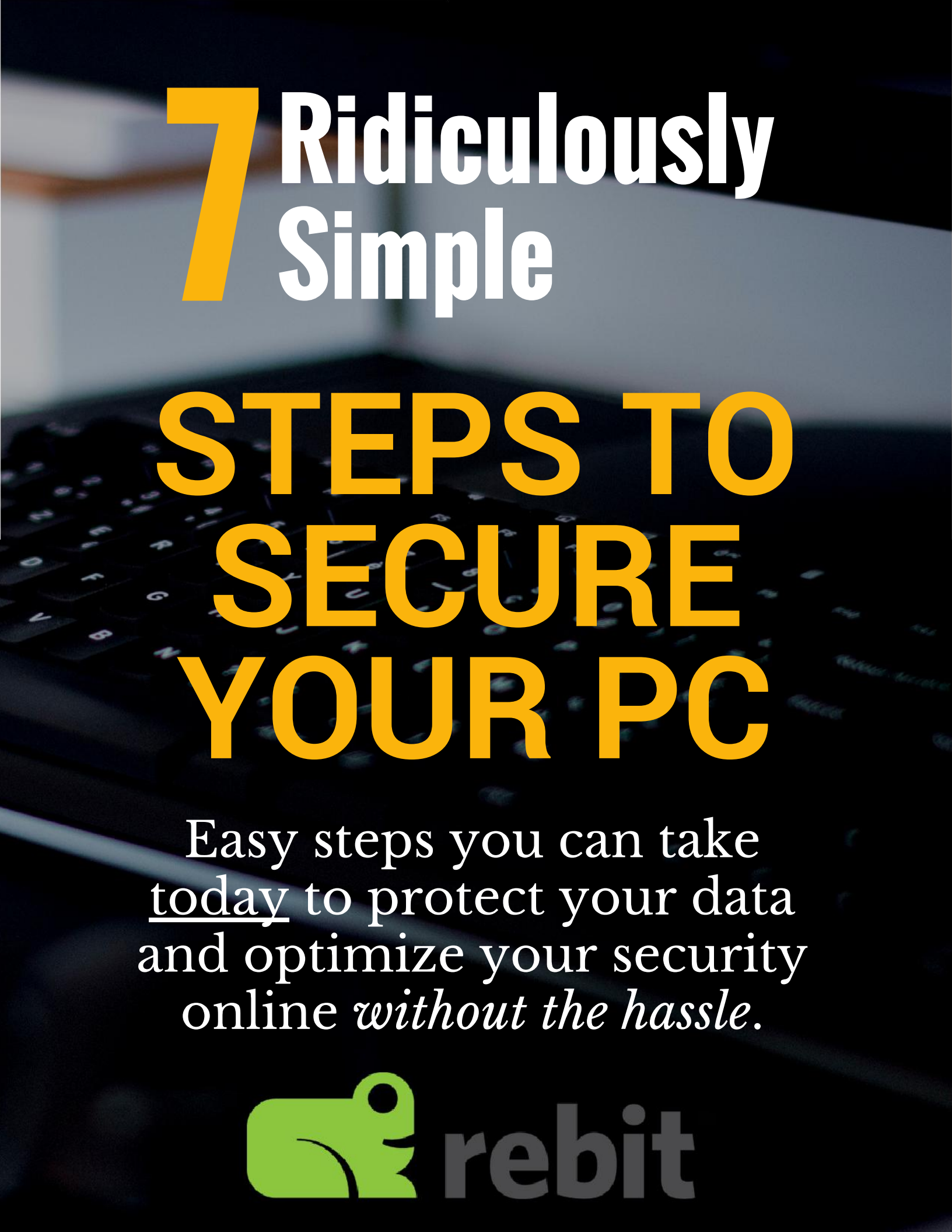


7 Ridiculously Simple STEPS TO SECURE YOUR PC

Easy steps you can take today to protect your data and optimize your security online *without the hassle*.

rebit

7 “Ridiculously Simple”
Steps to Secure Your PC

Easy steps you can take today to **protect your data** and **optimize your security** online *without the hassle*.

Rebit 2018

Table of Contents

Disclaimer

This guide is designed to provide practical steps to increase the electronic security of your PC and to better protect your digital data. These steps should reduce your exposure to threats, mitigate loss potential, and help provide a layer of systematic protection to your PC.

Following these steps, however, is not a guarantee you will be protected from PC threats, nor can any steps provide 100% security. Rebit makes no guarantees or warranties.

Changes in systems and practices, along with evolution and emergence of threats, require PC users to maintain ongoing responsibility for the security and protection of their systems, following the latest best practices.

Additionally, regardless of the systematic steps you take, you may still be exposed to behavioral targeting and social engineering. Even with a highly secure PC, do exercise caution in your online activities.

A Very Personal Introduction

Here at Rebit, we want to ensure you enjoy your time with computers! That's why we strive to make everything *ridiculously simple*.

