LastPass•••|

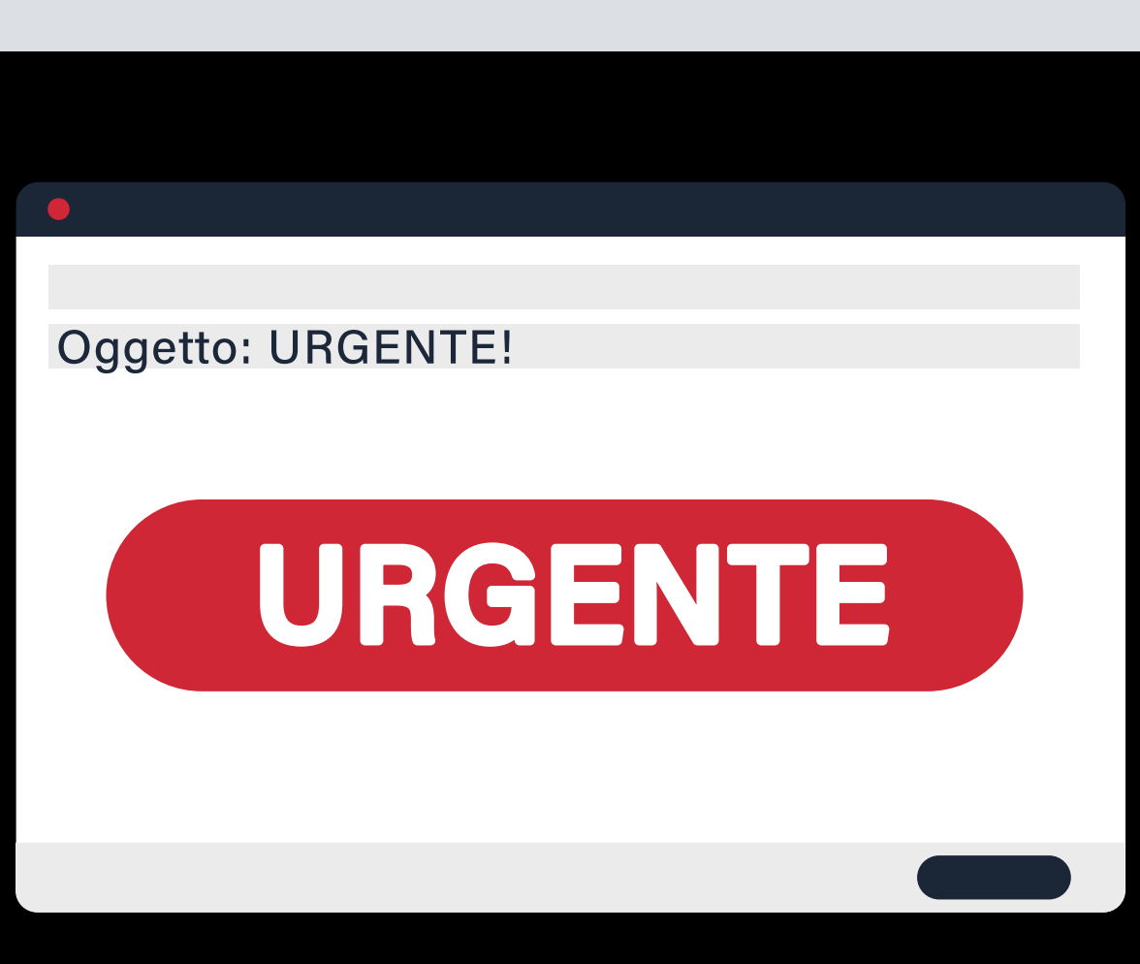
La miglior difesa contro l’ingegneria sociale?
Un gestore di password

Secondo le imprese, nel 2024 il phishing rappresenterà la principale minaccia di ingegneria sociale per il mondo imprenditoriale.[1]

