



AITS Newsletter

DECEMBER 2017

Should I Embrace an iPhone X or an Android? [By Abraham John, Executive Director, AITS]

I am usually not a technology platform evangelist. Since I come from the viewpoint of using technology that best addresses the problem and provides is benefit to my University, departments and users, it has never been too difficult to look at the various technology products in a dispassionate manner.

I tend to follow the same mode of thought when it comes to personal technology as well. Recently I had to make the choice of moving away from a Windows phone to something else. The Windows phone was a choice based on price and the productivity tools available on the device. The ecosystem at the time when my iPhone 3G left for cell phone paradise, wasn't as militaristic as it is now. The Windows phone still had a sliver of a chance. Well those days are no more! The choices are iOS or Android. Even Bill Gates, whose name is synonymous with Microsoft has moved to an Android device. It is understandable in Mr. Gates' case since the choice of an iPhone, may have had repercussions that affected Microsoft's share price if word leaked out that Mr. Microsoft was making calls using an iPhone.

So my choices were whether I should iPhone X or not or perhaps I should embrace the Android world. However, reason and not emotion prevailed in my decision 😊. My 3G, sitting lifeless in my desk drawer, reminded me about the elegance of Apple products and the complexity that is hidden by the very clean user interface (UI) Apple tends to have with its products. The quality of their hardware is beyond reproach. The step that Apple took towards using facial recognition as the method of unlocking the iPhone X was compelling from a technology perspective since they did not hedge their bets. This is tantamount to coming to a new world and then burning the ships. I found this commitment and confidence in their technology intriguing.

I'm sure you've already guessed by now that an iPhone X is in my very near future and I'll have follow-up articles detailing my iPhone X adventures.



I am eagerly looking forward to using Apple's flagship iPhone product – so perhaps not so dispassionate after all and yes, I know, fluff article this...!

As you read the articles included in this issue of our newsletter, we in Administrative Information Technology Services (AITS) wish you a happy and safe holiday season.



Cisco's iPhone launched 22 days before Apple's iPhone. The companies settled the trademark lawsuit initiated by Cisco and both kept rights to the iPhone name.

Enterprise Applications ERP vs. Best of Breed

[By Dorothy Flores]

In the world of enterprise applications, there has been a long-running debate about whether organizations should use an ERP system for core administrative business needs, or select from “best of breed” solutions for each particular business function and build integrations between them. Considering that an ERP (Enterprise Resource Planning) is a collection of applications built to work together using delivered data integration technology, it’s no wonder that many organizations have opted for a solution with a consistent “look and feel” across all functionality in terms of the user experience.

Selecting the “best of breed” for a finance system, human resources, and a student information system, for example, can present the user community with a disjointed experience and the need to learn how to navigate and work differently in each application. Terminology can also be different across those solutions, adding to possible frustration and confusion for users, as well as the technical staff who support them.

To put this into context regarding the UNT System organization and EIS, in 2002 the leadership of the System and campuses chose to move from a 35-plus year old mainframe system to a distributed platform called PeopleSoft, which is an ERP system. The final decision was based upon the desire to implement an industry-leading solution that would be viable for years to come, deliver the business functionality needed for students, employees, and financial management, while providing users with a consistent experience across all applications. And, from that decision, EIS was born in 2003 starting with Finance, then HCM (HR/Payroll) and Portal (my.unt.edu), and finally the Student system in 2004. CRM (for student recruiting) was added in 2007 and ELM (learning management for employees) in November 2017.

Apple's arch-rival Samsung makes the processors that power the iPhone.



When thinking about ERP systems that have an application for a student information system, there are very few options available, even now. Those are primarily Ellucian’s Banner systems and the Oracle’s PeopleSoft system, with up-and-coming cloud options from Oracle (Student Cloud; pieces released 2016) and Workday (released Sept. 2016). Interestingly enough, for an organization the size of the UNT

System, and specifically UNT, Banner and PeopleSoft are still considered the “best of breed” in student information systems, but Oracle and Workday could be close behind in a few short years. Maybe even Salesforce will a contender someday, as they move more into the higher education market, and with the announcement this year that they are teaming up with FinancialForce and ADP to offer a fully integrated solution.

As with many universities, the strategy to stay with an ERP for the UNT System has remained constant over the years, but assessments have been done periodically to ensure that this is still, overall, the right approach for the organization. Moving to a new ERP solution is no small undertaking...it is costly and time consuming. But sometimes it makes business sense to invest in a “best of breed” solution and integrate with the ERP; case in point, moving from the PeopleSoft CRM application to Salesforce. Routinely assessing current and future business needs against the enterprise application technology landscape is key to ensuring that those needs are being met, whether the answer is an ERP or “best of breed.”

This past summer Facebook chatbots Alice and Bob developed their own language of their own accord. A language the creators of the bots did not understand. Facebook directed the bots to stop creating languages!

EIS Fun Facts

EIS recorded 16,894 training courses completed by 6,373 employees during 2017.

EIS indicates active employees represent over 65,000 years of state service.

EIS says the “typical” student is a continuing senior, non-white female, 24 years old, enrolled in 11.7 hours.

EIS handled 9,947,525 student logins over the past year.

EIS processed \$197,810,397.76 in student payments over that same time-period.

Enjoy this brain teaser 😊

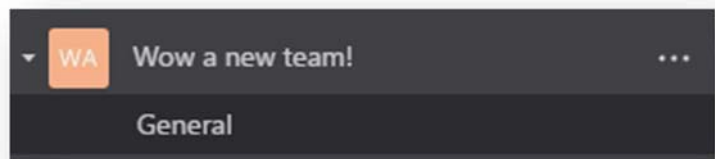
In special instances a apple costs 20¢, a banana costs 30¢ and a grapefruit 40¢. What do you suppose a pear costs?

Microsoft Teams [By Matthew Berry]

Microsoft Teams is a messaging program where everyone in the group can access conversations, files, and important information. It functions, by default, as a chat room but can quickly be changed into a voice-chat enabled meeting space. AIT has found it indispensable in day-to-day operations where we need to discuss something quickly. Traditional email becomes too bloated of a resource with out-of-sync threads when too many people become involved.

By utilizing a Teams channel effectively, you can vastly improve the collaboration of everyone on the team. Information, which needs to be disseminated quickly, can be posted in the general channel and this will reach every member on their Desktop and phone. It's built into the pre-existing O365 account framework which allows quick additions of users to the channel and group at large. A new teams channel can be setup very quickly!

But perhaps the best feature are the new tabs you can add which can house a multitude of different informational sources. Excel sheets to PDFs, powerpoint slides, and even an entire OneNote file.



With a wide-variety of bots to choose from every need you can imagine can be filled in one way or another. Try it out!

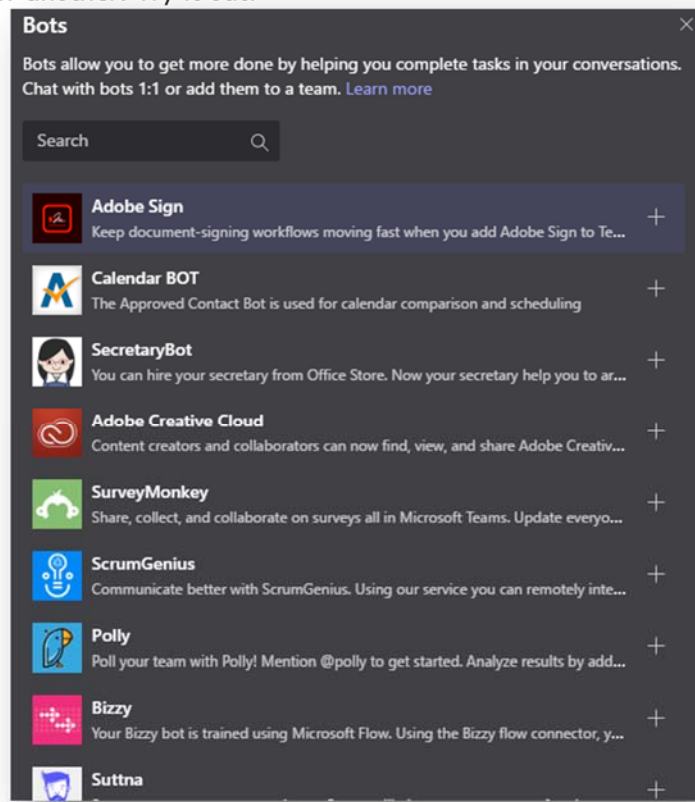


Figure 1 Wow so many bots!

Virtual Reality Training [By Matthew Berry]

VR has seen great strides in recent years: it has transitioned slowly from being expensive technology that only extremely high-end machines can run to an enthusiast's (expensive) hobby. The advent of cheaper alternatives to PC headsets for PlayStation have helped shift it even further into the layman's comfort zone. It now has a wide variety of uses from video games to accurate training in simulations.

However, what is VR? Many VR hardware developers related that describing VR to someone that has never experienced it is like "dancing about architecture." You put on the headset and you are immediately in a different world. The headset deceives your eyes, easily, and you immediately get a sense of depth perception in a world that only exists inside 3 inches of glass. The effect is so accurate that you still require your glasses. This realism coupled with the controllers that give you remarkable hand presence has caught the attention of many. Apple just recently announced its' partnership with HTC to use the new iMacs as a development platform. Facebook acquired Oculus, one of the first VR companies, in 2014 for \$2 Billion.



Terry Virts
@AstroTerry

Follow

Testing a new virtual reality system. It puts you "in" the #ISS. Best part is that stuff "floats" just like in space



6:33 PM - 23 Jan 2016

NASA has shown great interest in the HTC Vive headset in regards to its' Mixed Reality program. The positional tracking and room-scale nature of the HTC Vive system allows NASA to create photo-realistic simulations of the ISS for training purposes. When exposing previous ISS crew to these simulations they rated it favorably stating it was a very believable scenario.



3 Developers can quickly 3D print objects out of cheap material and rely on VR to give it a realistic look for high-fidelity

The Knights Hospitallers were founded in the early 12th century and are contemporaries to the Templars.

VR allows companies, like NASA, great cost-saving opportunities for training. By relying heavily on the graphics of an application for accurate models they can rapidly prototype 3D printed, low-cost, objects that only need to feel correct. By making the physical object low-fidelity and tracked with a VR device they can rapidly create high-fidelity objects in applications such as Unreal Engine to quickly and cheaply execute an idea.

The future of VR appears to be prosperous, at least for important training simulations, and I expect one day our field will be involved with certain aspects of supporting it. Luckily, it is making great advances lately and we have already made it past the prerequisite that you need to strap a laptop to your face in zero gravity.



