Security Awareness / Trends
July '16

OFFICE 365 SECURITY

Secure Use of Office 365

What are the concerns

Microsoft announced in its first quarter 2016 earnings report that there are 18.2 million Office 365 subscribers. With this wide adoption, it is not surprising that attackers would turn their attention to such a large target. Just this past June, Microsoft's platform was hit with a massive ransomware attack. Moving to cloud based applications and services does not eliminate cyber threats nor does it remove the need for formal security guidelines and controls. We need to take the appropriate steps to prevent loss of data due to accidental disclosure or cyber-attacks.

To accomplish Information Service's goal to provide secure and reliable systems, all users need to be aware of the risks and also how to avoid them. The most commonly used Office 365 applications are Email and OneDrive.

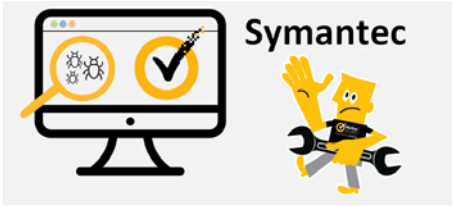
Using OneDrive at JCCC

How can OneDrive be used as a secure storage location for JCCC data? OneDrive for Business does encrypt data in its environment. However, because OneDrive is a cloud-based file storage and sharing utility, its use presents some potential risk to JCCC data.

- Data stored in the cloud can be accessed by any workstation or mobile device with access to the Internet.
- It is difficult for JCCC to govern how OneDrive is being accessed by non-college computers or Internet connections.
- Access to files and shares is largely managed by the user and it is possible to accidentally share files to those without appropriate rights.
- Access to files and shares can be granted to non-JCCC users using the "Get a link" option presenting another avenue for potential data loss.
- When using synchronization tools with a non-college device, sensitive data may be at risk of disclosure.

JCCC is adopting a new Data Classification policy and procedure. Guidelines will be published with this policy to help educate when it is appropriate and how to save restricted or sensitive data in OneDrive. Caution also needs to be exercised when using synchronization tools on non-college devices. If restricted data is synchronized to these devices it increases the chances of disclosure.

How is data backed up in OneDrive? The default retention policy in OneDrive is to retain deleted files for 30 days before they are permanently deleted. Microsoft also retains a file version history so that older copies of a document may be restored.



Responding to threats

On June 30th Information Services responded to a security advisory for our anti-virus product. In response an update was pushed to staff workstations to mitigate the threat. You may have noticed the pop-up message to reboot their workstation to complete the installation. An InfoList message was also sent to raise awareness regarding the update and the need to restart the workstation. The speed at which Information Services was able to respond was thanks in large part to the central monitoring and configuration systems in place along with internal cooperation, sound processes and procedures.

Doing our part

IT Security is everyone's responsibility and at times Information Services will send out targeted updates/announcements in response to security threats. Be sure to read these announcements and if you have questions, please call the Help Desk for assistance. As a result of this latest incident here is how we did as an institution.

Within 24hrs of the vulnerability being disclosed Information Services had begun its response. We tested the fix to ensure no adverse effects would be introduced, a message was drafted to announce the change, and then the update was pushed to more than 1,200 devices. As of July 24th, 90 percent of these devices had received the fix.