



Hackers Can Crack Passwords in Seconds

What You Need to Know to
Protect Your Business



The Swenson Group
People · Passion · Purpose

Hackers Can Crack Passwords in Seconds

What You Need to Know to Protect Your Business

Hackers are using AI technology that can crack passwords in the time it takes for you to make your morning coffee. With the rise of AI-driven tools and advanced computing power, cybercriminals can now process millions of password combinations in mere moments.



Our exclusive suite of Managed Security Services is ready to protect your data and your business.

Time It Takes Using AI to Crack Your Password [2023]

#OF CHARACTERS	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	4 Seconds
7	Instantly	Instantly	22 Seconds	42 Seconds	6 Minutes
8	Instantly	3 Seconds	19 Minutes	48 Minutes	7 Hours
9	Instantly	1 Minute	11 Hours	2 Days	2 Weeks
10	Instantly	1 Hour	4 Weeks	6 Months	5 Years
11	Instantly	23 Hours	4 Years	38 Years	356 years
12	25 Seconds	3 Weeks	289 Years	2K Years	30K Years



The Swenson Group
People · Passion · Purpose

How Hackers are Using AI to Crack Your Passwords

Brute-Force Attacks:

AI algorithms are used to rapidly generate and test millions of password combinations until the correct one is found.

Dictionary Attacks:

Hackers use AI to analyze massive word databases and common password patterns, enabling them to quickly guess commonly used passwords.

Password Pattern Recognition:

AI algorithms can identify patterns in users' password choices, such as sequential numbers or easily guessable variations, making it easier for hackers to crack them.

Adaptive Learning:

AI-powered tools can adapt and learn from previous successful password cracking attempts, improving their efficiency with each attack.

Social Engineering:

Hackers utilize AI to analyze social media profiles, public information, and personal data to create convincing phishing scams and targeted attacks aimed at tricking users into revealing their passwords.

Keyboard Acoustics Analysis:

Advanced AI techniques can analyze the sound patterns produced by keystrokes to infer the characters being typed, thereby bypassing encryption measures.



The Swenson Group
People · Passion · Purpose

Use AI to Stop Hackers in Their Tracks



Adaptive AI-Based Password Defenses:

Implementing AI algorithms that continuously learn and adapt to new hacking techniques can help identify and block AI-powered attacks.



Anomaly Detection:

User behavior patterns are analyzed and used to detect anomalies in login attempts, flag suspicious activity and trigger additional security measures or verification.



Biometric Authentication:

Using AI-powered biometric authentication methods, such as facial recognition or fingerprint scanning, adds an extra layer of security to password protection.



Password Strength Analysis:

AI algorithms can evaluate the strength of passwords used by users and provide feedback or suggestions for better passwords that are harder to crack.



Continuous Monitoring:

AI tools can monitor network traffic, user activities, and system logs in real-time, identifying any suspicious or malicious behavior.



Two-Factor Authentication (2FA):

Implementing 2FA, where users must provide an additional verification factor alongside their passwords, can significantly boost security.

Easy Targets

“

Roughly 40%

of Americans have had their accounts compromised at least once (47% of those who have lost money because of the hack).

“

Almost 70%

of employees have shared a private password with another employee.

“

51%

of people use the same password for their work and personal accounts.

– Source: ThriveMyWay (<https://thrivemyway.com/password-statistics/>)



The Swenson Group
People · Passion · Purpose

Is Your Business at Risk?

Ask yourself these questions:

1. Do we regularly change passwords?
2. How do we monitor login activity?
3. Are we training our team about phishing and social engineering?
4. How do we keep up with advancements in cybersecurity?

If you believe your business could be at risk of a cyberattack, don't hesitate to reach out to a cybersecurity specialist. They'll safeguard your business against potential threats and give you peace of mind knowing your valuable data and digital assets are protected.



Need help? We're ready when you are.

Call us:
(855) 234-2077

Visit us:
TheSwensonGroup.com



The Swenson Group
People · Passion · Purpose

About The Swenson Group

The Swenson Group is an award winning, privately owned Managed Service Provider that provides IT services, document management and office equipment at a low predictable monthly expense.