In 1785 Fredrick the Great signed a Treaty of Amity and Commerce with the United States of America, recognizing the new nation. A novel clause in the agreement guaranteed a special and humane detention for prisoners of war.

Asset Protection [By Larry Worthy]

At the University of North Texas, we have various types of assets that require protection and have a choice of controls to protect the asset depending on the risk. All protection controls are designed to provide the best control at the best cost. The strength of controls protecting \$10,000 would be materially more significant than those protecting \$50. Here's a quick look at various assets and how we provide protection.

Cash. Cash is a frequent target because with cash you can buy anything else you want. It's hard to trace and, in smaller quantities, don't raise suspicions. Cash does take many forms such as currency, credit / debit cards and electronic transfers. Each type of cash requires different controls. For example, a \$100 change fund just needs physical security controls such as storing in a cash register or safe. Protecting cash in your bank account requires physical security controls provided by the bank and logical access by controlling account passwords and debit / ATM card PIN number.

Inventory. Threat of loss of inventory items must be evaluated to determine the level of protection. For example, the loss of a case of asparagus may be low as there are no known asparagus theft rings. Therefore, we wouldn't acquire a vault to safeguard asparagus. However, dining services may develop a control to store asparagus in a cool environment to extend shelf life and employ a stock rotation system to minimize out of date product. A 65-inch television is another matter. While not something we would keep in a safe we do implement controls ensuring it doesn't "walk off". We might attach it to the wall and keep the door locked.

Data. Data is the most difficult asset to protect because you can't see it and can be taken (copied) and you may never know. Our data protection controls are extensive ranging from passwords to role based access controls to segregation of duties to data backup. In addition to theft, we employ controls to safeguard data from loss due to equipment failure and natural disaster. The Information Technology folks have developed an extensive method to backup data and store offsite to ensure lost data can be recovered.

People. Yes, people are an asset, actually the most important asset. We have controls in place to protect us too. For example, when a person takes cash to the cashier for deposit we require them to conceal the deposit in a nondescript bag. We actually care less about the cash than we do the person.

Controls range from simple controls such as locking doors and using safes, to complex passwords to dual custody of highly pilferable assets. A common control is segregation of duties where the authorization, custody and record keeping functions are separated between different employees. Controls only keep honest people honest and can be circumvented. Control is a constraint that comes with a cost so we don't always employ the most effective control, we implement the most efficient.

With all this said about protecting assets, controls are not infallible. People are going to steal and we can only control how much. Our goal of control is to make theft hard enough people will look elsewhere for a place to steal. Assume two houses side by side. One house is well lit, an alarm sign out front, windows secured and bushes trimmed. The other house is dark, windows open, bushes overgrown and several newspapers in the drive. Which presents an easier target for a thief?

Over the course of the next few articles, we will explore asset protection in more depth.

Our solar system had an interstellar visitor recently. An asteroid that astronomers are calling A/2017U1 or Oumuamua swept in from interstellar space. Unlike other asteroids this one is cigar shaped and is 800 meters long.



Machine Learning Defined [By Daniel Wiersema]

We used to hear about Artificial Intelligence, most in movies, but there are many different types of Artificial Intelligence. One of the most common ones that everyone uses is Machine Learning. It is everywhere from in our phones to commercial flights. Machine Learning at the most simplistic definition is a computer program that is designed to learn from experiences and predict. So this could be something we take for granted now days like traffic software. The data is being collected and outputted to your phone, but it is also predicting when there could be traffic with the info it has. I have seen this happen, when I don't run into traffic or the time to destination takes less time than the app says. Something else that uses Machine learning and is similar to traffic is commercial flights. The flights use Machine Learning to make flight plans and it is even being used in auto pilot. So we rely so heavily on Machine Learning, but we never really think about it.

Machine learning is far from perfect right now as everyone has probably experienced in your phone assistants, like Alexa and Siri. But it has come a long way. Think a few years ago and they could not even understand half of what you are saying. Now it does work, just not all the time. If the improvement continues one day we might all have a personal Artificial Intelligence assistant like Tony Stark in Iron Man.

Did you know that the ADA programming language was named after Augusta Ada, Countess of Lovelace?



UNT Facilities Department's Computerized Maintenance Management System, TMA [By Ginger Boone and Clint Mills]

To ensure the buildings and grounds of campus are kept looking good and running smooth takes a lot of record tracking and coordination. In 2007, the Facilities department purchased a Computerized Maintenance Management System (CMMS) to handle this task, TMA Systems. To put several acronyms together, TMA is the CMMS that is used by UNT.

Recently the Facilities Department has embarked on a journey to improve the CMMS to provide for more accurate data tracking, more robust reporting, and better access to technicians and end users. At the heart of any good data-based system is of course, accurate data. Several changes have been made to streamline what is being input in the system such as reworked drop-down lists, removal of unused and outdated task types, and the introduction of well-defined priority standards.

In addition to the above changes we are also working on updating the location information, parts inventory tracking, and project tracking. These updates will allow everyone that uses the CMMS to search for information more quickly and complete their tasks faster.

Another recent development is the introduction of mobile access to the CMMS for the technicians. By providing the technicians with tablets they now have the ability to view and update their work orders while in the field. This means faster updates to the customer, more information collected by allowing pictures to be uploaded, and much less paper being used. It also allows the technicians to keep more up to date on departmental/university events and more organized by connecting them with their email and calendar.

And in an effort to make requesting and tracking service easier for all of campus, a new Online Work Order tool will be implemented soon! This will allow anyone to enter requests for work and look at the status of any requests they may have made. Stay tuned for more information on this in a future communication.

The Egusi melon seeds are composed of almost 50% edible oil and 30% pure protein. This little melon's seeds pack quite a protein wallop.



Bitter melon, which originated in India, and was introduced to China in the 14th century is widely used in East Asian, South Asian and Southeast Asian cuisine. Yum!!!



Drone Usage for Disaster Recovery [By Alan Garrison]

As drones become a more common sight, there are increasing numbers of uses. Initially, drones were expensive devices that just a few people purchased to fly as a personal hobby. Since prices came down and more models were developed, drones have become more popular and the FAA has begun implementing more restrictions to control the airspace and prevent incidents with commercial aircraft. Currently, the FAA reports that there are over 20,000 licensed drone pilots nationwide in a program that just began a year ago.

Recently, drones have increased in usage following large disasters to help with assessing damage and planning for disaster recovery. This significantly helped Hurricane Harvey relief efforts in Houston earlier this year. Oil and gas companies used drones to assess their facilities and utilities to get production resumed as soon as possible. Pilots working on behalf of local government agencies also surveyed roads, bridges, and other utility systems for damage. Insurance companies are also using drones to assess damage to help with claim processing in a much faster method.

The National Guard along with Customs and Border Patrol also used drones to assess damage in Florida following Irma, which allowed it to prioritize resources to the areas that needed it most and identified roads and infrastructure that needed attention before residents could return home.

Closer to home, Professor Namuduri from UNT Department of Electrical Engineering has developed a drone system that is capable of providing cell phone communication systems to disaster hit areas. In a prior test, his drone utilized an emergency response bandwidth allocation, allowing first responders connecting to his drone top priority on all available cell phone traffic.

Through the innovation work of everyone from UNT professors to staff at insurance companies, local governments, and private companies, there is a combined focus on improving response time to help disaster victims start the recovery process as quickly and efficiently as possible. In a relatively short period of time, the hobby of flying drones has now turned into official relief efforts to help those in need.

Sources:

- https://www.wired.com/story/houston-recovery-drones/?CNDID=%%CUST_ID%%&mbid=nl_090417_daily
- <https://fcw.com/articles/2017/09/18/irma-drones-faa-rockwell.aspx>
- <https://news.unt.edu/news-releases/unt-demonstrates-first-ever-drone-provided-cell-service-disaster-response>

Data Breaches [By Matthew Fenton]

We have all heard about the Equifax data breach on the nightly news, but what exactly does it mean? A data breach is “the intentional or unintentional release of secure or private/confidential information to an untrusted environment.” They are becoming more and more common and have a great deal of impact on our daily lives. 2017 alone has seen over seven major data breaches across the world. To be clear, we are not referring to situations where a consumer, accidentally infects a computer with a virus or unintentionally provides information to hackers. The goal of this article is to discuss the necessary forfeiture of personal information to parties we trust – including retailers, healthcare providers, financial institutions, Internet service providers, and even the government – and their ability, or lack thereof, to protect this data.

Equifax is a consumer credit reporting agency and collects information on over 800 million individual consumers and 88 million businesses worldwide. According to the Federal Trade Commission, hackers gained access to Equifax’s systems in mid-May and maintained access until July. The information accessed included names, social security numbers, birth dates, addresses, and even driver’s license numbers. In other words, Equifax collects and stores our most important personal data with the expectation that it will be properly protected. Clearly that trust is being violated.

We continue to find that even a small amount of negligence or disregard for best practices can lead to malicious worldwide events.

What can be done?

Unfortunately, aside from suing or acts of Congress, the outlook from an individual’s perspective is fairly grim. There are, however, actions that can be taken to prevent already stolen data from being misused. Below are some recommendations from the Federal Trade Commission.

- **Check your credit reports** from Equifax, Experian, and TransUnion — for free — by visiting annualcreditreport.com. Accounts or activity that you don’t recognize could indicate identity theft. Visit IdentityTheft.gov to find out what to do.
- **Consider placing a [credit freeze](#) on your files.** A credit freeze makes it harder for someone to open a new account in your name. Keep in mind that a credit freeze won’t prevent a thief from making charges to your existing accounts.
- **Monitor your existing credit card and bank accounts closely** for charges you don’t recognize.
- If you decide against a credit freeze, **consider placing a [fraud alert](#) on your files.** A fraud alert warns creditors that you may be an identity theft victim and that they should verify that anyone seeking credit in your name really is you.
- **File your taxes early** — as soon as you have the tax information you need, before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.

Visit <https://www.identitytheft.gov/Info-Lost-or-Stolen> for more information.

Did you know that the sugar apple flesh is luscious but the seeds are toxic?



ITSS and the University of North Texas – Expanded Lab Access for Students and VDI for staff and faculty [By Gordon Albury]

Enabling greater student success through anywhere, anytime application and desktop access.

