

SECURITY STARTS AT LOGIN

Modern password habits that actually work



Kayvan Yazdi,
CEO of
TruAdvantage

OUR MISSION

Impacting our clients' success through trusting and meaningful partnerships and delivering strategic, secure, white-glove IT.



THIS MONTH'S TOPICS:

Common Password Mistakes
And How Attackers Take Advantage

How Hackers Crack Passwords
Tool and Tricks Attackers Use

Scam of the Month:
Brute Force Attacks

Benefits of Using Passphrases
Versus Traditional Passwords

Passwords play a critical role in protecting accounts, systems, and sensitive information—but they're also one of the most common points of failure. This month's newsletter explores the biggest password mistakes people make, how hackers are able to crack weak credentials, and why traditional passwords are no longer enough on their own.

You'll also learn how passphrases create stronger, more secure logins and take a closer look at brute force attacks, one of the most common methods cybercriminals use to break into accounts. Understanding how these attacks work is the first step toward preventing them.

COMMON PASSWORD MISTAKES

one



Using Short or Simple Passwords

- Automated tools can test thousands—even millions—of common combinations in minutes. Short and predictable passwords are often cracked almost instantly.

two



Reusing Passwords Across Accounts

- If one account is exposed in a data breach, attackers try the same credentials on other platforms. This tactic, known as credential stuffing, works when people reuse passwords.

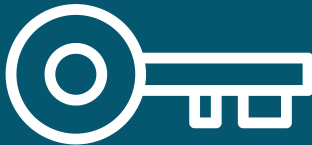
three



Relying on Predictable Patterns

- Attack tools are programmed to try common variations automatically. What feels “unique” to a user is often already built into an attacker’s guessing list.

four



Never Updating Old Passwords

- Older passwords are more likely to appear in breach databases. The longer a password is used, the greater the chance it has already been exposed.

five



Sharing Passwords

- Shared credentials can be intercepted, forwarded, or misused—intentionally or accidentally—creating unnecessary risk.



HOW HACKERS CRACK PASSWORDS

Brute Force Attacks

This is when automated tools try every possible password combination until one works. If passwords are short or simple and there are no login limits, attackers can keep guessing until they succeed.

Dictionary Attacks

This is when attackers use pre-built lists of common passwords, words, and phrases. Many people use familiar words, keyboard patterns, or predictable combinations like Welcome123 or CompanyName1.

Credential Stuffing

This is when stolen usernames and passwords from past data breaches are tested on other websites and systems. Password reuse is extremely common. If one account is compromised, others may fall quickly.

Password Spraying

Instead of trying many passwords on one account, this is when attackers try one common password (like Spring2025!) across many accounts. It avoids triggering account lockouts while targeting users who rely on simple, seasonal passwords.

Social Engineering Support Teams

This is when attackers trick help desks or IT staff into resetting a password. It works because people can be manipulated, especially if proper identity verification procedures aren't followed.

The Takeaway

Hackers don't rely on luck—they rely on automation, data from previous breaches, and predictable human behavior. The stronger and more unique your password habits are, the less likely these tools and tricks will succeed.



SCAM OF THE MONTH: BRUTE FORCE ATTACKS

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Late one night, Alex, the IT manager for a small healthcare office, was asleep when an automated program began targeting the company's remote login portal. The system was flooded with thousands of rapid-fire password attempts—common phrases, simple patterns, and reused credentials—tested over and over by a machine that never got tired. With no account lockout in place, the attempts kept coming.

By morning, Alex was staring at security alerts showing that one account had finally been unlocked. The attacker hadn't used a clever trick or insider access—just persistence. A weak password and unlimited guesses were all it took to turn a routine login into a full-blown security incident.



DID YOU SPOT THE RED FLAGS?

- ▶ A high volume of login attempts in a short period of time is a classic sign of a brute force attack.
- ▶ Late-night activity often goes unnoticed longer, giving attackers more time to succeed.

HOW TO PROTECT YOURSELF



Use strong, unique passwords or passphrases. Longer passwords made up of multiple words are much harder for automated tools to guess.



Enable multi-factor authentication (MFA) wherever possible to add an extra layer of verification beyond just your password.



BENEFITS OF USING PASSPHRASES

OVER TRADITIONAL PASSWORDS

For years, people were told to create complex passwords full of symbols, numbers, and random characters. The result? Passwords that are hard to remember—but still surprisingly easy for automated tools to crack. That's where passphrases come in.

A passphrase is a longer string of random words grouped together, such as: BlueRiverCoffeeTrain!

Because length is one of the most important factors in password strength, passphrases provide stronger protection while remaining easier to remember.

A STRONG PASSPHRASE...

- Uses at least 12–16 characters
- Combines unrelated words
- Avoids common phrases/words
- Adds a symbol or capitalization if required by your system



Encourages Unique Credentials

Because passphrases are easier to remember, users are more likely to create different ones for different systems—reducing the risk of credential reuse.



Determine Root Harder to Crack with Dictionary Attacks

When passphrases combine unrelated words in an unpredictable way, they don't match common password lists used in dictionary attacks.



Easier to Remember

A random mix of characters like T9\$kl2!vP is difficult to recall. But a short sentence or string of unrelated words is much easier for users to remember without writing it down.



Increased Security Through Length

Longer credentials dramatically increase the number of possible combinations attackers must try. Even automated tools struggle with properly constructed passphrases.

