Shinn Technology Services Corporation

P.O. Box 173
Fishers, IN 46038

(317) 545-3650
http://www.ShinnTechnology.com

Windows 10 Security & Privacy
_____

Windows 10 Profiles

When you purchase a new computer, you have a choice on the initial setup to configure a Microsoft account profile or a local offline profile. NOTE: Some businesses that have an onsite Microsoft server will login to a domain rather than a local workgroup. Our practice is to setup a local offline profile and it comes down to user security and privacy.

Microsoft implemented the Microsoft account profile back in Windows 8. It was meant, by giving Microsoft certain rights to your environment, to help provide a better environment and user experience. It is also a way to catalog and organize all of your Microsoft licenses to include MS Office and other MS App Store purchases. By using a Microsoft account profile, you are giving Microsoft rights to monitor your application usage and other data collection it deems needed to "enhance" your user experience.

When using a local offline profile, you are minimizing the data collection process and keeping all your apps and software local to the computer you are working on. For us it comes down to minimizing "Big Brother" looking in on your computing environment. You can still use a Microsoft account to inventory your software licenses, but it doesn't have to be linked to your active computing profile. *See the next article below for more privacy information*.

When you first turn on a new computer you will be asked to enter an email address or create a new Microsoft account. In small print at the bottom of the page will be "create an offline account". You will again be prompted to login to a Microsoft account…. again, in small print at the bottom of the page, choose local account. From there you will enter a username and password for your new profile. Follow the prompts to complete the profile setup. Microsoft is tricky in trying to get you to use a Microsoft account… just keep looking for the options of offline and local.

Windows 10 Data Collection and your Privacy

Microsoft has been criticized by the industry for its data collection process and techniques. This section will give you privacy information and settings that need to be updated on all Windows 10 computers. Microsoft, by default has diagnostic data settings set to FULL. That means the following information "could" be gathered and reported back to Microsoft: hardware configuration, hardware components, system error messages, user usage logs to include application use, songs listened to, movies watched, games played, web browsing history and local file searches. Microsoft declares that "typing input could be used to reconstruct the original content or associate the input to the user" (could tie your activity to your real name).

Here are some settings to change for better privacy

Click on the white Windows icon in the bottom left of your screen
Type   Privacy Settings   and press the Enter key

> *Click on General on the left menu*
> > Turn the first four options OFF

> *Click on Diagnostic & feedback on the left menu*
> > Change the setting from Full to BASIC (there is no way to turn off all reporting to Microsoft)

> *Tailored experiences section*
> > Turn this setting OFF

> *View diagnostic data*
> > You can set this option to ON and install the Diagnostic Data Viewer from the App Store. It will show you what information has been sent to Microsoft. It's kind of cryptic, but you can see general info.

> *Delete diagnostic data*
> > You can click the Delete button to remove all reporting data collected on your computer and the copies that have been sent to Microsoft. I do this weekly on my personal computer--- just to make sure minimal information is being sent.

> *Feedback frequency*
> > Change this setting to Never

We don't believe that reporting data to Microsoft is all bad. Some of the data collected from the masses has helped create better updates and patches for Windows 10 as well as better conduits to the wide varieties of application software being used today… but they certainly don't need to monitor your internet usage and be able to see me on my webcam while I'm working.

NOTE: There are many ways for hackers to gain access to your webcam through malware and viruses. If you are concerned about your webcam, put a piece of black electrical tape over it when you are not actively using it.