Common Vulnerabilities in Password-based Login

For as long as passwords have existed, their use as the primary means of authentication has been challenged. Passwords are intended to be used only by authorized users, but they are easily exploited by malicious actors, making them a growing security issue.

The following are some of the most common password-based login security issues:

1. **Brute Force Attack**: A brute force attack is a type of hacking that relies on trial and error to crack passwords (such as login credentials and encryption keys) by trying many different combinations. It's a basic but effective approach that's frequently used when the attacker only knows a small amount of information about the target, such as a username, or when they know the password's broad structure but not its precise content.

Consequences of brute force attacks:

- Your private and sensitive information is at risk.
- Hackers use malware to cause network disruptions.
- Hackers take over selected systems and use them for malicious purposes.
- Such attacks have the potential to harm your company's reputation.

How to prevent brute force attacks?

- Longer passwords with a variety of character types are better.
- Change your passwords regularly.
- For each site, use a separate username.
- To keep track of your internet login information, use a password manager.

- **Phishing Attacks:** A phishing attack is a sort of cyber attack in which hackers send fake emails that look to come from a trusted source. Hackers use this strategy to steal sensitive information such as credit card numbers and login credentials.

How to avoid phishing attacks?

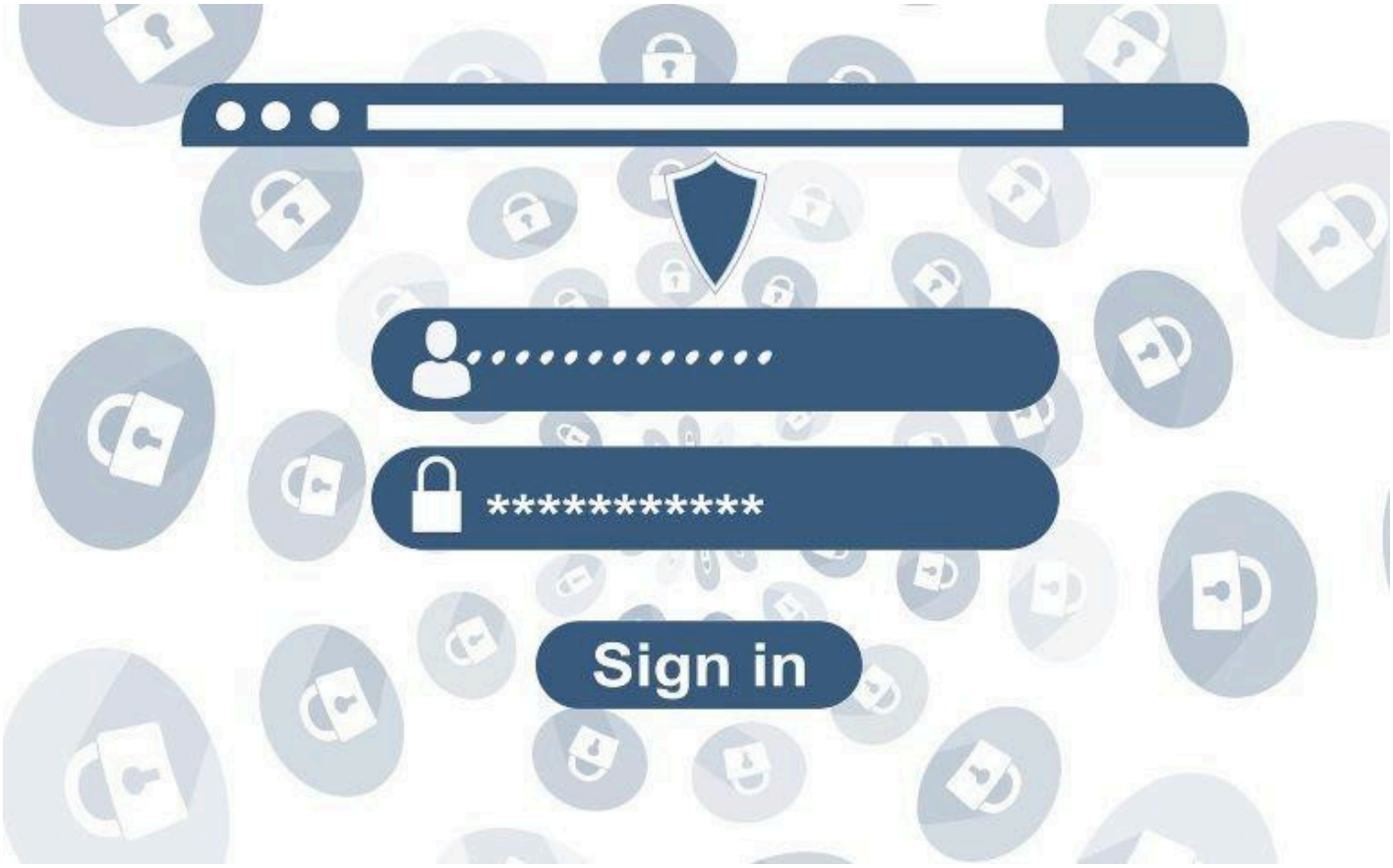
- Using security software, protect all devices in the organization.
- Use a policy that requires all devices connected to your network to be updated.
- Multi-factor authentication should be used.

- To avoid a security risk, open and read your emails with caution.

- **Credential Stuffing:** Credential stuffing is a sort of cyberattack in which attackers connect to another service using credentials stolen through a data breach on one service.

If an attacker gets a list of usernames and passwords from a popular department store hack, he attempts to enter a national bank's website using the same login credentials. The attacker is aware that some of that department store's clients are bank customers.

How to prevent credential stuffing?



- Use separate passwords for various web services.
- Authentication based on risk is a good idea.
- Bot management can prevent malicious bots from attempting logins while leaving valid logins unaffected.

Bottom line

The difficulty is that today's digital environment exposes authentication systems to more vulnerabilities than ever before, which are rapidly increasing.