ISSUE 022
May 2025
Independence, Missouri

FCS TECH TALK

Your Trusted Technology Partner Since 1989

INSIDE THIS ISSUE:

WHAT IS PASSWORD SPRAYING – AND WHY YOUR BUSINESS SHOULD CARE

Cyber Security headlines often focus on dramatic events—ransomware attacks, massive data breaches, and high-profile phishing campaigns. But one of the most effective and under-the-radar techniques used by attackers today is password spraying.

It doesn't require sophisticated malware or insider access—just a little patience, automation, and users with weak passwords.

Password spraying is a low-and-slow attack that can quietly compromise organizations of any size, including those who believe they've already implemented adequate cyber security protections.

As your trusted technology partner, we believe in proactive education and defense—and that starts with understanding the threats at your door.

What Exactly Is Password Spraying?

Password spraying is a type of brute-force attack, but with a key difference in strategy.

Traditional Brute-Force:

- Focuses on a single user account
- Tries hundreds or thousands of passwords
- Quickly triggers account lockouts or alerts

Password Spraying:

- Focuses on many user accounts
- Tries just a few common passwords per account
- Avoids detection by staying under lockout thresholds

Example: An attacker has a list of 500 employee email addresses. Instead of trying 500 passwords on one account (which would get it locked quickly), they try just 1–3 very common passwords (like "Summer2024!" or "Password123") once per user, then cycle back hours or days later with a different password.

This method:

- Avoids triggering account lockouts
- Evades traditional intrusion detection systems
- Takes advantage of users with weak or reused passwords

Why Is Password Spraying So Dangerous?

It's Incredibly Low-Cost and Low-Risk

- Tools for launching these attacks are widely available.
- Attackers don't need malware or exploit vulnerabilities—they just guess.
- The attack is distributed and automated.

It Exploits Human Behavior

- Many users still rely on predictable passwords.
- Organizations often have hundreds or thousands of accounts, increasing the chances of a hit.

It Scales Easily

- Attackers can target thousands of organizations with the same technique.
- Once inside one account, they can pivot—escalating privileges or harvesting data.

It Preys on Remote Access Tools

- In today's hybrid work environments, portals like Microsoft 365, Outlook Web Access (OWA), Google Workspace, and VPNs are exposed to the internet.
- These are high-value targets for password spraying attacks.

Anatomy of a Password Spraying Attack

Step 1: Reconnaissance

Attackers gather usernames and email addresses using:

- Public company websites
- LinkedIn profiles
- Previous breach dumps
- Email scraping tools

Step 2: Building a Password List

Rather than using millions of passwords, attackers choose a curated list of the most commonly used ones, such as:

- Password1!
- Spring2024
- Welcome123
- CompanyName2024
- Qwerty!@#

These are tested across many accounts to see if any users have opted for convenience over security.

Step 3: Spraying

The attack is executed slowly:

- A few passwords are tested across many accounts.
- Hours or days pass before the next round of attempts.
- This evasion tactic avoids detection and lockout mechanisms.

Step 4: Post-Compromise Actions

Once an account is accessed:

- Internal phishing campaigns may be launched.
- Sensitive files and emails are downloaded.
- Credentials stored in mailboxes or notes are harvested.
- If the account has high-level permissions, attackers can escalate quickly.

Real-World Examples

- 2021: U.S. Government Agencies
  - A well-known APT (Advanced Persistent Threat) group used password spraying to compromise Office 365 accounts of multiple U.S. federal agencies.
  - No malware was involved—just patient, strategic guessing.
- 2022: Healthcare Sector
  - An attacker used password spraying to compromise a healthcare provider's VPN portal.
  - Once inside, they accessed patient data and disrupted hospital operations.
- 2023: Microsoft 365 Attacks Rise
  - Microsoft reported a surge in password spray campaigns targeting Exchange Online and Azure AD.
  - MFA bypass was the goal after initial access.

How to Protect Your Business

Here's where prevention makes a world of difference. These strategies should be non-negotiable in today's threat landscape.

✅ *1. Enforce Strong Password Hygiene*

- Require longer, complex passwords (ideally at least 12 characters).
- Ban the use of known weak or leaked passwords (available from breach databases).
- Use password managers to generate and store strong, unique passwords.

✅ *2. Deploy Multi-Factor Authentication (MFA) Everywhere*

- MFA drastically reduces the effectiveness of password spraying.
- Require MFA not just for VPN or cloud services, but for any externally accessible system.

✅ *3. Implement Account Lockout or Throttling Policies*

- Avoid harsh lockouts (which can be abused for denial-of-service), but:
  - Use progressive delays on failed attempts.
  - Lock accounts based on geolocation anomalies or unusual behavior.

✅ *4. Monitor Authentication Activity*

- FCS can regularly review audit logs for:
  - Failed login attempts
  - Unusual access times
  - Unexpected IP addresses or user agents

✅ *5. Educate Employees*

- Enroll in FCS Security Awareness Training.
- This can teach users to recognize phishing attempts (common after a sprayed password works).
- Encourage reporting of suspicious login alerts and MFA notifications.