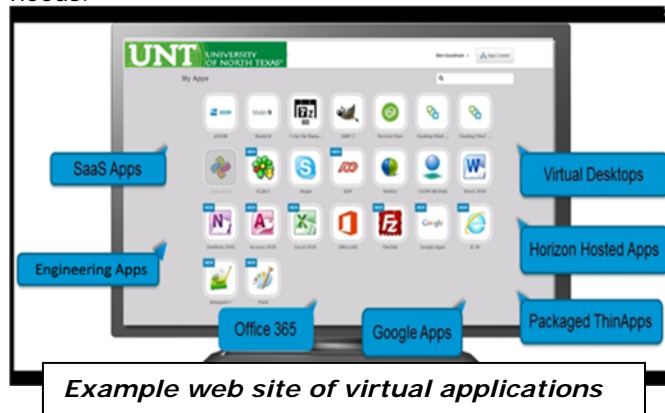
ITSS supporting the University of North Texas (UNT) with multiple colleges, utilizes traditional classrooms and lab rooms for many technical courses. UNT has a rapidly growing student population especially at the Denton campus, as well as a growing body of remote or distant students. Enabling all these students to access critical applications at any time on their own devices is a key goal to enabling their success as students.

In the past, students could only access the high end, complex and graphic intense applications on special PCs in classrooms and labs which had limited space and limited hours. Students had to plan their schedules around access to these labs and the software therein installed. Some courses allowed students to purchase temporary licenses for installation on their own devices, but most students did not have the expensive powerful laptops to run top graphics and math packages. The access to the labs presented a barrier not only to on campus students, but working and remote students as well.

Solution:

Creating virtual computer labs allows students to use their own devices at times that are convenient to them, and from any location enabling greater success and flexibility. The powerful hardware needs are provided by UNT on ITSS servers so that students can access that software remotely on almost any device including Chromebook, iPad and most all laptops, at any time. Built on VMWare's Horizon View Enterprise edition with NVIDIA GRID and VMWare App volumes, ITSS and the university are able to solve the issues for students both on and off campus. Horizon View is a unified platform that provides not only virtual application access, but also virtual desktops giving exceptional user experience and high performance graphics virtualization. "We have not only greatly expanded classroom and laboratory software access, but are also able to virtualized desktops for staff and faculty". UNT Staff desktop PCs are now easier to maintain and when replacement time comes, low-cost zero clients can be used saving cost and management support needs.

Did you know that the most venomous fish in the world is the Stonefish and is found in the coastal regions of the Indo-Pacific?

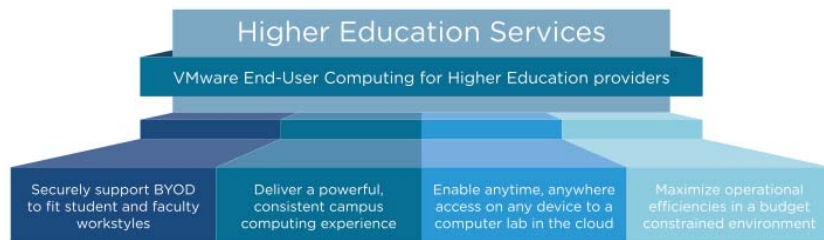


The virtual labs include provision for some of the top intensive applications today including SPSS, Esri ArcGIS, Adobe Creative cloud software, MathWorks MATLAB, and many more. This enables support for multiple colleges from College of

Engineering, College of Information Science, College of Arts and Science, and many more. UNT's continually accelerating growth in the North Texas area and to remote students worldwide is in part empowered by these solutions.

Continuing Success:

By supporting remote students as well as adding flexibility to on-campus students, UNT is able to improve the student, staff and faculty experience. This not only encourages and enables working students to continue at UNT, but enables growth and opportunity for distant students. UNT can add more students and allow them to study around-the-clock without adding costly 'brick-and-mortar' infrastructure, and better use what we have. The initial pilots and classes have been very successful and a growing list of faculty and staff wish to join the program.



The ITSS Virtual Desktop for End User Computing service vision

I'll bet you don't want to see this coming towards you or step on it! A stonefish relies on its speed to hunt.



The Babel Fish Is Real [Jennifer Lee]

For those who are not a fan of Douglas Adams' "Hitchhiker's Guide to the Galaxy" series, the Babel Fish is a plot mechanism used by the author to enhance believability of the situation by the reader. While originally a fictional construct in a science fiction universe, humans have managed to, yet again make fiction fact.

The first incarnation of this mythical fish was found as the AltaVista Translation Service. It allowed a person to enter plain text or a web link that would be magically translated with the simple of a button. Of course, there were issues with accuracy, however this was still a major step in removing language barriers worldwide.

Fast forward twenty years. The original Babel Fish website is now defunct, but progress has been steadily made in the interim by many sources, the most well-known being Google. Buzz has recently increased surrounding several purveyors of in-ear devices (thank goodness these ones are removable and not slimy) that work in conjunction with a mobile device to allow users instant translation of multiple languages. Some models use proprietary hardware while others use downloadable apps. Regardless, this new technology opens up new avenues of communication across a multitude of situations. It should not go unsaid that there is also a unit that is stand-alone (does not rely on bluetooth or wi-fi), but limited to eight languages for translation.

Little by little, the technologies we read about and dreamed of are becoming a reality. I can't wait to see what's next!

On September 21st, Microsoft and Facebook announced the completion of a 4,100 mile cable from Virginia Beach, Virginia to Bilbao, Spain.

ADA Compliance in Technology Projects [Keith Kellermeier]

Compliance with the American Disabilities Act across the University of North Texas is becoming increasingly important. As UNT expands, so does our population of students with disabilities, ranging from physical handicaps to visual impairment. These are all covered by ADA and ADAAA, and many UNT students are examples of these disabilities. ADA is not only about non-discrimination and equal opportunity, but also about safety.

By the end of this calendar year, we will have added over 20 new signage displays and almost doubled our Point-of-Sale devices within Dining Services since January 1, with the majority being added at the University Union. The Union is one of the most publicly accessible buildings on campus, and with this accessibility comes the concern about ADA compliance. As more and more technology projects are developed on campus, we need to remember to comply with ADA rules and regulations. This is not only to comply, but to keep our students happy and safe using our customer-facing technology.

Dining Services has been persistent in implementing self-service kiosk concepts throughout their entire operation – from Discovery Park all the way to the Union. These kiosks require shelving and additional space to hold not only the ordering modules, but the printers, credit card readers, campus card readers, and any other necessary peripherals. This requires the construction of additional shelving/counter space into public walkways. With all this equipment, shelving would have to extend up to 12 inches into walkways and could create a safety risk to someone who is visually impaired. Having new construction fail ADA compliance can result in disabled students getting hurt, excluding disabled students from the opportunity to use the self-order system, and also could pose risk to the technology involved in these concepts being damaged.

As a solution, we have begun implementing pole-mounted solutions for our self-ordering kiosk concepts all over campus. This will reduce the footprint of all existing concepts to reduce safety concerns for the visually impaired and also create a more wheelchair accessible kiosk concept. Plus, these pole-mounted solutions create a more aesthetically pleasing look:



As we continue to build innovative projects across campus for the departments we support, let us keep in mind those of us less fortunate, and make all of our student's experiences equal, accessible, and one of a kind.

Did you know that Tasmanian Devil's are monogamous? How can you not have a soft spot for an animal that is the epitome of grouchy!



Mobile Security [By Mickie Tate]

As our society becomes increasingly more mobile, maintaining information security on our mobile devices also becomes more challenging. In this article, we will discuss protecting information on mobile devices when in public settings. We are given a lot of information about being vigilant in our awareness of types of attacks involving social engineering such as phishing and more targeted attacks such as spear phishing. And well we should be as these attacks are very prevalent. But I'd like to talk about ways of being more proactive and not being a participant in handing over information to data thieves. How do we protect our mobile devices and the information on them?

When I first started to write this article my only thought was what happens when we travel to foreign countries with our devices and how are they scanned and potentially attacked when in countries that have a reputation for state sponsored cyber-attacks. But I was reminded of what happens when you're in your favorite coffee shop, a hotel, or doctor's office trying to get some work done making the most of available time. While I have had some security professionals tell me that you can be assured that your mobile device has already been compromised and scanned before you have left the airport in some countries, we would be remiss to not acknowledge and be aware of the threats that face us in our everyday lives. So what are some of the things we can do to help ensure the information on our mobile devices is protected?

Did you know that bulldog ants have very good vision and will chase an intruder a good distance away from its nest and its sting will make fire ant stings feel like butterfly kisses!



1. Ensure that you frequently dock your laptop to your docking station to ensure the device is receiving all of the current updates. Our laptops within the UNT Enterprise contain anti-virus and encryption software as part of the internal build process but the anti-virus software needs frequent updates to ensure the virus definition files are current. If you are uncertain if your machine has anti-virus and encryption installed, reach out to your IT representative and they will be able to validate the services are installed and running correctly.
2. Sensitive data should not be stored on mobile devices, but if there is a situation where the data must be stored there, the device must be encrypted.
3. When connecting your device to a wireless access point in a public setting, verify the access point is the one supported by the business you are visiting. It is very easy for someone (perhaps sitting right next to you) to set up a rogue access point that mimics (spoofs) the name of the business you are visiting such as adding guest or guest1 (or any other modification) to the name of the legitimate access point supported by the business. If you are in doubt, ask the business proprietor for the name of their wireless access point.
4. When connecting or accessing the UNT network, always use the Virtual Private Network (VPN) for access. This creates a secure virtual private tunnel to prevent compromises such as man in the middle attacks to further protect your (UNT) data.

In today's environment there is probably no such thing as being 100 percent secure, but we can certainly do everything in our power to make it as difficult as possible for cyber thieves to gain access to our information. Below are some links to IT security policies regarding mobile device security:

UNT System Policy 8.100, Section 3.

UNT System Information Security Handbook,

- 6.2.5 Custodian (Responsibilities)
- 11.4.5 (Operating System Access Control, "overriding system and application controls")

- 11.6 Mobile Computing and Teleworking
- 12.4 Cryptographic Controls
- 16.2 Data Protection Laws

International Traffic in Arms Regulations (ITAR)
Export Administration Regulations) (EAR)
NIST 800-171

Tough ant!



Windows 10 Home PC Maintenance Tips [By Matthew Trammell]

With the holiday season approaching, some of you might be hoping to upgrade your desktop or laptop. Or, perhaps you already have a desktop or laptop that is in need of some holiday cleaning. In either case, I hope to provide you with some tips and free software that you can use in order to help keep your new computer or old computer running smoothly for years to come. In this article, I use Windows 10 Home to demonstrate. If you have Windows 7 or another version of Windows 10, these tips still apply, but the steps may differ.

Before we get started, I have a few disclaimers:

- These tips are for use on your personal (non-UNT) computers. Apply them at your own risk
- If you have any questions or concerns about your UNT computer, please contact your respective IT support department
- If you have questions about any of the tips, steps, or software titles that I mention, please research them and/or contact your preferred IT support contact (friend, family, or business)
- Due to my capacity within the university, I am unable to work on computers for current UNT employees and students

Now that is out of the way, we can move forward to the tips!

