10 STEPS TO PROTECTING YOUR DIGITAL LIFE

WHY SHOULD I READ THIS?

No one really likes to take the time to be proactive. It’s inconvenient and difficult. This guide is meant to be a reference that is intentionally user-friendly. You don’t have to read it in it’s entirety, but keep it around. It may save your digital life one day.

WHAT YOU WILL FIND IN THIS GUIDE...

1. Windows Updates
2. User Passwords
3. Using Anti-Virus
4. System Cleaning
5. Data Backup
6. Browsers
7. Smartphone Security
8. Protecting Your Info
9. Physical Security
10. Social Networking
HuskyTech’s primary goal is to help students with establishing and maintaining their digital life at the University.

Our Services

**Shop Support**
Drop your computer off at our shop in McMahon if you would like a technician to diagnose and repair your corrupted operating system or virus-infected computer.

**Quick Support**
Visit our shop for direct, face-to-face assistance with a technician.

**Phone Support**
For over-the-phone troubleshooting, call 860 486 4087.

**Live Online Help**
Visit our website at huskytech.uconn.edu to chat with a technician.

**Email Us**
For general questions, send an email to huskytech@uconn.edu.

**Library**
Stop by our secondary location in Homer Babbidge Library to speak with a technician.

Hours and Locations

We have two locations. Our main location can be found in McMahon residence hall. We also have our satellite location in the Homer Babbidge Library.

<table>
<thead>
<tr>
<th>Location</th>
<th>Mon - Thurs</th>
<th>Fri</th>
<th>Sat - Sun</th>
</tr>
</thead>
<tbody>
<tr>
<td>McMahon</td>
<td>8am - 8pm</td>
<td>8am - 5pm</td>
<td>CLOSED</td>
</tr>
<tr>
<td>Call Center</td>
<td>8am - 8pm</td>
<td>8am - 5pm</td>
<td>11am - 8pm</td>
</tr>
<tr>
<td>Library</td>
<td>11am - 8pm</td>
<td>11am - 5pm</td>
<td>11am - 8pm</td>
</tr>
</tbody>
</table>

Contact Us

- **860 486 4087**
- **huskytech@uconn.edu**
- **www.huskytech.uconn.edu**
- **live chat with us on our website**
- **www.facebook.com/huskytech**
- **www.twitter.com/huskytechuconn**
## Contents

1. Perform Windows Updates Regularly ................................................................. 2
2. Setting up and Using Strong Passwords ............................................................ 2
3. Using and Updating Anti-Virus and Anti-Malware Programs ............................... 3
4. Cleaning Out Garbage and Freeing Up Space on Your Computer ............................ 4
5. Protecting Yourself from Data Loss with Data Backups ....................................... 4
6. Using New Browsers (Newest Version of Internet Explorer, Firefox, and Chrome) .... 5
7. Smartphone Security Precautions ......................................................................... 6
8. Protecting Your Sensitive Information on the Internet ........................................... 7
9. Making Sure Your Computer is Physically Secure ............................................... 8
10. Maintaining Safety in a Social Networking World ............................................... 8
1. **Perform Windows Updates Regularly**

**How to Perform Windows Updates**

To Perform Windows Updates in **Windows XP**: Open the start menu, navigate to all programs and select Windows Update.

To Perform Windows Updates in **Windows Vista or 7**: Open the start menu, navigate to the search box and type in, “Windows Update.”

Once you have opened Windows Update in any version of windows, select check for updates. This will allow your computer to communicate with Microsoft directly to download the newest security patches necessary to protect your computer and allow your computer to run without crashing or freezing.

Allow your computer to install all of the recommended updates. You can choose optional updates as you like but these are not the most important ones. Install the updates and allow your computer to restart as necessary. Sometimes this may require you to check Windows Updates again upon restart. Perform this after each restart during the update process to ensure that all updates have been found and successfully installed.

**How to Configure Automatic Updates**

Also in control panel, you will find the ability to set Windows to automatically install updates. This is important to allow your computer to have the most recent definitions to keep your computer safe and in operable conditions. For more information, go to the Microsoft help page.

