Inside this issue:

Willow Valley Computer Club Newsletter

Upcoming Computer Club Meeting Programs

May 2, Ed Dahrsnin, Keeping Your System Running Smoothly

June 6, Mike Scott, Digital Devices and Strategies in K-12 Education

No July or August meetings—Summer break!

All programs are held at 2:00 p.m. on the first Thursday of the month in the Cultural Center Theater unless otherwise noted.

Quick Notes

- Ed Dahrsnin's recycle team needs laptops, printers and USB keyboards
- See page 11 for *Renaissance* classes
- Some important information from prior newsletters is repeated in this newsletter

The President's Pen by Sid Paskowitz

Membership As of this writing, your Computer Club has 624 paid members including 466 who have signed up as Lifetime members. Please keep your email address on Club records current so we can send you important emails. ***Those emails only go to Computer Club members for whom we have a good email address***. Send email address corrections or updates to Lee Wermuth at lwermuth582@gmail.com.

Class and Program Volunteers. Willow Valley Residents have numerous different devices related to computers. The Computer Club would like to make information about those devices available to all Residents who might be interested. We are not looking for experts on those devices; only those who are willing to share what they know or are willing to learn and share. Different Residents learn in different ways and diversity enables broader opportunities for different Residents to benefit. Please let me know via email at wvcomputerclub@gmail.com if you think you could help.

Recycling Ed Dahrsnin and his team are accepting working computers and components for recycling, but no CRT monitors. Let Ed know if you would like to help recycle computers. See page 8. Thanks to Ed and his team, the Computer Club has given more than **230** computer systems to local community support organizations.

Patience!!! We continue to get phone calls and emails that report computers do not boot up quickly with a login screen or desktop when turned on. This is often due to Windows operating system updates that are installing. If you turn your computer off and turn it back on, the process just starts over again or introduces errors. If the drive activity light on your computer is flashing or lighted, your computer is working hard to get something done. **Be patient**. You may need to give your computer a couple of hours to catch its breath. If you still have a problem, see the next paragraph.

Continued on page 2)

(Continued from page 1)

President's Pen (Continued)

Help with PCs Cathy Thorn and Bob McRobbie (for Manor Residents) have volunteered to help with PC problems. Bob's and Cathy's phone numbers are at the top of the home page in Information Central. Also, please let Cathy know if you think you can help others with computer problems so she could contact you instead of her needing to go to the far reaches of Willow Valley to help others. Help with Apple computers is also listed at the top of the home page in Information Central.

Please Use Recommended Software PC owners are reminded that they will receive the best help if they use software that is familiar to other Resident volunteers who provide technical assistance. Recommended applications are CCleaner, Malwarebytes, Defraggler and Windows Defender (or Windows Security Essentials). We recognize there are alternatives; however, problems are more quickly diagnosed and repaired when the applications running on the PC are familiar to the helper.

Training Coordinator Chuck Smith is our Computer Club Training Committee chairperson. Please let Chuck know if you have suggestions for computer classes so they can be included in *Renaissance* publications. Also let him know if you could teach a class. Contact Chuck via email at csmithii@aol.com.

Information Central Highlights Google has produced a series of video tutorials to show how to use Google applications such as Gmail and Google Calendar. Check out the link to ***Google Tutorials*** in the left column of Information Central.

I continue to get phone calls and emails from Residents whose computer screens tell them they have been hacked! If that happens, use the power button to turn off your computer by pressing it until the power light turns off. Wait a few minutes and turn your computer back on. Chances are good that the warning will not reappear.

The Piriform.com Website that has been the source of applications such as CCleaner and Defraggler now goes by the name of CCleaner.com.

Quick Note: If you have given up on your inkjet printer because you don't use it frequently enough and the ink dries and kills the printer, consider getting an inexpensive laser printer. Laser cartridges don't dry and you can avoid leaving your apartment to print documents on the Willow Valley printers. (Notes continued on page 14)

Thanks to all of you who volunteer your time and knowledge to help other Residents.

We can always use the help of more volunteers!

Computer Club Leadership

Officers

President: Sid Paskowitz

Vice President: Peter Scott

Secretary: Gary Staton

Treasurer: Lee Wermuth

Committee Chairpersons

Program: Peter Scott

Training: Chuck Smith

Equipment: Ed Dahrsnin

Technical Support: Tony Poulos

Website: Sid Paskowitz

Publicity: Wally Gordon

Newsletter: Sid Paskowitz

Apple Interest Group: Steve Lynn

North Computer Lab Coordinator: Lee Wermuth

Community Representatives

Manor North: Charlie Trumbo

Lakes Manor: Gene Simasek

Providence Park: Peter Scott

Willow Gables: Cathy Thorn

Garden Apartments: Al Williams

The Mission

The Mission of the Willow Valley Computer Club is to:

- Provide the means to educate beginners or interested non-users on how to use a computer.
- Arrange for speakers to talk to the Club about subjects that would be of interest to those with some background and experience in computer use.
- Provide a forum for interchange of computer information among members.

For more information about the Computer Club, please contact Sid Paskowitz at 717-464-2127 or via email at wvcomputerclub@gmail.com

Making Life Easier Using Your Personal Computer

Sid Paskowitz has prepared a list of favorite things he does with his computer to make his own life easier. He will share that information in a one-hour program that will be given in each Community auditorium. Time permitting, a question and answer period will follow his remarks. If you can't attend the presentation in your community auditorium, you could attend in a different auditorium. The scheduled dates and times are:

Wednesday May 29
10:00 AM Lakes
2:00 PM Manor
Thursday May 30
10:00 AM North
2:00 PM Spring Run

Reviewer Acknowledgment

The following individuals kindly reviewed this issue:
Wally Gordon Jay Shah Ed Dahrsnin Tony Poulos Chuck Smith Steve Lynn Al Williams

Thank you,
Sid Paskowitz

Actions

Classes We know we need more classes on computer-related topics and we are looking for instructors who can teach those classes. If you can help other Residents with topics such as Word, WordPad, Notepad, browsers, email, etc., please send Chuck Smith an email at csmithii@aol.com.

CCleaner Issue (**Avast Installation**) Some recent updates to CCleaner included a **checked** box that allows the CCleaner update to install *Avast* on your computer. We have found the *Avast* software to be a memory hog and a program that interferes with protections that Windows provides. Our recommendation is to uncheck that box and do not install *Avast*. Use CCleaner -Tools to uninstall Avast if Avast has been installed.

Online TV Guide The Zap2it website was changed so the links that used to work in accessing the Willow Valley Senior (Campus) TV guide no longer work. Information Central has been updated to provide procedures that show how to access the current TV guide and links to other online guides. Left-click on *Senior TV Guide* in the right column of Information Central.

Windows Updates Although Microsoft had announced they were no longer providing updates to Windows 7 and Windows 8 operating systems, they recently found some computer chips and operating system computer code are susceptible to exploits and malicious software. Because of those findings, Microsoft has been sending software "patches" to older computers as well as newer Windows computers. Those software updates are generally being distributed on Tuesdays. Be aware these changes can be occurring even if you did not request an update, so if your computer seems to be unusually sluggish on a Tuesday or later startup, the issue may be a Windows update running in the background. **Be patient**!!!!!!!!!!!!!!!

