June 2025

Cirrus IT Services

TECH TALK

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing technology!

- **Scott Magee**
Managing Director

WHAT IS PASSWORD SPRAYING?

Password spraying is a complex type of cyberattack that uses weak passwords to get into multiple user accounts without permission. Using the same password or a list of passwords that are often used on multiple accounts is what this method is all about. The goal is to get around common security measures like account lockouts.

Attacks that use a lot of passwords are very successful because they target the weakest link in cybersecurity: people and how they manage their passwords.

What Is Password Spraying and How Does It Work?

A brute-force attack called "password spraying" tries to get into multiple accounts with the same password. Attackers can avoid account shutdown policies with this method.

Attackers often get lists of usernames from public directories or data leaks that have already happened. They then use the same passwords to try to log in to all of these accounts. Usually, the process is automated so that it can quickly try all possible pairs of username and password.

Password spraying has become popular among hackers, even those working for the government, in recent years. Because it is so easy to do and works so well to get around security measures, it is a major threat to both personal and business data security. As cybersecurity improves, it will become more important to understand and stop password spraying threats.

How Does Password Spraying Differ from Other Cyberattacks?

Password spraying is distinct from other brute-force attacks in its approach and execution. While traditional brute-force attacks focus on trying multiple passwords against a single account, password spraying uses a single password across multiple accounts.

Understanding Brute-Force Attacks

Brute-force attacks involve systematically trying all possible combinations of passwords to gain access to an account. These attacks are often resource- intensive and can be easily detected due to the high volume of login attempts on a single account.

Comparing Credential Stuffing

Credential stuffing involves using lists of stolen username and password combinations to attempt logins.

How Can Organizations Detect and Prevent Password Spraying Attacks?

Detecting password spraying attacks requires a proactive approach to monitoring and analysis. Organizations must implement robust security measures to identify suspicious activities early on.

•Implementing Strong Password Policies:
Organizations should adopt guidelines that ensure passwords are complex, lengthy, and regularly updated.

•Deploying Multi-Factor Authentication.
Multi-factor authentication (MFA) significantly reduces the risk of unauthorized access by requiring additional verification steps beyond just a password.

• Conducting Regular Security Audits.
Regular audits of authentication logs and security posture assessments can help identify vulnerabilities that could facilitate password spraying attacks.

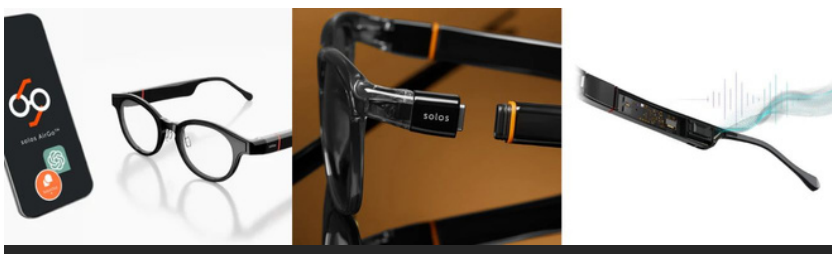
• Enhancing Login Detection.
Organizations should set up detection systems for login attempts to multiple accounts from a single host over a short period. Implementing stronger lockout policies that balance security with usability is also crucial.

• Educating Users.
Users should be informed about the risks of weak passwords and the importance of MFA.

• Incident Response Planning.
This plan should include procedures for alerting users, changing passwords, and conducting thorough security audits.

Taking Action Against Password Spraying

To enhance your organization's cybersecurity and protect against password spraying attacks, contact us today to learn how we can assist you in securing your systems against evolving cyber threats.



SOLOS AIRGO VISION

Elevate your eyewear experience with AirGo Vision Smartglasses, first with ChatGPT-enabled AI and a camera.

These glasses offer real-time visual recognition and hands-free operation.

AirGo Vision prioritizes user control, convenience, and personalization with its SmartHinge technology and USB-C connectors, allowing easy switching between camera-enabled and standard frames for flexibility and peace of mind.

COMPLETE GUIDE TO STRONG PASSWORDS AND AUTHENTICATION

Cyber risks are smarter than ever in today's digital world. People and companies can lose money, have their data stolen, or have their identities stolen if they use weak passwords or old authentication methods.
A strong password is the first thing that will protect you from hackers, but it's not the only thing that will do the job.

Why Are Strong Passwords Essential?

Your password is like a digital key that lets you into your personal and work accounts. Hackers use methods like brute-force attacks, phishing, and credential stuffing to get into accounts with weak passwords. If someone gets your password, they might be able to get in without your permission, steal your info, or even commit fraud.

Most people make the mistake of using passwords that are easy to figure out, like "123456" or "password." Most of the time, these are the first options hackers try. Reusing passwords is another risk. If you use the same password for more than one account, one breach can let hackers into all of them.

Today's security standards say that passwords should have a mix of numbers, capital and small letters, and special characters. But complexity isn't enough on its own. Length is also important— experts say at least 12 characters is best. Password tools can help you make unique, complicated passwords and safely store them.