2. **Setting up and Using Strong Passwords**

**Setting your Windows Passwords**

To change your Windows Password, navigate to the start menu or the start orb on the bottom left of your computer. Navigate to the control panel in your start menu. Under Control Panel you will see the User Accounts icon. Select your account, and then select Change Password. It is incredibly important to change your Windows passwords frequently along with your other accounts as well.

**Using Strong Passwords for all Accounts**

It is also important to use strong passwords for all of your digital accounts. As a student this may include your email, NetID, and Student Admin accounts. Though it is easy to have the same password across all accounts it also makes you very vulnerable to online hacking. Make sure to set diverse passwords across all accounts and change them frequently to avoid security risks.

**Password Complexity Recommendation**

In many ways, the longer any password is, the better. An extra character added onto an existing password can make it statistically more difficult to guess. If you are concerned with your password’s strength, visit HuskyTech’s Before Connecting Guide for Windows 7.

If you are concerned about your password’s security or think that your account has been breached, CONTACT HUSKYTECH TODAY! HuskyTech has the ability to reset your
Windows and UCONN passwords manually to keep your information safe and your accounts secure.

3. **Using and Updating Anti-Virus and Anti-Malware Programs**

**What are Anti-Virus and Anti-Malware Programs?**

Anti-Virus software (e.g. Microsoft Security Essentials) and Anti-Malware software (e.g. Spybot Search and Destroy) allow your computer to check for malicious programs that could put both your information and your computer’s usability both at risk. Running regular scans is important to keeping your computer safe and operable. HuskyTech configures weekly scans to be performed on every computer that goes through our shop workflow. We also recommend that users do the same on their computers as well.

**Microsoft Security Essentials:**

**Status Icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GREEN</td>
<td>No attention necessary, definitions are up to date and scan has been performed recently.</td>
</tr>
</tbody>
</table>
| ORANGE | Some attention necessary. Because:  
- Scans have not been performed.  
- Definitions need to be updated. |
| RED | Immediate attention is necessary. A threat was found and requires your attention. **Contact HuskyTech** if you have specific questions or concerns. |

**Updating Microsoft Security Essentials’ Definitions**

To update Microsoft Security Essentials, open the startup tray icon located on the bottom right side of your screen. Once open, select the update tab on the top of the window. Select update definitions. This will automatically search for new updates that will keep your computer protected. If Microsoft Security Essentials fails to update, contact HuskyTech for additional help.

**Performing Weekly Scans**

To scan using Microsoft Security Essentials, open the program and select the Home tab at the top. Next, select either Quick or Full depending on how in-depth you want to scan. Full scans take a much longer amount of time, so if you choose this, be prepared to leave your computer running throughout the whole scan. After this, select "Scan" on the right-hand side. The scan will then start and if any threats are found, a window will pop up displaying all the threats found. Select Remove from the drop-down menu next to each threat and then click “Clean Computer” at the bottom.
SpyBot: Search and Destroy:

Updating Spybot Definitions
Open Spybot from your Desktop or Programs. Select check for updates. Select any of the options with a U.S. flag next to it and select continue. Select ok when it instructs you to re-immunize.

Immunizing Spybot to Protect You from Malware Proactively
After updating Spybot’s definitions (see above), select immunize on the left. Once the immunize feature comes up, select the immunize option on the top. This allows Spybot to protect your computer from going to known malicious sites.

Performing Weekly Spybot Scans
To scan using Spybot, select Search & Destroy from the left-hand menu. Next, select Check for Problems. Spybot will now check your computer for problems. If it finds anything upon completion, select Fix selected Problems. If you are confused as to what to remove or something fails in this process, contact HuskyTech for further support.

4. Cleaning Out Garbage and Freeing Up Space on Your Computer

Running CCleaner
Has your computer become increasingly slow over time? If this is the case, you may just have to remove some of the temporary files that accumulate on your computer. To do so, download CCleaner, or open it from your Desktop if you recently picked up your computer from our shop or visited our computer setup location.

   a. Open CCleaner from your Desktop or Programs.
   b. Select Cleaner on the left hand side.
   c. Select Analyze which will allow CCleaner to look for garbage files that accumulate taking up unnecessary space.
   d. Once CCleaner has completed analyzing the files, select Run Cleaner. Upon completion, close out of CCleaner. If your computer is still running slowly after completing this, contact HuskyTech to determine whether additional troubleshooting is necessary.