Get Your Own Answers We are often asked questions that can be quickly answered without needing to ask another person. If you know the key words in posing questions to another person, you probably know enough to use those words in a Google search where you could get the answer as a text display you can select and print, or a You-Tube video you can watch. For example, to find how to do a channel scan on a Vizio TV, enter **Vizio TV channel scan** in the Google search box and choose the display that is most reasonable to you. If you are **not** comfortable with selecting a link on your computer, use a Resident Computer Kiosk to do your search. Be sure to restart the Kiosk unit when you finish in case a site you visited contained malicious software (malware). Restarting a Kiosk computer removes the history of what you did as well as any malware that may be on the Kiosk computer.

Warnings

Scams... No one who calls you, emails you or displays a message on your computer or device can tell you your computer or device is infected or running poorly. They have to have been given access. If you haven't given them access, you are being scammed. Don't give them access. Hang up. Disconnect. Shut down. Do not respond to emails that say your account is missing information or that say they were not able to deliver a package with something you did not order. Be skeptical. ***Protect yourself***.

Beware of using Google or another search engine to locate the phone number of a product manufacturer to get help with their product. Check the equipment manual to find their help line number. It is too easy for a bogus website to be made to look like a legitimate company site and the address of that website to be very similar to the legitimate company's name. Be especially suspicious when the address of the website as shown in the status display or text bubble ends in ".UR" or ".RU" or something other than .COM, .org or .info which legitimate companies are more likely to have.

Some new, but not surprising, information about malicious software: Google continues to find Android spyware in its app (application) store. **That spyware has been there for years without being noticed**. Millions are potentially affected. This brings up an interesting point I would like to emphasize. The Computer Club tries to be selective in the PC software we recommend, and those recommendations change over the years when we find software we like better. For example, a number of years ago we recommended Zone Alarm as the preferred firewall and AVG as the preferred anti-virus software. Today we recommend the Windows firewall and Windows Defender or Windows Security Essentials, and Malwarebytes as the anti-virus software. Other programs perform similar functions but we have experienced good results with the programs we recommend. We suggest caution in loading programs that may pop up on your computer screen or might be listed when you do an Internet search for software that might address a problem you are having. The experience with the Google store demonstrates that being skeptical can have its virtues.

Even Linux can be infected with malware. *Linux.MulDrop.14* is a malware program that can infect Linux devices. No operating system is immune from malware.

Sometimes, if you get a popup you can't clear, it is best to turn off your computer by pressing the power button until the power light goes off (this may take ten or fifteen seconds), even though the popup says not to turn off your computer. Next unplug your computer from its power source for about a minute. If you have a laptop computer, remove the battery for a minute before reinstalling it. Let Cathy Thorn know if you continue to have the popup problem.

Technical

Restore Point Al Williams has written a beneficial article on how to help protect your computer. His easy-to-follow instructions can be found by left-clicking on the link to **Restore Point** in the left column in Information Central.

RAM on new PCs Our experience when helping others with their older PCs indicates slow PCs are caused by insufficient RAM (random access memory) that may have met minimum requirements when the PC was bought, but software updates and newer software running in the background use more RAM than is available. Based on that experience we recommend new PCs have at least 12 GB of RAM for future needs. PCs can also run slow based on insufficient Graphics Processing Unit (GPU) performance.

Windows 10 Microsoft is still working hard to hit the one billion mark for Windows 10 users and recent reports have indicated their moves in that direction. First, Microsoft plans to have two major upgrades to Windows 10 and Office annually, probably in March and September. Second, reports have been received that some Windows 7 and 8.1 computers have been successfully upgraded to Windows 10 using old license keys. We are not recommending non-techies try to do this. We just want readers to be aware this may be possible if you want to upgrade to Windows 10 without needing to buy a new computer. On the other hand, Microsoft is now no longer providing updates to some old versions of Windows 10. See page 8 for replacement PCs.

Windows Updates Some computers can act strange when they are turned on. One thing that may be causing the change is that Microsoft has been sending out updates to Windows, even for Windows versions that Microsoft has reported they are no longer supporting. The updates being sent out contain patches to security vulnerabilities that have existed for years and are being exploited by current malware.

One problem being reported is the computer, or screen, or mouse, or keyboard is not being responsive. Those conditions are not unusual during a Windows system update, some of which can take up to a couple of hours. The solution in many cases can be ***patience***. If a computer is turned off during an update, problems can be created. Let your computer finish its update. Look for the light that shows activity on the hard drive. If it is flashing or stays lighted, your computer is probably working on installing an update. Let it finish and display a screen you recognize. If the computer continues to run overnight without restarting, press the power button until the computer turns off. Wait a couple of minutes and turn the computer back on.

If you still have concerns when your computer comes back under your control, run Malwarebytes and the full scan (after updates) using Windows Defender or Security Essentials to check for malware that may be on your computer.

Technical (Continued)

Mylobot shuts down Windows Defender and Windows Update when installed and blocks additional ports on the Firewall. It also shuts down and deletes any EXE file running from %APPDATA% folder. That action can cause a loss of data. The main function of the botnet is to take complete control of the user's computer, and damage to the computer depends on the payload the attackers decide to distribute. The best way to deal with malware is to **Keep Devices Current.** Almost all modern electronic devices that are susceptible to malware (malicious software) provide facilities to update their software (applications) and firmware (code that tells hardware what to do). There are too many devices and versions to provide a single set of instructions for keeping devices current. The best each of us can do is to learn how to keep our own devices current. Use Google or other search engines to get information on keeping devices current, or come to Computer Club meetings and classes and ask for help.

Printer Problems with Windows 10 Updates Several Residents have reported printer problems after a Windows 10 update. One solution has been to connect and turn on the desired printer, go to *Printers and Scanners* in System Settings, add the desired printer if it doesn't show up in the list, select the desired printer as the default printer, then check to see if the problem has gone away.

Interesting Self-help Article for those who want to learn more:

https://www.howtogeek.com/285361/the-complete-guide-to-giving-better-family-tech-support/

Drivers for 32-bit components Recent articles in the technical media have reported more companies are no longer updating drivers (software that tell components how to function) for 32-bit operating systems. Newer computers have 64-bit operating systems. If you want to check on what operating system is on your computer, an easy way is to open CCleaner and look at the top-left corner of the screen.

Spring Run Business Center The Spring Run Business Center on the 5th Floor of the Spring Run core building has a Windows 10 computer that is capable of reading SD cards and 3.5" floppy drives. The computer also has an attached flatbed scanner that can scan documents and pictures, as well as convert scanned text in a document to a digital text file (an Optical Character Reader—OCR). If you bring your own flash drive, you can copy any of those files onto your flash drive and take them home for later use. Many of us have a stack of 3.5" floppies we can't read. Here is a solution.

If you have a working laptop computer or printer you could donate, please give it to our computer recycling team on Mondays as described on the next page.

We recommend having at least 2 browsers on your Taskbar. Some web pages, such as WV Service Requests, may not work with Firefox but do work with other browsers. Firefox is probably the most secure browser. Be prepared to try a different browser if you get an error message on a web page.

