ISSUE 019
February 2025
Independence, Missouri

FCS

FCS TECH TALK

Your Trusted Technology Partner Since 1989

INSIDE THIS ISSUE:

UNDERSTANDING THE DIFFERENT TYPES OF TWO-FACTOR AUTHENTICATION (2FA)

In today's digital age, security is a top priority for individuals and organizations alike. One of the most effective ways to enhance account security is through Two-Factor Authentication (2FA).

2FA adds an extra layer of protection beyond just a username and password, making it significantly harder for unauthorized users to gain access to an account. However, not all 2FA methods are the same, and understanding their differences is crucial for selecting the best security approach.

In this article, we will explore the different types of 2FA, their advantages, their vulnerabilities, and best practices for implementation.

1. SMS-Based Authentication

How It Works:
SMS-based 2FA sends a one-time password (OTP) or verification code to a user's registered mobile phone via text message. The user must enter this code along with their password to log in.
Pros:

- Easy to set up and use, requiring no additional apps or devices.
- Works on virtually any mobile phone, making it widely accessible.

Cons:

- Vulnerable to SIM swapping attacks: Hackers can trick mobile carriers into transferring a victim's phone number to a different SIM card.
- Prone to phishing and interception: Attackers can use social engineering techniques to steal OTPs.
- Dependent on cellular network availability: If a user is in an area with poor reception, they may not receive the authentication code in time.

Best Practices:

- Avoid using SMS-based 2FA for highly sensitive accounts (e.g., banking, corporate logins).
- Enable additional security features like PIN protection for mobile carrier accounts to prevent SIM swap attacks.

2. Email-Based Authentication

How It Works:
Similar to SMS authentication, an OTP or login link is sent to a user's registered email address. The user must retrieve and enter the code to complete authentication.
Pros:

- Simple and widely accessible, as email is universally used.
- Can be accessed from multiple devices.

Cons:

- Email accounts themselves can be hacked: If a hacker gains access to a user's email, they can reset passwords and compromise security.
- Susceptible to phishing attacks: Fraudulent emails trick users into revealing login credentials.
- Slower than other methods: Email delivery may be delayed due to server issues or spam filters.

Best Practices:

- Use a secure, unique password for your email account and enable 2FA on the email service itself.
- Be cautious of phishing emails that attempt to steal login credentials.

3. Authenticator Apps (TOTP)

How It Works:
Apps like Google Authenticator, Microsoft Authenticator, and Authy generate Time-Based One-Time Passwords (TOTP). These apps continuously generate codes that change every 30 seconds, which must be entered along with the primary password.
Pros:

- More secure than SMS and email-based methods since codes are generated locally on the device.
- Works offline once initially set up.
- Resistant to phishing and SIM swap attacks since codes are not transmitted over a network.

Cons:

- Requires an initial setup: Users must scan a QR code or manually enter a key to link the app to an account.
- If the device is lost or reset, access may be difficult: Users must have backup codes or another recovery method in place.

Best Practices:

- Store backup codes in a secure location.
- Use an authenticator app that allows multiple device backups, such as Authy.

4. Hardware Security Keys

How It Works:
Hardware security keys, such as YubiKey and Google Titan, use the Universal 2nd Factor (U2F) standard. The user must physically insert the key into a USB port or tap it on an NFC-enabled device to authenticate.
Pros:

- Extremely secure and resistant to phishing: Attackers cannot replicate or intercept physical security keys.
- No reliance on network connectivity: Works without internet or cellular service.
- Works across multiple platforms: Compatible with various services and browsers.

Cons:

- Requires purchasing a physical device: Some users may find the cost prohibitive.
- Can be lost, leading to potential access issues: Users should have backup authentication methods in place.

Best Practices:

- Register multiple security keys in case one is lost.
- Store a spare key in a secure location.