5. Protecting Yourself from Data Loss with Data Backups

Why Back My Data Up?
Your Data is invaluable. On your computer, you store everything from sentimental pictures to valuable academic research. All of these items are irreplaceable. Hard drives, which are the devices that store your information, are prone to failure. As a result, it is essential to backup any information of value on your computer.
Options for Data Backup

External Hard Drives - The easiest way to backup your data is by purchasing an external hard drive. External hard drives because of their size and affordability can allow a user to backup their entire computer on a single device. These can range from about $50 and up. This can be setup to perform backups automatically as described below.

Thumb Drives – Are affordable ways to back up the bare minimum amount of files. They only store a handful of documents but they allow you to backup your information to a second location on a budget, as well as give you the portability to use your documents on the go.

Google Docs – For individuals with a UConn Google Apps account, they can backup their files using Google Docs. This allows you to upload up to 1 GB of files. For users that convert their documents to the Google Docs format, they are not taxed on their space usage (How it Works: Google Docs Storage). This is a great way of backing up your work as well as allowing you to work and edit your files on the go. For more information, visit, Google Docs' Help information.

Configuring Automatic Backups in Windows
Once you have purchased an external hard drive, if you have Windows 7 or Windows Vista, it is fairly simple to setup automatic backups directly in windows. Check out this HuskyTech Knowledge Base Page for more information.

If you have an older version of Windows or encounter issues during the setup, contact HuskyTech for additional troubleshooting.

Using Google Docs to Backup Your School Files
Backing up your MS Office documents is easy. Open Google Docs account from your UConn Gmail account. Select Upload on the upper left and select either Files… or Folders… For users utilizing either Google Chrome or Mozilla Firefox, simply drag and drop the documents you would like to upload directly on your documents listing in Google Docs.

For additional support information on Uploading Documents to Google Docs, consult Google’s documentation.

6. Using New Browsers (Newest Version of Internet Explorer, Firefox, and Chrome)

Why use a new browser?
The newest browsers protect you from the most recent security and malware threats you are vulnerable to on the web. They allow you to visit the newest websites developed with the most up-to-date web standards and the fastest web browsing experience. Most users have used Internet Explorer for the majority of their life. This is fine as long as you are
using the most up-to-date version. HuskyTech performs Windows Updates to make sure this is the case.

For many people, trying out a different browser may allow them to be more productive and tweak their browser to better suit their needs. For this reason, HuskyTech recommends students try Firefox or Chrome.

**Installing Mozilla Firefox**
To install the latest version of Mozilla Firefox, visit this link. If you want to know why Firefox might be a good fit for you, visit this Mozilla page. If you don’t know where to begin, visit this page to meet Firefox, and visit the recommended extensions we have listed below.

**Installing Google Chrome**
To install the latest version of Google Chrome, visit this link. If you want to know why Chrome might be a good fit for you, visit this Google page. If you don’t know where to begin, visit this page to take a tour of Chrome’s features, and visit the recommended extensions we have listed below.

**Recommended Add-Ons Available**
Many browsers have a range of possible add-ons to make your browsing an effective one. As a word of caution, when you install an add-on, know what information that add-on has access to and make a judgment with that in mind. Below you will find several recommended add-ons that HuskyTech technicians find useful.

*Ad-Block Plus*

[Link for Google Chrome Users](#).
[Link for Mozilla Firefox Users](#).

**7. Smartphone Security Precautions**

**Why do I need to protect my Smartphone?**
Your Smartphone now houses your digital life on the go. People can have sensitive information stored on their devices and depend on their device’s availability.

**Do I need an Anti-Virus program on my Smartphone?**
As with all electronic devices, malware is being written that targets Smartphone’s. By following the safe practices listed below, it is likely that you will not become a victim of malware.

*For iPhone and iOS devices:* Apple has very strict policies and procedures in place when it comes to allowing applications onto the App Store, which minimizes the need for an Anti-Virus program.

