ISSUE 020
March 2025
Independence, Missouri

FCS TECH TALK

Your Trusted Technology Partner Since 1989

INSIDE THIS ISSUE:

SPOTTING THE DIFFERENCE BETWEEN MALWARE AND RANSOMWARE

In the evolving landscape of Cyber Security, understanding the threats you face is key to protecting your systems and data.

Two of the most common and damaging threats are malware and ransomware. While these terms are often used interchangeably, they are not the same.

Each poses distinct risks and operates differently. Knowing how to spot the differences between malware and ransomware can help you respond more effectively and minimize potential damage.

What is Malware?

Malware (short for malicious software) is a broad category of software designed to damage, disrupt, or gain unauthorized access to computer systems. Malware comes in various forms and can serve different purposes, from stealing information to corrupting files or spying on user activity.

Types of Malware:

1. Viruses – Self-replicating programs that attach to files and spread when executed.
2. Trojans – Malicious programs disguised as legitimate software, used to create backdoors for attackers.
3. Worms – Standalone programs that spread across networks without user action.
4. Spyware – Software that secretly gathers user information without consent.
5. Adware – Programs that bombard users with unwanted advertisements.
6. Rootkits – Tools that enable unauthorized access to a system while hiding their presence.

Signs of a Malware Infection:

- Sluggish system performance
- Frequent pop-ups or unwanted ads
- Unexpected crashes or system reboots
- Unexplained network activity
- Files or programs disappearing or becoming corrupted

What is Ransomware?

Ransomware is a specific type of malware designed to encrypt a victim's files or lock them out of their system until a ransom is paid. Unlike other malware, ransomware's goal is financial extortion rather than data theft or disruption.

Types of Ransomware:

1. Crypto Ransomware – Encrypts files and demands payment for the decryption key.
2. Locker Ransomware – Locks the victim out of their system or files, but doesn't encrypt data.
3. Scareware – Displays fake warnings and demands payment to "fix" the issue.
4. Doxware (Leakware) – Threatens to release sensitive information unless a ransom is paid.

Signs of a Ransomware Attack:

- A ransom note displayed on your screen
- Files become encrypted and can't be opened
- File extensions change to unknown formats
- Increased CPU and memory usage
- Loss of access to certain system functions or files

What are the Key Differences Between Malware and Ransomware?

Malware:

- *Purpose:* Damage, disruption and information theft.
- *Visibility:* Often operates in the background, trying to avoid detection.
- *Impact:* May slow down systems, steal data, or damage files.
- *Removal:* Can often be removed with antivirus or anti-malware tools.
- *Spread:* Can spread through infected files, websites, email attachments, or networks.

Ransomware:

- *Purpose:* Financial extortion through encryption or locking access of a specific account that has been compromised.
- *Visibility:* Highly visible, with ransom notes and encryption warnings, you will not question if you have ransomware
- *Impact:* Immediate and severe, often preventing access to files or systems until the ransom is paid.
- *Removal:* Removal is difficult without an encryption key; even paying the ransom sometimes may not guarantee recovery.
- *Spread:* Often spread through phishing emails or exploit kits.

How do You Protect Against Malware and Ransomware?

✅ **Use Reliable Antivirus and Anti-Malware Software**

Having antivirus is a crucial step to ensuring that malware and ransomware are caught before they have time to wreak havoc on any devices that have been infected.

✅ **Enable Multi-Factor Authentication (MFA)**

MFA helps protect against unauthorized access, even if passwords are compromised a malicious actor would still need to get past MFA to be able to access the device that is being infected.

✅ **Keep Software and Operating Systems Updated**

Having regularly scheduled maintenance and patching on your device allows for crucial vulnerabilities to be patched as well as updates pushed to ensure that all systems are operating optimally leaving no easy areas open for attack.

✅ **Back Up Your Data Regularly**

Regular backups ensure that you can recover your data in case of an attack, without needing to pay a ransom. Having an offsite, geo-redundant backup helps to ensure your data is kept safe and accessible even if an attack has occurred.

✅ **Be Cautious with Email Attachments and Links**

Avoid opening suspicious emails, links, and attachments — common methods used to deliver malware and ransomware. Using an email protection filter is a great way to help prevent spam and phishing emails from reaching your inbox.

✅ **Use Network Segmentation and Firewalls**

Isolating critical systems and using firewalls can prevent malware from spreading across the network.

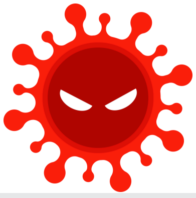
Attacks By the Numbers

Malware Attacks (2024):
- In 2024 there was an approximate 107% surge in IoT malware attacks during the year.
- There are around 190,000 new malware attacks every second, indicating the rapid evolution and proliferation of malicious software.

Ransomware Attacks (2024):
- Approximately 59% of organizations reported being victims of ransomware attacks in 2024.
- About 65% of financial organizations worldwide reported experiencing a ransomware attack in 2024.
- The year saw the rise of 55 new ransomware groups, marking a 67% increase compared to the previous year.
- December 2024 experienced the highest monthly volume of global ransomware attacks ever recorded, indicating a concerning escalation in cybercriminal activities.

