THE WYSIWYG

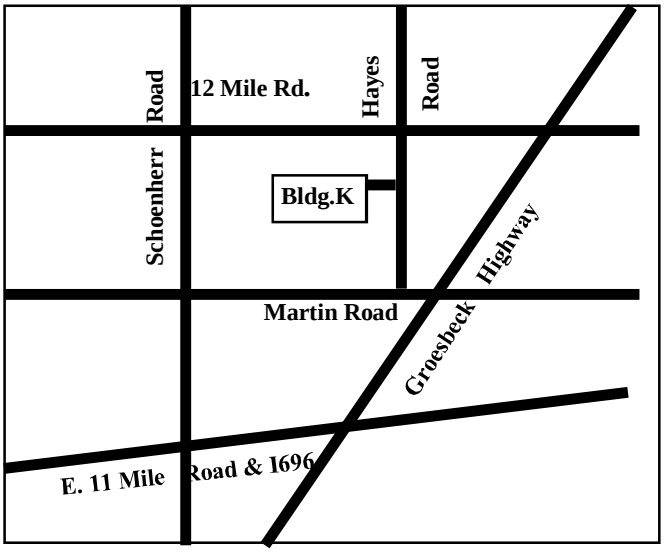
December 2017 Volume 29, Issue 10

STERLING HEIGHTS COMPUTER CLUB

PO Box 385
Sterling Heights, MI 48311-0385

$3.00

MAIN MEETING: TUESDAY DEC 5
6:30 PM
Macomb Community College
South Campus
14500 E 12 Mile Road, Warren
John Lewis Community Center (Building K)
[Second floor - left from steps or elevator]



Election for club Treasurer in December. (See page 3.)

IN THIS ISSUE:

This Month's Main Meeting Topic:

"Teach Yourself To Fly A Drone - Step By Step" by Dr. Robert Meier

The January club meeting will be on January 9, the second Tuesday of the month. MCC, and thus the meeting room, will be closed the first Tuesday in January.

Guests and visitors are welcome. People can attend any SHCC meetings during two consecutive months before deciding to become a member or not. Meetings include the main meeting and SIG. July and August don't count since there is no main meeting. Membership includes admission to all SHCC functions and the newsletter. Membership is open to anyone. It is not limited to the residents of Sterling Heights.

DUES: $25/YEAR

CLUB ADDRESS: PO Box 385, Sterling Heights, MI 48311-0385
CLUB E-MAIL ADDRESS: Info@SterlingHeightsComputerClub.org
CLUB WEB PAGE: http://www.SterlingHeightsComputerClub.org

Resource People:

Family Tree	Rick Schummer
Firefox	Don VanSyckel
FoxPro	Rick Schummer
General Computer Questions	Jack Vander-Schrier
Hardware	open
MS Publisher	Rick Kucejko
MS Word	Rick Schummer
Spreadsheets	Rick Schummer

SHCC Coordinators:

Associate Editor	Rick Schummer
Door prizes	Don VanSyckel
Greeter for visitors	Jim Waldrop
Newsletter publisher	Rick Kucejko
Program Coordinator	Mike Bader
Publicity	Patrick Little
Resource People	open
Welcome & check-in desk	Jim Waldrop
Web Site	Don VanSyckel
Web Watch column	Paul Baecker

2017 SHCC Officers

President: Don VanSyckel
V. President: Mike Bader
Secretary: Rick Kucejko
Treasurer: Paul Baecker

Four Month Meeting Schedule:

DECEMBER 2017

5 - SHCC - "Teach Yourself To Fly A Drone - Step By Step" by Dr. Robert Meier

6 - COMP meeting
10- SEMCO meeting

JANUARY 2018

9 - SHCC - "Home Security And Automation" by Derek Bricknell of the Madison Heights Best Buy store

3 - COMP meeting
14- SEMCO meeting

FEBRUARY 2018

6 - SHCC Main Meeting

7 - COMP meeting
11- SEMCO meeting

MARCH 2018

6 - SHCC Main Meeting

7 - COMP meeting
11- SEMCO meeting

Other Computer Clubs:

As a member of SHCC, you can attend meetings of other clubs where we have reciprocating membership agreements, at no charge.

Computer Club of Marysville and Port Huron (COMP)
Time: 1st Wednesday, 7:00PM
Place: Mackenzie Bldg, Room 201, St Clair Community College, Clara E McKenzie Library-Science Building, 323 Erie St.
Port Huron, MI (810) 982-1187
Web Page: http://www.bwcomp.org
Reciprocating: Yes

South Eastern Michigan Computer Organization (SEMCO) (new location)
Time: 2nd Sunday at 1:15PM
Place: Bloomfield Township. Library, 1099 Lone Pine Rd., Bloomfield Hills, MI 48302
Web page: http://www.semco.org
Reciprocating: Yes

Royal Oak Computer Club
Time: Every Wednesday at 12:30
Place: Mahany/Meineger Senior Community Center 3
500 Marais Ave. Royal Oak, MI 48073
248-246-3900
Reciprocating: No

Contact Information:

Paul Baecker	586-286-2314	webwatch@sterlingheightscomputerclub.org
Mike Bader	586-447-6683	mdbader@flash.net
Bernie DeFazio	586-864-6558	berniede1@wowway.com
Rick Kucejko	248-879-6180	rick@kucejko.com
Patrick Little	586-264-1497	pblittle@wideopenwest.com
Rick Schummer	586-254-2530	rick@rickschummer.com
Don VanSyckel	586-731-9232	don@vansyckel.net
Jack Vander-Schrier (**Call Jack after noon)**	586-739-5952	jvanders@comcast.net

Newsletter submissions are due 10 days before the club meeting, but the earlier the better. They should be sent to : newsletter@SterlingHeightsComputerClub.org

The President's Pen

by Don VanSyckel

The weather's turning nippy so it looks like winter is coming. Things continue to move along in the computer and electronics world. In particular, in the 'small electronics' world. The Raspberry Pi, UNO, Arduino, Beagle Bone, Bit Go Kit, ASUS Tinker Board, and Mega DIY Kit to name a few. Then there are several variations of the Raspberry Pi and the Arduino covering both the board features and the manufacturers.