5. Biometric Authentication

How It Works:
Biometric authentication uses biological traits like fingerprints, facial recognition, or retina scans to verify identity. This is commonly seen in mobile devices and high-security environments.
Pros:

- Fast and convenient: Eliminates the need to enter codes manually.
- Difficult to fake or steal: Biometric data is unique to each individual.

Cons:

- Some biometric systems can be bypassed: Advanced spoofing techniques can sometimes trick facial recognition.
- Requires compatible hardware: Not all devices support biometric authentication.
- Privacy concerns: Biometric data must be stored securely to prevent misuse.

Best Practices:

- Use devices that encrypt biometric data locally rather than storing it on a server.

6. Push Notification Authentication

How It Works:
Push notifications are sent to an authentication app, such as Duo Mobile or Microsoft Authenticator, where the user approves or denies the login attempt.
Pros:

- More secure than SMS or email authentication since no codes are transmitted.
- No need to enter codes manually, reducing user errors.

Cons:

- Requires an internet connection to receive notifications.
- If notifications are ignored, access may be delayed.

Best Practices:

- Ensure notifications are enabled for the authentication app.
- Regularly review and approve only legitimate login requests.

7. Smart Cards and USB Tokens

How It Works:
A physical smart card or USB token must be inserted into a reader to authenticate access.
Pros:

- Highly secure: Used in corporate and government environments.
- Difficult to clone or steal remotely.

Cons:

- Requires specialized hardware.
- Can be lost or damaged.

Best Practices:

- Have backup authentication methods in place.
- Store the smart card securely when not in use.

Choosing the Right 2FA Method

The best 2FA method depends on your specific needs:

- For everyday users: Authenticator apps (TOTP) are a strong balance of security and convenience.
- For high-security needs: Hardware security keys and biometric authentication offer the highest level of protection.
- For ease of use: SMS and email authentication are simple but less secure.

Understanding the strengths and weaknesses of different 2FA types allows users to choose the best security solution for their needs. Need help setting up 2FA? FCS is here to help with all your 2FA needs. Give us a call or submit a helpdesk request and we will be happy to help you!

TL;DR

Two-Factor Authentication (2FA) enhances security by adding an extra verification step beyond just a password. Different methods include SMS, email, authenticator apps, hardware security keys, biometrics, and push notifications—each with varying levels of security and convenience. SMS and email are easy but vulnerable to phishing and interception. Authenticator apps offer better security without network reliance. Hardware keys and biometric authentication provide the highest protection but require specialized devices. Choosing the right 2FA method is crucial to keeping your accounts secure.

ISSUE 019
February 2025
Independence, Missouri

THIS MONTH'S PRODUCT SPOTLIGHT

CLICK TO VIEW A SHORT VIDEO!

- Easy to use Smartphone App
- Fast and Clear Connection for Calls
- Designed to Grow With Your Business

- Add Devices Easily
- Only Internet Connection Required
- Access Your Office Phone Anywhere

MANAGED PHONE SERVICES

WHY YOU NEED TO BACK UP YOUR MICROSOFT 365 DATA

Many businesses assume that Microsoft automatically backs up all their Microsoft 365 (O365) data—but that's a dangerous misconception.

While Microsoft ensures uptime and redundancy, it does not provide full data backups in case of accidental deletion, cyberattacks, or compliance needs. Here's why having a third-party backup solution is critical for your business:

1. Accidental Deletion Happens

Users delete emails, files, or entire mailboxes—sometimes without realizing it. Microsoft 365 offers limited retention, but once that period expires, the data is permanently lost. A backup solution ensures you can restore lost files anytime.

2. Protection Against Cyber Threats

Ransomware, phishing attacks, and insider threats can encrypt or delete important business data. Having a backup allows you to restore your files quickly without paying a ransom or suffering major downtime.

3. Compliance & Legal Requirements

Many industries require businesses to retain data for years to meet regulations like HIPAA, GDPR, or FINRA. Microsoft's built-in retention policies may not be enough, but a backup ensures your data is stored securely and retrievable when needed.