81%

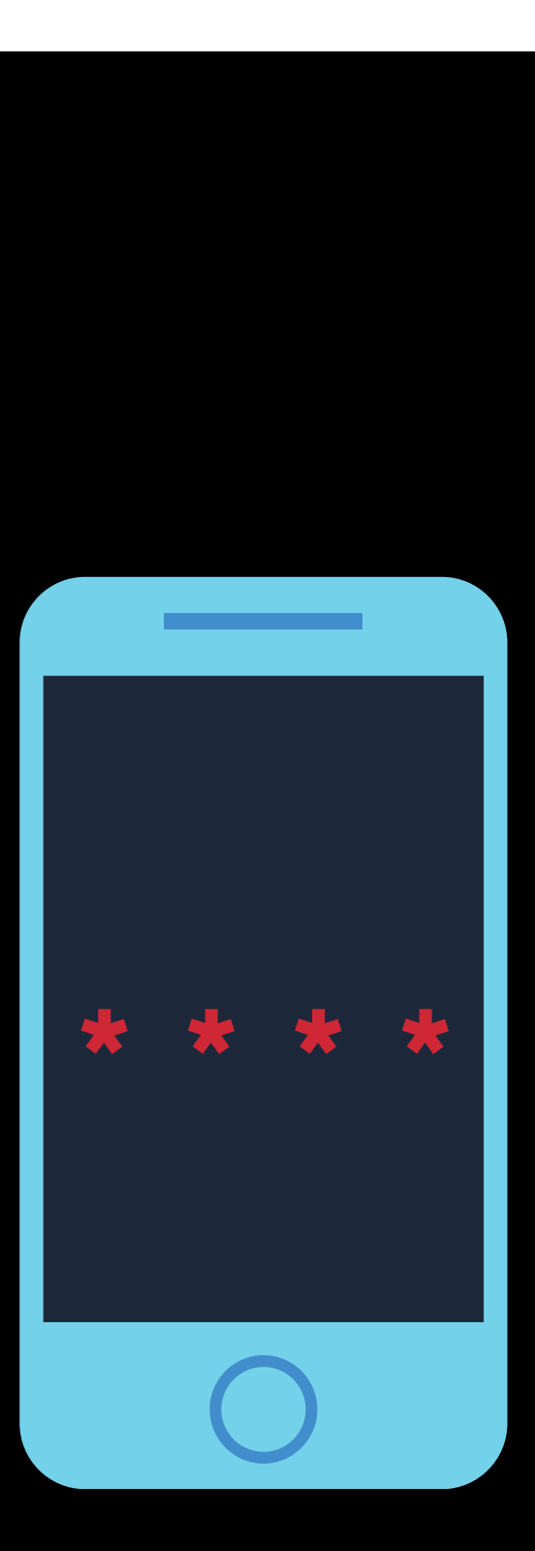
Le aziende che hanno registrato un aumento degli attacchi di phishing.[1]

Per proteggere la tua organizzazione, è essenziale anticipare gli attacchi dei malintenzionati.
L’ingegneria sociale sfrutta le debolezze umane attraverso manipolazioni psicologiche.



Le attività educative e formative hanno i loro limiti. L’arma migliore che puoi dare ai tuoi dipendenti per difendersi dall’ingegneria sociale? Un gestore di password!

Un gestore di password fa sì che i tuoi dipendenti:



Usino password complesse

I gestori di password creano e salvano password complesse per ogni account, riducendo così la necessità di usare password elementari e semplici da indovinare. Più sono difficili da violare, più rendono il phishing inefficace.

Non riutilizzino le password

Le password univoche contribuiscono a prevenire l’accesso non autorizzato anche se un’unica combinazione di credenziali dovesse essere compromessa in un attacco di ingegneria sociale.

Evitino i siti fraudolenti

Un gestore di password limita l’inserimento delle credenziali ai siti verificati, compilandone automaticamente i campi. Se non lo fa, potrebbe trattarsi di un tentativo di phishing.

Dotare i tuoi dipendenti di un gestore di password è fondamentale per l’integrità e la sicurezza dei dati aziendali di fronte alla crescente minaccia dell’ingegneria sociale.

Puoi ridurre la dipendenza della tua organizzazione dagli approcci individuali:

- Gestendo password univoche e complesse in modo centralizzato
- Condividendo le password in modo semplice e sicuro
- Liberandoti dalle password, non appena sarai pronto

Con oltre 1 miliardo di sedi protette, milioni di utenti e 100.000 clienti aziendali, LastPass rende la sicurezza online più semplice.

Contattaci

Fonte:
(1) Combattere l’ingegneria sociale, LastPass, 2024