Tip 1: Make your primary account a non-administrator account

One thing I come across, when working on computers for my family or friends, is that their primary account is also their administrator account. This is generally not a good idea because say your computer gets infected, despite your good intentions to not get it infected; your administrator account has access to more files and directories, including system files, than a standard account. Thus, an infection has a much better chance of affecting your entire computer. This can lead to you having to reinstall Windows and possibly losing your personal files and installed programs and settings in the process.

Microsoft encourages you to create an online account so you can access your documents, Internet favorites, contacts, and other files from any computer that you log on to. I am good either way you choose. However, for increased security, I prefer to use local accounts and keep my Windows account information local to my computer. Then, I can choose to log in to my cloud accounts such as OneDrive. In this way, I have more control over the information I choose to store online. I do like the cloud as a method to back up my files to an offsite location.

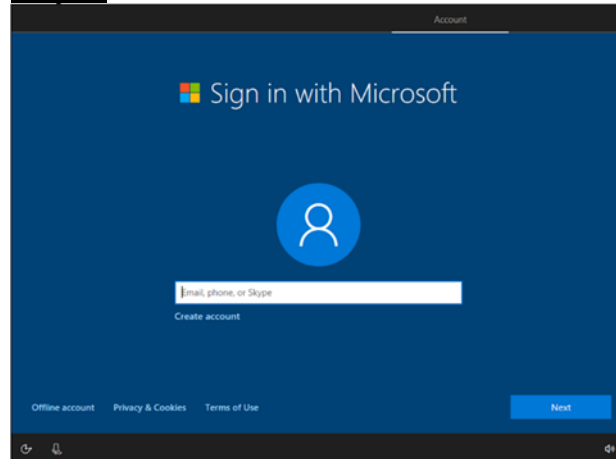
Creating Your Administrator Account

Initially, when you setup your computer, you will go through a set of initialization steps. One of those steps is to create your administrator account. If you are following along with your old computer, you can advance to the next section on Creating Your Non-Administrator Account. Still with me? Great! If you have Windows 10 Home, you will see the following screen. Let us set up your administrator account! First of all, I recommend creating an offline, local account:

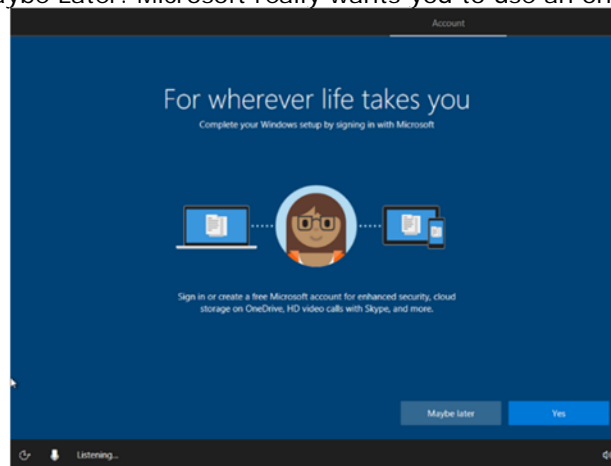
Did you know that the codename for Windows 10 versions 1607, 1703 and 1709 is Redstone?

*Prince Siddhartha
originated Buddhism
in northeastern India
in the 6th century
B.C.*

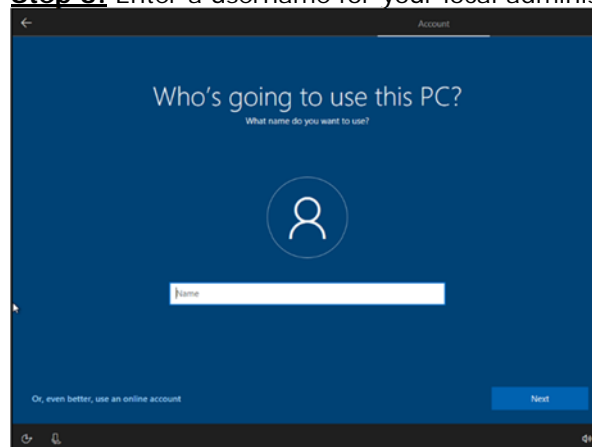
Step 1: Click Offline account



Step 2: Click Maybe Later. Microsoft really wants you to use an online account!

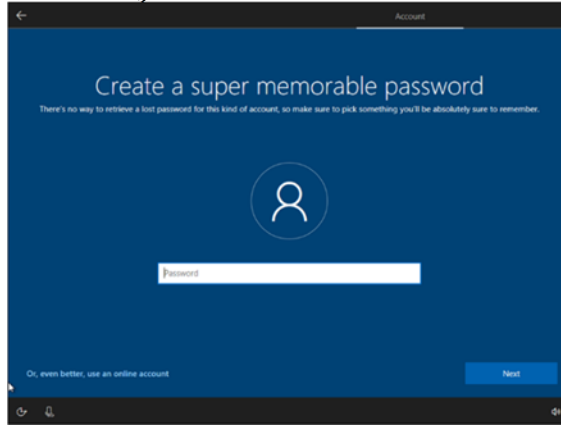


Step 3: Enter a username for your local administrator account



Name your account whatever you like, something like <Firstname>-Admin. For example, I chose to name my local administrator account Matt-Admin.

Step 4: Enter a password for your administrator account

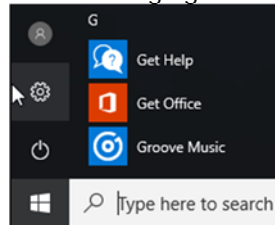


Be sure to create a strong, secure password that you can remember for your administrator account. Our April 2017 Newsletter has a great article titled "How Secure Is Your Password?" where Troy Bacon writes about using passphrases to help create a more secure password.

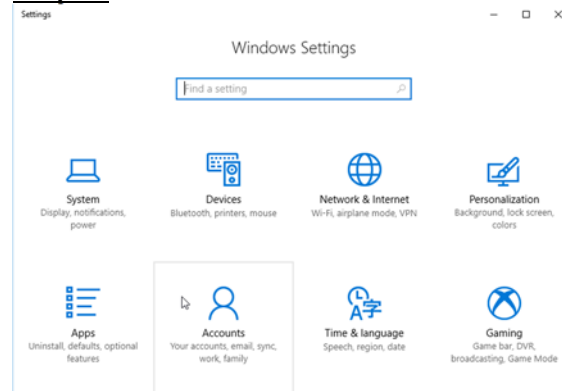
Creating Your Non-Administrator (Standard) Account

Now that you have your administrator account, let us go through the process of creating your local, standard account. If you are joining me here with your old laptop, chances are you already have an administrator account set up. Stay with me as this process is more complicated than it needs to be. Microsoft is really encouraging us to create online accounts!

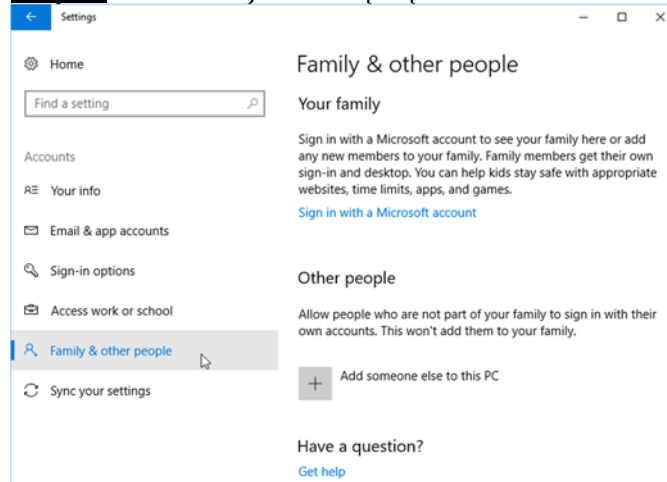
Step 1: Press Start and click on the Settings gear icon



Step 2: Click on Accounts



Step 3: Click Family & other people

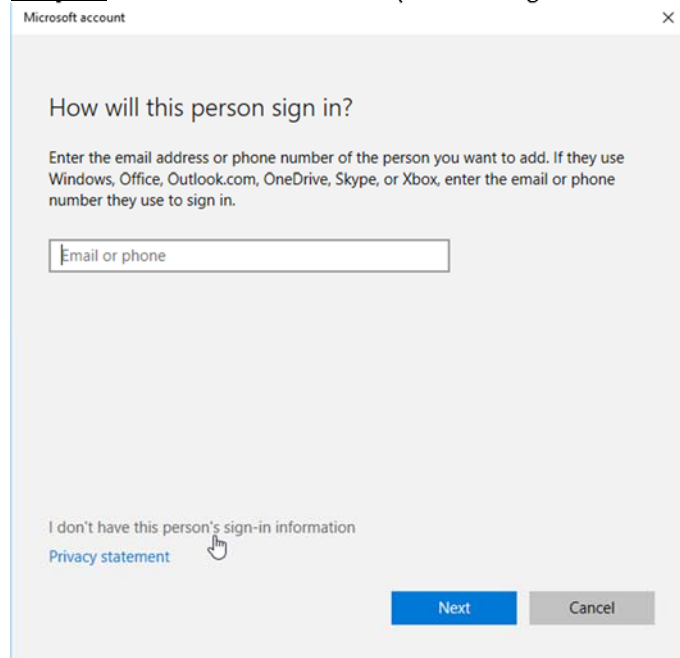


Step 4: Under Other people, click the plus sign to add someone else to the PC
Other people

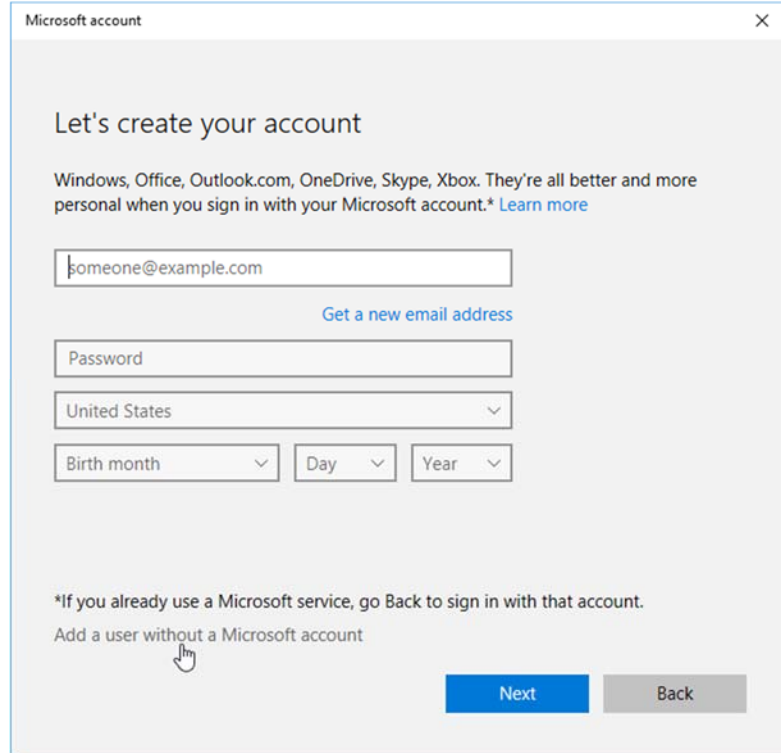
Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.