There are a number of accessories for the various boards and kits. There are power supplies, cases and boxes, and other input/output type peripherals to connect to stuff.

It's a good idea to investigate the different boards and kits available. Have in mind what you want to do with it, then also check out the available software. Much of it is open source or free to download. There is software available to do many things. As always, some software packages are better that others. Some of the software that's available include:

- Artificial intelligence
- Bit Torrent server
- Camera control
- Drone controller
- Educational programs
- Firefox OS
- Games
- Libre Office
- Media center
- Open GL 3D hardware graphics
- Pi-Hole, network ad blocker
- Robotics
- Solar panel battery charger controller
- Ubuntu Linux
- Video capture
- Voice HAT (similar to Amazon Echo)
- Voice recognition
- Weather station
- Web server
- Web browser

Some of the software is available on some boards and other software is available on other boards. So unless you're writing your own software, choosing which board to buy should include consideration of the activity you want to do and what software is already available to do it.

Make sure to plan for the power supply and a case to protect the board plus the connections to whatever you are having it connect to.

The December meeting will be timely. "Teach Yourself To Fly A Drone - Step By Step," presented by Dr. Robert Meier. Come see how it's done, then put a drone on your Christmas list. Maybe Santa will drop one off.

Treasurer Election - December Meeting

The club needs to have a treasurer for the operation of the computer club. There were no nominations for the position in November, for this important club position.

The treasurer duties were outlined in previous newsletters. For any additional questions, contact Paul Baecker at: **treasurer@sterlingheightscomputerclub.org**

Also the treasurer gets to attend the monthly officers' meetings, where all the "big decisions" for the club are discussed and the final decisions are made. These officers' meetings are fun, and are a large perk for the position. They are now held at "Don's house."

Please consider filling this important need for your computer club. You will likely enjoy the time.

Door Prizes

Door prize drawings are held at regular club meetings. The winner's circle for November included:

Bill Appleberry won the raffle for the laptop

Richard Jackson won an Office 13 book

Phil Reynaud won a pack of DVD-R discs

Martee Held won a 7-function miltitester

Ron Linsley won a wireless optical mouse

Irene Kramer won a CD/DVD holder

Richard Monk won a pack of DVD discs

Mike Bader won a Sata HD 160GB hard drive

Bill Kramer won an 80 GB hard drive

Paul Baecker won Quicken Deluxe software

Ken Belbot won Trapper Keeper for a notebook

Ralph Osinski won office 2003 software

Last Month's Meeting

Mr. Richard Tapaninen from Micro Center in Madison Heights was our presenter. Mr. Tapaninen had presented several times before and again had an interesting and informative presentation. The topic was "What's Hot For The Holidays" and was of interest to everyone. Visit Micro Center this season to see all the new interesting products.

What The "KRACK Attacks" Mean To You

From the Ask Leo Newsletter
https://askleo.com

Recently, a vulnerability was disclosed in the WPA2 security protocol that, in the worst case, could allow an attacker to potentially gain access to some or all of the encrypted information transmitted over a Wi-Fi connection.

This isn't a bug, and it's not a failure of one manufacturer or another. This is a weakness in the protocol itself.

If you use Wi-Fi on any device, it's worth understanding how big of a risk this might be, and what steps, if any, you might want to take.

The steps to take, if you need to take them
The single biggest mitigating factor for the average computer user is that this is a *wireless* vulnerability, and therefore requires proximity. You need to be using a Wi-Fi connection, and the attacker needs to be within wireless range of your computer.

If you don't use Wi-Fi, this is a non-issue. Nothing to see here. Move along.

If you do use Wi-Fi, then understanding your common surroundings is important. If you're in some isolated area where, like me, anyone close enough to listen in to your Wi-Fi would be obvious and out of place, it's possible you don't need to take any additional steps other than updating software, which I'll discuss below.

If, on the other hand, someone's within range, and particularly if you consider yourself or your business a potential target, then there's something you might want to do until the problems gets fixed: treat your wireless connection as if it were an open Wi-Fi hotspot with no encryption at all. In this case, that generally means:

- Use https wherever possible.
- Avoid sites that don't use https.
- Consider using a VPN.
- Consider using your mobile device's data plan instead of Wi-Fi in sensitive locations.
- Or, if you can, switch to a wired ethernet connection.

The steps you need to take regardless
As it turns out, this is a relatively easy problem to address in software. As a result, most major manufacturers are pushing out updates that will fix the issue. Once your software is updated, you're protected.

Take those updates as soon as they're available. Bleeping Computer reports that for Windows 10, at least, your system may already be fixed, as the update was apparently silently included in the most recent patch Tuesday. That fact was only revealed when the vulnerability itself became public. (Sadly, this comes on the heels of a Windows Update problem causing many people to try to avoid updates. When it's available, this is an update you *want*.)

