CREDENTIAL THEFT & MFA

What Is Credential Theft?

- When attackers steal your login details (username, password).
- They use phishing emails, fake websites, or malware.
- Stolen credentials allow them to enter your accounts.
- This is one of the most common cyber attacks today.

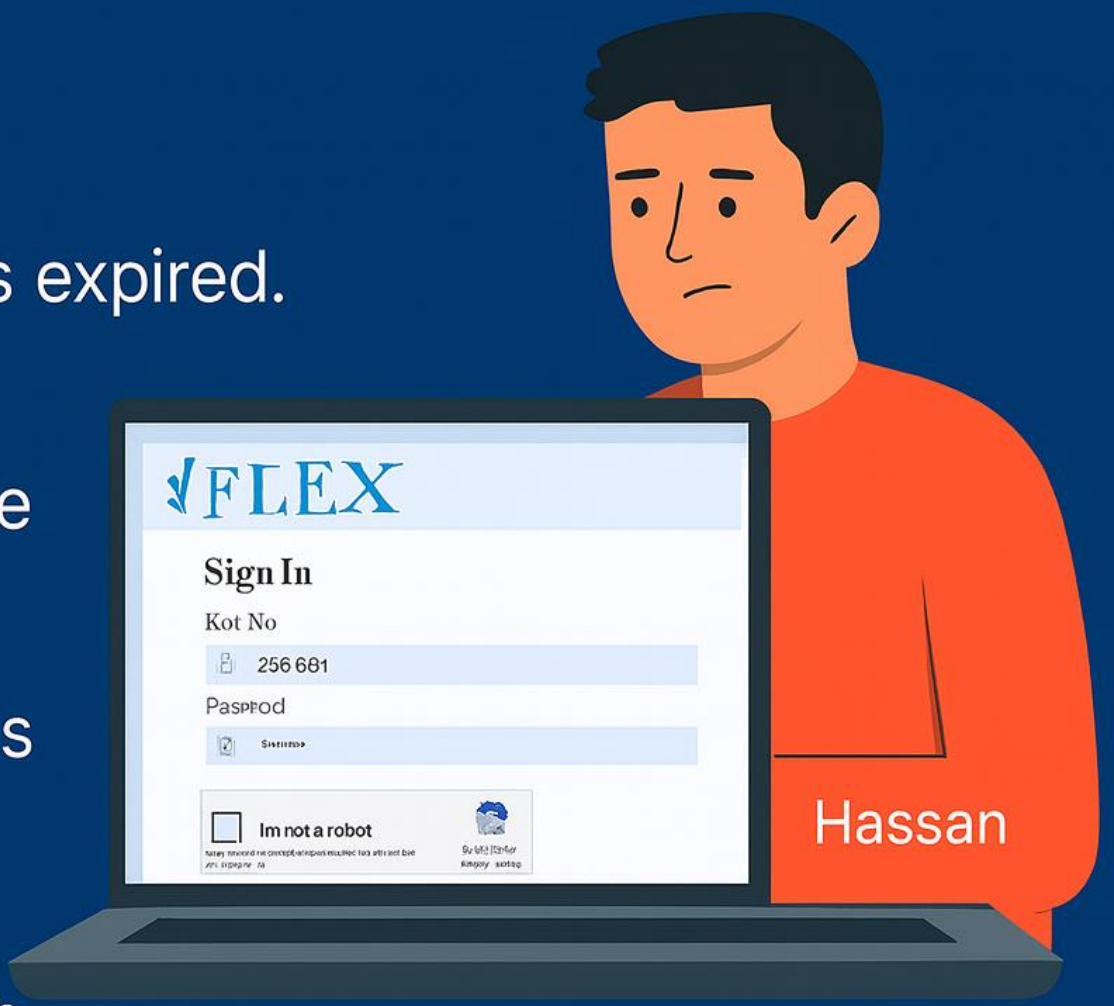
How Attackers Steal Credentials

- Fake login pages that look real (Google, Facebook, Bank).
- “Password expired” phishing emails.
- Password-stealing browser extensions.
- Messages asking you to “verify your account”.

Hassan's Login Gets Stolen

- Hassan gets a message:
  "Your FLEX password has expired. Click here to update."
- The page looks real, so he enters his login details.
- Attackers instantly use his password to access his email and FLEX.

› This is credential theft through **a fake site.**



What is Multi-Factor Authentication (MFA)?

- MFA requires users to verify identity using more than one method.
- Common combination: password + phone OTP/app approval.
- Even if passwords are stolen, MFA blocks unauthorized logins.
- A critical layer of defense against phishing attacks.

Common Credential Theft Methods

Fake login pages (phishing) capturing passwords.

Keyloggers recording keystrokes.

Credential stuffing using leaked username/password pairs.

Social engineering to trick users into sharing credentials.

MFA in Action (How It Works)

- User enters username and password (first factor).
- System prompts for second factor: OTP, push notification, or token.
- Access granted only after both factors are validated.
- Attackers cannot easily bypass MFA without physical access.

Types of Authentication Factors