Your password is probably NOT strong enough

Volume 23, Issue 7
July 2023

Microsoft is currently taking significant steps to enhance your security measures and help you protect your personal and organizational information. By updating and enforcing stricter password policies for Windows and Office users, Microsoft aims to fortify account protection and strengthen the resilience of its software ecosystem.

The two most significant changes and recommendations are the increasing of password length and complexity and the use of Multi-Factor Authentication.

Password Length and complexity:

Microsoft recommends a minimum password length of 12 characters or more. Longer passwords provide increased complexity and make it more challenging for attackers, including AI-driven algorithms, to crack them through brute-force methods. Microsoft is also encouraging users to create stronger passwords by incorporating a mix of uppercase and lowercase letters, numbers, and special characters. It is important to note that shorter passwords, especially those below 12 characters, can be vulnerable to AI-driven attacks that leverage computing power and advanced algorithms. Adhering to the recommended password length is **crucial** in mitigating the risk of password breaches.

USING CHATGPT HARDWARE TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 secs
9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months
13	Instantly	1 hours	12 months	10 years	47 years
14	Instantly	1 days	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

Multi-Factor Authentication:

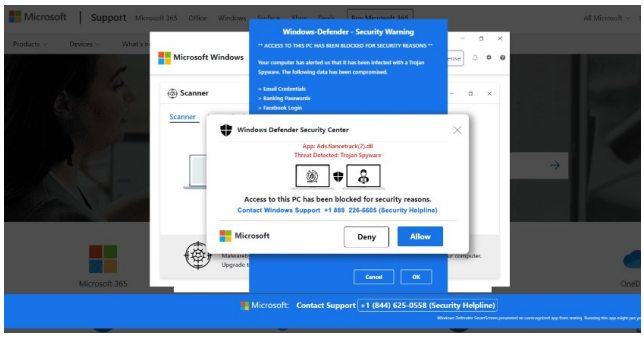
Multi-Factor Authentication (MFA) is vital in today's digital landscape due to the increasing sophistication of cyber threats. By requiring users to verify their identities through multiple means, such as biometric data or unique codes sent to their mobile devices, MFA adds an additional layer of security beyond just passwords. This extra step significantly reduces the risk of unauthorized access, even if passwords are compromised. MFA makes it exponentially more difficult for attackers to gain access to user accounts, as it requires possession or knowledge of multiple authentication factors.

If you are serious about the security of your data, both password length and complexity and Multi-Factor (MFA) are absolutely vital. Without them, you should consider your data and personal information very vulnerable and open to compromise at any time.

If you have any questions about how you can improve your security, **PLEASE**, reach out to us **BEFORE** something happens.

DON'T CALL THE NUMBER!!

In the digital era, encountering online threats is an unfortunate reality. One deceptive tactic used by cybercriminals is the notorious Microsoft virus warning popups. These popups claim your computer is infected and prompt you to call a specific number for immediate assistance. However, it's crucial to understand the risks associated with calling such numbers. Let's explore why you should **NEVER** call these numbers.



1. Phishing and Social Engineering: Microsoft virus warning popups are often used for phishing, a fraudulent attempt to obtain sensitive information. These popups create urgency, exploiting your fear of malware or system compromise. Calling the provided number may lead to divulging personal or financial details, exposing you to identity theft and other malicious activities.

2. Rely on Legitimate Support Channels: Reputable companies like Microsoft do not display warning messages with hotline numbers on random websites or popups. If you have genuine concerns about your computer's security, visit the official Microsoft website or contact their verified support channels for assistance. Seeking help from qualified professionals reduces the risks associated with scams.

Remaining vigilant and skeptical of unsolicited warnings and popups is essential in today's cyber-threat landscape. Microsoft virus warning popups, with their deceptive tactics and phone numbers, pose **significant** risks to your privacy, data, and financial well-being. Understanding these risks and practicing safe browsing habits helps protect you from falling victim to tech support scams and phishing attempts. Stay cautious and prioritize your digital security.

If you receive one of these popups and are unsure what steps to take **CALL US!!** We are always here to help.

Building Relationships in West Michigan since 1976!

Aeros

A DIFFERENT WAY TO I.T.

Aeros IT Group

6261 Lake Michigan Drive
Allendale, MI 49401

Phone: 616-997-8324
Email: support@aerosgroup.com

FIND US ON THE WEB!
AEROSGROUP.COM