This applies to any and all devices that use Wi-Fi.

And therein lies a different problem: not all devices will be updated.

Updates on older devices
It's unclear if Windows XP or Vista will get fixes for this. It's pretty clear older versions of MacOS and Linux may not get updates. In short: if your operating system doesn't get security updates now, it's probably not going to be updated for this protocol vulnerability. You'll either have to live with it (see "steps to take" above) or update to a newer OS or device.

And yes, I said "device". One of the areas considered particularly problematic is that of Android tablets and mobile phones. Almost all are at the mercy of the mobile company from which they were purchased, and many of the older models still in use are not getting updates of any sort. Some will get updates quickly, and some not at all. It'll be important to know which boat you're in.

When it comes to TVs and IOT devices, it's unclear when, how, or even if they'll ever be updated, and what the ramifications of that might be.

This is about clients, mostly
One final point: the fixes apply mostly to Wi-Fi clients — the computers and other devices you use which connect to the network wirelessly. Wireless routers and access points, as I understand it, may not be impacted in the same way. Nonetheless, be on the lookout for updates to your router or access point's firmware related to this issue.

There's one specific case that *is* impacted, and that's a wireless range extender or repeater. These act as both clients and access points. Since they act as clients, connecting to another wireless router or access point, they would likely be vulnerable to this issue. You'll want to update their firmware as soon as the manufacturer makes a fix available.

This article is republished, with permission, from the Ask Leo! Newsletter.

Rational Backup Strategy

by Dick Maybach, Brookdale Computer Users' Group, NJ
www.bcug.com n2nd@att.net

In developing a plan to defend against the loss of data and software from operator, hardware, and software failures and malicious acts, it's important to take a systematic approach rather than responding to the latest sensational article or alarming ad. Your first step should be to identify the threats. Otherwise, you could end up with a Maginot Line, an expensive defense against an attack that didn't occur and was ineffective against the one that did.

Common threats to PCs and the information they hold include the following:

- Operator errors are common. You mistakenly delete a file, a directory, or an entire partition. If this involves your software, it may disable the PC.

- Software sometimes contains coding errors that create problems, which if serious enough can crash the operating system. Simply repairing the resulting damage doesn't cure the root cause. However, often symptoms appear only under rare conditions, which means you can only repair the damage and hope these don't recur.

- Hardware malfunction often immediately disables the PC, and the solution is to repair the failure and then restore any damaged data. Some problems, such as intermittent RAM failure can be difficult to identify and may require a visit to the shop. Disk failure is common and this requires replacement of the disk and then restoration of the software and data it held.

- Malware is software that is designed to cause damage. Individual programs acquire colorful names, such as virus, ransomware, rootkit, and Trojan horse. Each newly discovered name results in a new commotion, but the remedy is the same for all – remove the malware and then repair the damage. A worry here is that the malware may reside for some time before damage appears, so that you back up the problem as well as your software and when you restore from a backup, you also restore the malware.

- PC loss can occur when traveling with a laptop or when one fails to the extent that repair isn't economically practical. You must replace not only the hardware, but any original equipment manufacturer (OEM) software that is licensed only for the lost machine. You can restore only your data from backup.

- Environmental catastrophe most commonly results from burglary, fire, storm, or flood. Here you lose not only the PC, but perhaps all the material associated with it, including documentation and backup media. At some level, perhaps nuclear holocaust or asteroid strike, you probably decide you don't care as the loss associated with your PC is trivial compared to other damage.

You will surely find that no single approach will protect against all of these, and you may decide to ignore some threats.

You have two software and data repair approaches:

1) reinstall from the original sources or
2) recover from a snapshot of your disk taken previously.

Only the latter is possible with data. The receipts needed to recreate your 2012 tax return are long gone, as are the vacation photos on your camera's SD card.

However, with software, you have choices.

Use the original distribution media to create a fresh installation, configure it, and apply any updates for the OS and all the applications. This is tedious, but the result is a clean system, free of whatever problem (assuming it's not with your hardware) that corrupted your system. Most PCs are delivered with the operating system already on the disk and without its installation media. They have instructions on how to create a repair disk, although you may have to dig to find them. Most also have a recovery partition on the disk that you can use to recreate the initial configuration.

In my experience, the hard disk is the PC component most likely to fail, which of course makes the recovery partition unavailable. The software supplied with a PC is almost certainly sold as OEM products, which means it is licensed only for that hardware, and it often includes a feature to prevent it from being used elsewhere. As a result, you need a separate set of recovery media for each PC, and you need to be able to identify to which hardware each set belongs.

Recovering the software from a backup is far simpler, because it restores all the software in one step, which has already been configured and updated. However, if the failure was the result of a developing software problem, you also install its root cause. For this reason, many keep backups made at different times, hoping that if they go back far enough, they'll find a clean one. Of course, when you restore an old backup, you most likely also restore your old data, destroying any acquired since. Your recovery plan must include a remedy for this.

There are several choices of backup media:

1. a backup directory on your system disk,

2. a backup partition on your system disk,

3. a separate internal backup hard disk,

4. an external backup disk, and a cloud service.

Only hard disks and cloud services have the capacity to back up modern disks. Optical media capacities have not kept up with those of hard disks, and far too much of it has poor reliability. Cloud service adds security concerns, both because your data travels over the Internet and because you have entrusted it to an outside entity.