The Equipment Corner by Ed Dahrsnin

699 Systems have been worked upon to this date (4/17/2019).

Systems available for Club Members:
Note: Tower systems include a tower, monitor, printer, keyboard, mouse and all cabling.
Laptops include a power adapter with unit, no printer or mouse.
System 654 (HP ProBook 4520S) Laptop Win 7 Home x64
System 688 (HP Compaq Pro 4300) Tower Win 10 Pro x64
System 691 (HP Pro 3500 Series) Tower Win 10 Pro x64
System 692 (HP Compaq 6005 Pro) Tower Win 10 Pro x64
System 693 (HP Pavilion GC381AV) Tower Win 10 Pro x64
System 694 (eMachines EL1360G) Tower Win 10 Pro x64
System 696 (Dell Inspiron 1501) Laptop Win 10 Pro x64
System 697 (HP Pavilion NY544AA) Tower Win 10Home x64
System 698 (HP 19-2120XT All-In-One Win 10 Home x64
System 699(HP Z210 Workstation) Tower Win 10 Pro x64

Systems passed on:
System 640 (Dell Inspiron 5520-6MKBGS1) Laptop, to Tony Poulos on 04 April 2019
System 671 (HP EliteBook 8570p) Laptop, to George McMurtry as a raffle prize on 04 April 2019
System 684 (Toshiba Satellite A305D-S6848) Laptop, to Reg Ohlsen as a raffle prize on 04 April 2019
System 650 (Compaq Minin102) Notebook to Trish Ullrich on 08 April 2019

Items passed on:
Two PS/2 Keyboards, one wireless mouse and keyboard, one PS/2 mouse and one USB mouse to Dale Mellinger on 04 March 2019
An HP 2311X monitor, plus two power adapter, to Terry Webb on 21 March 2019
An HDMI cable to Terry Webb on 28 March 2019
A Konica/Minolta Magicolor 1600W Laser color printer to Jay Shah on 01 April 2019

Scrap:
A Compaq Presario SR1214NX Tower on 04 March 2019
An HP 3520 printer on 18 March 2019
An HP Pavilion 22Xi monitor on 01 April 2019

Bill Scarpero has added his services to the Computer Recycling efforts in preparing mini-towers for additional add-ons.
With the work of Bruce Thompson in the Computer Recycle Room, we now accept Apple products for recycling.

The systems listed above, plus many computer power cords, coax TV, telephone and audio cables are available in various lengths. Check us for your needs – we may have it, and it is free to club members. Visit us at Manor North's Recycle Computer room on the fifth floor of Manor North 'J' building on Mondays only, after 1 p.m. and pick it up.

We are running low on laptops to work upon. We are seeking those no longer used units that you may have in your storage cage or elsewhere. Bring the items to Manor North's Recycle Computer room on the fifth floor of Manor North 'J' building on Mondays only, after 1 p.m.

We are also looking for supermarket paper bags, with handles – similar to those from Darrenkamp's.
We continue to accept printer cartridges and laptop computers with power adapters, also working printers with cartridges.

We no longer accept stand-alone scanners or monitors of the Cathode Ray Tube type. (Take them to the Solid Waste Management Recycling center on Harrisburg Pike).

Apple Information

Apple SIG Meetings Apple Special Interest Group (SIG) meetings are at 2:00 p.m. on the 4th Tuesday of the month in the Manor Orr Auditorium. Check the *Weekly Insider* for further information. In addition to a main topic, each session will also include News & Views, Appalooza (the app for the month) and Tips & Tricks.

Apple Store For purchases, learning or help, the Apple Store is located at 541 Park City Center, Lancaster, PA 17601. Their phone number is (717) 295-8800. Or Google "Apple Retail Store, Lancaster PA" or go to www.apple.com/retail/parkcity. The local site comes up with address, phone number, hours of operation. There are links to schedule either the "genius bar" (their support/ service team) or "workshops" (in house training sessions). While no ID is needed for the workshops, the site will query you for your Apple ID to register for the genius bar.

Apple Help

- For help at Manor campus, call Steve Lynn at 610-547-4615.
- For help at Lakes campus, email Ed Neff at neff.ews@gmail.com .

- Another recomended place for help with either MACs or PCs is TCW-GAV located at 254 South Esbenshade Road, Manheim, PA 17545. Website: www.tcw-gav.com then select Home Services & Products and then Support & Repair.

- Apple online help is at getsupport.apple.com where you can select specific devices and issues and then it will suggest several options for the solution.

- AppleCare warranty service, call 1-800-692-7753

- Telephone assistance for iMac, iPod or iPad, call 1-800-275-2273

- Telephone assistance for iPhones, call 1-800-694-7466

- Lastly, a person can Google the problem they are having and a list of suggested sites will be listed as possibilities for the answer.

Apple Information from Steve Lynn

Apple Watch

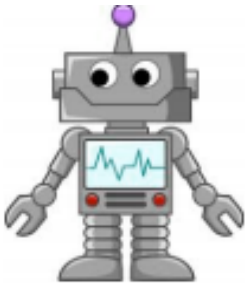
Apple watch series 4, watchOS 5, brings a beautifully redesigned watch to the market. Amongst it's new features are a larger more easily readable face, advanced activity and communication features, a fall detector and a heart rate sensor. A new accelerometer and gyroscope sense when a person has fallen and gives them a chance to send an emergency SOS or to designate that they are OK. The most amazing feature is the electrical heart rate sensor which uses electrodes to detect for an irregular heart beat such as Atrial Fibrillation (A-Fib) and sends a notification if one occurs. All recordings and any noted symptoms are stored in a Health app which can be later shared with physicians. It can also alert the user if the heart rate exceeds or falls below a specified threshold.

Apple Information (Continued)

The next operating system, watchOS 6, will undoubtedly be announced at the next World Wide Developers Conference (WWDC) in June 2019 with a final release to the public around September. It is hoped by Apple Watch aficionados that it will contain improvements in sleep tracking which now requires a third-party app to work. Also, some experts would like to see the watch be compatible with the Android smart phones as well as iPhones.

Artificial Intelligence

Apple's voice Siri is really a form of artificial intelligence (AI) which will now be getting more attention from Apple after a recent shakeup of it's employees. The recent head of it, Bill Stasior has been placed in a lower role of the company by John Giannandrea who was promoted to senior vice president. Giannandrea is said to be "looking to improve Siri's accuracy and performance." Siri is used in a number of devices including desktop/laptop computers, iPhones/iPads and it's in-home speaker unit HomePod. It has reportedly been criticized for not keeping up with Amazon's Alexa and the Google Assistant. The recent purchase of a host of smaller tech firms such as Laserlike, Silk Labs and PullString which have specialized AI knowledge should boost the competitiveness of devices that use Siri such as the HomePod in the very near future.



Question, what pluses and minuses might be in store for us as humans as AI continues to be developed world wide? A study was done in the summer of 2018 with 979 technology pioneers, innovators, developers, business and policy leaders, researchers and activists being asked the question of whether people will be better off than they are today with the spread of AI. The general consensus on the positive side was that it will greatly help in the medical field with such things as diagnosing and treating diseases and helping people to live fuller and healthier lives. Also, a number of experts expect AI to help produce changes in formal and informal education systems. Per pewinternet.org, "smart systems in communities, vehicles, in buildings and utilities, on farms and in business processes will save time, money and lives and offer opportunities for individuals to enjoy a more-customized future." However, there are concerns that these tools will have a long term impact on the essential nature of being human. Some of the negative aspects mentioned in the article were: individuals experiencing a loss of control over their lives, abuse by dictator led governments and companies striving for profits, job loss, the erosion of peoples ability to think for themselves and loss of life and mayhem created by autonomous military applications and increased cyber crime.