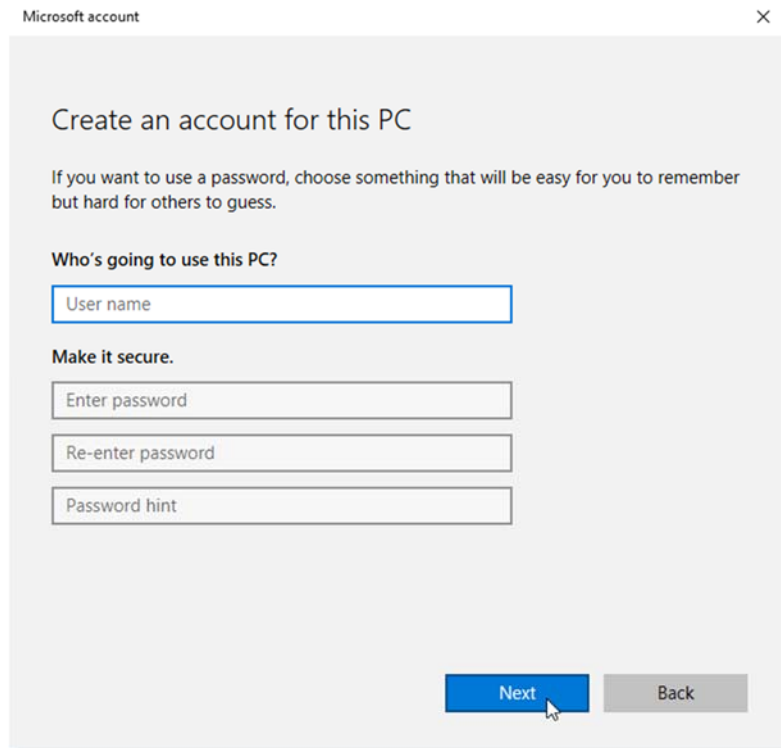
Step 5: Click "I don't have this person's sign-in information"



Step 6: Click "Add a user without a Microsoft account"



Step 7: Enter the information for your local account. I called my administrator account, Matt-Admin. I will call my user account, Matt. Once done, click Next.

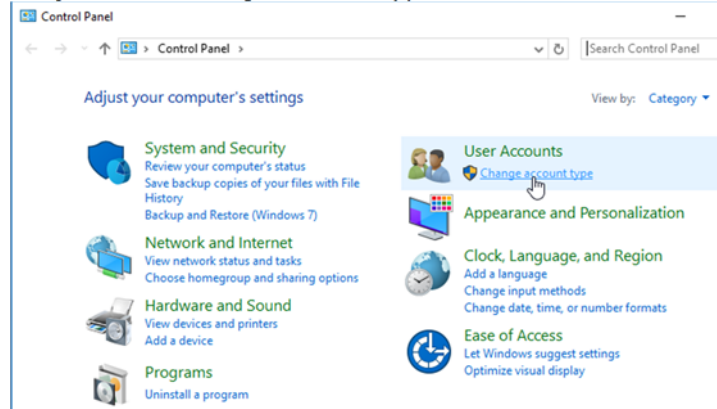


Verify Account Types

Now that we have created our standard account, let us quickly check the permissions for each of our accounts.

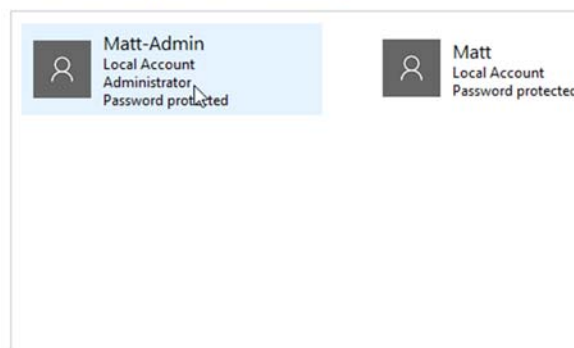
Step 1: Open Control Panel: Press Start. Search for Control Panel. Then click Control Panel.

Step 2: Click Change account type under User Accounts



Step 3: Verify that your administrator account shows the "Administrator" label. Your primary account should not have the "Administrator" tag.

Choose the user you would like to change



Add a new user in PC settings

Make Changes to User Account

If you need to make changes to one of the listed accounts, click on the account name.

Make changes to Matt's account

- Change the account name
- Change the password
- Change the account type
- Delete the account
- Manage another account



If you have an old computer, your administrator account may already have tons of personal files under it. No worries! Simply follow the steps under Creating Your Non-Administrator (Standard) Account to create a new administrator account, named appropriately. Then you can use Make Changes to User Account to change the account type.

Step 1: Change the account type of your newly created account to Administrator.

Step 2: Change the account type of your old administrator account to Standard. Now that you have a standard account created, log out of your administrator account and start using your standard account! Should you need to install a program, access a folder location, if a program requires elevated permissions, simply enter your administrator credentials as requested.

Tip 2: Install one Antivirus program on your computer

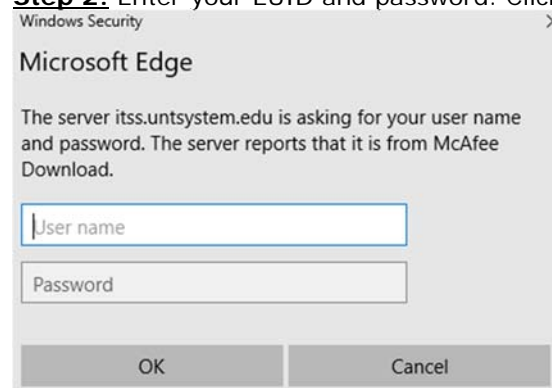
I have also run into cases where I have seen multiple Antivirus programs installed on a computer. Having more than one primary Antivirus program can slow down your computer, especially if both programs are actively scanning your computer and competing for system resources. If you have more than one Antivirus program, pick one and uninstall the others. Fortunately, Windows 10 comes with decent Antivirus solution, Windows Defender. So, you do not need to rush out and purchase an Antivirus program. If you do have a preferred Antivirus program, Windows Defender will disable itself once you install that program and let your preferred program protect Windows. Windows Defender does have a neat feature called Periodic scanning where Windows Defender scans your computer periodically in conjunction with your primary Antivirus program.

Installing UNT's McAfee Endpoint Encryption

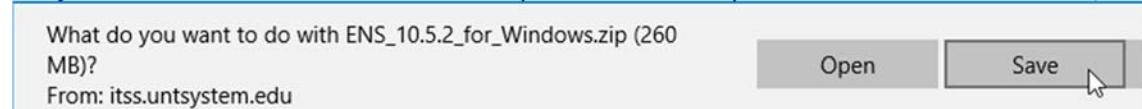
I do want to highlight that UNT Information Technology and Shared Services has McAfee Endpoint Security available for download to students, faculty, and staff with a valid EUID, for free.

Step 1: Download McAfee from:
<https://itss.untsystem.edu/divisions/mrs/is/antivirus-download>

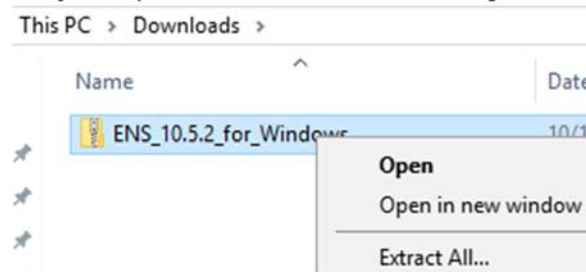
Step 2: Enter your EUID and password. Click OK



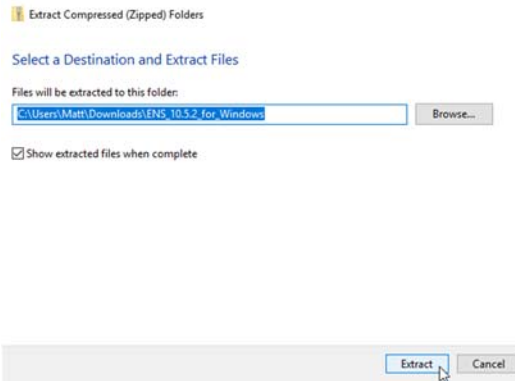
Step 3: Save the download. Downloads by default save to your Downloads folder



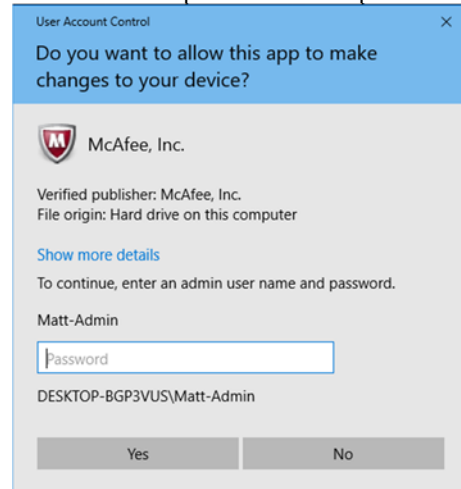
Step 4: Open the Downloads folder. Right click on the zip file and select Extract All



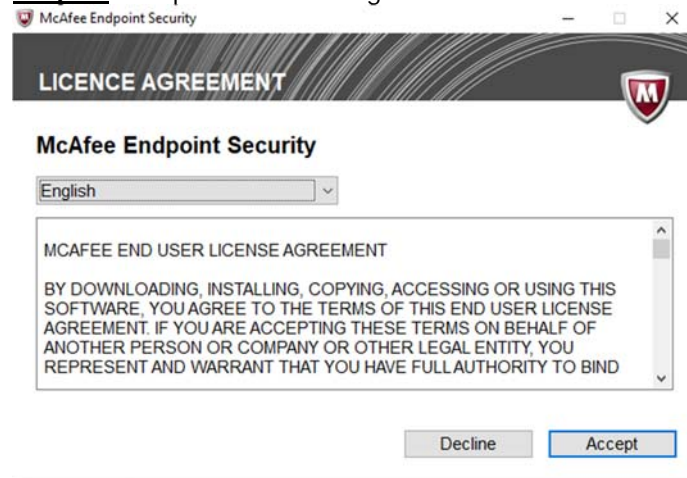
Step 5: Extract the files. Click Extract.