As with the backup medium, you have choices about what to back up. These include:

1. a complete disk image,

2. all the data files in the home directory, and only those data files in the home directory that have changed since the last backup.

Some strategies include backing those OS and application files that have changed, but this can be risky, as these often depend on each other. If you replace a file but not something with which it interacts, the result can be an inoperable system. With software, it's safer to replace everything.

Some backup program developers recommend that your PC have constant access to the backup medium. While this insures that all your data is backed up as soon as its created, it also insures that malware also always has access to the backup. This is a good scheme for protecting against operator error, but less so for protecting against malware and software errors. For the latter, you want your backup medium to be accessible for only very short periods of time. You may decide to use two methods, one that backs up continually to protect against operator error, which are common, and a second that backs up only periodically to protect against such threats as malware.

Backup software is a poor area in which to experiment. Obtain it from well-known vendors with good reputations. Consider only products with favorable reviews from responsible experts. Microsoft includes a suite of recovery software with its operating systems, and you should have a good reason for using something different. I discussed their Windows 7 version of this in the February 2012 issue of BCUG Bytes and the Windows 10 version in the May 2016 issued, available at www.bcug.com.

After obtaining your choice, test it as best you are able. For a thorough test, you would have to erase your disk and restore a backup, but don't do this. Instead, make a copy of just one file or directory; then backup, delete, and restore it. Compare the original and restored versions. If the recovery software includes a bootable disk, test it on the PC where you will use it to be sure it does boot. This will probably require that you make some changes in your BIOS. Record these before you change them back, as frequently, the BIOS settings must be different for internal disks and external media.

You may also wish to obtain and test a reliable repair utility disk. If you suspect a virus infection, you can boot with it and the virus won't be active. This will allow you to copy your data files to an external drive without its interference. I discussed some of these tools in articles in the April, June, July, and August 2012 issues of Bytes.

My strategy is that every week I have a scheduled backup of all the data files that have changed since the previous backup. This is to an internal hard drive, separate from my system and data drives. As a result, I limit my loss from most causes to the data I generate in one week. Once a month, or when I think of it, I back up to an external

hard disk, all the data files that have changed since my last external backup.

My operating system is Linux, and I have its installation USB memory stick. Almost all my applications are available from the distribution's repositories. As a result, it's convenient to restore all my software as a fresh install, and I do this every two years, even if I have no problems, just to clean out the accumulated cruft. Reviewing this plan against my list of threats, we see the following:

- An operator error can destroy at most a week's work.
- Similarly, most software errors and hardware failure can delete up to weeks of work. Although if one affects both the service and the on-line backup disk, I could lose up to a month's worth, but this is very rare.
- Malware could cost me up to a month, if it affects all the disks. But malware in Linux is uncommon and, so far, I have not had this problem.
- Although I do have a laptop, I transfer any data to my desktop as soon as I get home. As a result, losing it would lose only the data acquired on that trip.
- The weak point in my plan is environmental catastrophe, as all my PC gear resides in one room, and I could lose all of it in one incident. I could improve it by adding a backup file server to our home network and locating it in the basement or better by storing a backup drive at a neighbor's or in my bank deposit box or using a cloud storage service.

You should make a similar assessment of your backup plan against your own list of threats to see if it needs adjustment.

Your recovery approach of course depends on what is damaged. Your data resides in what is often called the home directory, and this can be restored only from a data backup. However, Windows may store some of your data (such as Internet favorites and e-mail data) in the system area, and recovering them requires a system restore. The operating system and applications reside in what's known as the system area. They can be recovered by restoring a system backup or by making a fresh install from the original distribution media.

If you use Microsoft's backup software, system backups are in the form of full disk images. If your system won't boot, it may be because the boot loader, or in new PCs the UEFI partition, has been damaged. These can be repaired in Windows system using the Windows recovery disk. See the MS Website for instructions. If the BIOS ROM is corrupted, a competent shop may be able to help, but you may have to return the machine to its manufacturer.

How you recover depends of course on how you backed up:

1. The fastest is to restore from backup as the result will be software that is updated to the last version of your data. If this includes restoring the OS, you must be able to boot from live media, which means you have to properly set up your BIOS. Later PCs use UEFI, which adds complexity.
2. If you decide to re-install the OS you can try to restore from the PC vendor's recovery partition, which places your computer to its state when you first purchased it. You will have to reinstall all your applications from their distribution disks and your data from a recent backup.
3. If the recovery partition isn't available, you'll have to use the OS distribution disk if you purchased it separately or its recovery disks if the OS was installed by the PC vendor. (This of course assumes you created these.)

As a last resort, if the former isn't possible or if you doubt your abilities, you can take your PC back to the vendor who sold it to you or to an independent shop to have the OS re-installed. You then must restore any applications and your data yourself. It should be clear that record-keeping is a very important component of your plan. In particular, be sure to label your external backup media and any notes. You don't want to restore from the wrong computer.

Creating and following a good backup discipline require more than trivial knowledge, thought, and time. Many computer owners choose to take a "Do nothing and hope for the best" approach or they follow the advice in the latest article or ad they've read, and neither approach is sound. As a last resort, there are commercial firms that will attempt to recover data from damaged or corrupted storage media, but the results aren't certain and the costs are high (up to multiple thousands of dollars).

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.

Member Ads

Ads are available free to SHCC members, and are limited to computer related items for non-commercial purposes. Any ad shall be a maximum of twelve newsletter lines of text.

How Can A Hacker Try All Possible Passwords If System Blocks The Login Attempts?

