# Artificial Intelligence is Rewriting the Rules of Password Security: Are You Protected?

Artificial intelligence (AI) is revolutionising the way we live and work, but it’s also enabling cybercriminals to crack passwords faster and smarter than ever before. What used to take hours or days, can now happen in minutes as AI analyses vast amounts of data. Supercharging traditional phishing scams and password-attacks, making them significantly more effective. By identifying patterns in real-world data, AI allows cybercriminals to predict password combinations with alarming accuracy.

**Why Simple Passwords Are No Longer Enough**

Passwords like "Password123" or "Welcome2023" are easy targets for AI. Even complex passwords that combine letters and numbers can be cracked if they follow predictable patterns. AI tools analyse common sequences and generate accurate guesses, enabling cybercriminals to break into accounts more efficiently than ever.

**What You Can Do to Stay Safe**

1. **Use Long, Random Passphrases**: Instead of a short password, use a long passphrase that combines unrelated words. For example, "BlueDogRunsQuickly" is both easy to remember and much harder for AI to crack. A passphrase can be stronger because it’s less likely to follow predictable patterns, making it difficult for AI to guess.
2. **Avoid Predictable Patterns**: Avoid using common words, dates, or predictable number sequences like “123” or “qwerty.” AI is good at identifying patterns in these combinations. Choose passwords that are random and unique for each account.
3. **Create Unique Passwords: Use a Password Manager**: A password manager can help you generate and store strong, unique passwords for all your accounts. This eliminates the need to remember them all and ensures that you’re not reusing weak or compromised passwords across multiple platforms.
4. **Enable Multi-Factor Authentication (MFA)**: Even if an AI-powered tool cracks your password, MFA provides a second line of defence by requiring additional verification (like a code sent to your phone) before granting access to your account. It’s one of the most effective ways to protect your data.
5. **Monitor for Breaches**
Use services such as *haveibeenpwned.com* to see if your passwords or personal information have been compromised in a breach. This allows you to quickly change any exposed passwords before cybercriminals can exploit them.

**The Importance of Staying Ahead**

AI is making it easier for cybercriminals to launch attacks and guess passwords at lightning speed. The best way to stay secure is to take proactive steps now—long passphrases, password managers, and MFA are key defences in this evolving digital landscape.

**Want to learn more about how AI is impacting cybersecurity?** Follow detective Webb Stirling’s chase of The Whisper in our exclusive audio narrative!