With the never-ending emergence of malware, viruses, ransomware, and more, it's never been more important to keep your PC safe and secure.

Let's have a quick look at what's at stake…

- Your documents and work
- Your photos and your videos...your memories
- Your music
- Your identity and banking information
- So much more

Isn't it worth taking a few deliberate actions to ensure you have a strong baseline of security?

In this guide, you'll find seven steps you can take to make your Windows PC safe and secure to use. Each step will be simple and will give you peace of mind.

When disaster strikes...

While this guide is presented by Rebit, it comes from a very personal and human place.

About two years ago, my parents' PC was hit by ransomware. It was a seemingly random event that occurred despite using their computer trouble free for years.

In many ways, it was no different than a home robbery or car accident. It happened with zero warning and was massively devastating.

My mother had recently retired and was chasing down a dream of hers...to write a book. She had completed the manuscript and was shopping editors. It was a labor of love and something she poured countless late nights into.

My father pursued photography. And between the two of them, they had about a decade's worth of photos and videos on their computer. These spanned their own vacations, the wedding of their child, their grandchildren, holidays, family events, and countless other irreplaceable memories.

They knew the value of what lay on their computer, but it's easy to take for granted when everything works. To be safe though, they also had a separate hard drive which they manually copied things onto every so often, just in case.

But it wasn't enough…

One morning, they woke up and were confronted with a message on their screen demanding payment to unlock their computer.

Ransomware struck.

Every file on their computer was now encrypted and inaccessible. The ransomware even reached out to the external hard drive and encrypted their copied files.

Paying to unlock their files was never really an option, as it was unlikely their files would actually be decrypted. It also appeared the instructions were no longer valid.

What followed was extremely sad, expensive, and deflating. My parents lost 90% or more of their files. I was able to share some of my pictures with them, but theirs were gone. My mother did recover an older revision of her book she had emailed, but it wasn't her finalized manuscript.

The files and memories they lost were priceless, so they were willing to pay anything to get them back. Ultimately, they spent thousands of dollars with PC recovery technicians in an attempt to decrypt and unlock their files, but to little avail.

We ultimately traced the source down to an out-of-date piece of software that had been compromised.

Regardless of how it happened, my parents were truly robbed...no different than if someone had broken into their home.

Since that date, I vowed to learn as much as I can in this space and help out those who need it. I've changed a lot of my practices and hopefully I've helped many around me.

My point in sharing this story is to add a human element and show just how devastating complacency can be. I hope this document starts you on a safe journey and helps you stay safe yourself!

The state of PC security

Before we get started, let me share a few facts to show you the scope of the impact. Again, I share this in hopes you take action to secure your PC now rather than waiting until something bad happens.

So heading into 2018, here are some bigger-picture stats about the state of PC security:

- 24% of PCs are not protected by up-to-date antivirus software (Microsoft). [1]
- One in three Americans were hacked in the past year (ITSP Magazine). [2]
- 2017 saw a 36 percent increase in ransomware attacks worldwide (Symantec). [3]
- One in 131 emails contains malware, the highest rate in five years (Symantec). [3]
- More than 4,000 ransomware attacks have occurred every day since the beginning of 2016 (Barkly). [4]

Alright, let's get you protected

So without further introduction, let's get you started on some ridiculously simple steps to protect your PC!

1. Keep Windows up-to-date

One of the common threads you'll see throughout this document is to keep your system up-to-date. Threats are constantly evolving and emerging. But fortunately, your software providers continuously evolve their solutions to protect against these threats as well. This only works if you update your system though.

Windows provides the base layer of defense, so as a first steps, let's ensure you allow automatic updates and that you apply them regularly.

In fact, as I write this, a significant vulnerability was just announced that impacts "virtually every PC user." Fortunately Microsoft is deploying security updates to Windows users, but you must be setup to receive them!

As a first step, it is vitally important to be on a supported version of Windows. If you are using Windows XP or another common, yet unsupported, version of Windows, you are putting yourself at undue risk. This guide focuses on Windows 10 to ensure you have the latest security updates and support.

Check your Windows Update status

Here are the steps to take:

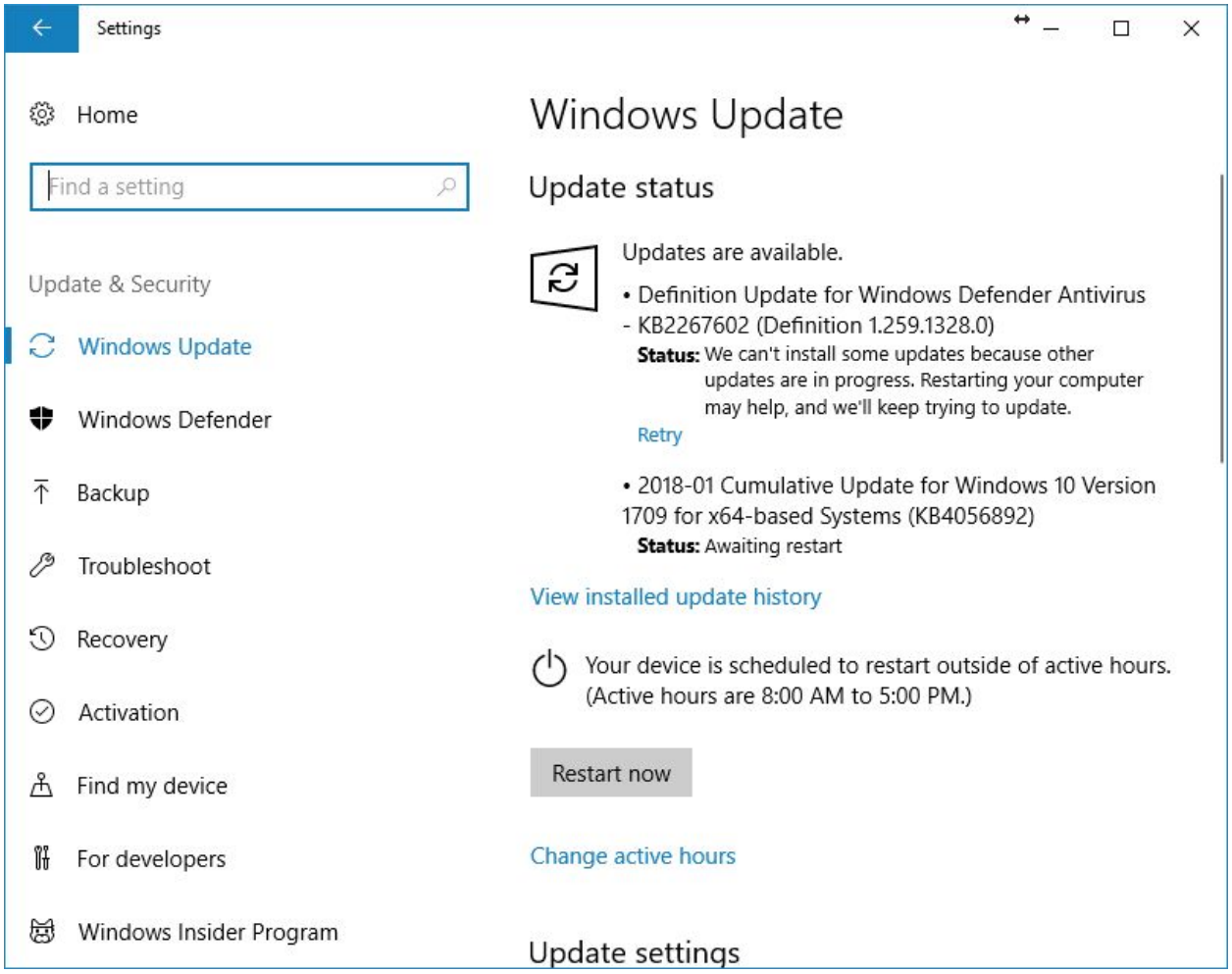
1.  Click Start
2.  Settings
3.  Update & Security

You should find that your system has a nice green checkmark. If not, it's time to make some tweaks!

If your machine is not updated, it's time to dig through the settings and ensure you are allowing Windows to automatically update.