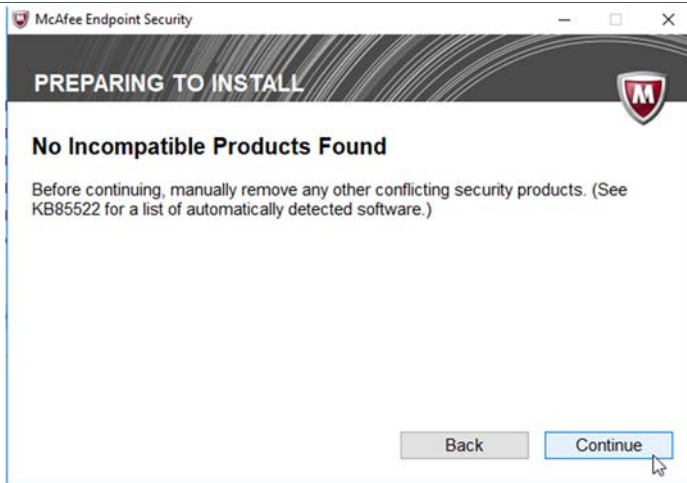
Step 6: Run setupEP.exe. If you are on your Standard account as I mentioned in the previous tip, you should see a dialog asking for credentials. Enter your administrator password and press Enter



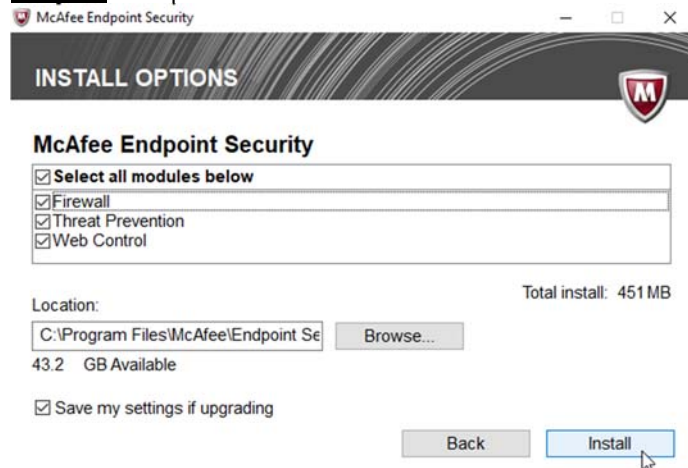
Step 7: Accept the License Agreement



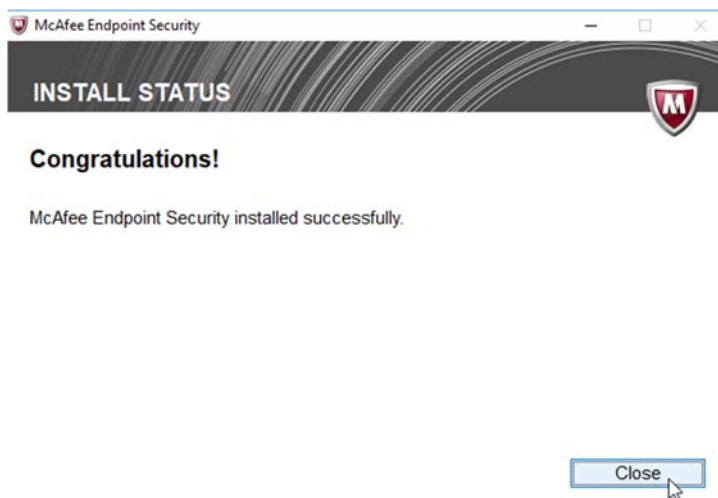
Step 8: McAfee Endpoint Security will scan for incompatible products. Click Continue once finished



Step 9: Accept the defaults and click Install



Step 10: Once the install completes, click Close

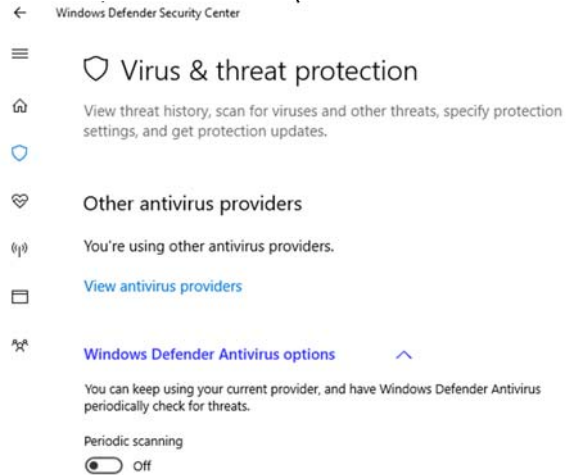


Turn on Window's Defender Periodic Scanning

I mentioned earlier that Window's Defender can scan your computer periodically in conjunction with your primary Antivirus provider. If interested, you can turn it on using the following steps:

Step 1: Launch the Windows Defender Security Center app

Step 2: Click on the shield, Virus & threat protection



Step 3: Click the arrow by Windows Defender Antivirus options

Step 4: Turn Periodic Scanning on. In order to turn this option on, you will need to enter administrator credentials

Tip 3: Protect your computer from malware with Malwarebytes and Microsoft Safety Scanner

Unfortunately, Antivirus software is not enough to fully protect your computer these days. Attackers are constantly trying to find new ways to obtain your critical information. In fact, it is more likely that your computer will get some other malware infection over a virus infection. You should use software tools such as Malwarebytes and Microsoft Safety Scanner to help protect your computer. If I see that a computer gets a virus on it, I am always going to run an Antimalware software tool on it as well.

Installing Malwarebytes

If you search for Antimalware software, Malwarebytes will show up at the top, if not close to the top, of the list. It is one of the best programs for detecting malware. And best of all, it is free for personal use.

Step 1: Navigate to <https://www.malwarebytes.com/> or search for Malwarebytes and click the link

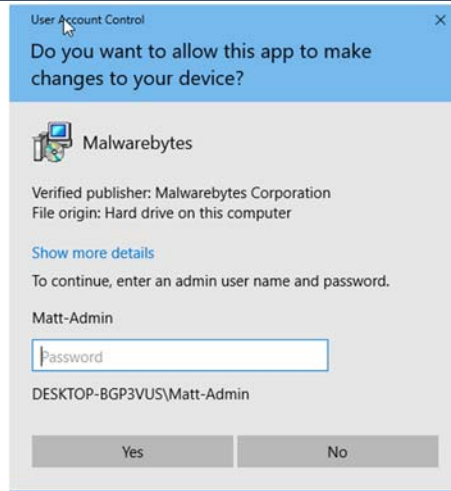
Step 2: Click Free Download



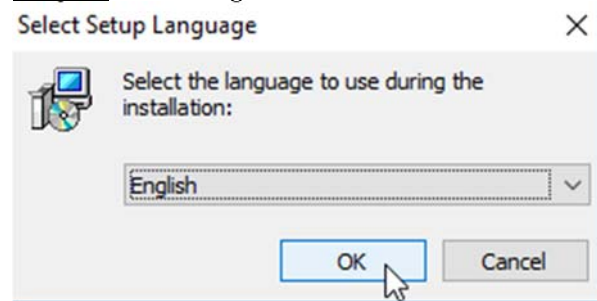
Step 3: Save the setup file to your computer

Step 4: Run the setup file

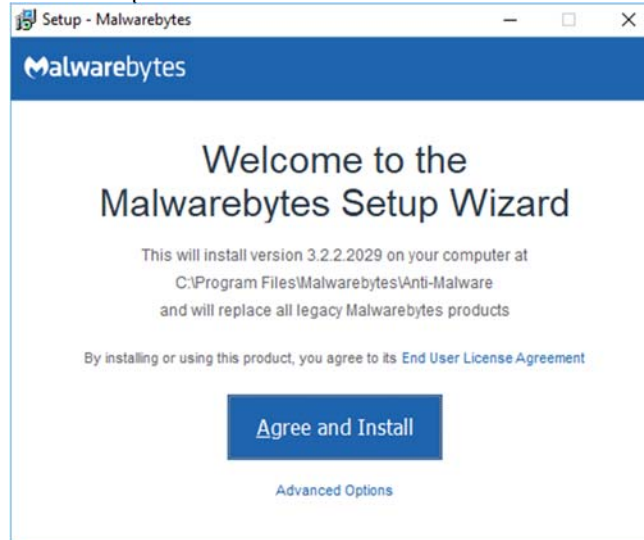
Step 5: Enter your administrator password



Step 6: Select English and click OK

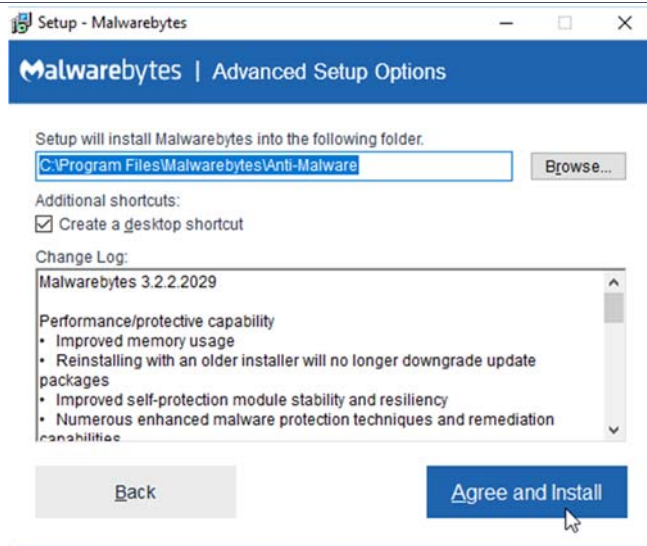


Step 7: Click Advanced Options

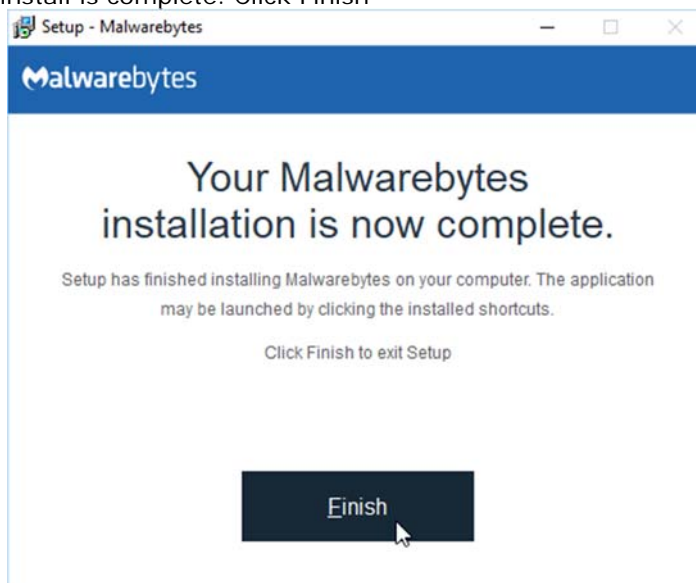


Bonus Tip: If I ever see a Custom install or Advanced Options button or link, I like to see what features the software is trying to install.