4. Microsoft's Shared Responsibility Model

Microsoft protects its infrastructure but expects businesses to be responsible for data protection and recovery. If critical emails, Teams conversations, or SharePoint files are lost, it's your responsibility to restore them—unless you have a proper backup in place.

5. Business Continuity & Peace of Mind

Data loss can lead to downtime, lost productivity, and financial losses. A backup solution guarantees quick recovery, ensuring business operations continue without disruption.

How We Can Help

Interested in O365 backup for your Microsoft? We offer reliable O365 backup solutions that safeguard your emails, OneDrive, SharePoint, and Teams data—so you never have to worry about losing critical business information. With infinite retention and backups that run every 2 hours, your data is always safe and protected!

Contact us today to set up your Microsoft 365 backup!

USEFUL COMPUTER TIPS YOU MIGHT NOT KNOW

Want to work smarter and not harder? Here are five quick computer tricks to boost productivity and have some fun!

1. Instantly Reopen a Closed Tab

Accidentally closed an important browser tab? Press Ctrl + Shift + T (Windows) or Cmd + Shift + T (Mac) to bring it back!

2. Quickly Take a Screenshot

Windows: Press Windows + Shift + S to snip a portion of the screen.

Mac: Press Cmd + Shift + 4 to select an area to screenshot.

3. Quickly Lock Your Computer

Stepping away? Press Windows + L (Mac: Cmd + Ctrl + Q) to instantly lock your screen and keep your data safe.

4. Use Spacebar to Scroll

Did you know you can scroll down a webpage by pressing the spacebar? Press Shift + Spacebar to scroll back up!

5. Snap Windows for Faster Multitasking

Press Windows + Left/Right Arrow to snap a window to one side of your screen, making multitasking a breeze!

Try these out and let us know your favorite! These small tips can end up saving you hours of time over the course of a working year

QUICK TIPS

QUANTUM COMPUTING VS AI

Quantum computing and artificial intelligence (AI) are both cutting-edge technologies, but they serve different purposes and operate on fundamentally different principles.

Here's a breakdown of Quantum Computing vs. AI:

1. What is Quantum Computing?

Quantum computing is a revolutionary field of computing that uses the principles of quantum mechanics to process information in ways that classical computers cannot. Instead of using binary bits (0s and 1s), quantum computers use qubits, which can exist in multiple states simultaneously due to superposition and can be entangled with one another.

Key Features of Quantum Computing:
- Superposition: Qubits can exist in multiple states at once, allowing quantum computers to process complex problems faster.
- Entanglement: Qubits can be linked, meaning the state of one qubit can instantly influence another, regardless of distance.
- Massive Parallelism: Can explore multiple solutions simultaneously, making it ideal for solving certain types of problems much faster than classical computers.

Applications of Quantum Computing:
- Drug discovery and molecular simulations
- Cryptography and cybersecurity
- Optimization problems (e.g., logistics, finance)
- Solving complex equations in physics and chemistry

2. What is Artificial Intelligence (AI)?

AI refers to the development of algorithms and systems that can perform tasks that typically require human intelligence. This includes machine learning, deep learning, natural language processing (NLP), and computer vision.

Key Features of AI:
- Pattern Recognition: AI models learn from data and identify trends.
- Decision-Making: AI can automate decisions and improve over time.
- Learning Ability: Machine learning models improve based on new data.
- Automation: AI powers everything from chatbots to self-driving cars.

Applications of AI:
- Virtual assistants (Siri, Alexa)
- Fraud detection in banking
- Autonomous vehicles
- AI-driven medical diagnostics
- Personalized recommendations (Netflix, Amazon)

3. How Do Quantum Computing and AI Differ?

Quantum Computing

Core Concept: Uses quantum mechanics to perform computations.
Processing Power: Can solve highly complex problems exponentially faster.
Data Handling: Works best for problems requiring massive parallelism.
Use Cases: Cryptography, simulations, optimization problems.
Limitations: Expensive, requires extreme cooling, still in early development.