To read the original article, please click on the link Pew Research Center .

Any comments on the subject of AI or other information shown in the Apple section would be appreciated by Steve Lynn. Also, you are welcome to make suggestions for other topics that you would like see in upcoming issues. Send responses to me at slynner15@icloud.com .

Computer Classes

The classes listed below are sponsored by the Computer Club. To register for a class, use your web browser (Edge, Internet Explorer, Safari, Chrome or Firefox) to access the Willow Valley Resident login at https://resident.willowvalley.org. In the Username box enter the *values* for the first initial of your first name, your last name and your Willow Valley 5 digit Resident account number (no spaces). Enter your Willow Valley 5 digit Resident account number in the Password box. On the resulting page, left-click on the **Event Registration** tile; left-click on the **RENAISSANCE** tab; left-click on the down arrow to the right of the Special Events box; and left-click on the **Computer Classes** link in the pull-down menu. Locate the class you want and click on links and boxes to register. Note the dates and times displayed — they can change. There is no charge for any of these classes. **Classes are in the Cultural Center Education Room unless otherwise noted.**

Renaissance Computer Classes – Spring 2019

Managing the Modem and Router in Your Network
Computer, tablets, smartphones, and electronics of all types are dependent on connecting to the Internet. How does your home network work? This class will provide modem, router, and network basics. You will also learn troubleshooting tips useful when your home network is not working correctly.
Monday, April 29
10:00 a.m. – 11:00 a.m.
Presenter: Tom Fleischmann, Spring Run Resident

Microsoft Word – Questions and Answers
This class is being presented in a new format where early registrants will be sent an email asking for email responses with questions about Microsoft Word matters they would like covered in the class. The class will then focus on those questions, first received, first covered. If time permits, other questions may be raised and other information presented. Please verify you have a good email address in the online Resident Phone Directory.
Wednesday, May 1
1:30 p.m. – 3:00 p.m.
Presenter: Sid Paskowitz, Spring Run Resident

Individualized Quicken, Family Tree Maker and Ancestry.com Program Training
Individualized instruction is offered to persons who have mastered computer basics and are seeking a program for maintaining financial records. Learn how to download your banking information and more. The Quicken program will give you the ability to manage your financial records. Family Tree Maker and Ancestry.com are programs designed to help you learn more about your genealogy. **Use your own computer on dates scheduled between student and instructor after registration**.
Instructor: Bob McRobbie, Manor Resident

Individualized Help with Word, Excel, and Power Point for Intermediate and Advanced Users.
The Computer Club is offering individualized instruction for Word, Excel and Power Point to intermediate and advanced users. You choose the topic; they provide the instruction. Experience with the basic functions of the software is a prerequisite. **Use your own computer on dates scheduled between student and instructor after registration**.
Instructors: Carolyn Bugel and Tony Poulos, Spring Run Residents

President's Pen (Continued)

Another Reminder If you get an unexpected pop-up on your computer telling you an update is available and if you should click on the pop-up, there is a chance that pop-up is bogus and clicking on it will result in malware being put on your computer. A general recommendation is to go to the application itself and update from the application.

Fake Emails A day doesn't go by without someone at Willow Valley getting an email from someone they don't usually get emails from. They are almost always scams or contain malicious software. **Don't open them. Don't click on their links. Don't call the phone numbers they display.** I continue to receive emails from someone who had passed away several years ago. *That makes me suspicious.* If you think the email might be real, call the sender on the phone using a phone number you know is valid.

Avast, McAfee, Kaspersky and Norton security software (and possibly others) have been known to block security features and updates to Microsoft security programs (Firewall, Defender and Security Essentials). Some have also been known to slow computers to the point of not being useful, and not just during updates. For those reasons we do not recommend the installation of Avast, McAfee, Kaspersky and Norton security software for PCs.

Let Windows 10 updates install automatically. Do not manually update Windows 10 – you may inadvertently install an update that's not fully tested. We have found recently that Microsoft is making pre-release Windows 10 updates available to Windows 10 users who don't want to wait for the final release version. Those pre-release updates are accessed by ***Checking for updates*** and clicking on the ***Check for updates*** button. Final release versions should load automatically on your computer without your needing to do anything. If you believe your Windows 10 is not updating automatically when it should, call one of the contacts listed at the top of the page in Information Central and ask for help.

If you're planning a presentation or class and don't want an update to occur during the presentation or class, check https://www.howtogeek.com/224471/how-to-prevent-windows-10-from-automatically-downloading-updates/ for details on how to prevent the update from occurring.

TiVo update

The TiVo Roamio OTA had been the only TiVo unit "authorized" by Senior TV for use at Willow Valley. It was discontinued several months ago. Senior TV has not provided a recommendation on what unit we should be using. Recently, TiVo released a new model to the current Bolt line, the TiVo Bolt OTA. Willow Valley has tested it and found it doesn't work with our Senior TV signals.

Residents wishing to purchase a new TiVo should buy the TiVo Bolt VOX with either the 500 GB hard drive or the 1 TB hard drive. Unfortunately, there's a significant increase in price. The Roamio OTA with lifetime service and a 1 TB hard drive was available for $350–$400. The Bolt VOX with lifetime service and a 500 GB hard drive is $750 ($200 + $550). It's also available with a monthly plan for $15/month with a 1 year commitment or an annual plan for $150.

Beware!! *HotHardware.com* has reported: “Amazon Shreds User Privacy By Sharing Personal Alexa Voice And Data Recordings” which should serve as a warning that anything we say or do that involves the Cloud is susceptible to capture and sharing.

Backup files Please remember to periodically back up your important files to a flash drive or external hard drive. You never know when a computer might have a problem, and being able to put those saved files on a replacement computer can save a lot to time, money and headaches. Do not back up your files after your computer has been compromised. That can cause your backup drive to be compromised as well. Get professional help if your computer has been compromised.

Microsoft News

Windows 7 extended support will end on January 14, 2020. Office 2010 support will end on October 13, 2020.

The next major update to Windows 10 is codenamed 19H1. Microsoft has committed to upgrading Windows 10 twice each year. The 19H1 build will be the first for 2019 when it rolls out, presumably sometime this spring.

Microsoft CEO has said Cortana will never be able to compete with Alexa. He wants Cortana be a valuable skill that works with Google Assistant and other applications.