How Does Multi-Factor Authentication Enhance Security?

Multi-factor authentication (MFA) requires users to provide two or more verification methods before accessing an account. This significantly reduces the risk of unauthorized access, even if a password is compromised.

Types of Authentication Factors

- Something You Know – Passwords, PINs, or security questions.
- Something You Have – A smartphone, hardware token, or security key.
- Something You Are – Biometric verification like fingerprints or facial recognition.

Common MFA Methods

- SMS-Based Codes – A one- time code sent via text. While convenient, SIM-swapping attacks make this method less secure.
- Authenticator Apps – Apps like Google Authenticator generate time-sensitive codes without relying on SMS.
- Hardware Tokens – Physical devices like YubiKey provide phishing-resistant authentication.

Despite its effectiveness, MFA adoption remains low due to perceived inconvenience. However, the trade-off between security and usability is minimal compared to the risks of account takeover.

Ready to Strengthen Your Digital Security?

Cybersecurity is an ongoing effort, and staying informed is your best defense. Strong passwords and multi-factor authentication are just the beginning. Whether you're an individual or a business, adopting these practices can prevent costly breaches.

ULTIMATE GUIDE TO SAFE CLOUD STORAGE

Since we live in a digital world, cloud storage is an important tool for both personal and business use. So long as they have an internet connection, users can store and get to their info from anywhere at any time. But while cloud storage is convenient, there is a chance that your data could be stolen or accessed by people who aren't supposed to.

To avoid losing money and keeping private data safe, it's important to make sure that your cloud data is safe.

What Is Cloud Storage and How Does It Work?

Cloud storage lets you put your data online and have a cloud storage service provider keep, manage, and back it up for you. Users can view their files from any internet-connected device with this service, which makes it very easy to work together and keep track of data.
Based on how much room is needed, cloud storage companies usually offer different plans, ranging from free to paid.

Key Features to Look for in a Secure Provider

- Encryption: Look for providers that use end-to-end encryption, which ensures that your data is encrypted both in transit and at rest.
- Data Backup: Ensure that the provider offers regular backups of your data to prevent loss in case of technical issues or cyberattacks.
- Access Controls: Opt for providers that offer strong access controls, such as two-factor authentication (2FA) and granular permissions, to limit who can access your files.
- Compliance: Check if the provider complies with major data protection regulations like GDPR or HIPAA, depending on your specific needs.
- Customer Support: Good customer support is essential in case you encounter any issues or have questions about security features.

Most importantly, read reviews and ask about their security practices directly to give you a clearer understanding of their commitment to data security.

BEST PRACTICES FOR DATA MANAGEMENT

1.Transparency and Consent
Websites should clearly communicate how user data is collected and used. Users should have the option to opt-in or opt-out of data collection, and they should be able to access, modify, or delete their personal information.

2.Data Minimization
Collecting only the data that is necessary for the website's functionality.

3.Secure Data Storage
Encrypting data both at rest and in transit ensures that it remains secure even if intercepted. Regular security audits and updates are also crucial to prevent vulnerabilities.

4.User Control
Providing users with tools to manage their data preferences fosters trust and accountability. This includes options to download, edit, or delete personal information.

7 UNEXPECTED WAYS HACKERS CAN ACCESS YOUR ACCOUNTS

1.Cookie Hijacking
Cookies can be used to access your accounts without your password.

2.SIM Swapping
Hackers deceive your provider to transfer your number to a new SIM card they control.

3.Deepfake Technology
Hackers pose as a trusted colleague or family member through realistic audio/ video.

4.Exploiting Third-Party Apps.
Hackers exploit vulnerabilities to gain access to linked accounts.

5.Port-Out Fraud
Like in SIM swaps, your number is transferred to another provider without your consent.

6.Keylogging Malware
Keyloggers are malicious programs that record your keystrokes.

7.AI-Powered Phishing
AI is used to craft highly convincing emails.

CAN MY DATA BE REMOVED FROM THE DARK WEB?

Removing data from the dark web is extremely challenging due to its decentralized nature and the rapid dissemination of information.

Once data is posted on the dark web, it is quickly copied and distributed among numerous cybercriminals, making it virtually impossible to remove completely.

Proactive Measures for Protection

- Use identity and credit monitoring services to detect any suspicious activity related to your personal information.
- Enable two-factor authentication and use strong, unique passwords for all accounts.
- Regularly monitor your online presence and use privacy tools like dark web scans.
- Use a VPN to mask your IP address and protect your browsing activity from being tracked.

Protect Your Future Today

If you're concerned about your data security, we can provide expert guidance and tools to help safeguard your identity and ensure your peace of mind in the digital world.

TECHNOLOGY TRIVIA TIME

Each month you have a chance to win an Amazon Gift Card! Our May competition winner (randomly selected from correct entries) was:

Karen Wheeler of AO Seafoods!

Congratulations, Karen!

The question this month is:

What was the first text message ever sent?

To enter the competition, please go to this link and enter your answer by 15th June 2025: cirrusits.co.uk/tech-trivia

Last month's answer was
2012