**CONSEQUENCES & REMIDIES**

**Most common consequences (When clicked on the link provided in the phishing email):**

**1. Credential Theft (Fake Login Page):**

The link usually takes you to a fake website that looks like a real one (e.g., Microsoft, Gmail).

It will ask for your username, password, or 2FA code.

Once entered, the attacker immediately gets access to your real account.

**2. Malware or Virus Installation:**

The link may trigger a download of a malicious file (e.g., .exe, .pdf, .doc with macro).

It could install:

* Keyloggers
* Remote Access Trojans (RATs)
* Ransomware

**3. Browser Exploits:**

Even without downloading, visiting the link could exploit vulnerabilities in your browser.

May result in drive-by downloads, which silently install malware.

**4**. **Tracking and Fingerprinting:**

The phishing site may collect:

* Your IP address
* Browser info
* Location
* Device type

Useful for targeting future attacks or selling data on the dark web.

**5.** **Financial Theft or Identity Fraud:**

If you enter sensitive information like:

* Credit card numbers
* Social Security numbers
* Bank login details

The attacker could perform fraudulent transactions or steal your identity.

**6.** **Session Hijacking:**

Some advanced phishing kits can hijack your session if you're logged into the real site.

They mimic your actions and steal session tokens.

**What You Should Do If You Clicked:**

1. Disconnect from the internet immediately
2. Run a full antivirus scan
3. Change all passwords (starting with email & financial)
4. Enable multi-factor authentication (MFA)
5. Check for unauthorized logins
6. Report the phishing attempt to your provider (e.g., Microsoft, Google)