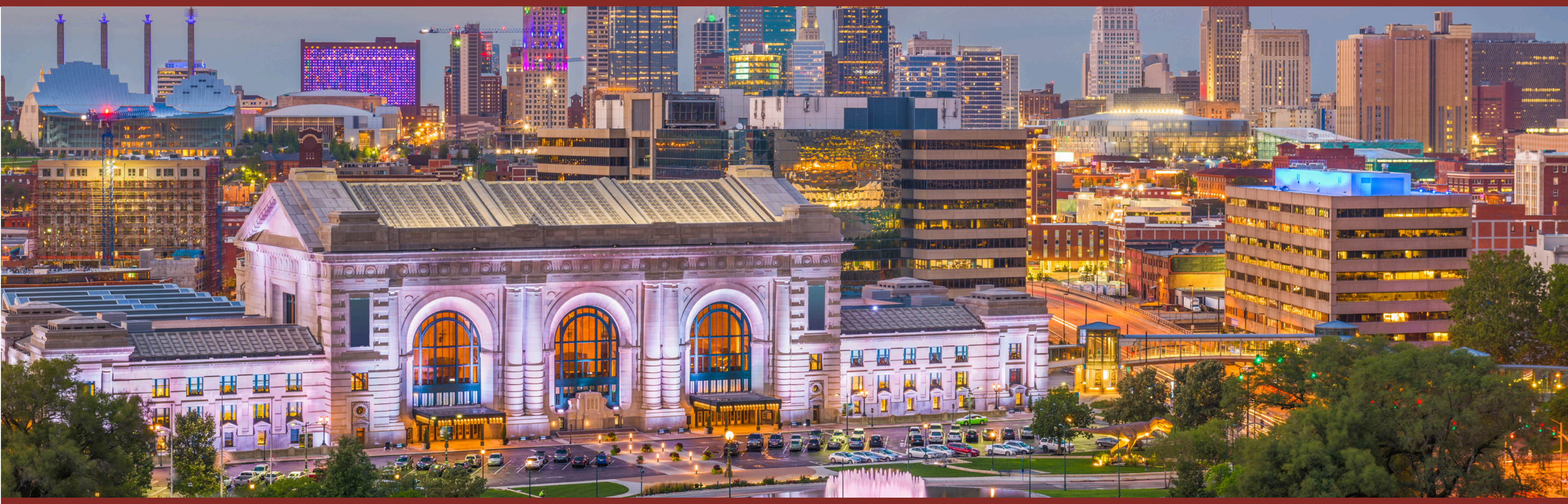
ISSUE 015
October 2024
Independence, Missouri



# FCS TECH TALK

Your Trusted Technology Partner Since 1989

## INSIDE THIS ISSUE:

## WEBSITE SECURITY: WHY HTTPS IS A MUST

In today's digital landscape, the security and privacy of online interactions have become increasingly critical. For many years, websites were primarily built on the HTTP (Hypertext Transfer Protocol) framework.

While HTTP was sufficient for basic web communication, the advent of cyber threats, data breaches, and privacy concerns led to the development of HTTPS (Hypertext Transfer Protocol Secure) as a more secure alternative.

The "S" in HTTPS stands for "secure," indicating the use of encryption to safeguard the data transferred between a user's browser and a website's server.

Here are some of the key differences between HTTP and HTTPS websites.

**1. Data Encryption and Security**
The most fundamental difference between HTTP and HTTPS lies in the encryption of data. HTTP transmits information in plain text, meaning that anyone with the technical skills to intercept the communication can read it. This vulnerability leaves users at risk of cyberattacks like man-in-the-middle attacks and data theft.

HTTPS, on the other hand, encrypts the data exchanged between the browser and the server using SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols. This encryption ensures that even if the data is intercepted, it cannot be read or tampered with by malicious actors. By using HTTPS, websites protect sensitive information such as passwords, credit card numbers, and personal data from being exposed during online transactions or login sessions.

**2. Trust and Credibility**
With rising awareness about online security, internet users are becoming more informed about the risks of browsing unsecured websites. Modern browsers like Chrome, Edge, and Safari have taken significant steps to warn users when they access an HTTP site. HTTP websites are often marked as "Not Secure" in the browser's address bar, making visitors question the credibility of the site.

In contrast, an HTTPS website displays a padlock icon next to the URL in the browser, signaling to users that their connection is secure. This visual cue fosters a sense of trust, which is essential for businesses, especially e-commerce sites, financial institutions, and service providers. A secure connection reassures users that the website takes their privacy and security seriously, enhancing the website's overall credibility.

**3. SEO and Ranking Boost**
Google, the world's leading search engine, has incorporated HTTPS as a ranking factor in its search algorithms since 2014. This means that websites using HTTPS are given preference over HTTP websites in search engine rankings. Google's reasoning is simple: they want to promote a more secure internet for all users.

Therefore, adopting HTTPS can lead to better search visibility, higher rankings, and increased organic traffic. For businesses that rely on search engine optimization (SEO) to drive website visitors and conversions, migrating to HTTPS is not just a security upgrade—it's a key factor in improving their overall online presence.