Step 8: In this case, there is nothing that I want to change. Click Agree and Install



Step 9: The install is complete. Click Finish



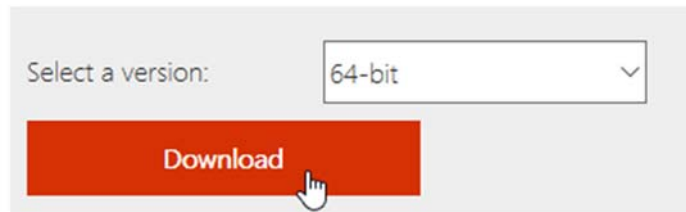
Malwarebytes does have a premium version. It will give you 2 weeks to try it out before reverting to the free version. This is one program that I would consider purchasing to actively monitor your computer. The premium version starts at \$39.99 /computer / per year with discount pricing for multiple devices.
Using Microsoft Safety Scanner

Microsoft Safety Scanner is another great tool that you can use. It is a self-contained EXE file that you manually run to detect and remove malware. **Note:** The tool expires after 10 days requiring you to download it again should you wish to run another scan.

Step 1: Navigate to: <https://www.microsoft.com/en-us/wdsi/products/scanner> or search for Microsoft Safety Scanner and click on the respective link

Step 2: Select the version of Windows, 32 bit or 64 bit, that you are running and Click Download

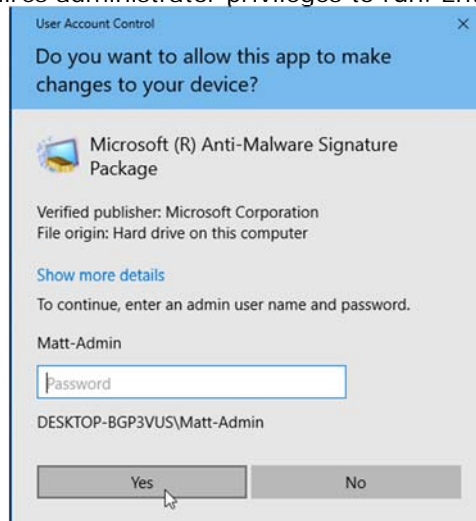
Microsoft Safety Scanner



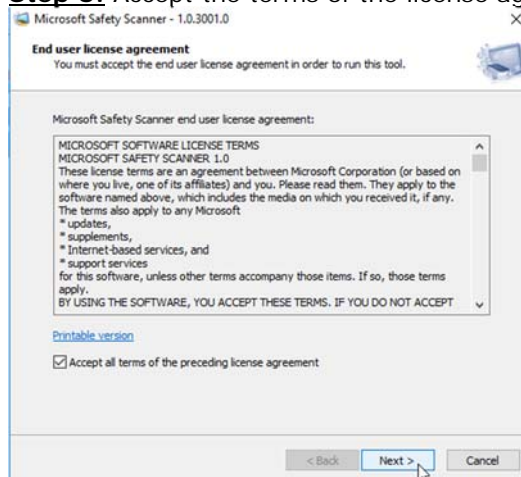
Step 3: Save the file to your Downloads directory

Step 4: Run the msert.exe file

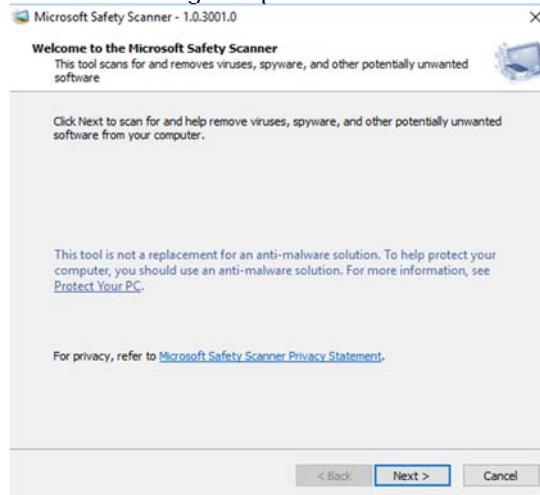
Step 5: This tool requires administrator privileges to run. Enter your password



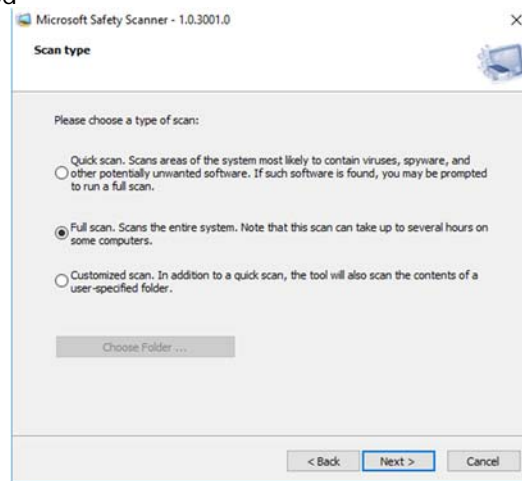
Step 6: Accept the terms of the license agreement and click next



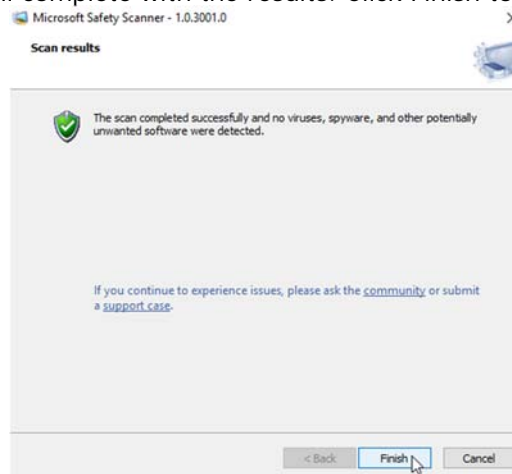
Step 7: Click Next to start scanning computer



Step 8: Choose the type of scan. I typically run a full scan to make sure that my entire system is good



Step 9: The scan will complete with the results. Click Finish to acknowledge results



Tip 4: Clean up your computer with CCleaner and Disk Cleanup

Over time, your computer accumulates temporary files and Windows registry entries that you no longer need and are safe to delete. While Windows does a good job managing these items, there are times where tools like CCleaner and Disk Cleanup are helpful to have in your toolbox. The combination of these programs help you locate these temporary files and unneeded registry entries and delete them. Disk

Cleanup is already included with Windows and CCleaner is a free download.
Installing CCleaner

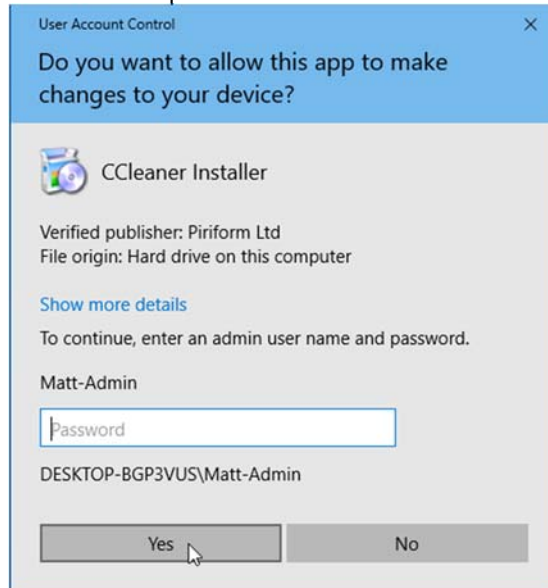
Step 1: Navigate to: <https://www.piriform.com/ccleaner/download> or search for CCleaner and click the respective link

Step 2: Like Malwarebytes, you can purchase a Professional version of CCleaner. For our needs, the free version will do just fine. Click Download under the free version column

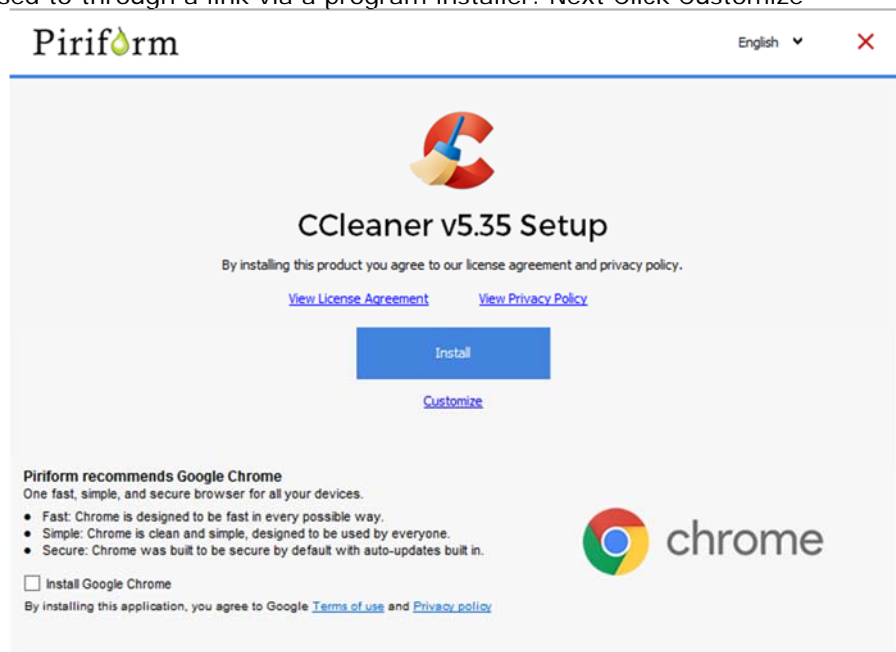
Step 3: Save the download to your computer

Step 4: Open the folder location and run the ccsetup###.exe, where ### corresponds to the version of CCleaner that you download

Step 5: As before, this install requires administrator access. Enter your password