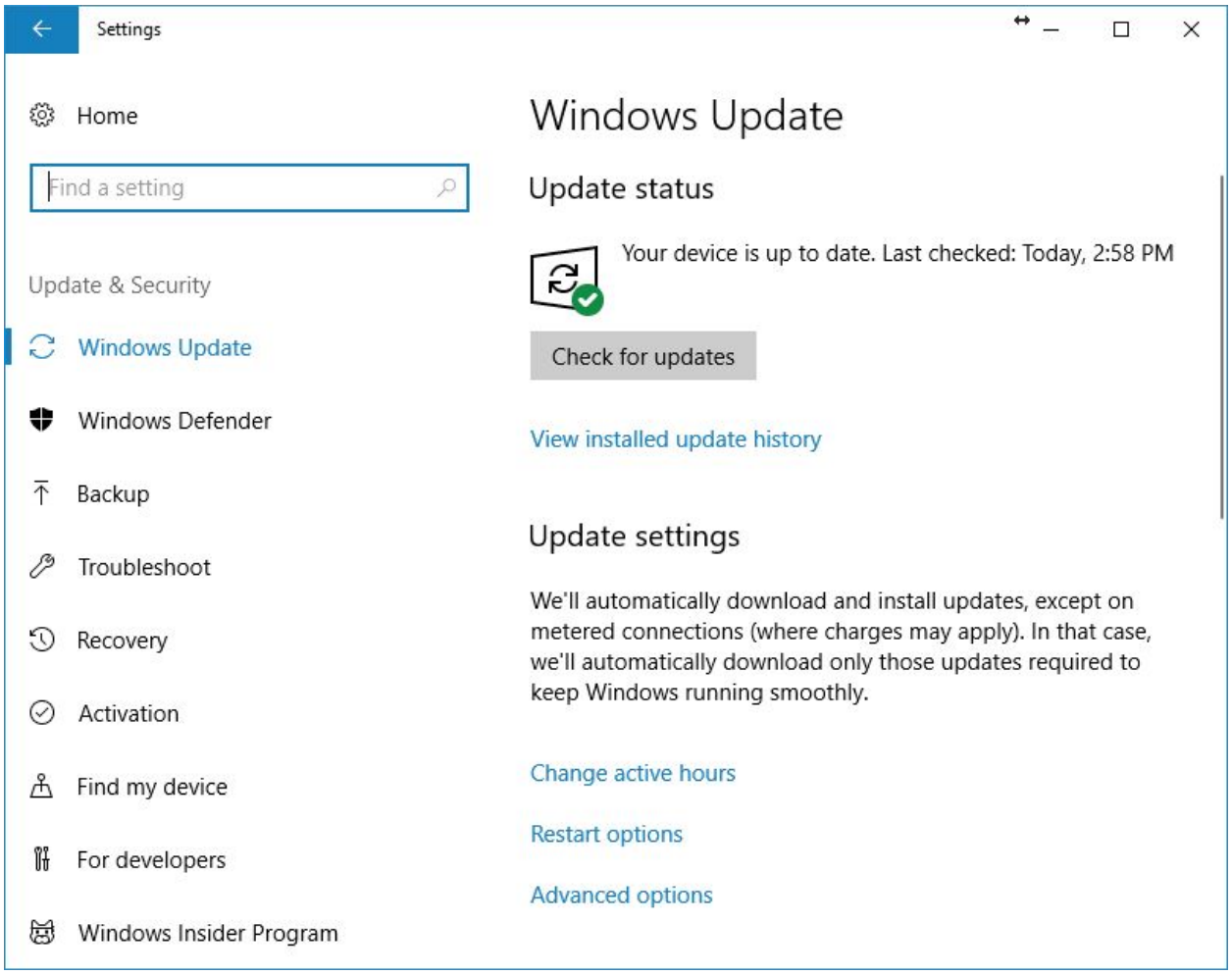
Examples of update status

Here's a screenshot of a computer that is not up-to-date. You'll note that there is a virus definition update and a general Windows patch available. These are actually related to the Intel vulnerability that was announced at the start of 2018.



After letting the updates install and rebooting my PC, I get a green checkmark showing me everything is happy and up-to-date.

Here’s a screenshot showing a happily-updated copy of Windows:



Changing your auto-update settings

You can click through “Change active hours,” “Restart options,” and “Advanced options” to ensure updates are allowed to download and install. You can set off times that are convenient for you.

You may also find that you have an update pending and you may just need to restart your machine to let the process finalize. Getting in the habit of regularly restarting your PC can help keep updates coming in a timely manner.

2. Ensure your antivirus is running and up-to-date

Windows now comes with antivirus and protection software. Microsoft cannot have a reputation for having an insecure operating system, so they have a vested interest in keeping you secure.

Where you use the built-in antivirus or a 3rd-party solution, you just must be sure it's running and up-to-date.

For the purpose of this tutorial, we'll look at Windows Defender Security Center. It's included with Windows (free) and easy to configure.

