

# TECH BYTES

## March 2025

Your Monthly Update on Technology  
and Cyber Security News



Keep up with the latest  
technology advancements  
and trends.

**Matthew DeWees**  
-President

Have you ever worried about keeping your online files safe? In today's digital world, protecting your files is super important.

From keeping your personal papers safe to protecting work information, how you store and share files can totally change your digital safety. What does this mean for you and your online life?

Understanding file protection isn't just about stopping hackers—it's about feeling confident online. Whether you want to keep your stuff private or share files easily with friends and coworkers, the right file safety steps can make a huge difference.

Curious about keeping your digital files secure? Reach out to us at [everythingit@virtualdataworks.com](mailto:everythingit@virtualdataworks.com) to learn how you can protect your online files and make sharing simple.

Until then, stay safe,



President - Virtual DataWorks

### WHAT'S INSIDE?

**02** GUIDE TO SECURE FILE  
STORAGE AND TRANSFERS

**03** 10 STEPS TO PREVENT A  
DATA BREACH

**04** HOW TO SPOT HIDDEN  
MALWARE


**05** MINIMIZE RANSOMWARE  
DAMAGE

**06** BOOST DEVICE PRODUCTIVITY


## DID YOU KNOW?

In 2017, a cybersecurity researcher accidentally stopped the WannaCry ransomware attack by registering a domain name found in the malware's code.

**Virtual DataWorks**

 475 Wolf Ledges Parkway  
Akron, Ohio 44311

 [virtualdataworks.com](http://virtualdataworks.com)

 (330)800-2186

## 02 GUIDE TO SECURE FILE STORAGE AND TRANSFERS

File storage and transferring hold a very dear place in most people's lives. However, the safety of files is really tough to maintain. In this guide, we are going to help you protect your files. We will explore ways to store and send files securely.

### What is secure file storage?

Secure file storage protects your files. It prevents others from accessing your files or altering them in any way. Good storage grants protection to your files using locks. You alone can unlock such files.

### Types of secure storage

Files can be stored securely in various ways, as listed below.

- Cloud
- External hard drives
- Encrypted USB drives

Cloud storage saves files on the internet. External drives save files on a device you can hold. Encrypted drives use special codes to lock files.

### Why is secure file storage important?

Secure storage keeps your information private. It stops thieves from stealing your data. It also helps you follow laws about data protection.

### Risks of unsecured storage

Unsecured files can lead to huge troubles, including but not limited to the following:

- Identity theft
- Financial loss
- Privacy breaches

These risks give a reason why secure storage is important. You need to protect your personal and work files.

### How Can I Make My File Storage Safer?

You can do so many things to make your storage safer, such as:

- Using strong passwords
- Enabling two-factor authentication
- Encrypting your files
- Keeping your software up to date frequently

Strong passwords are hard to guess. Two-factor authentication adds an extra step to log in. Encryption scrambles your files so others can't read them. Updates fix security problems in your software.

### Best practices for passwords

Good passwords are important in keeping your files safer. Here are some tips:

- Use long passwords
- Mix letters, numbers, and symbols
- Don't use personal info in passwords
- Use different passwords for each account

### What is secure file transfer?

Secure file transfer is a way of sending files safely between individuals or devices. It prevents unauthorized access to files and prohibits modification of files while in transit. The better methods of transfer protect the files with encryption.



### Common secure transfer methods

Here are several ways to securely transfer files:

- Secure FTP (SFTP)
- Virtual Private Networks (VPNs)
- Encrypted email attachments
- Secure file-sharing services

### How to Transfer Files Safely?

These steps will keep your files safer while in transit:

- Select a secure method of transfer
- Encrypt the file before you send it
- Give strong passwords for file access
- Authenticate the recipient
- Send the access details separately

### How to email attachments safely

- Encrypt important attachments
- Use a secure email service
- Avoid writing sensitive information in the body of an email
- Double-check the recipient's email address

### Ready to Secure Your Files?

Protect your data from thieves and snoopers. Use strong passwords, encryption, and safe methods of transfer.

Need help with secure file storage? Feel free to reach out today and let us walk you through setting up safe systems for your files to take the next step in protecting critical data.

## MICROSOFT 365 BACKUP

### Unlimited Third-Party Backup for Microsoft 365

Virtual DataWorks provides instant data access and comprehensive M365 coverage, with blockchain encryption to guard against ransomware and accidental deletions.

We store four backup copies in two locations. With unlimited storage and fast restore, we minimize downtime, making M365 data protection easy and cost-effective.

 **VISIT NOW**





Data breaches can harm your business. They can cost you money and trust. Let's look at how to stop them from happening.

### What is a data breach?

A data breach is when someone steals information. This can be names, emails, or credit card numbers. It's bad for your customers and your business.

### Why should you care about data breaches?

Data breaches will cost you money. Perhaps your customers will stop trusting you. You may even be fined. It is vital to try to prevent them from occurring in the first place.

How do you prevent a data breach?

