Research › Exclusive by Ivica | How to share your most sensitive data securely (without losing your mind)?

21

September 2021

Tuesday

Exclusive by Ivica | How to share your most sensitive data securely (without losing your mind)?

In **Research**

0 Comments

What is File Sharing? It is the act of allowing two or more people who have been given access to the same file to share that file with other people.

There are **many ways** that you can put your personal or business information at risk when using the Internet. One of the most common ways is through email. Anyone can send an email message to another person without them ever knowing it came from you. Using a free email account for important communications is not recommended. Instead, you should consider another form of communication, such as by phone or face-to-face.

If someone else is monitoring the emails going out from that account, they can see all the email addresses you are sending messages to. This will give them a link to click on to find out who you are and send you an email message. This is called a “phishing” attack and is a very serious form of identity theft.

The more information you reveal about yourself, the more the identity thief knows about you. We have all seen or heard about the news reports about identity theft. Identity theft and credit score ruin have happened to people. For some, their lives have been **completely ruined by identity theft.**

So, sharing file is great, but don’t forget about security.

Sharing files is common for small businesses, but it’s important to do so securely to protect sensitive data

There are many services you can use for secure file sharing, including Dropbox, Google Drive, Box.net and SkyDrive. If you use a paid service like Dropbox or Box.net, we should point out to hat the owner of the site you are sharing files on **cannot see** what files you are sharing. He can only see your shared folders that contain text files. He will not know how many large graphic files you are sharing or how large those files are. There is no way for him to know if you are sharing proprietary information that belongs to you or to someone else.

If you choose to use a paid service for secure file sharing, be sure to use NOT a free email account for that purpose. Someone can easily send you a link that appears to be from you, but is actually installing malicious software on your computer, if you’re using a free email account. Malware is a real threat and the number of online threats is rapidly increasing.

The most important rule is: invest in security and do not underestimate your company or the information you share.

How can you be sure the information you store on the cloud is safe?

The short answer is **you can't.** However, there are some steps you can take to protect yourself.

Here are few tips for protecting your data that will help you get a handle on the cloud privacy problem.
Tip #1: Use a password-protected folder

When you share your files with others through the cloud using the "Share" button, you are giving them access to those files through your account. Your files will still be accessible even if you change the password later. Using a password protected folder will prevent this from happening.

Tip #2: Use the "View" option

If you share a file and give others the "View" option, they can still see the file… But… they cannot download it or open it. The file can only be viewed by them. You can use this option for files that are confidential and you don't want everyone to see.

Tip #3: Encrypt your data

Data encryption involves encrypting data (information) into a format that cannot be read. It's like putting a lock on your data. A software program is used to do this (that you probably already have on your computer) called "encryption software" or "encryption program".

Types of File Sharing>

1. File Transfer Protocol (FTP)

An older standard for file sharing. It's still in use today and works with most any FTP server. WebDAV (a more recent standard) is also used for file sharing but works only with Web-based file servers.

2. Peer to Peer (P2P)

File Sharing When two or more people use P2P for file sharing, there is no connection to a central server. Instead, both of them acts like a server for the other users. They all share the work of keeping their files up to date and available to everyone else. P2P is great for people whose files are very time-sensitive, such as sales presentations, project work, etc. Since there is no central server holding everyone up, you can get the most current versions of files when you need them. However, because there's no central server keeping everyone in check, P2P may lead to rampant piracy.

3. Store files in the cloud

…but keep them on your local computer. If you use the cloud to share files, you should remember that it is NOT the same as sharing these files on your own computer or storing them on a server you control. Despite paying for the service, there is still the chance that something will happen to your account, leading to all your files being inaccessible. Many companies offer "cloud" services for sharing files. These services are like the email hosting services, except that you can upload files instead of sending emails.

Backing up your files is crucial whether you use P2P or not. You should also test your backups and restore procedures regularly. If you use more than one computer, test restoring files from different computers and make sure they work as expected.

There are also email providers through which you can share files and removable media like USB, like wetransfer or plustransfer.

10 tips to protect your confidential data on the cloud and beyond

1. Evaluate the confidential data you keep
2. Encrypt sensitive data
3. Physically secure your devices
4. Treat passwords seriously
5. Watch for Bluetooth vulnerabilities
6. Beware of public Wi-Fi
7. Update your operating system regulary
8. Back up your data
9. Securely dispose of your devices

10. Simply, don’t share confidential data

Conclusion

In today’s world, **data sharing is a must**. It makes our work processes easier and faster, allows us to network with different people, no matter where they are in the world. It encourages us to be more efficient.

But, always that but. Don’t overlook security. Do not forget the many thefts that have happened and are still happening in the history of the Internet. Also, **don’t forget to make your network sites as secure as possible**.

______

Article by Ivica Delic
founder of FreelancersTools,
exclusively for Virusdie.

Join our private Facebook group to get help from other security experts, and share your own web security experiences and expertise. Group members receive exclusive news and offers. They can also communicate directly with the Virusdie team. Join us on Facebook.

Comments

Search form

Type and hit Enter...

Tweets by @VirusdieCloud

Categories

Add-on for WHMCS 1

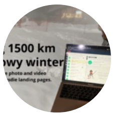
API and Integrations	1
Company	15
For partners	2
Malware and Threats	4
News	42
Patch manager	1
Research	22
Uncategorized	1
Updates	65
Website Cleanup	8
Website Firewall	5
Website malware check	4
Website protection	4

LATEST

POPULAR

Exclusive by Ivica | How to share your most sensitive data securely (without losing your mind)?

21 September 2021



Behind Virusdie | How we made a 1500 km flight to snowy mountains to make unique media content for the new Virusdie landing pages!

17 September 2021

Exclusive by Ivica | What are WordPress vulnerabilities and why every security breach can cost you time and money.

15 September 2021

Exclusive by Ivica | 10 most famous WordPress' security myths revealed.

31 August 2021

Exclusive by Ivica | 27 tips to keep your WordPress websites secure.

24 August 2021

Contacts

Narva maantee 5, Kesklinna linnaosa, 10117 Tallinn, Harju maakond, Estonia

☎ 8 800 770 07 63

✉ support@virusdie.com

SAAS TOOLS

- Website Antivirus
- Website Firewall
- Blacklist monitoring
- External Site Scan
- Built-in File manager
- Built-in File editor
- RegEx/Text Search
- Automatic backups

SOLUTIONS

- Malware Detection
- Malware Removal
- Website Protection
- Blacklist Removal

FOR AGENCIES, EXPERTS AND DEVELOPERS

- Website Security Tools
- Special Plans for Agencies
- Start Site Security Business
- Affiliate program

FOR SOFTWARE VENDORS AND SERVICE PROVIDERS

- Stand-alone Web-Antivirus
- Kit for Software Vendors
- External Site Scan API
- SaaS Deep Level API
- File Cleanup API

FOR HOSTING PROVIDERS

- Antivirus for Shared Hosting
- Expert Cyber Security Center
- Module for ISPmanager
- Imunify360 for Servers

FOR ALL CUSTOMERS

- Complete Website Security

Ask us for advice if you doubt to choose which solution is best for you: partners@virusdie.com

HELP & SUPPORT

- Helpdesk
- Incurable file analysis

Use tickets or write on: support@virusdie.com

ABOUT US

- How it Works
- Our story
- Terms of use
- Privacy policy
- For media
- Contacts
- Security
- Blog

English

Monday - Friday 10:00 - 18:00

☎ 8 800 770 07 63

✉ support@virusdie.com