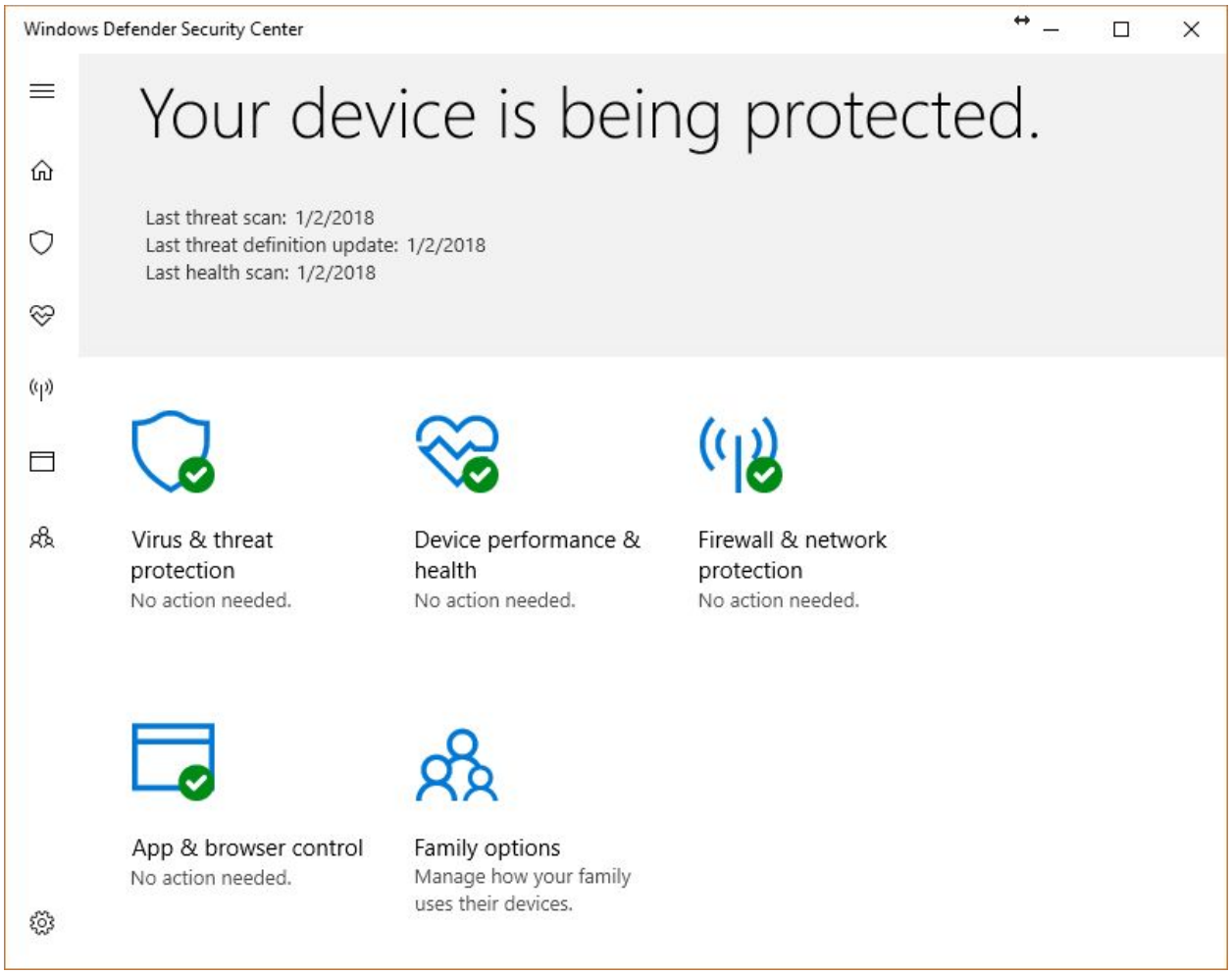
Check your update status

Here are the steps to take:

1.  Click Start
2.  Settings
3.  Update & Security
4.  Windows Defender (on the left)
5. Open Windows Defender Security Center

You should then be presented with a screen with green icons and a message that you are being protected.

Here's a screenshot of Windows 10 confirming it is protected:



If you are not being protected

Windows 10 is very good about letting you know where gaps are in your security. If you are missing the healthy green checks, you will instead see scary red marks. Clicking on these will guide you through remediation.

This might mean you need to update your virus protection, turn it on, or enable your firewall. Windows will guide you through all of these scenarios.

If you use a third-party antivirus software, you may have some different steps, but the fundamental pieces remain the same: ensure it is running and ensure it is up-to-date.

3. Keep your software up-to-date

My parents had Windows and their antivirus up-to-date, but they had several instances of old software applications, which was ultimately their downfall.

This is particularly true of software that accesses files online or that you use to open downloaded documents. For example, if you download and read PDFs regularly, you want your PDF reading software to be up-to-date. That way, if the PDF file contains something malicious, your reader will be more likely to catch it and prevent you from opening.

The same goes for programs such as Microsoft Office, accounting software, and more. Keep these programs updated!

Keeping your software updated

Let's make sure you keep this final piece updated. Here are some tips:

Tip 1: Consider web applications instead of desktop applications

How do you check your email? Using an outdated version of Outlook or Thunderbird can be a problem. But if you check your email on Gmail.com or Outlook.com, you know your email system is the latest and greatest.

Many applications, whether financial, image editing, or otherwise are now online for this reason. It's easier to keep users safe and updated. If there is an online version of software that you're currently using, consider making the change.

Tip 2: Use a software store

In order to improve security, Apple, Google, Microsoft, Amazon, and others have created their own app stores. These stores contain free and paid applications, and have minimum requirements application developers must meet to list software.

These stores also centralize updates and feed them to your PC as long as you have updates activated.

Instead of downloading software from random websites, consider only choosing software from app stores.

Tip 3: Clean out unused software

Before going through and manually updating any remaining software, it's a good idea to remove software you no longer need.

Click Start > Settings > Apps to see a list of software installed on your computer. You can go through the list and click to uninstall.

Tip 4: Manually update remaining software

After reviewing what is installed on your machine, go and open any of the software remaining that you do use. Typically programs have a mechanism to update.

Oftentimes, you can click on the menu on About > Check for Updates (or something similar).

