OUCH! | September 2014

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- Overview
- Selecting a Cloud Provider
- Securing Your Data

Using the Cloud Securely

Overview

"The Cloud" is a powerful technology that both people and organizations are rapidly adopting. "Cloud" can mean different things to different people, but it generally means using a service provider on the Internet to store and manage your data for you. An advantage of the Cloud is not only can you easily access and synchronize your data from multiple devices anywhere in the world, but you can also share your information with anyone you want. The reason we call these services "The Cloud" is you often do not know where your data is physically stored. Examples of Cloud computing include creating documents on Google Docs, sharing files via Dropbox, setting up your own server on Amazon Cloud or storing your music or pictures on Apple's iCloud. These online services have the potential to make you far more productive, but they also come with unique risks. In this newsletter, we cover how you can securely leverage the Cloud.

Guest Editor

James and Kelli Tarala (**@isaudit** / **@kellitarala**) are principal consultants at Enclave Security and have authored numerous SANS training courses, including SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls and MGT 415: A Practical Introduction to Risk Assessments.

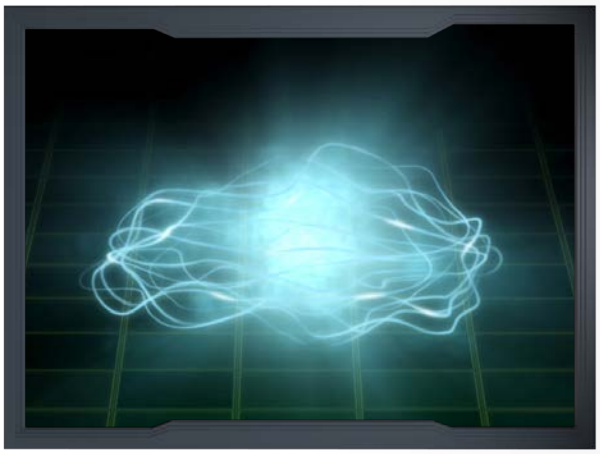
Selecting a Cloud Provider

The Cloud is neither good nor evil; it is a tool for getting things done, both at work and at home. However, when you use these services, you are handing over your private data to strangers and you expect them to keep it both secure and available. As such, you want to be sure you are choosing wisely. For your work computers or work-related information, check with your supervisor to see if you can use Cloud services. If you are allowed to use the Cloud, please be sure to confirm which Cloud services you can use and what the policies are on how to use them. If you are considering a Cloud service for your personal use, consider the following:

1. **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?

Using the Cloud Securely

2. **Simplicity**: How easy is it to use the service? The more complex the service is, the more likely you are to make mistakes and accidentally expose or lose your information. Use a Cloud provider you find easy to understand, configure and use.
3. **Security**: How will your data get from your computer to the Cloud? Is the connection secured by encryption? How is your data stored in the Cloud? Is it encrypted? If so, who can decrypt your data?
4. **Terms of Service**: Take a moment to review the Terms of Service. (They are often surprisingly easy to read.) Confirm who can access your data and what your legal rights are.



The Cloud can make your information more accessible and help make you more productive, but be careful how you store and share your information.

Securing Your Data

Once you have selected a Cloud service, the next step is to make sure you use it properly. How you access and share your data can often have a far greater impact on the security of your files than anything else. Some key steps you can take include:

1. **Authentication**: Use a strong, unique passphrase to authenticate to your Cloud account. If your Cloud provider offers two-step verification, we highly recommend that you enable it.
2. **Sharing Files/Folders**: The Cloud makes it very simple to share -- sometimes too simple. In a worst-case scenario, you may accidently make your files or even entire folders publicly available to the entire Internet. The best way to protect yourself is to not share any of your files with anyone by default. Then only allow specific people (or groups of people) access to specific files or folders on a need-to-know basis. When someone no longer needs access to your files, remove their access. Your Cloud provider should provide an easy way to track who has access to your files and folders.
3. **Sharing Files/Folders Using Links**: One common feature of some Cloud services is the ability to create a web link that points to your files or folders. This feature allows you to share these files with anyone you want by simply providing a web link. However, this approach has very little security. Anyone that knows this link may have access to your personal files or folders. If you send the link to just one person, that person could share that link with others

Using the Cloud Securely

or it could show up on search engines. If you share data by using a link, be sure you disable the link once it is no longer needed or, if possible, protect the link with a password.

4. **Settings**: Understand the security settings offered by your Cloud provider. For example, if you share a folder with someone else, can they share your data with others without your knowledge?
5. **Antivirus**: Make sure the latest version of your antivirus software is installed on your computer and on any other computer used to share your data. If a file you are sharing gets infected, other computers accessing that same file could also get infected.
6. **Backup**: Even if your Cloud provider is backing up your data, consider making regular backups on your own. Not only does this protect your data should your Cloud provider go out of business, be shut down or for some reason be inaccessible, but it can be much easier to recover large amounts of data from your local backup than it is pulling it down from the Cloud. Also, confirm how frequently your Cloud provider backs up your files. Do they allow you to recover prior versions of your files? How long do they keep your backups available?

SANS Network Security 2014

Join SANS Institute, the world's most trusted source for computer security training, at Caesar's Palace in Las Vegas October 19-27 for Network Security 2014! Choose from more than 40 hands-on, immersion-style security training courses taught by real-world practitioners. Learn more at https://www.sans.org/event/network-security-2014.

Resources

Strong Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
Backups:	http://www.securingthehuman.org/ouch/2013#september2013
Security Terms:	http://www.securingthehuman.org/resources/security-terms

License