The Cloud

Cloud services can help our organization be more productive, but they also come with additional risks. As such, please be sure to follow these steps whenever working with cloud services.

This newsletter is published by Villanova University's security team.
For more information, please contact us at:

support@villanova.edu

UNIT INNOVATIVE
TECHNOLOGY SOLUTIONS & SERVICES

The Cloud

The cloud is a powerful technology that our organization uses. Cloud computing is nothing more than using an outside service provider to store, manage or process our data. The reason we call this service "the cloud" is you never know where our data is physically stored. It is being served somewhere in the "cloud." Examples of cloud computing include creating documents on Google Drive, sharing files via Dropbox or storing your music or pictures on Apple's iCloud.

Solution

Cloud services enable our organization to be more productive, but they also come with additional risks. As such, please be sure to follow these steps whenever working with cloud services.

Permission

Ensure that you have permission before using any cloud technologies and that you use only organization-approved cloud vendors. Do not sign up for a new service without permission. Also, be sure you understand our policies on which information can and cannot be stored in the cloud and whom you can share it with.

Personal Cloud Accounts

Ensure that any work-related data is never copied or stored on any of your personal cloud accounts, such as Apple's iCloud or your personal Dropbox account. In addition, do not access any personal cloud accounts from work computers or devices unless you have prior permission.

Unique Password

Use a unique password for each of your cloud accounts. If your cloud service supports two-step verification, we highly recommend you use it. This adds an additional layer of protection to your account. Never use the same password for your cloud accounts as any of your personal accounts.

Configuration

By default, configure your cloud account so that it does not share information or files with anyone. Only share specific files with specific people or groups of people who have authorization and a need to know that information. Once they no longer need access to those files or information, remove their access to the data.

Anti-Virus

Be sure you scan any shared files with anti-virus before opening them. Since the cloud may be storing these shared files on other people's computers, these files may be infected, as other people may not have the same level of security as you. For example, an organization was once sharing files through the cloud with several different people. One of the individuals did not have their computer secured and accidently infected it and all of their files, including any files shared through the cloud. The virus worked by encrypting all the files, then demanding the organization pay a ransom to decrypt them. Since these files were shared over the cloud, it meant that all the shared files on everyone's computers were infected and encrypted.

Administration

Be careful what rights or privileges you assign to others. Some cloud services not only allow you to share files, but allow you to assign administrative rights to other people. This means you can give people you are sharing your files with the ability to allow others to access or edit them. Only give people the least amount of access they need to get the job done. If you have any questions about which cloud services you can use for work or what data can be shared and with whom, please ask your supervisor or information security team.

Sharing Files Using Links

The cloud is an amazing tool for sharing information; however, you can easily share the wrong information with the wrong people (or even the entire Internet). One common feature of some cloud services is the ability to create a web link that points to files or folders on your computer. This feature allows you to share these files with anyone you want by simply providing a web link.

The problem with this method is that there is very little security. Anyone that knows this link has access to your personal files or folders. If you send the link to just one person, that person could share that link with others or Google could harvest it. Before you know it, anyone can access the files. If you are authorized to share data by using a link, be sure you disable the link once it is no longer needed.

This newsletter is published by Villanova University's security team.
For more information, please contact us at:

support@villanova.edu

UNIT INNOVATIVE TECHNOLOGY SOLUTIONS & SERVICES