If you cannot find the option to update the software from your PC, you can check your app store or go to the software's website and check for an update there.

If you find the application is no longer supported or hasn't been updated in awhile, you need to consider the risk this is introducing.

Summary

This step is by far the most labor intensive, however it should not be neglected. By changing your habits to working primarily through a browser and through software on an app store, you can greatly reduce vulnerabilities on your system.

4. Configure your browser for security

Most people do the vast majority of their PC work on a web browser. Your internet browser functions in a similar way as your PC. It allows you to perform a broad variety of tasks and can have its own software added in. By having an improperly configured browser, you may be opening yourself to vulnerabilities.

Keeping it configured properly can help protect you from malicious sites, bad downloads, exploits, and much more.

Here are three tips to secure your browser:

Tip 1: Update your web browser!

Swiss Federal Institute of Technology found that "using the most recent version of a browser will lower the risk associated with drive-by-downloads and other Web-based attacks, which start by targeting the browser."

Here are some links to ensure common browsers are kept updated:

- Google Chrome: https://support.google.com/chrome/answer/95414
- Mozilla Firefox: https://support.mozilla.org/en-US/kb/update-firefox-latest-version
- Microsoft Edge: This one is automatically updated with Windows updates. As long as you follow our section on "Keeping Windows up-to-date," you'll be set.

Tip 2: Review extensions and addons

You can install additional functionality to your browser by adding extensions and addons. These can be themes, functional software, or even games. But the more you add, the more likely you are to expose yourself to a vulnerability. Just like software for your PC, software for your browser should be kept updated, should be from a trusted repository, and should be deleted if not in use.

Also, in many cases, malware may install itself in the form of a browser extension, hijacking information, redirecting you to bad websites, showing you ads, and slowing down your experience. Following the steps in this guide should help prevent problems, but it's good to review what's installed.

Here are instructions for reviewing what is installed on your browser:

- Google Chrome: https://support.google.com/chrome_webstore/answer/2664769?hl=en
- Mozilla Firefox: https://support.mozilla.org/en-US/kb/disable-or-remove-add-ons
- Microsoft Edge: https://docs.microsoft.com/en-us/microsoft-edge/extensions/guides/adding-and-removing-extensions

Tip 3: Validate website security

Updated browsers provide you real-time feedback about websites you are visiting. One of the most important is to look for the green secure padlock next to web address when visiting websites.

This padlock means that information you enter on the site will be sent encrypted and cannot be viewed by a third party. If you ever enter a password, banking information, or other personal information, ensure you see the green padlock.

See the example green padlock and “Secure” wording next to this web address:

Summary

Following these steps will provide a safer browsing experience for you. Regardless of the system protection in place, follow common safe and work with websites you trust.

5. Manage your passwords effectively

How often do you see a news headline announcing a major company has been hacked, compromising millions of username and passwords? This is a common story, but your exposure can be easily mitigated.

Passwords are the keys to our virtual worlds, and just like we exercise great care with our physical keys, so must we with our passwords.

Password best practices

When it comes to unlocking your files, your computer, your bank information, and your personal data, all that may be between you the bad guys is a password. So you need to follow these three best practices:

1. Change your passwords regularly. We recommend monthly. This will limit the chances that past exposures won’t cause you problems today.
2. Keep your passwords different for each website. If your password to one site is compromised, the impact will be limited.
3. Use complicated passwords that aren’t based on dictionary words.

The only problem with these rules is they create complexity! It becomes hard to remember your passwords in this schema.

Password managers handle complexity for you

The best way to utilize complex passwords and avoid the headache is to use a password manager. Password managers are life savers. Personally, I'd be lost without one.

Commonly used password managers are Lastpass, 1Password, and Dashlane, but there are many to consider. If you operate exclusively out of a single browser, you can even consider the built-in password managers in Google Chrome or Firefox.

Here's the trick…

How to lock down your password manager

You will have now have one master password that provides access to all of your online accounts. This creates a new point of risk. In order to overcome this, your password manager will ask you to set up "two-factor authentication."

Two-factor authentication means you will need a password and something else to gain access. This is typically your mobile phone, but there are many simple options. When you attempt to access your password manager, you'll enter your username, a password, and then your phone will send you a code. This provides exceptional lockdown and security for your passwords.