✅ *6. Subscribe to FCS Managed Cyber Security*

As your trusted IT provider, we can:

- Monitor login activity and authentication patterns
- Remediate and lock accounts with suspicious activity
- Deploy security agents on all devices to protect from Cyber Attacks
- Stay ahead of emerging threats and adapt your defenses

TL;DR

Password spraying is a stealthy Cyber Attack where hackers try a few common passwords (like "Password123" or "Spring2024") across many accounts to avoid detection and lockouts. It exploits weak user passwords and is often used to breach Microsoft 365, VPNs, and other remote access systems. Once inside, attackers can steal data, spread malware, or launch phishing campaigns. Why it matters: It's cheap, effective, and increasingly common—even in well-defended environments. How to protect your business: Enforce strong, unique passwords. Require multi-factor authentication (MFA). FCS can monitor login activity for suspicious patterns. Enrolling in FCS Security Awareness Training can educate users on what phishing emails may look like to be able to spot and report malicious emails that can occur from sprayed passwords. Don't wait until it happens—prevent it now.

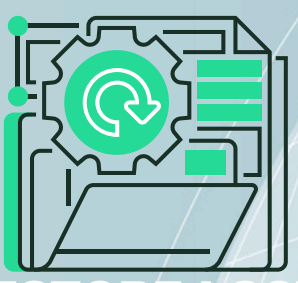
ISSUE 022
May 2025
Independence, Missouri

THIS MONTH'S PRODUCT SPOTLIGHT

CLICK TO VIEW A SHORT VIDEO!

MANAGED BACKUP SERVICES

BACKUPS DONE DAILY



RESTORE LOST/ CORRUPT FILES

GEO-REDUNDANT

FULLY ENCRYPTED

SAD NEWS FROM MICROSOFT FOR NON-PROFITS

The Microsoft 365 Business Premium grant, which provided up to 10 free licenses to eligible Non-Profits, will be retired. This means that upon renewal after July 1, 2025, organizations who were using this program will no longer receive these licenses for free.

Instead, they will need to purchase licenses at discounted nonprofit pricing.

What's Still Available?

While the Business Premium grant is ending, Microsoft will continue to support nonprofits through:

Microsoft 365 Business Basic: Up to 300 free licenses, offering web and mobile versions of Office apps, Teams, SharePoint, and OneDrive.

Discounted Pricing: Nonprofits can purchase Microsoft 365 Business Premium licenses at a discounted rate, typically around $5.50–$6.00 per user per month.

Timeline and Transition

Before July 1, 2025: Organizations can continue using their existing Business Premium grants.

On or After July 1, 2025: At the next renewal date, the free Business Premium licenses will expire, and organizations will need to transition to paid licenses or alternative plans.

Grace Period: Microsoft will provide reminders 30, 60, and 90 days before any changes take effect. Data will remain accessible for 90 days after license expiration if organizations choose not to move to paid licenses.

Action Steps for Nonprofits

Review Renewal Dates: Determine when your organization's Microsoft 365 Business Premium licenses are set to renew.

Evaluate Needs: FCS can help assess whether Microsoft 365 Business Basic meets your organization's requirements or if the features of Business Premium are necessary.

Budget Accordingly: Plan for the potential costs associated with transitioning to paid licenses.

Seek Assistance: We are here to help! FCS can help guide you through this transition and answer any questions you might have.

WHAT HAPPENS IF YOUR DATA IS ON THE DARK WEB

What Is the Dark Web?

The dark web is a hidden part of the internet that isn't indexed by standard search engines and requires special software, such as Tor, to access. While not inherently illegal, its anonymity makes it a breeding ground for illicit activities, including drug trafficking, illegal weapons sales, and the trading of stolen personal data.

How Does Data End Up on the Dark Web?

Your information might land on the dark web through:

- Data breaches: Hackers infiltrate companies and extract massive amounts of data—email addresses, passwords, credit card numbers, social security numbers, and more.
- Phishing attacks: You unknowingly provide data to malicious actors through fake websites or emails.
- Malware infections: Keyloggers and other malware silently harvest your information and send it to cybercriminals.

Once harvested, this data is often packaged and sold in bulk on underground forums or marketplaces.

What Happens If Your Data Is Found on the Dark Web?

If your data is circulating on the dark web, several consequences can follow:

- Identity theft: Criminals may use your personal information to open accounts, apply for credit, or impersonate you online.
- Account takeovers: Compromised login credentials can lead to unauthorized access to your email, banking, or social media accounts.
- Financial fraud: Credit card numbers and banking information may be used or sold, leading to unauthorized charges or drained accounts.
- Targeted scams: Knowing your full name, address, or employer, scammers may craft more convincing phishing attacks.