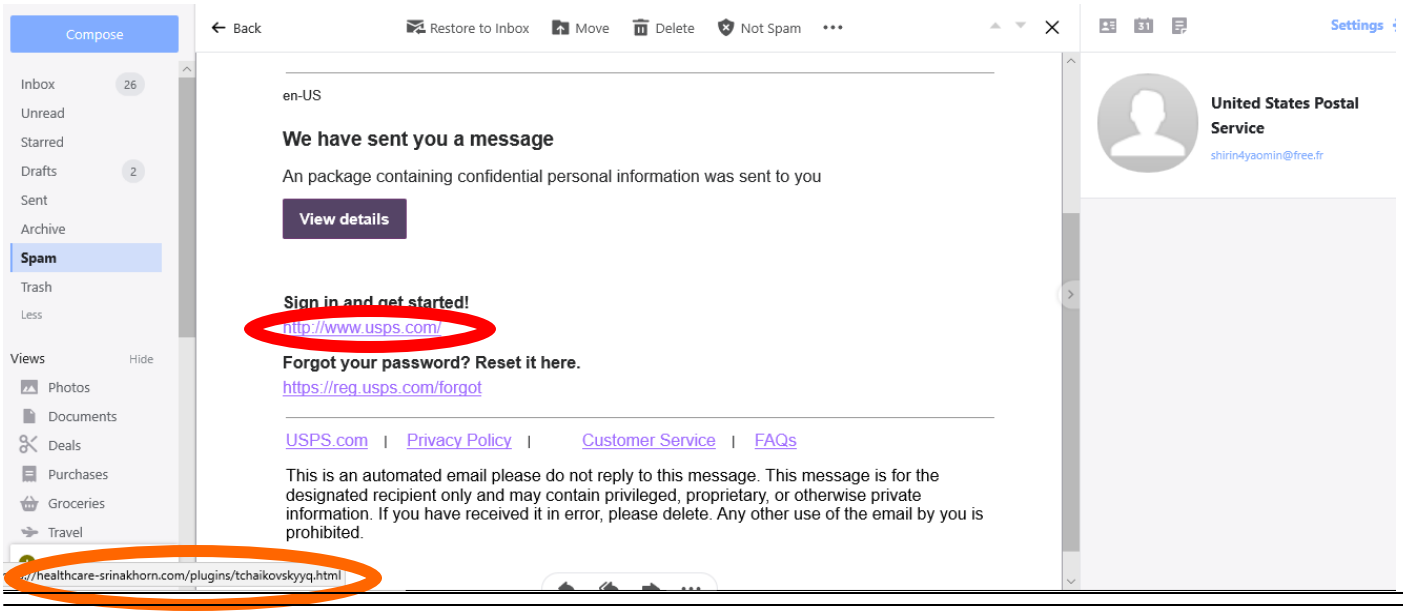
Microsoft announced the end date for Windows 10 Mobile support as it focuses on Android and iOS. The final end date for Windows 10 Mobile support: December 10th, 2019. The last major release of Windows 10 Mobile occurred in October 2017, and Microsoft has only provided security updates since that time. Microsoft *recommends that customers move to a supported Android or iOS device.* Microsoft is winding down its Windows 10 Mobile operations and beefing up its apps and services for Android and iOS. Microsoft apps/services like Bing, Cortana, OneDrive, Office 365, Xbox, Edge are readily available for Android and iOS.

Microsoft has made no bones about embracing subscription services for their products. Office 365 has largely phased out its perpetual licensed counterpart - e.g. Office 2019 - by enticing users with a low up-front cost, continual updates, and additional perks utilizing Microsoft's cloud services

Stop using Internet Explorer. Use more modern browser such as Edge, Firefox, Chrome,

If you find you have problems with certain web pages, try accessing the page with a different browser (e.g., Edge, Firefox, Chrome, Safari). You might consider having more than one browser on your taskbar to facilitate the change. Also, if you have a problem reading a file such as the PDF file used for this newsletter, try reading the file with a different PDF reader. Default applications for accessing different file types can be set by typing **Choose a default app for each type of file** in the search box at the bottom left of the screen and then scrolling down to the name of the file extension (e.g., .PDF) to see your choices to read that type of file. We have found **Adobe Reader DC** works well with reading our newsletters. If you don’t have Adobe Reader DC, you can download it at no cost at *https://get.adobe.com/reader* .

Email Scam Example Below is an image of a scam Amazon Order Status Email that indicates it was sent by the US Postal Service. A quick way to show it is a scam was to put the cursor over the link in the red oval below. The address that then displays in the status bar in the orange oval below shows the true link is bogus and not to usps.com.



Planned RENAISSANCE COMPUTER CLASSES – Summer 2019

The following computer classes are planned for inclusion in the next *Renaissance* publication. They are provided so you can decide what classes you want to attend before needing to wait until the *Renaissance* publication is distributed, can be ready to sign up when sign-up is available, and can avoid scheduling activities such as doctors' appointments when you want at attend a class and you have some flexibility in setting up your appointments. **As always**, schedules are subject to change and the information below is our best information at the time of the publication of this newsletter.

There is no charge for any of these classes. **Register using Event Registration. Classes are in the Cultural Center Education Room unless otherwise noted.**

Note: For the Summer 2019 Renaissance Classes we have three new classes:
(1) Windows Speech Recognition
(2) Safe and Effective Internet Search
(3) Apple Security

Gmail - Questions and Answers

This class is being presented in a new format where early registrants will be sent an email asking for email responses with questions about Gmail matters they would like covered in the class. The class will then focus on those questions, first received, first covered. If time permits, other questions may be raised and other information presented. Please verify you have a good email address in the online Resident Phone Directory.

Wednesday, June 5th
1:30 pm – 2:30 pm
Presenter: Sid Paskowitz, Spring Run Resident

Planned Computer Classes (Continued)

Apple Security
Security is a big issue today as hackers become smarter and more sophisticated in their attacks on us. This presentation will offer pointers on how to stay safe while using an Apple device whether it is a desktop, laptop, iPad or iPhone.
Monday, June 10th
1:30pm – 3:00pm
Presenter: Steve Lynn, Manor Resident

Just the Basics
Already know how to use Email and browse the Web, but want to know more and to prepare for using programs such as Word, PowerPoint, and Excel? Then this class is for you.

We'll review some basic things such as how to properly turn off the computer, the Windows desktop, working with windows, and safely removing a USB drive. Then we'll cover working with files and folders, and how to open programs. And finally, how to find answers to your questions and what to do when something goes wrong. Even though Windows 10 will be used for the class, the concepts apply to Windows 7 and 8.
Thursday, June 13th
1:30 pm – 2:30 pm
Presenter: Tony Poulos, Spring Run Resident

Safe and Effective Internet Search
The Internet has trove of information - good, bad and ugly!
We will show you a few searches you can do safely using the Google search Engine. Google is the search engine on the public computers used throughout Willow Valley. The goal of this course is to teach some techniques to speed your basic searches like definition of words, news, vacation spots, and more. In addition, we will share some safety measures while searching.
Monday, June 24th
10:00 am – 11:30am
Presenters: Carolyn Bugel, Spring Run Resident and Jay Shah, Manor North Resident

Microsoft Word – Questions and Answers
This class is being presented in a new format where early registrants will be sent an email asking for email responses with questions about Microsoft Word matters they would like covered in the class. The class will then focus on those questions, first received, first covered. If time permits, other questions may be raised and other information presented. Please verify you have a good email address in the online Resident Phone Directory.
Monday, July 8th
1:30 p.m. – 2:30 p.m.
Presenter: Sid Paskowitz, Spring Run Resident

Planned Computer Classes (Continued)

Windows Speech Recognition
Due to popular demand, this class will cover the presentation made at the February 7, 2019 Computer Club meeting for those who were unable to attend or have questions about Windows Speech Recognition. Windows Speech Recognition can be a powerful assistance tool if you have dexterity problems, limited typing skills or hand tremors.
Tuesday, July 16th
1:30 p.m. – 2:30 p.m.
Presenter: Sid Paskowitz, Spring Run Resident

Understanding TiVo
The TiVo is the Digital Video Recorder of choice and is becoming more popular with Residents. If you already have one, this class will show you how to use it to its fullest by looking at features you may not be aware of such as options for displaying the Guide, showing just your favorite channels, using the Wish List, accessing premium services, and more.