Summary

Alright, we discussed a lot in this section. Here is a quick summary:

1. Keep your passwords unique, cycled, and complicated
2. Use a password manager to eliminate the complexity
3. Enable two-factor authentication on your password manager

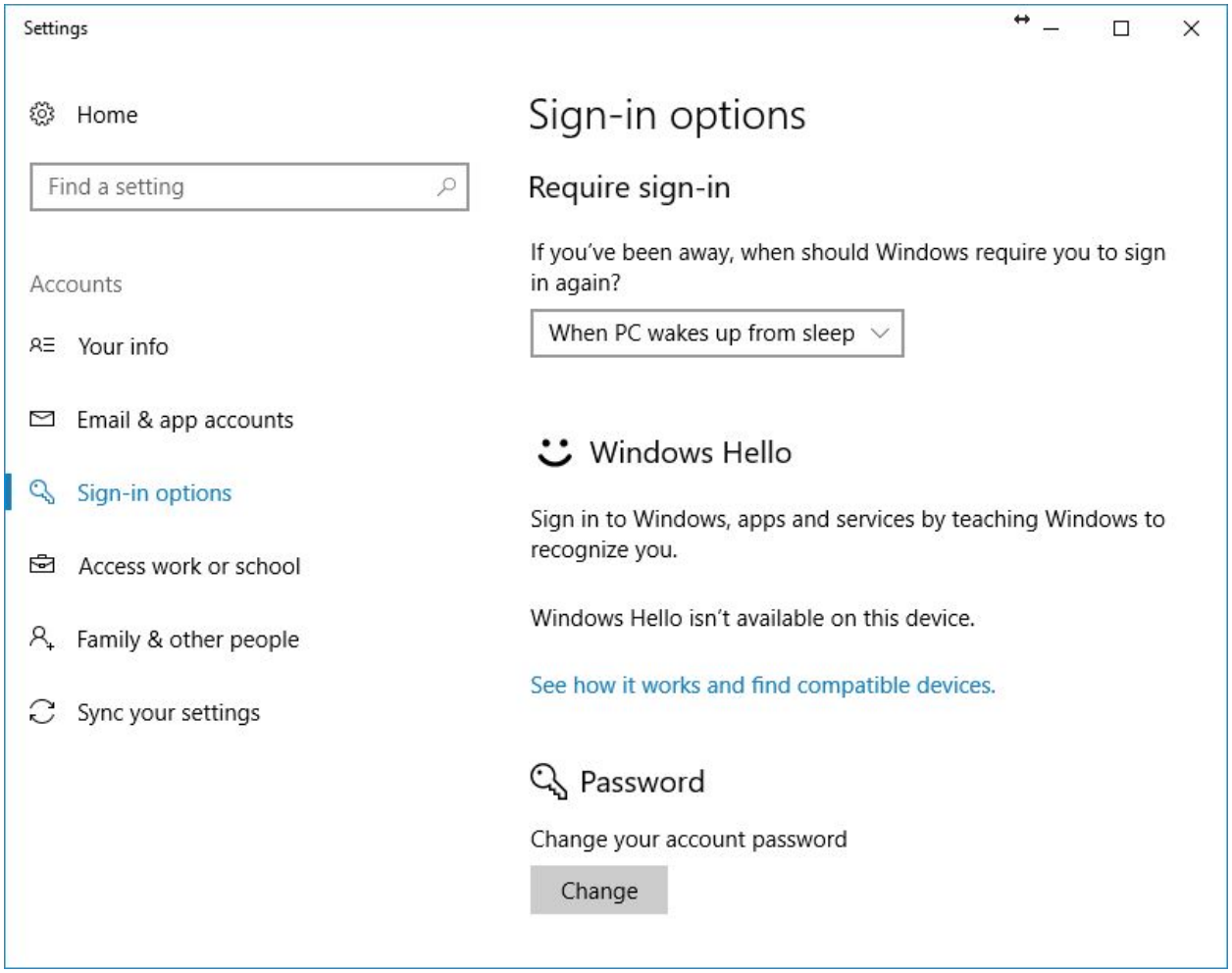
With that, you should accounts should be much more difficult for hackers to compromise.

6. Set up a Windows user account password and PIN

Once you have your Windows PC nice and secure, it's time to ensure the entry to it is also handled!

Windows 10 offers several methods to access it. We want to ensure you have a password, at minimum. Additional options can make it even more locked down.

To start click Start, your profile picture, and then Change Account Settings. From here, click on "Sign-in options."



Tip 1: Click “Change” under Password

First, ensure you have a password setup. Assuming, you have a password, now follow the best practices you learned above in Step 5 “Manage your passwords effectively” with your Windows password.

Tip 2: Configure a PIN

The PIN is a secondary layer of protection that is easier to remember and actually more secure than passwords in a variety of ways. Namely, it is specific to your machine and is not shared in any way. To set this up, just click “Add” from the same page as your password configuration.

Tip 3: Check “Privacy” settings

Staying on the same screen, scroll down to “Privacy.” Here, you can turn off the options here to enhance security and privacy.

Summary

This section provides a layer of security to your PC overall. And don’t forget...when you leave your PC, you should lock it using the keyboard (Windows Key - L) or Start > Profile > Lock.

7. Backup your files...the ultimate failsafe

Regardless of the steps you take to protect yourself, there’s always a chance something can happen. Perhaps a new threat emerges, you have a lapse in updates, or you accidentally delete files yourself! That happens all the time. Some of the worst issues I’ve had with my PC have been entirely self inflicted.

