

Tech Tuesday: Protecting Your Cloud

April 12, 2022

A graphic with a dark blue background featuring a circuit board pattern. In the center, there is a faint, circular seal of the Federal Bureau of Investigation. The text is white and bold. The title 'TECH TUESDAY: Protecting your Cloud' is at the top. Below it is a list of five bullet points. At the bottom left is the FBI logo and the text 'FBI FEDERAL BUREAU OF INVESTIGATION'. At the bottom right is the text 'Portland Field Office'.

TECH TUESDAY: Protecting your Cloud

- **Backups:** Make sure you have a well-tested backup plan in place to guarantee a quick recovery in case of an attack.
- **Monitor Upgrades:** Keeping an eye on your cloud hosting provider's upgrade schedules ensures no exploits exist for hackers to take advantage of.
- **Take regular inventories of what you keep in the cloud:** Up-to-date inventories are essential to data management. As you add data that may require more protection, re-evaluate your security settings and amp them up accordingly.
- **Don't store personal information when it's not necessary:** Ask "Do we have a legitimate need to store this information?" If the answer is no, dispose of it securely. No one can breach what you don't have.
- Report fraud to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

Welcome to the Oregon FBI's Tech Tuesday segment. Today: Building a digital defense to protect your cloud.

You probably keep a lot in the cloud today. Between preparing for tax season and home refinancing, you could be sitting on a pile of PDFs, all full of detailed personal information. So how secure is your cloud?

Here are a few steps you can take directly in the cloud to keep your private information as secure as possible.

- **Backups:** Make sure you have a well-tested backup plan in place to guarantee a quick recovery in case of an attack. So, opt for a hosting package that includes regular backups.
- **Monitor Upgrades:** Keeping an eye on your cloud hosting provider's upgrade schedules ensures no exploits exist for hackers to take advantage of.
- **Take regular inventories of what you keep in the cloud:** Whether you store data in the cloud, on your network, or in a file cabinet, you can't keep data safe if you don't know where it is. That's why up-to-date inventories are essential to data management. As you add data that may require more protection, re-evaluate your security settings and amp them up accordingly.

- **Don't store personal information when it's not necessary:** As you conduct that inventory of what you keep in the cloud, resist the temptation to hold on to data "just because." Instead, be ruthless in posing the question, "Do we have a legitimate need to store this information?" If the answer is no, dispose of it securely. No one can breach what you don't have.
- **Protect Your Data:** Have the latest versions of the best antivirus, anti-malware and network security technology in place. Always go for a company that takes its server and network security seriously.

Also remember to follow basic cyber hygiene rules:

Use multi-factor authentication and strong passwords to protect against the risk of unauthorized access.

Avoid accessing sensitive data using public networks and devices

Encrypt sensitive data

If you are the victim of an online fraud, you should report the incident to the FBI's Internet Crime Complaint Center at www.ic3.gov or call your FBI local office.