OUCH! August 2021

SANS SECURITY AWARENESS

The Monthly Security Awareness Newsletter for You

# Securely Using the Cloud

## Overview

You may have heard of a concept called "the cloud." This means using a service provider on the internet to store and manage your data. Examples include creating documents on Google Docs, accessing email in Microsoft O365, sharing files via Dropbox, or storing your pictures on Apple's iCloud. While you access and synchronize your data from multiple devices anywhere in the world and share your information with anyone you want, you often do not know and cannot control where your data is physically stored.

## Selecting a Cloud Provider

Cloud services are neither good nor evil. They are tools for getting things done. However, when you use these services, you are essentially handing over your private data to strangers, expecting them to keep it both secure and available. As such, you want to be sure you are choosing your service provider wisely. For work-related information, check with your supervisor to see if you are allowed to use cloud services and which ones are authorized. If you are considering using cloud services for personal use, consider the following:

1. **Trust:** Can you trust the cloud provider? Is this a well-known, public company that millions of people are already using, or is this a small, unknown company based out of a country you never heard of?
2. **Support**: How easy is it to get help or have a question answered? Is there a phone number you can call or email address you can contact? Are there other options for support, such as public forums or Frequently Asked Questions on their website?
3. **Simplicity**: How easy is it to use the service? The more complex the service is, the more likely you will make mistakes and accidentally expose or lose your information. Use a cloud provider you find easy to understand, configure, and use.
4. **Security**: How will your data get from your computer to the cloud service? Is the connection secured by encryption? How is your data stored? Is it encrypted, and if so, who can decrypt your data? As you migrate your data, remember security is a shared responsibility between you and the vendor.

5. **Compatibility:** Does the service provider support all of the devices and operating systems that you use or are planning to use?
6. **Terms of Service**: Take a moment to review the Terms of Service (they are often surprisingly easy to read). Under which country's laws does the service provider operate? Pay particular attention to rights that you cede to your service provider.

## Securing Your Data

The next step is to make sure you use your cloud services properly. How you access and share your data can often have a far greater impact on the security of your data than anything else. Some key steps you can take include:

1. **Authentication**: Use a strong, unique password to protect your cloud account. If your cloud provider offers two-step verification, we highly recommend that you enable it.
2. **Sharing Files / Folders**: Cloud providers make it very simple to share data - sometimes too simple. It can be very easy to accidentally share your information publicly. Protect yourself by only allowing specific people (or groups of people) access to specific files or folders. When someone no longer needs access, remove them. Your cloud provider should provide an easy way to track who has access to your files and folders.
3. **Settings**: Understand the security settings offered by your cloud provider. For example, if you share pictures, files, or a folder with someone else, can they share your data with others without your knowledge?
4. **Renew**: Do not forget to renew your subscription or you could lose access to your data.

## Guest Editor

Tameika Reed (@womeninlinux), Founder of Women in Linux. She leads initiatives with a focus on exploring careers in infrastructure, cybersecurity, DevSecOps, and leadership. She hosts a weekly meetup with topics ranging from Infrastructure to Blockchain. She has spoken at OSCon, LISA, Seagl and HashiConf EU.

## Resources

Social Engineering Attacks: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Making Passwords Simple: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Password Managers: https://www.sans.org/newsletters/ouch/password-managers/
Power of Updating: https://www.sans.org/newsletters/ouch/the-power-of-updating/