From the Ask Leo Newsletter
https://askleo.com

I understand that my password, especially if it's not very strong, can likely be figured out by a computer driven program using trial and error. For example, all permutations, combinations of numbers, letters and special characters. What I don't understand is this – wouldn't a hacker, be it a person or a machine, have to actually try each and every one of these computer derived guesses on the sign-in screen of the website that they are trying to access to see if they get lucky? My experience tells me that after just a few failed attempts at entering a password, the website will not allow any more tries. So how in the heck are they able to try out all of the thousands of possible passwords that he comes up with?

What you've described is called a "brute force attack", and you're quite right; it's a rare system that allows such an attack to proceed past the first few errors.

However, hackers have other options.

Simple brute force
As you said, this type of attack involves the hacker trying to log in using your user ID with every possible password in turn.

Most good systems note that the same person has tried to log in unsuccessfully too many times and lock the account, either for a few minutes or an extended period of time. A brute force attack is most often attempted using a computer, so locking the account for just a few minutes makes even the fastest automated attack impractical.

But to be honest, even when systems are operating at full speed, the log-in process is usually slow enough on its own to make this type of brute force attempt impractical anyway.

Not surprisingly, it's not what hackers do. If they're going to attack by simply logging in, they'll stack the deck instead.

Targeted brute force
You've probably seen those reports that come out every year revealing the top 100 most popular passwords. We use it as an example of how awful these popular passwords really are.

Don't use them.

But those lists are just the top 100. Hackers can and do "stack the deck" by taking the top 1,000 or 10,000 or 100,000 passwords and trying them in order of popularity. Given how many people use bad passwords, it's worth the hackers' time to try them, even if there are periodic delays.

Just the top 1,000 passwords tried against a large number of accounts will probably get them access to a surprisingly and depressingly large number of accounts.

But there's a very practical and reasonable way for hackers to try *every* possible password. They do it by stealing user account databases.

How passwords are stored
We need to focus on an important definition before we proceed.

I've talked and written before about how most services store your password. They create what's called a *hash* of the password.

Think of a hash as a kind of a one-way encryption that can't be undone. You can create a hash from a password, but you can't get the password from the hash. And it's statistically impossible[1] for two passwords to generate the same hash.

When you set your password, the service creates the hash associated with it and stores the hash, not your actual password.

When you log in, the service again creates the hash of whatever you typed in as your password. It compares this hash with the hash it created when you set your password. If those two hashes match, then you must have typed in the same password this time as you did when you created the password in the first place.

In other words, if the hashes match, you typed in the right password, and the system allows you to log on.

Databases of passwords
Now that we've seen how passwords are stored, we can look at how hackers leverage that approach to their advantage.

You've probably heard about various data breaches at large companies. A hacker gets in and gains access to things they're not supposed to.

One of the goals of most of these breaches is to get a copy of the user account database. That's the list of user IDs *and password hashes*. Once they have a copy of that database, they can go to work.

Later, on their own computers, and at *extremely* high speed, they literally try every possible password. With each attempt, they create the hash; then they see if it's in the database they just stole. If it is, they now know the password for the user account that had that

hash; it's the password that created the hash like they just did.

This is where password length and complexity come into play.

It's currently feasible to try all possible eight-character passwords in a short amount of time. That's why most industry experts now say 12 characters is the new *minimum* length of a password. The amount of time required to try them all increases exponentially each time you add a character to the length. It's just not practical for hackers to try all possible 12-character passwords today. It would take years, even with the best equipment.

So, yes, there are absolutely scenarios where hackers can and do try all possible passwords. They just don't do it by trying to log in with each one. Using those stolen user account databases, they work *offline* to figure out your password's hash. When they later arrive at the log-in screen, they know exactly what to type in, and only need one try to get into your account successfully.

It all comes down to good passwords

The lesson here, of course, is to choose long, complex passwords. The longer the better, in fact. I now use passwords with 20 random characters whenever I can. I let LastPass create and remember them for me.

Yes, it's possible that even those can be compromised by malware such as keyloggers, which is why I also advise adding two-factor authentication to your important accounts. With two-factor authentication enabled, even knowing the password isn't enough to get in.

This article is republished, with permission, from the Ask Leo! Newsletter.

The Case Of Random Keystroke Repeats

by Bob Woods, Under the Computer Hood UG Webmaster
www.uchug.org webmasters@uchug.org

A couple of years ago I decided I needed a new laptop. At the time, Costco was running a sale on a nicely appointed Acer laptop. Since Acer makes a pretty decent product I took the plunge and bought one. Overall, it has been an excellent choice with one exception, the keyboard. The keyboard has a nice feel to it and is well-made, but has a problem with randomly repeating keystrokes. This problem was present in the 'as-shipped' Windows 8 and followed through with the Windows 10 update. Resetting keystroke repeat rates and doing a BIOS update did not alleviate the issue.

The problem was more annoying than anything, but one day I decided to try to fix the problem once and for all. I tried doing a search in the Acer support site and saw others with the same model as I have and other models as well. In most cases the owners were asked to return the units for keyboard replacement under warranty. In most cases the problem was not resolved by the keyboard replacement. Seeing as this did not help, I decided to not go through the repair hassle with so little track record of success. So, onto a Google search of the issue.