Artificial Intelligence

Core Concept: Uses algorithms to mimic intelligence.
Processing Power: Works with classical computing power but improves efficiency.
Data Handling: Works best for large structured or unstructured datasets.
Use Cases: Image recognition, speech processing, automation.
Limitations: Requires large datasets, can be biased, needs constant updates.

4. How Quantum Computing and AI Can Work Together

Instead of competing, quantum computing and AI could work together in the future. Quantum computers could supercharge AI by solving problems faster and handling massive datasets more efficiently. Some potential areas where quantum and AI could intersect include:
- Quantum Machine Learning (QML): Using quantum computing to improve machine learning models.
- Optimized Neural Networks: Enhancing AI's ability to learn and make decisions.
- Better AI Training Models: Reducing the time needed to train deep learning algorithms.

Quantum computing and AI are distinct but complementary technologies. Both have their strengths and weaknesses but one thing is certain, they both will be crucial in technological advancements for years to come!

ISSUE 019
February 2025
Independence, Missouri

WHY YOUR BUSINESS NEEDS MICROSOFT 365 BUSINESS PREMIUM

In today’s digital landscape, businesses of all sizes face increasing security threats, operational challenges, and the need for seamless collaboration.

If your organization relies on Microsoft tools, upgrading to Microsoft 365 Business Premium is one of the smartest decisions you can make. This license isn’t just about accessing Microsoft apps—it’s a complete business solution designed to enhance security, productivity, and IT management.

Key Benefits of Microsoft 365 Business Premium

1. Advanced Security for Your Business

Cyber threats are evolving daily, and small to mid-sized businesses are prime targets. Microsoft 365 Business Premium includes:

✅ Defender for Office 365 – Protects against phishing, malware, and ransomware.
✅ Intune (Mobile Device Management) – Secure company data across employees’ devices.
✅ Conditional Access & MFA – Enforces identity protection with multi-factor authentication.
✅ Azure Information Protection – Ensures sensitive documents stay encrypted and controlled.
With these tools, you can safeguard your business from cyberattacks and data breaches.

2. Productivity Without Compromise

Your team needs reliable tools to work efficiently, whether in the office or remotely. Business Premium offers:
✓ Microsoft Teams – Seamless video conferencing, chat, and collaboration.
✓ Office Apps (Word, Excel, PowerPoint, Outlook, OneNote) – The latest versions, always updated.
✓ OneDrive & SharePoint – 1TB of secure cloud storage per user.
✓ Windows 11 Business – Enhanced security and management features for work devices.
This ensures that your team stays connected, collaborative, and productive from anywhere.

3. Simplified IT Management

Managing IT infrastructure can be complex and costly. Microsoft 365 Business Premium simplifies this with:
🔹 Autopilot & Intune – Easily deploy and manage devices without manual setup.
🔹 Automatic App Updates – Keeps your team on the latest, most secure software versions.
🔹 Remote Management – Control and secure devices remotely in case of loss or theft.
This means less downtime, reduced IT workload, and greater operational efficiency.

Why Upgrade to Business Premium?

Many businesses start with Microsoft 365 Business Standard, but the jump to Business Premium is worth it for:

- Better Security – Protects users from cyber threats beyond basic antivirus.
- Stronger Compliance – Helps meet industry regulations and data protection standards.
- Cost Savings – Combines security, collaboration, and management into one affordable package.

For businesses that prioritize security, productivity, and IT efficiency, Microsoft 365 Business Premium is the ideal solution.

Need Help Upgrading?

As your trusted IT partner, we can help you implement, manage, and secure your Microsoft 365 environment. Contact us today to discuss how Business Premium can benefit your business!

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 February's question of the month:

What is SMS-Based Authentication vulnerable to?