If you're just curious about how a TiVo could be helpful to you, then this is your chance to learn more about it. You'll see the great program guide, how to easily replay dialog you may have missed, skip through commercials, and how to always record a program when it's shown even if you're not at home.

The class includes the basics of installation, basic use, and several intermediate and advanced features. Bring your questions! We'll try to supply the answers.
Wednesday, July 24th
1:30 pm – 2:30 pm
Cultural Center Theatre
Instructor: Tony Poulos, Spring Run Resident

Windows 10 – Questions and Answers
This class is being presented in a new format where early registrants will be sent an email asking for email responses with questions about Windows 10 matters they would like covered in the class. The class will then focus on those questions, first received, first covered. If time permits, other questions may be raised and other information presented. Please verify you have a good email address in the online Resident Phone Directory.
Monday, August 5th
1:30 p.m. – 3:00 p.m.
Presenter: Sid Paskowitz, Spring Run Resident

Managing the Modem and Router in Your Network
Computer, tablets, smartphones, and electronics of all types are dependent on connecting to the Internet. How does your home network work? This class will provide modem, router, and network basics. You will also learn troubleshooting tips useful when your home network is not working correctly.
Thursday, August 22nd
10:00 a.m. – 11:00 a.m.
Presenter: Tom Fleischmann, Spring Run Resident

Planned Computer Classes (Continued)

Individualized Quicken, Family Tree Maker and Ancestry.com Program Training
Individualized instruction is offered to persons who have mastered computer basics and are seeking a program for maintaining financial records. Learn how to download your banking information and more. The Quicken program will give you the ability to manage your financial records. Family Tree Maker and Ancestry.com are programs designed to help you learn more about your genealogy using your own computer. **Use your own computer on dates scheduled between student and instructor after registration**.
Instructor: Bob McRobbie, Manor Resident

Individualized Help with Word, Excel, and Power Point for Intermediate and Advanced Users.
The Computer Club is offering individualized instruction for Word, Excel and Power Point to intermediate and advanced users. You choose the topic; they provide the instruction. Experience with the basic functions of the software is a prerequisite. **Use your own computer on dates scheduled between student and instructor after registration**.
Instructor: Carolyn Bugel, Spring Run Resident

Some input from readers

How to Install and Manage Extensions in Chrome from Jay Shah

Check out https://www.howtogeek.com/406829/how-to-install-and-manage-extensions-in-chrome/

Google Confirms Serious Chrome Security Problem - Here's How To Fix It from Jay Shah

https://www.forbes.com/sites/daveywinder/2019/03/07/google-confirms-serious-chrome-security-problem-heres-how-to-fix-it/

WVGuest Security

Recent questions about the security of using WVGuest in accessing websites such as banking or brokerage accounts have resulted in our sharing the following information: **If you are using an up-to-date browser and you are accessing a web address that starts with HTTPS://, the information you send and receive is encrypted but may not be completely secure.** Wikipedia states "A site must be completely hosted over HTTPS, without having part of its contents loaded over HTTP—for example, having scripts loaded insecurely—or the user will be vulnerable to some attacks and surveillance. Also having only a certain page that contains sensitive information (such as a log-in page) of a website loaded over HTTPS, while having the rest of the website loaded over plain HTTP, will expose the user..." The bottom line is you are somewhat secure with a WVGuest Wi-Fi connection so long as your browser and the web pages you visit meet these criteria; however, for better security, we strongly encourage the use of a VPN described elsewhere in this Newsletter.

The two articles on the following pages were provided by Al Williams and are re-published with permission of The ProtonVPN team and ProtonMail team. Al has added the following comments: Much of what is said in these articles has already been said by the Club. Note, however, that 2FA (two factor authentication) is becoming more and more important as a way to avoid password problems. Also, note the emphasis on encrypting communications and the data on devices as well as avoiding the sharing too much information on social media. You may think the information in these articles is overwhelming. However, the start to putting good security into practice is becoming familiar with the problems.

(Note: if text is too small for comfortable reading, copy and paste into a word processor and set the text size at a comfortable level.)

12 mistakes that can get your data hacked – and how to avoid them

Posted on August 24th, 2018 by Richie Koch in Privacy & Security, Security. Whenever you store or transmit data online, there is a risk of getting hacked. However, there are actions you can take to protect yourself. Here are 12 common mistakes that can jeopardize your online data, along with simple fixes.

Along with the unprecedented convenience of the Internet has come the increasing risk of hacks and identity theft. Every day there are new examples of an individual or organization suffering a major cyber-attack, and each attack offers a warning to the rest of us. For instance, after the University of Michigan had three of its Facebook accounts hacked, they published a detailed breakdown of what happened. Their case study illustrates how one weakness can compromise an entire system.

As more of your data gets uploaded to the web, it is more important to safeguard yourself. We've compiled 12 of the most common mistakes that could compromise your data.

Reusing the same password While using the same password for all your accounts is convenient for you, it is even more convenient for hackers. Cracking one password would be enough to expose all of your data. Each account you own should have its own strong password. Given the difficulty of memorizing dozens of passwords, we suggest you use a reputable and encrypted password manager.

Not activating two-factor authentication In the worst-case scenario where a hacker learns your password, two-factor authentication (2FA) can still prevent them from accessing your account. With 2FA enabled, any login to your account will require your account ID, your password, and a special code, typically generated by an app on your phone. (Note: 2FA that relies on sending you an SMS is still not secure. See the recent Reddit hack.) A strong, unique password paired with software or token 2FA is the best way to secure your data.

Clicking on links or opening attachments from uncertain sources Phishing is one of the most effective ways hackers can penetrate security. A phishing attack is an attempt to trick you into giving up your credentials or downloading malware onto your device. The University of Michigan hack mentioned above began with phishing on Facebook Messenger. The infamous 2016 hack of the DNC began with a phishing email. If you receive a message from an unknown person asking you to click a link or download an attachment, inspect the URL and file closely. Sometimes the phishing email may even seem to come from somebody that you know. If anything seems suspicious, contact the person to verify they sent the email.

Not having an anti-virus or anti-malware program Having a reliable anti-virus or anti-malware program installed on your device is one of the basics of preventing online hacks. There are numerous services that will protect your device from malicious URLs, ransomware, and other threats. Many operating systems such as Windows come with free anti-virus included (Windows Defender).

Skipping software updates Developers release software updates in response to identified security vulnerabilities. If you are running outdated versions of programs, you are putting your data needlessly at risk. This applies to computers and mobile devices. To ensure you do not miss any updates, we suggest you enable these applications to update themselves automatically when possible.

Not using HTTPS It may seem like a small change, but the "S" at the end of the hypertext transfer protocol (HTTP) can make a big difference to your online security. The "S" means you will force the HTTP protocol to go through another protocol, the secure sockets layer (SSL), which will encrypt and transport your data more safely. Sites without HTTPS can expose your data to anyone monitoring their traffic. Fortunately, the EFF has a downloadable app that will force sites to use HTTPS whenever possible called "HTTPS Everywhere."

For those looking to add additional security, consider using a VPN to secure your internet data.

Not turning off AirDrop or Bluetooth Unless you are actively sharing files or paired with another device, your Bluetooth and AirDrop networks should always be turned off. Bluetooth exploits like BlueBorne can allow hackers to connect to a device undetected and then take control of it, even forcing it to send out sensitive data. However, this is only possible if your Bluetooth connection is left on. As a bonus, keeping Bluetooth turned off will improve the battery life of your device.