**4. Data Integrity**
Another advantage of HTTPS is data integrity. With HTTP, data can be altered or injected into the communication channel without the user's knowledge. This means that hackers can tamper with the content delivered to users or inject malicious scripts into the website.

With HTTPS, the encryption and authentication process ensures that the data sent and received is unaltered. This means users can trust that the content they're viewing has not been manipulated by third parties, further ensuring a safer and more reliable browsing experience.

**5. Protection Against Phishing Attacks**
Phishing is a technique where attackers trick users into providing sensitive information by impersonating legitimate websites. While HTTPS does not eliminate phishing attacks entirely, it provides an additional layer of security. Most phishing sites still rely on HTTP, which can alert users to their fraudulent nature.

Moreover, when users see the padlock icon of HTTPS and the presence of a valid SSL certificate, they are more likely to identify authentic websites. Phishing sites struggle to obtain SSL certificates, making it harder for them to mimic legitimate websites effectively.

**6. Browser and App Compatibility**
Another reason to transition to HTTPS is its wide compatibility with modern web technologies. Many new web features, such as HTTP/2, progressive web apps (PWAs), and service workers, require HTTPS for full functionality. Websites that remain on HTTP may not be able to take advantage of these cutting-edge features, leaving them at a competitive disadvantage in terms of performance, speed, and user experience.

The transition from HTTP to HTTPS has shifted from being a choice to becoming a necessity for any website that values security, trust, and user experience.

HTTPS is now the industry standard, providing encryption, authenticity, and data integrity while helping websites rank higher in search results and appear more credible to visitors.

In an era where cybersecurity threats are increasing and user trust is paramount, HTTPS is an indispensable component of a website's infrastructure.

Whether you run a personal blog, an e-commerce store, or a large corporate website, adopting HTTPS protects your users and strengthens your brand's reputation.

Ultimately, HTTPS ensures that websites are not just functional, but also secure and trustworthy—a crucial factor in succeeding online today.

**Need help with your website?**
Is your website still using HTTP? Ferguson Computer Services is here to help. We can make all the necessary changes needed for your website to upgrade from HTTP to HTTPS.

ISSUE 015
October 2024
Independence, Missouri

# COPILOT IN TEAMS - NEW FEATURES, AGENTS & MORE

Microsoft Teams continues to evolve. It is a powerful hub for collaboration and communication in the modern workplace. With the integration of AI-driven Copilot, Teams is pushing the boundaries. It's innovating how we interact with technology to improve and unlock business value.

### What is Copilot in Microsoft Teams?

Copilot is Microsoft's AI-powered assistant. In Microsoft Teams, Copilot acts as an intelligent agent. It helps users by doing things like:

- Automating processes
- Managing tasks
- Analyzing data
- Providing real-time insights

Copilot provides actionable recommendations, transforming how teams collaborate.

### New Features of Copilot in Teams

These features help users navigate complex tasks and much more.

### Enhanced Collaboration Features

- Automated Meeting Summaries. A standout feature is generating meeting summaries automatically.
- Intelligent Task Management. It analyzes conversations in chats or meetings, then automatically identifies task, assigns them to team members, and tracks progress.

### Smarter AI Suggestions

- Context-Aware Responses. Copilot's AI has become more context-aware. This minimizes irrelevant suggestions and keeps teams focused.
- Personalized Insights. As Copilot interacts with a team, it learns from past behaviors. For example, it can suggest the best times to schedule meetings.

### Agents in Copilot: A New Way to Work

Copilot agents are task-specific AI-driven assistants. You can customize them to handle particular functions or workflows. Agents focus on specific domains such as customer support, sales, or project management. This makes them a valuable asset for small and medium-sized businesses.

Here are some of the key capabilities these agents bring to Teams:

- Automating Routine Tasks
- Integration with Business Tools
- Multitasking Capabilities

Benefits of Using Copilot in Teams

- Increased Productivity. Copilot frees up time for employees to focus on more important activities.
- Improved Communication. Copilot can summarize meetings, track action items, and offer context-aware suggestions.
- Enhanced Decision- Making. Copilot helps highlight trends, provide performance metrics, and identify areas of improvement
- Better Workflow Management. Agents and automation tools help manage workflows.

The future of AI in tools like Teams presents an exciting opportunity. By adopting these AI-powered tools now, businesses can stay ahead of the curve.

# SOCIAL ENGINEERING: WHAT IS IT?

### What is Social Engineering?

Social engineering is a form of cybercrime that involves manipulating people into divulging confidential information or performing actions that compromise security.

Unlike hacking, which typically targets technical vulnerabilities, social engineering exploits human psychology, such as trust, fear, or urgency, to deceive individuals.

Cybercriminals use social engineering tactics to trick victims into providing sensitive data, such as passwords, financial details, or even access to secure systems. These attacks often come in the form of emails, phone calls, or even face-to-face interactions.