Financial Impact:
- In the first half of 2024, the average extortion demand per ransomware attack exceeded $5.2 million, with a record victim payment of $75 million in March 2024.
- Despite the increase in attacks, ransomware payments decreased by 35%, totaling $814 million in 2024 compared to $1.25 billion in 2023. This decline is attributed to improved law enforcement actions and enhanced organizational defenses.

We are here to help with any of your security needs to protect against all cyber security attacks including malware and ransomware.



TL;DR

Malware is a broad category of malicious software designed to damage, disrupt, or steal information from computer systems. Common types include viruses, trojans, spyware, and worms. In contrast, ransomware is a specific type of malware that encrypts files or locks users out of their systems, demanding payment (ransom) to restore access. Key Differences: Malware – Focuses on disruption, data theft, or spying. Ransomware – Focuses on financial extortion through encryption or system lockouts. Signs of Infection: Malware: Slow performance, pop-ups, missing files. Ransomware: Files become inaccessible, ransom notes appear. Prevention Tips: Use antivirus and anti-malware tools. Keep systems updated. Enable multi-factor authentication. Back up data regularly.

ISSUE 020
March 2025
Independence, Missouri

THIS MONTH'S PRODUCT SPOTLIGHT

CLICK TO VIEW A SHORT VIDEO!

MANAGED CYBER SECURITY

- 24/7 Security Alerts for Endpoints
- External Vulnerability Scanning
- Dark Web Password/ PII Monitoring

- Security Awareness Training
- 24/7 Microsoft Account Monitoring
- Advanced Web Content Filtering

WHY HARDWARE PROCUREMENT IS ESSENTIAL TO A SMALL BUSINESS

In today's digital-driven world, having the right hardware is crucial for the success of any small business.

Hardware procurement—the process of selecting, purchasing, and managing computer systems, servers, networking devices, and peripherals—ensures your business runs smoothly and efficiently. Here's why it's essential:

1. Improved Productivity & Performance

Outdated or low-quality hardware can slow down operations and reduce employee efficiency. Investing in reliable computers, servers, and networking equipment helps your team work faster, reduces downtime, and supports business growth.

2. Cost Savings in the Long Run

Proper hardware procurement prevents unnecessary expenses on frequent repairs and replacements. By choosing high-quality, scalable technology, you minimize maintenance costs and extend the lifespan of your equipment.

3. Enhanced Security & Compliance

Older hardware can be vulnerable to cyber threats and data breaches. Procuring updated hardware ensures better security features. Such as encryption and compliance with industry regulations, keeping your business and customer data safe.

4. Scalability & Future-Proofing

As your business grows, so do your hardware needs. A solid procurement strategy allows you to plan for future expansion, ensuring your IT infrastructure can support additional employees, increased workloads, and evolving technology trends.

5. Better Future Proofing

Hardware procurement isn't just about buying computers—it's about strategically investing in the right technology to boost efficiency, security, and long-term savings.

Having a plan to consistently update hardware helps to ensure your small business is prepared for the future as well as secured with up to date, reliable hardware that you can rely on.

FCS is here to help you with all your hardware needs ensuring you get the proper specs to fit your business needs at an affordable price!

MORE USEFUL COMPUTER TIPS

Most of us use computers daily, but there are some lesser-known tricks that can boost productivity and make life easier. Here are four helpful computer tips you may not have tried:

1. Clipboard History

Press Windows Key + V to access your clipboard history. This allows you to paste previously copied items without having to copy them again.

2. Restore a Closed Tab

Accidentally closed a browser tab? Just press Ctrl + Shift + T to reopen it instantly.

QUICK TIPS

3. Dark Mode Shortcut

Switch to dark mode quickly by pressing Windows Key + I to open settings, then go to Personalization → Colors and select Dark under "Choose your color."

4. Instantly Minimize All Windows

Press Windows Key + D to minimize all open windows and show your desktop.

Press it again to restore the windows.

These few helpful tips and shortcuts can end up saving you hours and hours of time once implemented on a daily basis.

Knowing tips and tricks like these can increase productivity as well as overall user experience when using a computer.

PHYSICAL SERVER VS. SHAREPOINT

Data storage is a critical component of any business, and two popular options for managing files and information are physical servers and SharePoint. While both solutions help store, organize, and retrieve data, they operate differently, offering unique advantages and drawbacks.

Similarities Between Physical Servers and SharePoint

Despite their differences in setup and functionality, physical servers and SharePoint share some key similarities:

1. Data Storage & Management
- Both store and manage business-critical data, including documents, databases, and applications.
- Provide structured storage solutions that allow users to organize, retrieve, and edit data efficiently.

2. Access Control & Security Features
- Offer user permissions and access restrictions to control who can view, edit, or delete files.
- Support encryption and backup options to protect against data loss or unauthorized access.

3. Collaboration Capabilities
- Both allow multiple users to access and work on shared files, though the extent and method of collaboration differ.
- Teams can store and manage project files, reports, and client data on either platform.

4. Integration with Business Applications
- Physical servers can be configured to work with business applications like email, databases, and customer management software.
- SharePoint integrates natively with Microsoft 365, Teams, and OneDrive, offering a seamless cloud-based experience.

