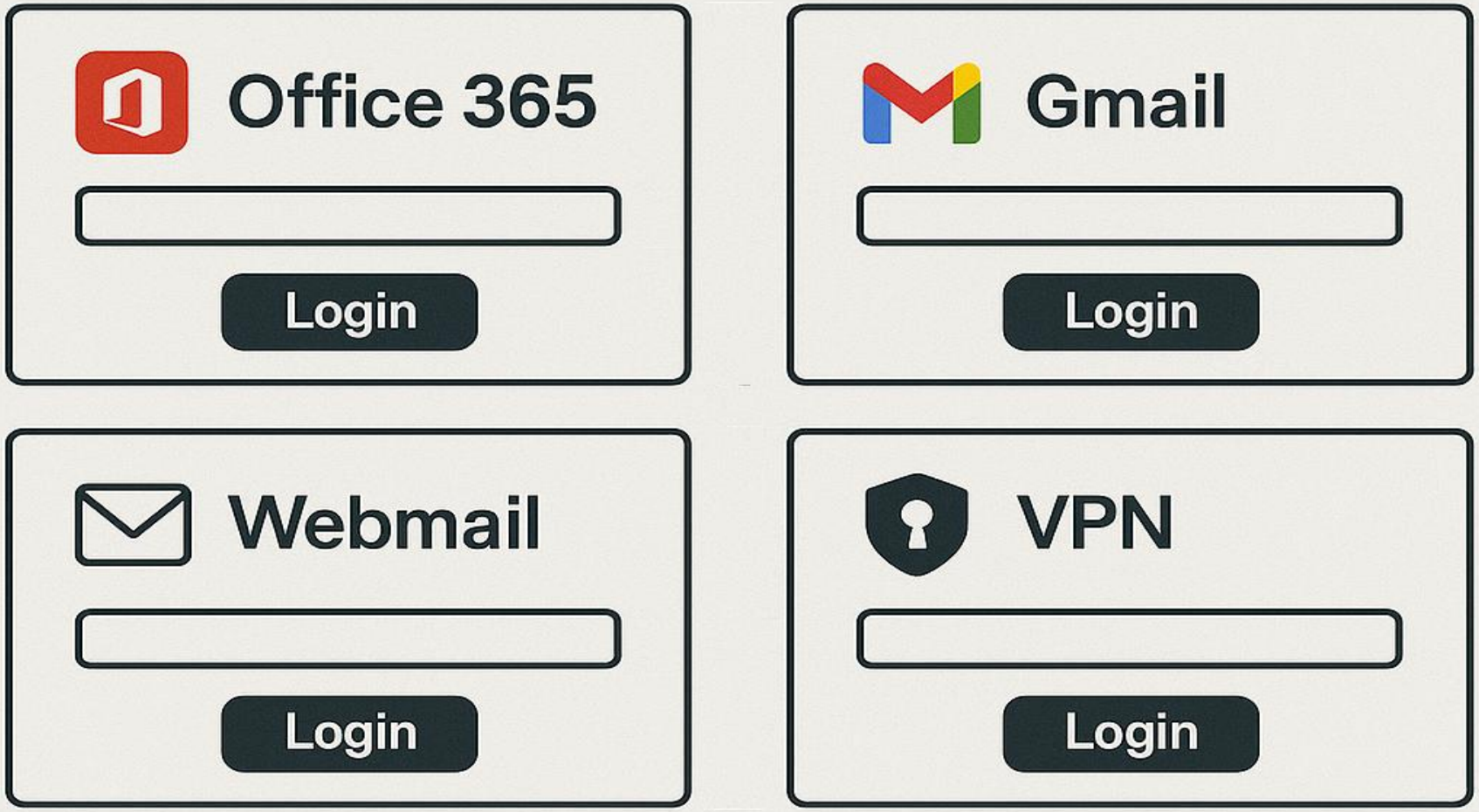
8. CREDENTIAL-HARVESTING (FAKE LOGIN PAGES)

Attackers create fake login pages that look identical to real portals like Office 365, Gmail, webmail, or VPN sites.

Their goal is to trick users into entering their credentials, which are instantly stolen and used to access real accounts.

What Are Credential-Harvesting Pages?

Attackers create fake login portals mimicking:



Scenario: Maryam Clicks a Fake “Password Expiry” Link

Maryam receives:
“Your password expires in 24 hours. Update here.”

The page looks **exactly** like Microsoft login,
but the URL is:
office365-login-security-verification.com/login

She enters her password, the attacker gains access instantly.

Lesson: Always check the URL carefully before entering credentials, and never click links from unexpected emails.


Your password expires in 24 hours. Update here.
office366-login-security.verJfication.com/logIn
Microsoft
Your password expires in 24 hours. Update here.
Enter password
Sign in
Maryam

How Fake Pages Are Made?

- HTML clones
- Lookalike domain names
- Stolen logos
- Fake HTTPS certificates

Red Flags to Detect

- URL slightly different
- Missing corporate branding
- Login page opens unexpectedly
- Requests for multiple passwords

Prevention Tips

- Always check URL
- Never reset password from email links
- Use bookmark for real portals
- Enable MFA everywhere