*For Android Devices:* HuskyTech recommends the free version of [Lookout Mobile Security](#). This program offers many great features, including Security, Find My Phone, and Backup and Restore. There is also a Premium version that can be
activated, which offers **Remote Lock** and **Remote Wipe** features, which can be used if your device is stolen.

---

**Questionable Applications in App Stores**

Similar to the problems posed by browser add-ons, specific applications you install will have specific access to information on your mobile device. Many app stores reserve the right to remove questionable or malicious applications remotely for their users. Android and Apple both do this based on their findings with the security of applications. When you are determining whether or not to install an application, make an educated judgment with this in mind.

**SMS Phishing Scams**

Individuals can use text messages for malicious purposes similar to attempts made with e-mail phishing scams. When you receive a text message from an individual you do not recognize, do not give them your personal information. Do not click a link if they included a link in the message. This could be a ploy to try and access your address book and other information on your phone similar to an e-mail that would try and retrieve your sensitive information on your computer.

**Security Patches**

Your phone will frequently get security patches from the manufacturer. Make sure to either plug your phone into your computer or check for these “over the air.” These are important because they fix “holes” that hackers can take advantage of on your device.

**Phone Tracking and Remote Data Wipe**

If your phone is lost or stolen, there are ways to track and retrieve your phone. In the case of theft, you can also remote wipe your phone. Check out the following sites if you are interested in finding out more information about configuring your device for this functionality.

- For iPhone and iOS devices: [Find My iPhone by Apple](https://www.apple.com/)
- For Android devices: [Lookout Mobile Security](https://www.lookout.com/)

---

**8. Protecting Your Sensitive Information on the Internet**

**What is considered sensitive information? Why is it important?**

Sensitive information can include social security numbers, credit card numbers, account information, passwords, and other personal information you would not want someone else getting a hold of.

**Looking for HTTPS and Secure Webpages**

The easiest way to make sure that your information is protected is by looking at the site you are using and making sure you see [https://](https://) before the address you have typed in (instead of [http://](http://) like you normally would). For an example, see the image below:

![Bank of America Corporation](https://www.bankofamerica.com)
By making sure you have the lock and the https:// before the address, you are ensuring that you have a “secure” connection that is password protected between your computer and the destination for the information. This protects people in between from seeing your information.

9. Making Sure Your Computer is Physically Secure

Why should I physically secure my computer?
Your computer is invaluable and if you have a laptop, the same mobility that you love will also make your computer vulnerable to theft. Stolen computers are fairly infrequent given the size of the student body but it comes down to a crime of opportunity.

Good Practices
- Don’t leave your computer unattended in the library. Find a friend who can watch your computer while you step away.
- Don’t leave your computer in the dining hall. Most dining halls on campus offer either a receipt system for valuables or a lock that can be borrowed with a photo I.D. as collateral.
- Don’t leave your room unlocked or open. It seems meaningless, but even a few moments create an opportunity for someone to come in and swipe your computer or other digital devices.

Laptop Locks
The Co-op Technology Department and other technology stores offer laptop locks for sale that can physically protect your computer like a bike chain lock would. They are available in both combination and key lock formats.

User Passwords
Set a user password on your computer so that people cannot access your information if they were to walk by. This also helps you to protect against malware and other malicious abuse.

10. Maintaining Safety in a Social Networking World

Why should I be concerned about my Social Networking Accounts?
Social Networking accounts are the norm today. Everyone has one and everyone wants to share information and content with others. This is an incredible ability but with great capability comes great risk for that information falling into unwanted hands.

Facebook Privacy and Spam
Be careful of Facebook spam that seems out of place. Chances are that if it seems out of place, that’s because it is. This could be an easy way of compromising your account and your contacts.
Check out Facebook’s privacy settings. Make sure to check that the information you post falls into the hands you expect it to be.

**Twitter Privacy and Spam**

Be careful of undesired friend requests from very weird looking accounts. Twitter is known for its vast spamming population. If you do not want your tweets made public, make sure to enable **private tweets** so only your followers see your posts. For more information about best practices, visit Twitter: Following Rules and Best Practices.