Using public WiFi without a VPN Even if you know who is running the network, public WiFi networks are rarely secure. They often lack proper protection protocols, leaving you exposed to man-in-the-middle attacks or WiFi sniffing. Both MITM attacks and WiFi sniffing can give hackers a window into your browsing history and let them read your keystrokes. Even worse, neither of these attacks is particularly complicated. But a very easy solution is to set up a VPN which will hide your data from attackers.

Not setting a screen lock or password protection To protect your data, physical security is just as important as network security. Smartphones and laptops go with you everywhere, meaning there are lots of opportunities for intruders to access them. Never leave your device unattended and set a password to help ensure hackers cannot install malware on your computer.

Not encrypting the data on your device Setting a password on your devices is a good first step, but pairing it with device encryption is the best way to secure your data if your device is lost or stolen. It is important to note that device encryption and setting a password are not the same thing. While both require a password, device encryption is a separate, additional step that prevents anyone from accessing data on your device without your password. Most Android and iOS devices come pre-loaded with encryption programs while Windows and Mac both support it.

Not using encrypted means of communication The Snowden revelations revealed that most of our means of electronic communication is subject to mass surveillance, including phone calls, SMS, and email. By using communication services that are equipped with end to end encryption, such as Signal or ProtonMail, you can ensure that no one other than the intended recipient of your message can access it.

Sharing too much information on social media Hackers can gain a lot of information simply by looking at your social media. Some of this information can then be used to reset passwords, apply for credit cards, or create more convincing phishing emails. The best option would be to set your Facebook profile to private. Otherwise, think twice when posting anything that contains the following information:

(1)Names of family members (especially your mother's maiden name) (2) Your date of birth (3) Where you were born (4) Where you went to college (5) Names of pets (6) Old or current addresses (7) Details about daily routines ——Hackers can use any of these to target you or to answer your security verification questions.

These are just some of the steps that the average person can take to significantly reduce the exposure of their online data. As more and more of your sensitive data is handled online, knowing basic cyber security skills becomes critical. None of these fixes require advanced knowledge of computers or programming, just a little discipline and attention to detail. Of course, even if you implement all of the safeguards we suggest here, we cannot guarantee you will be 100% secure — but you will have made it significantly harder for an attacker to access your data.

(See next page for author information)

Re-published by permission

About the Author

Richie Koch

Prior to joining ProtonVPN, Richie spent several years working on tech solutions in the developing world. As a senior editor and writer at Latterly, he covered and commented on international human rights stories. He joined ProtonVPN to advance the rights of online privacy and freedom.

Not everyone needs the same level of Internet privacy. This guide will help you determine your threat model and take steps to achieve online privacy that meets your needs.

Total Internet privacy is impossible, and any service that claims to offer it is lying. But anyone can increase their Internet privacy by adjusting their online behavior, like choosing privacy-focused online service providers and limiting the amount of information they store on the Internet.

Many Internet privacy guides promote unrealistic goals with inconvenient solutions, like using Tor all the time (which will slow your Internet) or communicating only through Signal encrypted messenger (which is useless unless your contacts are using it too). While such technologies provide a high level of privacy, they may not be necessary under your personal threat model. In other words, you probably don't need to take the same privacy precautions as a Turkish dissident or an NSA whistleblower. And the best privacy recommendations can be counterproductive if you burn out following them, like one writer for Slate did.

In this guide to Internet privacy, we'll show you how to understand your own threat model and take practical steps to protect your online privacy. At the end of the article, we also include our online privacy checklist.

Internet privacy is important for everyone

If you use the Internet at all, then privacy issues directly impact you. Without Internet privacy, someone can steal your credit card or even your identity, potentially causing problems for your credit score or at the very least inconveniencing you while a replacement card is shipped. Internet privacy keeps hackers from infiltrating your online accounts (you don't want to be this guy) and spying on your activity while using public WiFi.

As both citizens and users of the Internet, we all have a stake in the quality of our society. Privacy is a fundamental human right and a prerequisite for democracy. For authoritarian governments and profit-seeking companies alike, invasions of privacy are a useful means of control. If you value your freedom, then Internet privacy should matter to you.

Understanding your threat model

A threat model is a method of evaluating security and privacy risks in order to mitigate them strategically. You can define a personal threat model to understand your own Internet privacy priorities. Start by answering the following questions:

What information do you want to protect?

Who might want to gain access to that information?

Where is that information stored and transferred?

It helps to draw a diagram of the information, where it moves and rests, and who could gain access at each location. For instance, you have data stored locally on your devices. When you use online services, like email or web browsing, your data travels across the network and gets stored on servers that belong to those companies. Along the way, it could be exposed to people in your house, your Internet service provider, hackers, third party websites, or even governments.

Now that you know which personal data you need to keep private and from whom, you can start to protect it. In the next section, we list a number of steps to protect Internet privacy and what threats they mitigate.

Limit the information you share publicly

A lot of sensitive information about you is publicly available on the Internet. Some of it is a matter of public record, like court records, addresses, and voter registration. But much of it we put on the Internet voluntarily, usually via social media: photos (often location tagged), family members' names, work history, and a variety of clues about our daily lives.

Hackers can use these clues for social engineering and to answer security questions. Photos of you on social media can even be used to create deepfake videos of you. Almost all online services and Internet-connected devices have privacy settings you can update to restrict the amount of information collected and/or posted publicly online.

Limit the information you share privately

Online service providers can be vulnerable to data breaches, which can instantly compromise your privacy, sometimes in embarrassing ways. Even large services like Google or Facebook are not immune to data breaches. You can mitigate the privacy threat of data breaches by limiting the information you share with these services. For instance, you can use Google Chrome or Google Maps without logging into your account, or simply switching to a more privacy-friendly browser like Firefox.

If the services themselves (and their third-party partners) are part of your threat model, then you can switch to privacy-focused services that do not collect user data (and therefore cannot share it with third parties). With ProtonMail, accounts are anonymous (not linked to your real life identity), and we collect as little user information as possible. Unlike other email service providers, we also have no ability to read your inbox due to end-to-end encryption.

Learn more: How to protect your children's privacy online

Strengthen your account security

Your password is your first line of defense. Make sure you use strong, unique passwords. A password manager can help you generate and store them so that you don't have to write them down.

Your second line of defense is two-factor authentication (2FA). This is a way to secure your account with a second piece of information, usually something you have with you on your person, like a code created on an authenticator app or fob.

Avoid using public computers to access your accounts because these can be compromised by keyloggers. And if you absolutely must use a public computer, be sure to log out of your accounts.

Many services (such as ProtonMail and ProtonVPN) allow you to see when and from what IP address your account has been accessed and log out of other sessions remotely.

Protect your devices

Most threat models should include the possibility of your device getting stolen or lost. So it's important to also have strong passwords protecting your devices. There are apps that allow you to wipe, locate, and potentially identify the thief if your device is stolen.

Another important part of protecting your device is maintaining its software. You can help prevent attackers from installing malware on your device by keeping your apps and operating systems up to date. Software updates often include security patches for recently discovered vulnerabilities. You can also use anti-virus software.

