Understanding the Essential 8: A Guide for End Users

What is the Essential Eight?

The Essential Eight are a set of strategies designed to provide a baseline for cybersecurity. They include:

1. **Application control**: Only approved applications are allowed to run within our network.
2. **Patch applications**: All applications are regularly updated to their latest versions to fix security vulnerabilities.
3. **Configure Microsoft Office macro settings**: Macros can be used maliciously. Configuring these settings can prevent such attacks.
4. **User application hardening**: Features in Microsoft Office, web browsers, and PDF viewers that can be exploited are disabled.
5. **Restrict administrative privileges**: The number of users with administrative privileges is minimized.
6. **Patch operating systems**: The operating system is regularly updated to its latest version to fix security vulnerabilities.
7. **Multi-factor authentication**: More than one method of authentication is used.
8. **Daily backups:** Important data is regularly backed up.

How Will This Affect You?

The implementation of the Essential Eight will have some impact on your daily work, but it is designed to provide a safer and more secure digital environment for everyone.

- **Application Control**: You may notice that some applications you previously used are no longer available. This is because we are only allowing approved applications to run on our network.
- **Patch Applications and Operating Systems**: There may be more frequent updates to your applications and operating system. While this may cause minor disruptions, it is crucial for maintaining the security of our systems.
- **Configuring Microsoft Office Macro Settings and User Application Hardening**: Some features in your applications may be disabled. If you find that a necessary feature has been disabled, please contact the IT department.
- **Restricting Administrative Privileges**: Some users may find that they no longer have administrative access to their systems. This is a necessary step to reduce the potential damage from a breach.
- **Multi-factor Authentication**: You will be required to use more than one method of authentication. This could be something you know (like a password), something you have (like a security token), or something you are (like a fingerprint).
- **Daily Backups**: Your work will be backed up daily. This ensures that we can recover your data in the event of a ransomware attack or other data loss event.

We understand that these changes may require some adjustments. However, they are crucial for protecting our organization and your work from cyber threats. We appreciate your understanding and cooperation.

The Essential Eight for Security program :

Below are some pre-recorded webinars from Microsoft to explain in a little more detail.

1. The Essential Eight for Security Explained – View On Demand
2. The Essential Eight for Security in Practice, Multifactor Authentication & Restrict Admin Privileges - View On Demand
3. The Essential Eight for Security in Practice, Daily Backups - View On Demand

https://info.microsoft.com/AU-SCRTY-CATALOG-FY21-02Feb-14-TheEssentialEightforSecurityinPractice-SRDEM61939_CatalogDisplayPage.html