NOW SHOWING

PASSWORDS AND PASSWORD MANAGERS

Both employee and personal passwords are a common target for hackers. Just this year, Hackers stole Slack employee password tokens and broke password controls through brute-forcing (trying every possible combination of characters until they find the correct password). The hackers uploaded Slack's code repositories, and there could still be consequences going forward.

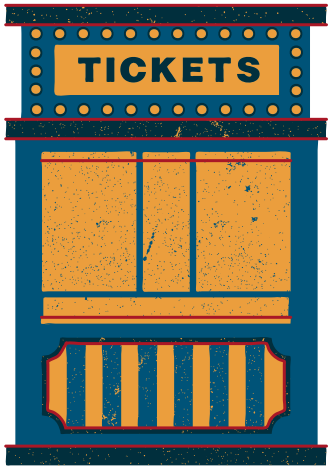
Stronger passwords might have prevented this breach.
Read on to see how to develop and maintain strong passwords.

Creating passwords

According to Nordpass, big box office films are popular passwords. In 2022, with the release of their respective films, "Batman" was used 2,562,776 times and "Encanto" 10,808 times. But these popular passwords are also easy for hackers to guess. Using a strong password or a passphrase will help keep you and your data secure.

Passphrases are great because they are easy to remember and hard for hackers to guess or crack. This is because they tend to be longer and more complex than traditional passwords. Two examples of a passphrase could be: "m0viesPopcornTreat!" or "M@yTHEforceb3withYou".

For up-to-date best practices, visit the National Institute of Standards and Technology (NIST).



Storing your passwords

You always hear about creating a secure password, but how do you keep your secure passwords secure? A password manager app is your ticket to remembering (or forgetting) passwords.

A password manager is a secure vault for all your passwords — like a glorified password notebook but a lot more secure! You only have to remember one password, allowing you and your computer to access the rest of your passwords for all your logins. This also means you can (and should!) create different passwords for each account, keeping you ahead of any hackers!

INFOSEC
SECURE YOUR SCREEN

E-TECH