# Credential Stuffing - What It Is & How To Combat It

cyber security business customers

**Summary:** Credential stuffing is a common cyberattack that can lead to account takeover. What you should know to stay safe.

Since Thanksgiving is tomorrow, there may be a few of you who will be stuffing a turkey and getting out your favorite green bean recipes, even though this year is markedly different from Thanksgivings of years past. Whatever Thanksgiving dishes you enjoy, we hope you stay safe.

Having stuffing and staying safe can be a challenge in another way too -- in the cyber world. Credential stuffing is a common cyberattack type in which thieves use lists of compromised user credentials to gain illicit entry to a system. Attackers automatically enter the logins for thousands to millions of previously stolen credentials until they are potentially matched to an existing account, knowing that many people reuse passwords across accounts. This growing threat is relatively easy to instigate and is extremely dangerous to consumers and community financial institutions (CFIs) because it can lead to account takeover.

The Open Web Application Security Project (OWASP), a nonprofit foundation dedicated to improving software security, developed a cheat sheet to help organizations prevent credential stuffing. Here are a few of the group's recommendations which can help keep your institution safe:

**MFA.** Require multi-factor authentication (MFA), which research has shown to be a critical line of defense in mitigating account compromises of this nature.

**Necessitate secondary credentials.** In addition to requiring a password, users can be prompted for additional information such as a PIN, security questions and answers, or specific characters from a secondary password or memorable word.

**Employ CAPTCHA.** This type of system allows web hosts to distinguish between human and automated access to websites. It's not fool-proof, but requiring a user to solve a CAPTCHA to log in can help prevent automated login attempts.

**IP Blocking.** Since less sophisticated attacks may use a small number of IP addresses, it's possible to ban those addresses after a number of failed login attempts. CFIs can also utilize publicly available abusive IP lists. One is AbuseIPDB, which offers a central repository to report and identify IP addresses known to be associated with malicious online activity.

**Device fingerprinting.** This can be matched against any browser attempting to login. In the case of an unrecognized device, a user should be prompted to enter additional credentials.

**Require unique usernames.** Many credential lists only include email addresses, so requiring a unique, non-email username when users register can make life more difficult for an attacker.

It's also important to help customers protect themselves. One way is by allowing them an option to disable their account as soon as they get a suspicious login alert -- since time is of the essence. Another is to remind customers not to share passwords across accounts. You may feel like a broken record, but fraudsters are getting more savvy; You need to remain vigilant by continuing to educate your customers on the latest cybercriminal techniques and how to appropriately combat them, while keeping them at bay from your institution.

## ON-DEMAND HELP FOR FINANCIAL INSTITUTIONS

Financial institutions face many difficult challenges, but you are not alone. Our experts stand ready to help you address a variety of issues. Find out more about our solutions today.