastPass kontaktieren

Quelle:
[1] Social Engineering – gefährlich wie nie, 2024, LastPass