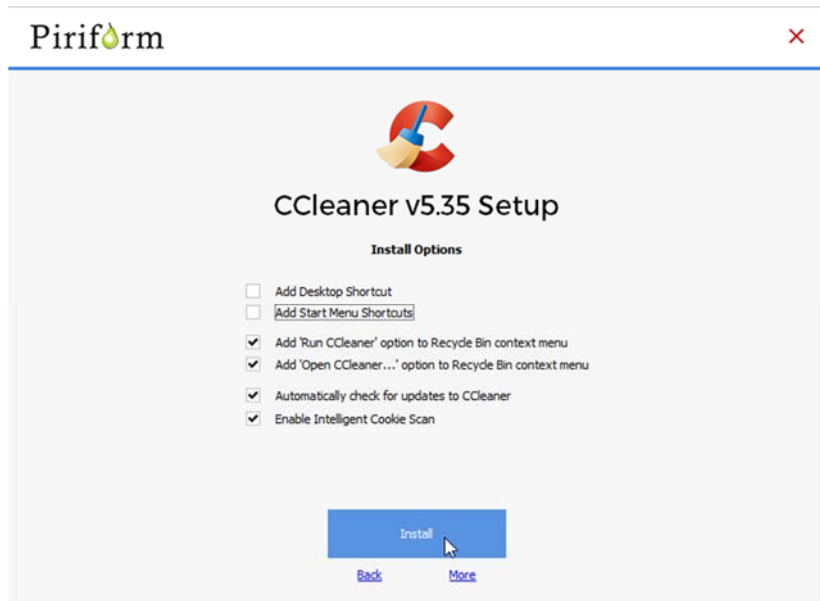


Step 6: The CCleaner setup launches. Uncheck Install Google Chrome. I generally prefer to download browsers and other software directly from their official website as opposed to through a link via a program installer. Next Click Customize

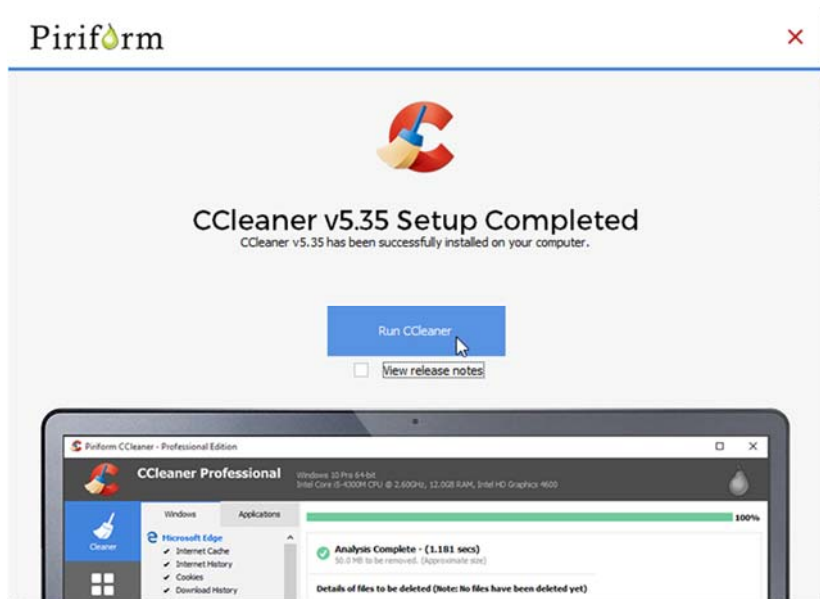


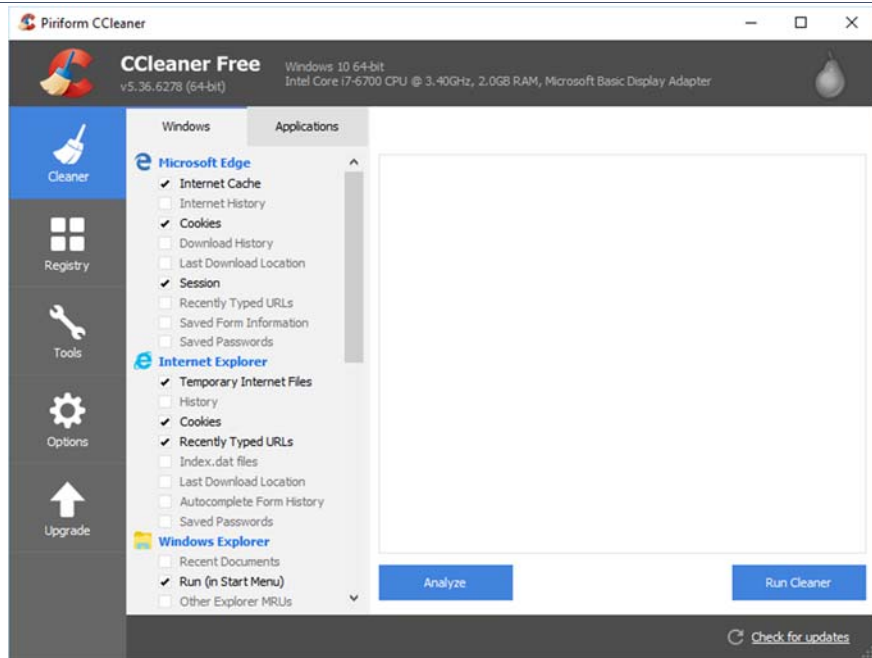
Step 7: I prefer to run CCleaner from the Recycle Bin, so I will choose to uncheck

Add Desktop Shortcut and Add Start Menu Shortcuts. Click Install



Step 8: Uncheck View release notes and click Run CCleaner





The two primary sections of CCleaner are the Cleaner and Registry sections. The Cleaner will analyze your computer for temporary files that are safe to delete. Before analyzing your computer, look over the items listed under the Windows tab and the Applications tab. I would like to highlight a few items that I think you should uncheck:

- Windows → Microsoft Edge. Uncheck Internet History, Download History, Last Download Location, Recently Typed URLs, Saved Form Information, and Saved Passwords
- Windows → Internet Explorer. Uncheck History, Recently Typed URLs, Index.dat files, Last Download Location, Autocomplete Form History, and Saved Passwords
- Windows → Windows Explorer. Uncheck Recent Documents
- Windows → System. Uncheck Empty Recycle Bin and Windows Log Files
- Applications → Applications. Uncheck MS OneDrive and all Office entries

I recommend unchecking these items because these are useful files to keep for tracking down sources of computer malware infections and to help you and your IT support person understand computer errors and crashes. It is also very helpful to keep recent documents. Definitely uncheck applications such as MS OneDrive and Office so that you can quickly find documents that you recently worked on. When you click Analyze, you will get an idea of how much disk space you can free up. To delete these temporary files, click Run Cleaner and viola, you now have a cleaner computer!

The Windows Registry is a repository of important keys and values that keep Windows and your other programs running smoothly. Incorrectly modifying the registry can prevent Windows or other programs from running, so it is important to understand what you are doing before editing the registry. As you install Windows updates and add or remove programs, the Windows registry can collect keys that you no longer need. This is where the Registry section of CCleaner comes in handy! CCleaner will analyze the Windows Registry and delete the keys that it determines are no longer necessary. In the majority of cases, it is safe to delete these keys. Best of all, no dangerous registry editing is required!

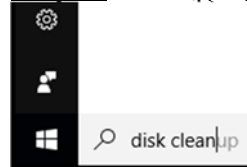
Using Disk Cleanup

Disk Cleanup is a great tool already built into Windows that you can use to clean up disk space on your computer. Downloaded Program Files, Temporary Internet Files, and Windows Update Cleanup are three items that Disk Cleanup addresses. Windows Update Cleanup will appear if Disk Cleanup detects unneeded Windows Update setup files. This option is especially useful on older computers where you have applied

many updates. This option alone can free up gigabytes of space!
To launch Disk Cleanup:

Step 1: Click Start

Step 2: Start typing Disk Cleanup



Step 3: Click on the Disk Cleanup app



Step 4: After reviewing the Files to delete, click OK

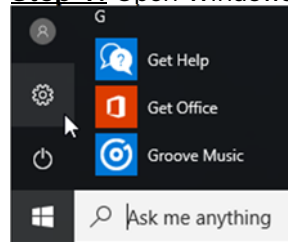
Tip 5: Update Windows and Applications periodically

The final tip that I have in this article is probably the most important, but often most overlooked item: install updates!

Install Windows Updates

Microsoft updates their Windows operating system and Microsoft applications once a month. Make sure that you install both Windows and Microsoft updates.


Step 1: Open Windows Settings by clicking the Start button and then the gear icon



Step 2: Click Update & Security



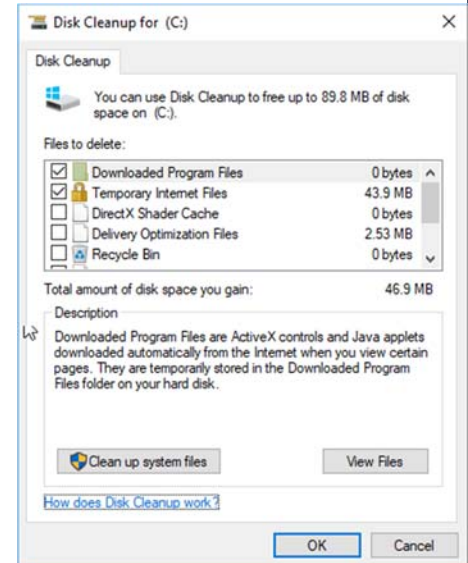
Step 3: Click Advanced options under Update settings. Make sure that you check get updates for other Microsoft products. This will ensure that other Microsoft applications such as Office stay up to date

 Advanced options

Choose how updates are installed

Give me updates for other Microsoft products when I update Windows.

Step 4: Click Check for Updates



Windows Update

Update status



Your device is at risk because it's out of date and missing important security and quality updates. Let's get you back on track so Windows can run more securely. Select this button to get going:

Check for updates

Install Applications Updates

For each application, make sure that you have the latest version installed. Java is one application often overlooked when it comes to installing updates. So, make sure to update Java, if you have it! The newer Java updaters now check for and remove outdated Java installs, which is great. Adobe Flash Player and other web plugins are good to check as well. Finally, do not forget to update your other web browsers such as Firefox and Chrome!

Concluding Thoughts

I hope that these tips help you keep your new or old computer running smoothly for years to come. Remember:

- Tip 1: Make your primary account a non-administrator account
- Tip 2: Install one Antivirus program on your computer
- Tip 3: Protect your computer from malware with Malwarebytes and Microsoft Safety Scanner
- Tip 4: Clean up your computer with CCleaner and Disk Cleanup
- Tip 5: Update Windows and Applications periodically

I hope that you have a wonderful holiday!