What You Can Do

While you may not be able to remove your data from the dark web, you can take steps to protect yourself:

1. Change passwords immediately. If any login credentials are compromised, change those passwords—preferably using a strong, unique password for each account. Use a password manager to keep track.
2. Enable multi-factor authentication (MFA) MFA provides an extra layer of security that can prevent unauthorized access even if your password is stolen.
3. Use dark web monitoring services. FCS offers Dark Web scanning for you and your company's data. Once any data is found you will be immediately alerted on what was found.
4. Report identity theft If you suspect you've been a victim of identity theft, report it to the relevant authorities such as the Federal Trade Commission (FTC) at IdentityTheft.gov.
5. Monitor your accounts Keep an eye on bank and credit card statements. Sign up for fraud alerts and consider credit monitoring services.

HEADED OUT THIS SUMMER? 7 CYBER SECURITY TRAVEL TIPS EVERY EMPLOYEE SHOULD KNOW

Summer is a time for travel—whether it's a cross-country vacation, a weekend at the lake, or a business trip to meet clients. But while you're focused on flights and fun, cybercriminals are focused on opportunity.

Travel increases cybersecurity risks. You're more likely to connect to public Wi-Fi, use personal devices, or let your guard down while away from the usual office routine.

To help you stay safe on the go, here are 7 practical tips to protect your data and devices while traveling—whether you're checking emails from a beach chair or logging into systems from a hotel lobby.

1. Avoid Public Wi-Fi (or Use a VPN If You Must)

Public Wi-Fi in airports, hotels, and cafes is a hacker's playground. Without encryption, anyone on the same network could intercept your data.

✅ *Do this instead:*

- Use your phone's hotspot for a secure connection.
- If you must use public Wi-Fi, connect through a VPN (Virtual Private Network), which encrypts your data and keeps it private.

2. Update Devices Before You Leave

Outdated software can be full of security holes that hackers exploit.

✅ *Before traveling:*

- Update your laptop, phone, and any apps you'll use.
- Make sure your antivirus software is current and running.

3. Use Strong, Unique Passwords and MFA

If you're using the same password across accounts, one breach could give hackers access to everything.

✅ *Secure your accounts:*

- Use a password manager to generate and store strong, unique passwords.
- Turn on Multi-Factor Authentication (MFA) wherever possible—it's a powerful extra layer of protection.

4. Turn Off Bluetooth and Auto-Connect Features

Leaving Bluetooth or auto-connect enabled makes it easier for malicious devices to connect to yours.

✅ *Be cautious:*

- Turn off Bluetooth when you're not using it.
- Disable "auto-connect" to unknown Wi-Fi networks on your devices.

5. Be Smart About What You Share Online

Posting real-time vacation updates might seem harmless—but it can signal to attackers that you're away and potentially off-guard.

✅ *Stay private:*

- Wait until you're back to post photos.
- Keep travel plans off public social media if possible.

6. Keep Devices Physically Secure

A stolen laptop or phone can lead to a massive data breach if it's not properly secured.

✅ *While traveling:*

- Don't leave devices unattended.
- Use password protection and full-disk encryption.
- Consider privacy screens for working in public spaces.

7. Know What to Do If Something Goes Wrong

Even with precautions, things happen. Knowing what to do can limit the damage.

✅ *Before you go:*

- Let us know you will be traveling, we can help prepare for your travel and monitor accounts.
- Report lost devices, suspicious activity, or account access issues immediately.

Bonus: Traveling with a Work Device? Treat It Like a Company Asset

If you're bringing your work laptop or accessing business tools while away, remember: it's not just personal security at stake—it's company data too. Following these tips helps protect both.

Enjoy the Trip, but Stay Cyber Smart

Summer travel should be relaxing—but don't let a security mishap turn your trip into a tech nightmare. By taking a few simple precautions, you can stay safe, productive, and protected while on the road.

As your IT partner, we're always here to support you—whether you're in the office, working remotely, or checking in from the beach. If you have questions or want help setting up secure remote access before you go, just reach out.

ISSUE 022
May 2025
Independence, Missouri

COMPLETE GUIDE TO STRONG PASSWORDS AND AUTHENTICATION

Cyber risks are greater 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, use your account to purchase items without your knowledge 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?

Cyber Security 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.

There is no time like the present, start using a strong mix of passwords and enable MFA on all accounts today, your future self will thank you!

WE LOVE REFERRALS

The greatest gift anyone can give us is a referral to another business in need of IT services. Referrals help us keep costs down so we can pass the savings to our clients.

If your referral ends up becoming a client - we'll gift them their first month of service at no charge AND we'll gift you a $500 Amazon Gift Voucher.

Simply introduce me via email to stan@fcskc.com and I'll take it from there. I personally promise we'll look after your referral's business with a high level of care and attention (just like we do with all our clients).
-Stan

We Want Your Feedback

Here at Ferguson Computer Services, we value your feedback greatly and would appreciate if you took time from your busy schedule to leave us a review. These reviews let us know what we are doing well and what we might be able to improve on in the future.

Leave a Google Review Leave a Facebook Review

TECHNOLOGY TRIVIA TIME

Technology Trivia Question of the Month! Send the correct answer to winner@fcskc.com to be entered to win a $50 gift card to Amazon.

Here is May's question of the month:

Does Password Spraying focus on a single user account?