Doing a Google search revealed that the issue of randomly repeating keystrokes was experienced by owners of many other brands and models. Very rarely did keyboard replacement or resetting keyboard repeat rates help. After digging around a while and trying various recommendations that did not work I came across an article in the HP Support Forum that sounded feasible. The link to the page is http://hp.care/2uauUco

Basically, the problem is some keyboards have more key bounce than others. With the short key travel on laptop keyboards the key bounce allowed the keys to inadvertently register as a double key stroke. Resetting the keyboard repeat rate will not resolve key bounce. The article describes how to use the Ease of Use settings in the Control Panel to turn on a key filter for Windows 7 or 8. On Windows 10:

- Open Control Panel, click on Ease of Use and click "Make the keyboard easier to use."
- Then under "Make it easier to type" click the check box "Turn on Filter Keys".
- Next, follow the rest of the article for Windows 7 - 10 to make a change to a registry key that sets the bounce rate for the keyboard keys to 35 milliseconds.

Wow, that worked like a charm. No more random character repeats while typing. One thing to watch for. All was going splendidly until after a patch one day. I started to get the random keystrokes again. So, I checked the Ease of Use settings and found the patch had unchecked to box for "Turn on Key Filters". Gee, thanks Bill!

Once I turned back to the problem, once again the problem resolved itself and the patch did not change the bounce rate in the registry. Oh, happy typing again!

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.

If your e-mail or mail address changes, please e-mail: secretary@SterlingHeights ComputerClub.org

A Club Meeting Writeup - A Genealogy SIG: The Anatomy Of A Death Certificate

by Harold D. Kelley, SIG Leader Horizon newsletter
ww.cuerie.com bookworm1707@gmail.com

Sue Mueller, Contributor, Family Grave, presented a program entitled "The Anatomy of a Death Certificate." She provided the SIG members with a handout, "Find Death Certificates Online (Free)." It is included, with Sue's permission, at the end of this meeting's summary.

Sue explained that the new death certificates don't have as much information on them as the old ones. However, since it is 50 years before you can obtain death certificates that are available to the public, most of the ones we see will be very interesting because they are older.

Different states handle death certificates differently, but in Pennsylvania, you can get them free. Overall, the best site to use for various states, is the one listed second on the handout sheet. When you have to pay a fee for a death certificate, the best site is the one listed last on the handout sheet.

On a death certificate, you can get **death facts, personal facts, genealogical information, w**hat happens to the body, **medical and health information** such as the cause of death, and what contributed to the death and how long it had been going on.

Concerning **death facts,** those who are using either Family Tree Maker or Ancestry.com, not all the information on the death certificate is merged into those programs. There is some good information that doesn't get merged. The only things that are merged are the name, the city or town and county of birth and the death. The only thing you are guaranteed to get accurately is where the person died.

On a death certificate, the parents' names will be there, including the mother's maiden name, if the informant providing the information knows it. Sometimes they write "unk" for unknown. What is merged into Family Tree Maker is how it is indexed. Death facts include the deceased's name, where he/she died, the specific location of death, such as a hospital, state hospital or alms house. If a person dies in a hospital, state hospital or almshouse, some information may not be accurate, because the informant may not be knowledgeable, but in these cases, the medical information and cause of death are likely to be accurate.

You also get **personal information** on a death certificate. If the deceased is a family member, the live people, if they are family giving the information, are upset, so if they know the information, they may not get it right, or they may not even know the information, in which case they have no hope of getting it right. For example, they may not know the state in which the person was born.

Sue said she will sometimes check the census data to check whether the person was born in Ohio or Pennsylvania, for example. The personal information also includes whether the person was married, divorced, single or widowed, place of residence and occupation. Social Security numbers didn't come into play until the late 1930's, so someone born after that may have a number listed. It is usually asked if the person served in the military. Since many of these facts would not be merged into Family Tree Maker or Ancestry.com, one would have to enter them manually into Facts in their program.

What kind of **genealogical information** can you get on a death certificate? Included is the father's name and sometimes where he was born, and sometimes the town or city, not just the state. The mother's name and maiden name is asked for, and often where she was born. The full name of the spouse, and if the spouse is still living, is asked for; this can be important for searching for more information. It is not asked whether or how the informant is related to the deceased.

The death certificate is created right away. The funeral home obtains the number of copies of the death certificate that will be required. The certificate will also have the place of burial and sometimes the name of the cemetery. It will tell whether the dispersal of the body is by cremation or burial. It is noted if the body is taken out of state. The funeral home will be listed as well as the coroner.

With regard to **medical and health information,** the death certificate will give the cause of death, contributory causes, how long the person was sick, name of the attending doctor and the name of the doctor who pronounced the death.

Concerning the cause of death, in addition to what is written on the death certificate, there is an ICD code (International Classification of Diseases) which identifies the cause of death. It is maintained and updated by the World Health Organization regularly. It was developed in the late 1880's. We started using it in 1898. One should always check out the revision to the ICD code right before the death date to be sure to get the most updated information. If the written cause of death is difficult to read, one should go with the ICD code given on the death certificate. The address for the ICD information is:

http://www.wolfbane.com/icd/index.html.

The information is free and is intended to be used universally.

For those using Ancestry.com and Family tree Maker, there are some facts that will not be merged into Family Tree Maker, such as the name of the informant, the deceased's occupation and the cause of death. Where the burial is will be noted, but not the name of the cemetery. The name of parents may be given, if still living; this information could be important for genealogical purposes. Facts that are not merged into Family Tree Maker will have to be put into FTM by hand, using the FTM protocol for adding facts.

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.