If your device somehow is compromised with spyware, a low-tech privacy solution, ironically popularized by Mark Zuckerberg, is to cover your webcam with a piece of opaque tape

Learn more: How to protect your phone or computer when crossing borders

Practice email safety

Email is one of the easiest ways for hackers to get into your computer. So it's important to be alert for phishing attacks, in which the attacker tries to trick you into clicking on a link, downloading an attachment, or giving up sensitive information (such as entering your username and password into a spoofed webpage).

Learn more: Five essential steps to keep your email safe

Use encryption as much as possible

Encryption is the process of converting readable information into an unreadable string of characters. Without encryption, anyone monitoring the Internet could see the information being transmitted, from credit cards to chat messages. The vast majority of online services use some form of encryption to protect the data travelling to and from their servers. But only a few tech companies encrypt your information in such a way that even the company cannot decrypt it. This kind of encryption is called end-to-end encryption(E2EE). Whenever possible you should use services that offer E2EE because your privacy is protected by default.

Often, there is an E2EE alternative to less private services. For example, ProtonMail is a private alternative to Gmail. Instead of Google Drive, which can access your files, you could use Tresorit. DuckDuckGo is a private alternative to Google Search, and Brave is one example of an Internet browser that doesn't track your browsing activity. For notes, Standard Notes is one E2EE option.

For instant messaging, you have a number of options. WhatsApp is one of the most popular chat apps, and it features E2EE. But Facebook (which owns WhatsApp) can see who you communicate with and when, and there may even be ways for Facebook to gain access to your messages if it wanted to. Facebook Messenger is not E2EE by default. WeChat offers no E2EE. For better chat security and privacy, we recommend using Wire or Signal.

For web services that are not E2EE, you should at least ensure that your Internet connection is encrypted from your device to the company's servers. You can check that this is the case by making sure the URL of the website begins with "https". There's a browser plugin called HTTPS Everywhere to help you do this automatically.

Learn more: What is end-to-end encryption?

Use a virtual private network (VPN)

A VPN encrypts your Internet connection from your device to the server owned by your VPN service provider. Using a VPN can help keep your web traffic safe from anyone monitoring the network at the local level: hackers, your Internet service provider, and surveillance agencies. A VPN will also mask your true location and IP address, allowing you to browse more privately and access geo-restricted content.

A VPN will not, however, protect your web traffic against the VPN provider. That's why it's important to choose a VPN service you trust that does not keep logs of your activity. ProtonMail also provides ProtonVPN, a specialized high-security VPN service.

Learn more: Your Internet service provider is spying on you

Use Tor

If your threat model requires a very high level of Internet privacy, you should connect to the Internet through Tor. Tor is a technology maintained by the nonprofit Tor Project, which allows you to use the Internet anonymously. It works by bouncing your connection through multiple layers of encryption, both protecting your data and concealing its origin. Tor also allows you to access blocked websites (such as those offering E2EE services) via the dark web. However, the downside of Tor is that it is generally significantly slower compared to using a VPN.

Learn more: How to use ProtonMail with Tor

Internet privacy checklist

– Check your public social media profiles for sensitive personal content.

– Adjust the privacy settings on your online accounts.

– Use a strong, unique password for all your accounts.

– Update security settings and enable two-factor authentication.

– Inventory your online service providers and determine if there is a viable private alternative.

– Install software updates for all operating systems and apps.

– Review email safety practices and be alert to phishing attacks.

– Start using end-to-end encrypted services.

– Install the HTTPS Everywhere browser extension.

– Connect to a trusted VPN.

– Connect to Tor.

We hope this guide has helped to simplify your Internet privacy efforts.

At ProtonMail, we believe a more private Internet is possible, but it will require a major shift from the Internet's current ad-based business model. With your support, we will continue to develop tools that enable privacy, security, and freedom online.

Best Regards,
The ProtonMail Team

*You can get a **free secure email account from ProtonMail here**.*

*We also provide a **free VPN service** to protect your privacy.*

*ProtonMail and ProtonVPN are funded by community contributions. If you would like to support our development efforts, you can upgrade to a **paid plan** or **donate**. Thank you for your support!*

About the Author

Irina M

Irina is part of ProtonMail's communication team. With a background in graphic design and digital communications, she strongly supports the protection of private data and wishes to help build a safer internet for generations to come.

ProtonVPN:

ProtonVPN is a highly secure, community-supported VPN service from the creators of ProtonMail, the world's largest encrypted email provider. Our mission is to make secure and private Internet browsing available to all. Our free VPN plan is the only one in the world with no privacy invading ads, no malware, no logs of user activity, and no bandwidth limits. We provide IP addresses in 30 countries and counting. ProtonVPN is headquartered in Geneva, Switzerland, home to some of the world's strongest privacy laws.

ProtonMail:

ProtonMail is the world's largest encrypted email provider. Developed in 2014 by CERN physicists and engineers, ProtonMail makes secure encryption easy and accessible to everyone. Our mission is to protect the universal right to privacy to which all citizens are entitled. ProtonMail is headquartered in Geneva, Switzerland, home to some of the world's strongest privacy laws.

by **Brandon Hill** — Thursday, April 04, 2019 in HotHardware.com

Microsoft Announces Windows 10 May 2019 Update And Gives Users Control Over Updates

Microsoft has announced that official name of the next major release of Windows 10. And unlike previous reporting which suggested an April launch, it will actually be called the Windows 10 May 2019 Update.

The latest update to Windows 10 will bring new sandbox functionality and will decouple the Cortana digital assistant from Windows Search. However, perhaps one of the biggest changes to Windows 10 will come in how much granular control that users will have over the update process. This latest move is no doubt a side effect of the immense negative backlash that was unleashed on the Windows 10 October 2018 Update after a laundry list of epic fails.

Under previous Windows 10 versions, Microsoft would automatically push a major update to systems when its telemetry data "gave us confidence that device would have a great update experience." However, instead of continuing to force updates on its users, Microsoft says that it will instead provide a popup notification to let users know that a new major update is available and if the install is recommended based on your current system configuration.

The actual option to install the update will be left completely up to the user – *in most cases*. Microsoft will still force an install of a major feature update for Windows 10 if your current version will soon be reaching end-of-support status. While users will be able to hold off on installing major updates, Microsoft will still automatically push monthly security updates to ensure that systems are protected against fresh threats.

Microsoft will also enable users to pause all updates for up to 35 days (a week at a time, up to five times). This will apply to all versions of Windows 10.

In addition, Microsoft is taking big steps to ensure that the quality of its Windows 10 releases is improved over previous releases.

"The final May 2019 Update build will spend increased time in the Release Preview Ring of the Windows Insider Program, allowing us to gather more feedback and insights on compatibility and performance at scale before making the update more broadly available," Microsoft writes. "With a more robust and longer Release Preview and further investments in machine learning for both high-severity issue detection and our next generation of intelligent rollout, our goal is to provide the best, transparent Windows update experience."

According to Microsoft, the Windows 10 May 2019 Update will be made available on the Release Preview ring starting next week, and will be available to the general public next month.

The following edited article from HotHardware.com provides insight as to why the Computer Club suggests the use of recommended software and not software with which we are not familiar:

by Brandon Hill - Fri, Apr 12, 2019

Microsoft's April Patch Tuesday Updates Are Freezing Windows PCs, Here's How To Fix It

Earlier this week, Microsoft issued another round of monthly "Patch Tuesday" updates, but things didn't go so swiftly for those that have Sophos Endpoint Protection installed on their systems. Sophos acknowledged the problem.