This is where the beauty of true backup comes into play.

If you backup your PC completely, you’ll be able to truly “undo” any mistake, virus, malware, or other issue. Proper backups store many “points in time,” allowing you to instantly revert either a single file or your entire system to the last known point of safety.

See, my parents simply copied files to a backup drive. This wasn’t enough.

Had they instead had access to a true backup of the prior day, they could have wiped their PC completely clean (to remove any bad code), and simply restored their files to before the ransomware struck.

What cost them weeks, thousands of dollars, and massive loss of files and memories, could have been entirely resolved in a couple of hours.

Features to look for in a backup solution

There are a few key features that backup software should provide to be a complete solution, including:

- **Restore points and file history.** This feature allows you to recover files or your whole system as it was yesterday, the day before, or 30 days back. Having this history is key to recovering from problems and mistakes, especially if you don't know when they originated.
- **Full-system backup and recovery.** File recovery is critical, but some solutions also allow you to restore your entire PC. This allows you to completely wipe your computer clean--or even buy a new computer--then replicate your entire original PC with the click of a button. All of your software, your configuration, and your files are back in a snap.
- **Online and local backup.** Backing up your PC and its files to a hard drive at your home will protect you in most situations, but not all. If you were robbed, have a hardware failure, or even something like a fire, your backups would not be safe. So backing up your files to online storage offers an additional layer of protection. No matter what happens at your home, your files are safe and encrypted at an online storage provider.
- **Easy to use.** This "feature" is underrated, but if your backup software is complicated, you may not spend the time to set it up properly. And what if it stops working and you aren't protected, but don't realize it? Last, what happens when it comes time to recover? Will you be able to use it?
- **Human support.** The last point brings me to this....even with easy-to-use software, recovering your files and PC can be a challenge, especially if you've been hit by something malicious. Trained experts standing by to help you can be a lifesaver.

Should I use Windows Backup?

Windows offers a Backup option, which you may have seen when we configured Updates. The Windows update option gives you the ability to store past versions of files or an external hard drive.

Once this is configured, Windows will automatically backup changes to your files. If you want to go back to an older version of a file, you can do this by “stepping” back revisions at a time. You’ll actually find “Forward” and “Backward” buttons within Explorer.

While this a type of backup, it is missing a few key items:

- It is not a full-system image backup.
- It does not save your files offsite.
- The usage is a bit confusing and doesn’t conform to the traditional backup approach.
- Microsoft support is primarily handled through knowledge bases and forums. Most phone or direct conversation support is typically done through Microsoft-authorized partners, which will charge a few to help you with restoring backups as needed.

Is a cloud account like OneDrive, Google Drive, or Dropbox sufficient?

Many people utilize cloud storage for their files. This does offer an additional layer of protection, especially if that provider offers file history.

However, it is not true backup for a few reasons:

1. Your computer and the online storage sync. Thus, if your files are deleted or corrupted on your PC, those changes will be synced online.
2. If you accidentally delete files or if someone gains access to your account, your files can be lost.
3. Full-image backup is not available.
4. Human support is typically not readily available or is email only, which can complicate recovery.

Special offer for best-in-class backup from Rebit

Rebit provides best-in-class backup software that is designed to be ridiculously easy to use. We take your backups, your safety, and you peace of mind seriously.

Rebit covers all of the key PC backup features and does so without the fluff.

- Easy-to-use continuous backup with file history and full-system recovery
- 50GB of included online backup storage
- 24*7 human support!

If you want to ensure your computer has the failsafe of easy-to-use backup, Rebit is an easy choice. We've been protecting hundreds of thousands of customers for over a decade. We're also the backup partner of choice for major companies such as Dell.

So here's how to get your deal...

As a thanks for reading this guide, I'd like to personally offer you something you won't find on our website...**30 days with Rebit entirely risk free**. If you like it, you can move forward at just $4.99 per month. If you don't, no problem! No commitment and no hassle.

Simply go to: https://rebitgo.com/product/rebit-pro-personal/

At checkout: enter coupon code: **TRYME18**

That coupon code will make your first month 100% free. You'll be able to download the software and get it running, totally risk free.

Conclusion

It is our sincere hope that you have found value in this guide and that you have been able to improve the security of your PC. Thank you for reading.

You can connect with us any time at https://rebitgo.com or https://facebook.com/rebitgo.

And if you have a question at any time, just reach out support@rebitgo.com.

Best regards,

Justin Gesso

Director of Marketing | rebitgo.com

Sources and References

1. https://blogs.microsoft.com/blog/2013/04/17/latest-security-intelligence-report-shows-24-percent-of-pcs-are-unprotected/
2. https://itspmagazine.com/from-the-newsroom/keep-calm-and-here-is-a-list-of-alarming-cybersecurity-statistics
3. https://www.symantec.com/security-center/threat-report
4. https://blog.barkly.com/cyber-security-statistics-2017