Find Death Certificates Online (Free)

Generally accepted standard
for release of vital records to public:
***Birth** - 105 years; **Census** - 72 years; **Death** - 50 years*

Vital Records, http://vitalrec.com/: a comprehensive resource for locating vital records

https://www.deathindexes.com/: death records listed by state

Cyndi's List Death Records: http://www.cyndislist.com/death/

National Archives: https://www.archives.gov/research/vital-records

Family Search: https://familysearch.org. Step=by-step wiki: https://www.archives.gov/research/vital-records

Death resources, by state: http://publicrecords.onlinesearches.com/Death-Records.htm

Genealogy bank, free SSDI search: https://www.genealogybank.com/explore/ssdi/all

CDC Vital records: https://www.cdc.gov/nchs/w2w/index.htm

Free access to Pennsylvania death certificates for PA residents who are not ancestry subscribers. How to register on this site: http://www.phmc.pa.gov/Archives/Research-Online/Pages/Ancestry-PA.aspx#.V1V8k-SgSqQ

Pennsylvania death certificates for ancestry subscribers http://search.ancestry.com/search/db.aspx?dbid=5164

State by state death certificate ordering information ($ fee) https://www.everplans.com/articles/state-by-state-death-certificate-ordering-information

Presenters Wanted

The officers invite any member to make a presentation at the main meeting.

If there is some software you have been using and think others may be interested as well, or there is a computer topic you would like to present to other members, please call or e-mail Don VanSyckel. Making presentations is not that difficult. The hour goes by before you know it and there is always enough material to cover in a software package so that the hour is easy to fill.

If there is a topic you are interested in or something you would like demonstrated, please see any of the officers. They are always interested in what the members would like to see.

SHCC Post Office Box

After 9-11 some of the rules have been changed concerning post office boxes. These changes are intended to make it more difficult for persons using post office boxes to remain anonymous, at least to the post office. If you send anything to the club's PO box, don't put a person's name on it. It's OK to use titles such as President, Treasurer, and such. If you use a person's name, your mail will sit at the post office until that person can get to the post office with ID and claim the mail. This just slows down your mail and inconveniences the addressee.

VISIT THE SHCC WEB SITE:
http://
www.SterlingHeightsComputerClub.org

The HDMI Cable And Connectors

by Jim Cerny, Sarasota Technology User's Group, FL
www.thestug.org jimcerny123@gmail.com

As technology changes, hopefully for the better, more and more devices are available to us. For most of us who use technology for personal and home use, we would like to connect some devices to our TVs to enjoy the big screen video and great sound experience. The latest connection cable type that does this for us is HDMI which stands for "High Definition Media Interface". The cable connectors (the standard size and a mini size) are shown in the photo. They have a shape to them that allows them to be inserted only one way, so do not force it into the port. Try turning it over (180 degrees) and try again.

The purpose of HDMI is to replace different kinds of connectors and cables with one type that, hopefully, can handle all your device connections. Do you remember the old days when there were separate audio/stereo and video cables? Today almost all of the newer devices (laptops, TV's, DVD players, etc.) will come with at least one HDMI connector port. The older style connectors may also be present, but if possible, HDMI should be your first choice to make those connections.

Your TV remote control will have a button labeled "input", and when you press this button different input options (that is, what is coming INTO your TV) will be displayed and allow you to select which one you want. One option will be "cable" which means your TV will show your cable programs – the cable you pay for each month. But other choices will include one or more HDMI inputs, usually labeled HDMI-1, HDMI-2, etc. If you have more than one device connected to your TV it is best for each device to connect to its own HDMI port on the back of the TV. You select which of the inputs you want to view on your TV by using the "input" button on your remote. Of course, there must be something (video and sound) coming into that port to the TV for you to see anything. For example, you may have a DVD player connected to HDMI-1, but if your DVD player is not on and playing something, you will not see anything on your TV when you select that input option. If you have some older devices which may not have an HDMI connector, you can purchase a converter device to allow it to connect.

Lastly, I am always amazed by the cost of cables – after all, they are just wires with plugs on the ends, right? If you checkout the prices of cables at stores and the prices on the internet, you will be shocked at the high prices they can charge for these things. Yes, some cables are higher quality than others and may come with better "shielding" to protect the signal, but most prices are much too high for what you get. My advice would be to shop on-line and get the cheapest cable that meets your needs, but make sure you can return it if you are not happy with it. If it doesn't work for you, then return it and move up to the next higher-priced (and hopefully better quality) cable.

You can find out more about HDMI cables and connectors by asking Google, of course. But connecting them is easy, even for us amateurs.

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.

If your dues are paid in the month they are due, as shown on the invoice the club sends, you automatically get an extra month of membership. This policy has been in effect for many years but newer members may not be aware of this "free month" policy.

SHCC Emergency Cancellation

Sterling Heights Computer Club meets at Macomb Community College (MCC). We will meet if MCC is open and will not if MCC is closed. MCC closure is announced with other school closings on many local TV and radio stations and on their web site. All members of SHCC have an email address. One of the SHCC officers will send an email to the addresses SHCC has on file alerting members to the event cancellation. If your email is broken, call an officer; don't leave a message, call another officer if you don't talk to someone live. It is your responsibility to keep the email address you have listed with SHCC current.

WYSIWYG WEB WATCH (www)

by Paul Baecker webwatch@sterlingheightscomputerclub.org

This column attempts to locate sites containing valuable, amusing, and free content, with no overbearing pressure to purchase anything. Club members are encouraged to submit favorite sites (a description is optional) to the e-address noted above, for inclusion in a future WYSIWYG issue. Also check the SHCC web site ("Web Page Reviews") for previous gems.