### Common Types of Social Engineering

**1. Phishing:** Attackers send fake emails or messages posing as trusted entities (like a bank) to steal sensitive information.

**2. Pretexting:** The attacker creates a fabricated scenario, pretending to be someone of authority (like IT staff) to gather personal details.

**3. Baiting:** The attacker offers something enticing (e.g., free software) to trick the victim into providing access or downloading malware.

**4. Tailgating:** A physical security breach where an attacker follows someone into a restricted area without proper credentials.

### How to Protect Yourself

**Be Skeptical:** Don't trust unsolicited requests for sensitive information. Always report these emails immediately.

**Verify Requests:** Confirm identities before sharing confidential data, especially if the request seems urgent or unusual.

**Use Security Tools:** Enable email filters, two-factor authentication, and strong passwords to reduce risks.

Social engineering attacks prey on human nature, making awareness and caution essential in protecting personal and organizational security.

# DATA BREACH DAMAGE CONTROL:

Data breaches are an unfortunate reality for businesses of all sizes. When a breach occurs, the immediate response is critical. How you manage the aftermath can significantly impact your reputation and financial stability.

Effective damage control requires a well-planned approach. But there are common pitfalls that can exacerbate the situation:

- Delayed Response. The longer it takes to respond, the more damage can happen.
- Inadequate Communication. It leads to misunderstandings, frustration, and further reputational damage.
- Failing to Contain the Breach. Once your business detects a breach, take immediate action to prevent further damage.
- Neglecting Legal and Regulatory Requirements. Failing to comply can result in significant fines and legal action.
- Overlooking the Human Element. Addressing the human element is essential for a comprehensive response.

If your business does fall victim to a data breach Ferguson Computer Services can help you every step of the way making sure common pitfalls are avoided and damage is mitigated.

# 5 FACTORS AFFECTING YOUR INTERNET SPEED

**1. Internet Plan and Bandwidth**
Your internet service plan plays a foundational role in determining your internet speed. Internet service providers (ISPs) offer different plans based on speed, typically measured in megabits per second (Mbps). The higher your plan's Mbps, the faster your internet connection can potentially be.

However, the advertised speeds (e.g., 100 Mbps) are usually the maximum possible under ideal conditions. Factors like the number of devices connected or network congestion can prevent you from consistently reaching this speed.

Bandwidth refers to the maximum amount of data that can be transmitted over an internet connection in a given amount of time. If you have multiple devices streaming, downloading, or uploading content at the same time, it can strain your bandwidth and slow down your connection.

**2. Network Congestion**
Network congestion occurs when too many users are trying to access the internet through the same network, especially during peak hours. For instance, if you're using a shared network in a densely populated area or an office environment, the available bandwidth is distributed among all active users. This can slow down individual speeds as the network becomes saturated.

Congestion is particularly noticeable during times when internet usage is high, such as in the evening when people are streaming movies or gaming. In such cases, your internet speed may decrease due to high demand.

**3. Wi-Fi vs. Wired Connections**
The way you connect to the internet—via a Wi-Fi network or an Ethernet cable—can significantly impact your speed. Wired connections (Ethernet) tend to be faster and more stable than Wi-Fi because they aren't affected by signal interference or physical obstructions.

Wi-Fi signals, on the other hand, can be weakened by walls, distance from the router, or interference from other electronic devices.

For users relying on Wi-Fi, signal strength can fluctuate, causing slower speeds, especially if you are far from the router or in a room with thick walls.

Upgrading to a high-quality router, placing it in a central location, and using extenders can help improve Wi-Fi performance.

**4. Router and Modem Quality**
The hardware you use to connect to the internet—your router and modem—also plays a critical role in determining internet speed. If you have an outdated or low-quality router, it may not support higher speeds or the latest Wi-Fi standards, limiting your connection's performance.

Router: Newer routers typically support higher speeds and more simultaneous connections, which is important for households with multiple devices. Upgrading to a router that supports modern Wi-Fi standards (such as Wi-Fi 6) can enhance performance.

Modem: Your modem must be compatible with your ISP's service and capable of handling the speed your plan offers. Older modems might cap your speed, even if your internet plan offers higher rates.

Regularly updating your firmware and ensuring you're using hardware that matches your internet plan's potential can help optimize your connection.

**5. Device Performance and Capacity**
The speed and performance of the device you're using to connect to the internet can also impact your overall experience. Older devices, such as laptops, smartphones, or tablets, may not be equipped to handle high-speed internet connections.

For example, an outdated Wi-Fi card, a lack of support for newer Wi-Fi standards, or insufficient processing power can result in slower browsing, even if your internet connection itself is fast.

Running software updates, upgrading hardware, or using devices with better network capabilities can help improve internet performance.

# 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

# THIS MONTH'S PRODUCT SPOTLIGHT

CLICK HERE FOR MORE INFO!

## We Want Your Feedback

Here at Ferguson Computer Services, we value your feedback greatly. We 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 October's question of the month:

What does the "S" stand for in HTTPS?