H E A D Q U A R T E R S
CYBER COMMAND, ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN 2026-05

Weak Passwords Remain a Major Cybersecurity Risk

Overview

Cybersecurity researchers reported that approximately 60% of MD5 password hashes can now be cracked in less than one hour, while nearly half can be cracked in under one minute using a single high-performance graphics card.

Modern attackers no longer require advanced infrastructure to conduct password-cracking operations. Cloud-based computing services allow threat actors to rent powerful hardware at low cost, making password attacks faster, cheaper, and more accessible.

The continued use of weak passwords and outdated password protection methods significantly increases the risk of account compromise following data breaches or credential leaks.

Why This Threat is Dangerous

Passwords remain one of the primary defenses protecting:

- Official accounts
- Financial systems
- Emails and communication platforms
- Operational information

- Personal and organizational data

When passwords are weak, reused, or predictable, attackers can quickly gain access to accounts and move further into systems or networks.

Compromised accounts may lead to:

- Unauthorized access to sensitive information
- Identity theft and impersonation
- Financial fraud
- Data breaches
- Lateral movement across systems
- Operational disruption

Even complex passwords may become vulnerable if not combined with additional security measures such as Multi-Factor Authentication (MFA).

Common Weak Password Practices

Personnel are reminded to avoid the following:

- Reusing the same password across multiple accounts
- Using common words, names, birthdays, or predictable patterns
- Creating short or simple passwords
- Sharing passwords with others
- Storing passwords in unsecured locations
- Using outdated password-only security methods

Attackers commonly exploit predictable behaviors and frequently used password patterns to accelerate password-cracking attempts.

Recommendations

In this regard, all AFP personnel are strongly advised to adopt the following cybersecurity practices:

- **Use Strong and Unique Passwords**

  Create passwords that are:

  - Long and difficult to guess
  - Unique for every account
  - Free from personal information or predictable words

- **Enable Multi-Factor Authentication (MFA)**

MFA adds an additional layer of security beyond passwords and significantly reduces the risk of unauthorized access.

- **Use Password Managers**

Authorized password managers help generate and securely store strong passwords.

- **Avoid Password Reuse**

A compromised password from one account can be used to access other accounts if reused.

- **Keep Systems Updated**

Maintain updated systems, browsers, and applications to reduce exposure to credential-related attacks.

- **Be Alert for Phishing Attempts**

Attackers often steal passwords through fake emails, websites, and login pages.

Conclusion

Cybersecurity is everyone's responsibility. Every user account represents a potential entry point into the organization. Weak passwords continue to be one of the most exploited vulnerabilities in cyberspace. As cybercriminal capabilities improve, outdated password practices place both individuals and organizations at increased risk.

One compromised password can become the gateway to a larger security breach.

Protect your accounts. Strengthen your security. Stay vigilant.

Source: https://www.theregister.com/security/2026/05/07/60-of-md5-password-hashes-are-crackable-in-under-an-hour/5234954