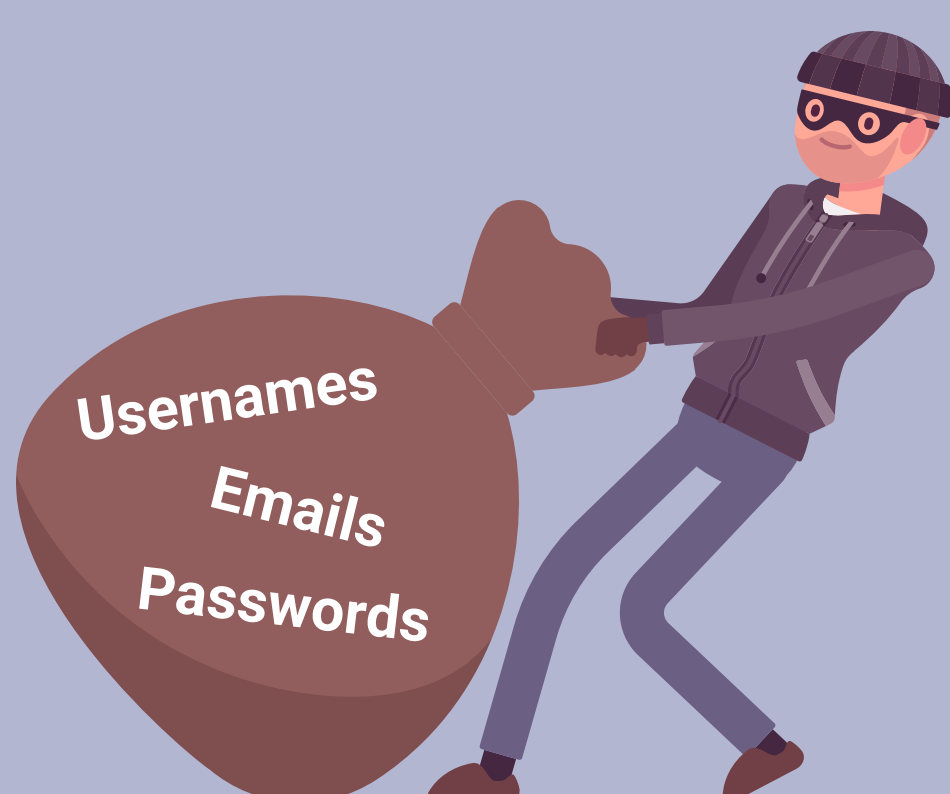
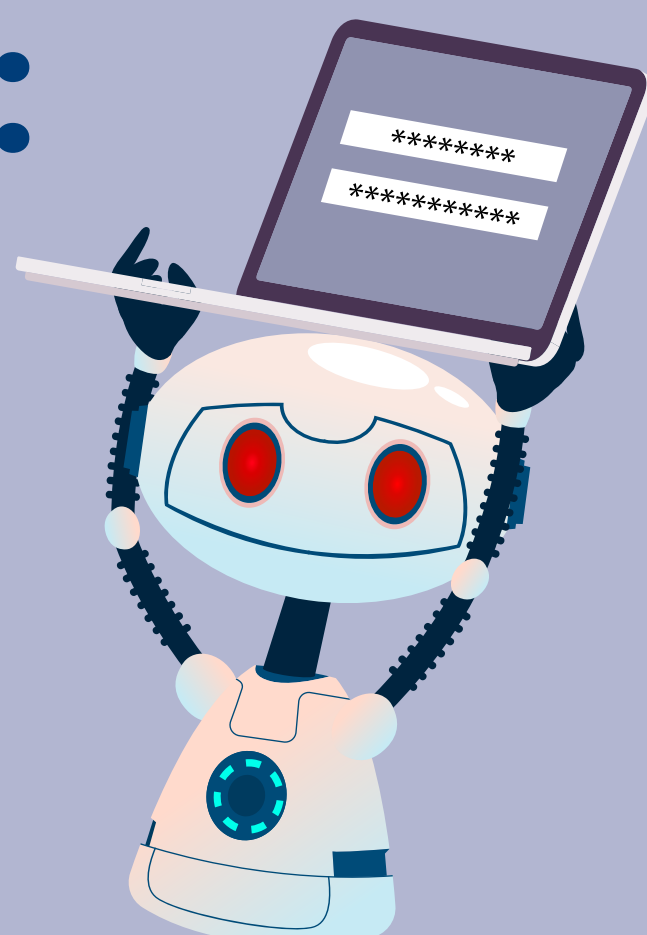


Credential Stuffing: The Silent Siege of Secure Accounts

Credential stuffing is a type of cyber-attack where stolen account credentials, typically consisting of lists of usernames and/or email addresses and the corresponding passwords, are used to gain unauthorized access to user accounts through large-scale automated login requests.

This attack method relies on the fact that many people reuse the same username/password combination across multiple services.

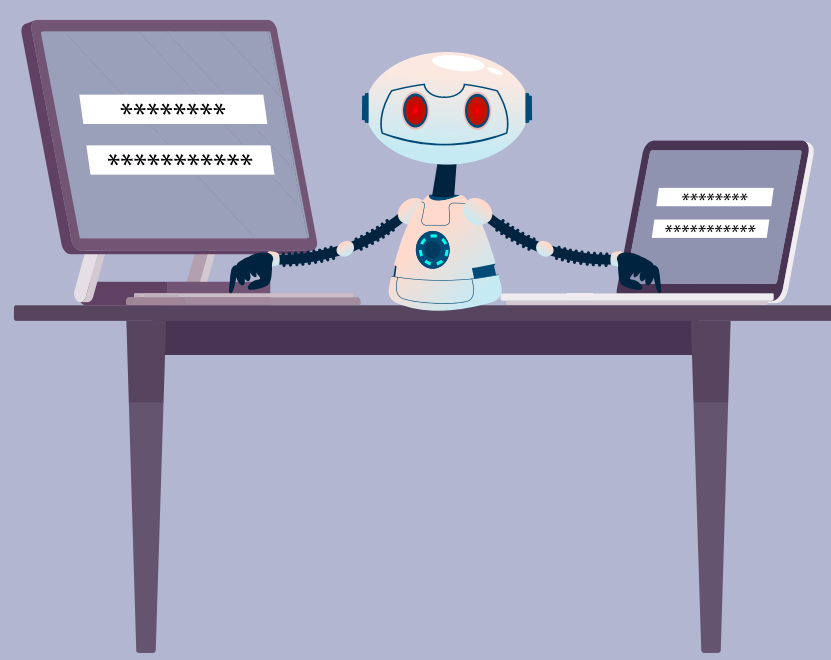


Acquisition of Credentials

Attackers obtain lists of usernames and passwords from one source, which may be a result of a data breach at another company.

Automated Login Attempts

The attackers use automated tools to try these credentials on many different websites (banking, shopping, social media, etc.).



Account Takeover

If any of the login attempts are successful, attackers can gain unauthorized access to accounts, leading to identity theft, financial loss, or data breaches.

BTC Tech Protect®: Safeguarding Against Credential Stuffing

With sophisticated monitoring tools to detect unusual login patterns and robust authentication systems, BTC Tech Protect® ensure that your digital identities and assets are well-protected.

In a world where digital identities are as valuable as physical assets, protecting against credential stuffing is not just an IT concern but a fundamental aspect of digital hygiene.

With the right tools, strategies, and a proactive mindset, you can effectively shield your digital life from the silent siege of credential stuffing.



**Your security is our priority.
Let's protect it together.**

(918) 366-8000

BOOK A MEETING

BTC Tech Protect.
BTCBroadband.com