# PTA Security Advisory-No: 48

**08, April 2019**

**Threat Classification:** Security Attack

**Name:** Credential Stuffing and Password Spraying Attacks

**Overview:** Many financial Institutions are at risk of money theft due to several data breaches through various electronic gateways and services. People who often use the same credentials / passwords / PIN codes for multiple online accounts are an easy target for attackers, as sensitive public credentials are sold on the Dark Web, which can be used to gain unauthorized access to victim's personal accounts through Credential Stuffing and Password Spraying Attacks.

**Impact:** Hackers can take advantage of the stolen credentials obtained from past security data breaches from multiple online services. The attacker could gain unauthorized access to victim's personal accounts for any malicious activity, who use the same username and password for different online accounts.

**Recommendations:**

- Change your password periodically; use a long and random password/passphrase that consists of uppercase and lowercase letters, numbers and symbols.
- Use different passwords for different online accounts.
- Enable Multi-Factor Authentication where possible.
- Whenever possible, run software with minimal access rights and privileges.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoids download/use of crack and pirated software.
- Designate PoC from your security / network team (if yet not designated), for seeking assistance and reporting security issues.
- In case of any incident, please report to this office.