Here are 10 steps to help keep your data safe:

- Use strong passwords. Include letters, numbers, and symbols. Do not use the same password for all of your accounts.
- Update your software. Updates usually patches security holes. Have your computer set to update automatically.
- Train your employees. Teach them how to identify fake emails. Inform them to not click on suspicious links.
- Use encryption. Encryption scrambles your data.
- Limit access to data. Only give people access to what they need for their work.
- Create backups of your data. Keep these copies in a safe location.
- Use a firewall. A firewall acts like a guard for your computer.
- Be careful with emails. Almost every data breach starts with a trick email.
- Protect your Wi-Fi. Use a strong password on your Wi-Fi.
- Protect your Wi-Fi. Use a strong password on your Wi-Fi.

Have a plan. Know whom to contact and what you should do. Do a practice drill so you are ready if there is an intrusion.

Even with well-thought-out plans, data breaches can still occur. If one does happen, it's crucial to act swiftly.

Analyze the incident to understand what went wrong and use those insights to strengthen your security measures. This proactive approach will help prevent future breaches and improve your overall security posture.

## HOW TO SPOT HIDDEN MALWARE ON YOUR DEVICES

Malware is bad software that can hurt your computer or phone. It can also make your device run slow and steal your info.

Here is how you can spot hidden malware on your devices.

### What is Malware?

The word "malware" is short for "malicious software." It is a program that tries to harm your device or data. The most common types of malware are created by hackers looking to cause trouble.

There are lots of different types of malware.

#### Viruses

Viruses will spread from device to device. They can destroy your files or make your computer run really slow.

#### Trojans

Trojans act like they're good programs, but they actually aren't. They might steal your information.

Ransomware Ransomware will lock your files. It will then ask you for money in exchange for your files.

### How Does Malware Get on Your Device?

**Malware can creep onto your device** in so many ways:

#### Downloading Bad Files.

Sometimes you might download a file that has malware in it. Be careful what you click on!

**Visiting Bad Websites.** Some websites can put malware on your device when you visit them.

#### Opening Weird Emails.

Hackers can send emails with malware attached. Don't open emails from people you don't know.

#### What Are Signs of Hidden Malware?

Malware can be sneaky. But there are some signs to look out for:

- **Unexplained Slowdowns:** Your device becomes noticeably slower without any clear reason.
- **Frequent Crashes or Freezes:** Applications or the entire system crashes more often than usual.
- **Unusual Pop-ups:** You encounter unexpected pop-up ads, even when not browsing the internet.
- **Unauthorized Changes:** Settings, files, or browser configurations change without your knowledge.

## HOW TO MINIMIZE RANSOMWARE DAMAGE

Ransomware is a serious threat, but you can protect yourself with these key steps:

- Regularly update your operating system, applications, and security software to fix vulnerabilities that ransomware can exploit.
- Invest in strong antivirus software, keep it active, and ensure it's always updated to detect and block ransomware.
- Be vigilant with emails, especially from unknown senders. Avoid opening attachments or clicking links unless you're certain they're safe.
- Make regular backups of important files and store them on an external device or cloud storage not connected to your primary computer.
- Use firewalls to block unauthorized access and prevent ransomware from communicating with its command-and-control servers.
- Stay informed about the latest ransomware threats and educate others in your household or organization about safe online practices. Awareness is a powerful tool in preventing ransomware attacks.
- Implement strong, unique passwords for all your accounts and change them regularly. Consider using a password manager to keep track of your passwords securely.
- Restrict administrative privileges to only those who need them. Limiting user access can reduce the risk of ransomware spreading across your network.

By following these steps, you can significantly reduce the risk of a ransomware attack. Have you implemented any of these measures already?

## BOOST PRODUCTIVITY BY ORGANIZING YOUR DEVICE

Our devices are essential, but they can sometimes hinder productivity. Here's how to organize your device to boost efficiency:

- **Update Software:** Regularly updating your operating system and applications helps fix vulnerabilities that ransomware can exploit.
- **Use Antivirus:** Invest in strong antivirus software and ensure it is always active and updated.
- **Be Cautious with Emails:** Avoid unknown attachments and links.
- **Back Up Files:** Regularly back up your important files using external drives or cloud storage. This keeps your data safe and prevents loss from ransomware or other issues.
- **Enable Firewalls:** Use firewalls to block unauthorized access to your network. This enhances security and helps block malware and other threats.

Organizing your device saves time and reduces stress. Start with one tip and add more as you go! Need help? Reach out for personalized advice.

4th March, 2025

www.virtualdataworks.com

# BUSINESS CONTINUITY AND DISASTER RECOVERY

## CRITICAL CAPABILITIES INCLUDED:

- Backups as often as every 15 minutes
- Local virtualization in seconds
- Appliance-free option with Cloud backup for disaster recovery and endpoint protection
- Recovery Point Objective of 15-minutes
- Recovery Time Objective of less than 1-hour
- No data corruption worries because your backup is chain-free

Watch our Datto Backup introduction video to discover its features and understand why it's essential for your business!



**WATCH NOW**

**DITCH OUTDATED BACKUPS!**

Upgrade your strategy with our cutting-edge solutions.



## TOTAL DATA PROTECTION BY VIRTUAL DATAWORKS

**Business Continuity:** Beyond Backup  
Ensure your business is always protected with the most reliable and cost-effective BCDR solution. Data protection and business continuity should be accessible to every business.