Legal, Policy, and Consequences of Phishing

Why This Topic Matters

- Phishing isn’t “just a mistake.”
- It has **legal**, **organizational**, and **personal** consequences.
- Employees/students must follow rules to stay protected.

National & International Cybercrime Laws

- Many countries classify phishing under fraud, identity theft, and computer misuse laws.
- International cooperation frameworks (e.g., INTERPOL, Budapest Convention) support prosecution.
- Penalties may include fines, imprisonment, or asset seizure.
- Laws apply even if the attacker is in another country.

Organizational Security Policies

Most companies/universities require:

- Safe email handling
- Strong password practices
- Reporting suspicious messages
- Never sharing login credentials
- Following device/security rules

Breaking these → disciplinary action.

Hassan Clicks a Phishing Link

Consequence:

University IT blocks his account

He has to give a written explanation

Incident gets logged under security violations

What Happens After a Phishing Incident

- IT investigates the compromised account
- Logs checked → to find who accessed what
- Password resets enforced
- Systems cleaned
- User is interviewed about the incident

Possible Consequences

For individuals:

- Account suspension
- Academic/HR warning
- Required security training

For organizations:

- Data leaks
- Financial loss
- Reputation damage
- Legal penalties

How to Protect Yourself

- Follow all security policies
- NEVER share credentials
- Don’t forward suspicious emails
- Always report incidents properly
- Keep your devices updated

Key Message

Policies exist to *protect you*.

Breaking them — even by mistake — can create serious consequences.

Stay alert, stay safe, and follow your organization’s guidelines!