A penguin dilemma – which way to go? (2-min. video)
https://www.youtube.com/watch?v=3H2FLRUtdmU

Step-by-step guide to getting your first blog up and running.
https://startbloggingonline.com

How is your phishing IQ? Try this phishing IQ test.
https://www.sonicwall.com/en-us/phishing-iq-test

Learn how pioneering software engineers helped NASA launch astronauts into space, and bring them back again -- pushing the boundaries of technology as they did it.
https://www.techrepublic.com/article/nasas-unsung-heroes-the-apollo-coders-who-put-men-on-the-moon/

How to back up and transfer settings for your Windows programs to a new PC with CloneApp.
https://www.howtogeek.com/howto/microsoft-office/save-and-restore-your-microsoft-office-settings/

The universe in 4 minutes. (4-min. video)
https://www.youtube.com/watch?249=&v=mheHbVev1CU

How to fix a loose USB cable.
https://davescomputertips.com/how-to-fix-loose-usb-cable

You forgot your Windows 10 login password? Or maybe you 'inherited' a Windows 10 computer and you can't log in. There's hope, but there are several complication factors.
https://askbobrankin.com/forgot_your_windows_10_password.html

You can save your laptop battery by getting the system to automatically disable Wi-Fi when connected to a LAN connection. Here's how in Windows.
https://www.maketecheasier.com/disable-wifi-on-lan/

Everything you need to know about Intel's CPUs getting hacked.
https://www.maketecheasier.com/intels-cpu-hacked-what-you-need-to-know/

Although sharing small amounts of "human food" with your dog on occasion isn't usually cause for concern, it's important to note that many foods have the potential to be extremely poisonous for dogs. Here are 27 toxic foods for dogs.
https://www.certapet.com/27-toxic-foods-for-dogs/

A Jell-O shaker, a cigarette lighter, a finger tapper, an automatic unplugger, and other useless inventions. (3-min. video)
https://www.youtube.com/watch?v=jgbkByOfPCA

African Animal Assembly -- footage of various African animals in Zambia's South Luangwa Valley. There is an incredible amount of diversity in this region. (6-min. video)
https://www.youtube.com/watch?v=FCb-fjkfYBU

A list of pros and cons of several highly regarded VPN services. The displayed spreadsheet can be downloaded.
https://thebestvpn.com

100 most often mispronounced words and phrases in English.
http://grammar.yourdictionary.com/style-and-usage/mispron.html

How to easily remember Linux commands (including link to a cheat sheet).
https://www.maketecheasier.com/remember-linux-commands/

Facebook removes the 'delete post' option from the desktop web version.
https://venturebeat.com/2017/11/17/facebook-removes-delete-post-option-from-the-desktop-web-version/

Microsoft does it again -- confirms Epson Printer bug was caused by November 2017 updates. Here are the fixes.
https://www.ghacks.net/2017/11/17/microsoft-confirms-epson-printer-bug-caused-by-november-2017-updates/

How to run Windows apps on the Raspberry Pi.
https://www.techrepublic.com/article/how-to-get-windows-apps-running-on-the-raspberry-pi/

Daring young men climb the 2100 ft tall Shanghai Tower building (second tallest in the world), and then onto a crane at the top. (5-min. video)
https://www.youtube.com/watch?v=gLDYtH1RH-U

Type or paste any amount of text. Learn word count, types and lengths of words, paragraph and syllable counts, reading level, much more.
https://wordcounttools.com

If you really want to grasp control of your disk partitions, skip Windows' Disk Management tool. Here are six free worthy alternatives.
http://www.makeuseof.com/tag/best-free-windows-partition-manager/

20 bad tech gifts to avoid giving during the 2017 holiday season.
https://www.techrepublic.com/pictures/gallery-10-bad-tech-gifts-to-avoid-giving-during-the-2016-holiday-season/

Self-Destructing Cookies is no longer supported as a Firefox add-on, to control cookies and other tracking mechanisms. Here are some alternatives.
https://alternativeto.net/software/self-destructing-cookies/

How to keep email from disappearing on your Android device -– basically just understand how IMAP and POP work.
https://www.techrepublic.com/article/pro-tip-keep-email-from-disappearing-on-your-android-device/

One of the worst parts of using a computer is just how mindlessly repetitive it can be. Here are 7 free Windows tools to automate repetitive tasks.
http://www.makeuseof.com/tag/automate-repetitive-tasks/

How to block robocalls and get your sanity back.
https://www.maketecheasier.com/howto-block-robocalls/

What is a "firmware"? What does it do, and where is it stored?
https://www.digitalcitizen.life/simple-questions-what-firmware-what-does-it-do

An infographic detailing the history of the Bitcoin crypto-currency.
http://infographicjournal.com/the-history-of-bitcoin/

Your math and physics questions answered.
http://www.askamathematician.com

Select any element in the Periodic Table and view the element's appearance and uses.
http://images-of-elements.com

4 reasons to always use a VPN when you're online.
http://www.makeuseof.com/tag/online-vpn-use/

NOTE: Many of the links in the digital newsletter connect to the Internet if clicked. For those that do not, copy and paste the link into your Internet browser.

World Wide Web Column on the Club Web Site

Check out the WebPageReviews section on the club's web site. You can see past web sites reviewed in this column on our club web site. They are arranged into various key word categories to help locate a specific site.