Key Differences Between Physical Servers and SharePoint

While they share some functions, physical servers and SharePoint differ in how they operate, store data, and provide access.

Physical Servers
- Location: On-premises, stored physically within the organization.
- Access: Local network access, limited remote capabilities.
- Scalability: Requires hardware upgrades for additional storage.
- Security: Fully customizable security settings, physical control.
- Maintenance: Requires IT staff for upkeep, updates, and troubleshooting.
- Collaboration: File sharing via internal network or VPN.
- Cost Structure: High initial cost, but lower long-term costs.
- Backup & Recovery: Must be managed manually or with a backup system.

SharePoint
- Location: Cloud based hosted by Microsoft.
- Access: Accessible from any internet-connected device.
- Scalability: Easily scalable with cloud storage plans.
- Security: Microsoft-managed security with compliance features.
- Maintenance: Automatic updates and maintenance handled by Microsoft.
- Collaboration: Real-time collaboration with multiple users online.
- Cost Structure: Subscription-based, ongoing monthly/annual fees.
- Backup & Recovery: Built in automatic backups and disaster recovery.

✅ ***What Physical Servers Do Best:***

- Data Security & Control – Best for organizations needing full control over their data, especially in industries with strict compliance requirements (e.g., finance, healthcare).
- Performance & Speed – Ideal for businesses needing high-speed access to large files without internet dependency.
- Customizability – Allows businesses to custom-configure hardware, software, and security settings based on their needs.
- One-Time Cost Investment – While expensive upfront, owning a physical server avoids recurring subscription fees.

✅ ***What SharePoint Does Best:***

- Remote Accessibility – Enables users to access and edit documents from anywhere, perfect for remote and hybrid workforces.
- Scalability & Flexibility – No need to upgrade physical hardware; storage can expand as needed.
- Collaboration & Integration – Offers real-time document editing and seamless integration with Microsoft 365 apps.
- Automatic Backups & Updates – Data is automatically backed up with Microsoft handling system maintenance.

ISSUE 020
March 2025
Independence, Missouri

HOW TO STAY SECURE WHEN USING MOBILE APPS ON YOUR PHONE

1. Download Apps Only from Trusted Sources

The first and most important step to staying secure is to download apps exclusively from official app stores like the Google Play Store or Apple App Store.

These platforms have strict security measures and review processes to minimize the chances of malicious apps being listed. Avoid downloading apps from third-party websites or unverified sources, as they may contain malware or spyware.

Pro Tip:

- Check the app developer’s name and read reviews before installing.
- Avoid apps with very few reviews or those with suspiciously high ratings but vague comments.

2. Keep Your Apps and Operating System Updated

App developers frequently release updates to patch security vulnerabilities and improve performance. Failing to update your apps or operating system leaves you exposed to known threats that hackers can exploit.

What to Do:

- Enable automatic updates on your phone.
- Regularly check for and install updates manually if automatic updates are turned off.

3. Use Strong and Unique Passwords

Weak or reused passwords are one of the easiest ways for hackers to gain access to your accounts. Use complex, unique passwords for each app and account.

Best Practices:

- Use a password manager to generate and store complex passwords.
- Combine uppercase and lowercase letters, numbers, and special characters.
- Avoid using personal information (e.g., birthdays, pet names).

4. Enable Two-Factor Authentication (2FA)

Two-factor authentication adds an extra layer of security by requiring you to verify your identity using a second method, such as a code sent to your phone or email.

Why It Matters:

Even if a hacker steals your password, they won’t be able to access your account without the second verification step.

How to Enable:

- Most popular apps (e.g., Google, Facebook, WhatsApp) offer 2FA under security settings.
- Use an authenticator app like Google Authenticator or Authy for added protection.

5. Pay Attention to App Permissions

Many apps request permissions that aren't necessary for their core functionality. Granting unnecessary permissions can expose your personal data to potential misuse.

How to Protect Yourself:

- Review the permissions before installing an app.
- Disable permissions that seem excessive (e.g., a flashlight app shouldn’t need access to your location).
- Revisit and adjust app permissions periodically in your phone’s settings.

6. Avoid Public Wi-Fi for Sensitive Transactions

Public Wi-Fi networks are often unsecured, making it easier for hackers to intercept your data.

Safe Alternatives:

- Use a VPN (Virtual Private Network) when connecting to public Wi-Fi.
- Turn off Wi-Fi auto-connect to prevent your phone from automatically connecting to unknown networks.

7. Be Cautious with In-App Links and Messages

Phishing scams are common in mobile apps, where hackers disguise links and messages to steal your login details.

What to Watch For:

- Avoid clicking on suspicious links or attachments within apps.
- If an app asks for sensitive information via a link, go directly to the official website instead of clicking the link.

Staying secure when using mobile apps requires a combination of smart habits and proactive measures.

By downloading apps from trusted sources, using strong passwords, enabling two-factor authentication, and monitoring permissions and activity, you can significantly reduce the risk of cyber threats.

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 March's question of the month:

In 2024 what percentage of organizations reported being victims of ransomware attacks?