Interface

Lorain County Computer Users Group
www.LCCUG.cominfo@LCCUG.com
Volume 32 Number 9 September 2021

Tuesday
September 14, 2021

2021

Inside This Issue

Evernote

Presented by

Hewie Poplock
from APCUG

Our links can be found at:

LCCUG.com/links, There you will find many interesting places to visit. Check them out and see what you can find interesting

UNTIL FURTHER NOTICE MEETINGS ARE HELD ON ZOOM DUE TO COVID19

Meeting opens at 6:00 PM, program starts at 6:30 PM

GENERAL MEMBERSHIP MEETINGS CONDUCTED VIA THE ZOOM APP UFA

A Word From Our President

It's hard to believe the year is more than half over!! I wish the virus was farther in the background than it is.

NEWS: We are thinking about an option to meet in person **in addition to** ZOOM as soon as our October meeting.

NEWS: We are also moving to a new location!!! We are moving 2 miles north of where we have been meeting. We are moving <u>from</u> LCCC Community Learning Center @ Lorain High School on Ashland Ave. to LCCC Lorain Learning Center at City Center, 203 W. Erie.

We will see what the Covid statistics are at the time of this meeting in October and decide if we will try to go forward with this **in person - Hybrid meeting**.

This location on W. Erie and 4th St is entirely the property of LCCC so there will not be issues with sharing it with the Lorain school system. The rooms are bigger and without computers on the desk. There is space there for refreshments and extra room to socialize and touch base with others about your questions.

There are no stairs and lots of parking and little walking!! Yeah!!

NEWS: The other important change is the time of our meeting. We have been meeting on the evening of the 2nd Tuesday of the month for over 20 years. Starting in October, we want to change from the evening of the 2nd Tuesday to the **morning.** We want to meet from **10 am to Noon**. This will help those who prefer not to drive at night. We hope this won't interfere with schedules of any members who would want to attend. And we will continue to have ZOOM for times when the weather is bad.

** LCCC is requiring masks this year so that will be in place.

We would like your feedback on these changes!!

The August meeting on printers was very good!! I think we all liked it. If you would like to watch this recording about printers that we watched at the meeting, it can be found at: https://www.youtube.com/watch?v=xET1PP5z2v8

Our September meeting will be about using a free note organizing program called Evernote. A great tool that anyone can use and access your important items from any computer or tablet or smartphone!!

Please log into our September meeting on ZOOM and we can discuss these changes further!!!!

Sandra Ruth
LCCUG President

LCCUG Officers For 2021

President	Sandee Ruth president@lccug.com
Vice President	**Vacant** vp-programs@lccug.com
Secretary	Don Hall secretary@lccug.com
Treasurer	Micky Knickman treasurer@lccug.com
Newsletter Editor	Pam Rihel newsletter@lccug.com
Web Page Editor	Richard Barnett webpage@lccug.com
Statutory Agent	Sandra Ruth statutory_agent@lccug.com
Director of Membership	Dennis Smith membership@lccug.com
Director of Advertising	Richard Barnett advertising@lccug.com
Director of Education	Neil Higgins education@lccug.com

Tuesday
September 14, 2021

Evernote

Presented by

Hewie Poplock
from APCUG

Evernote is a free app **for your smartphone and computer that stores everything you could possibly imagine losing track** of, like a boarding pass, receipts, articles you want to read, to do list, or even a simple typed note. The app works brilliantly, keeping everything in sync between your computer, smartphone, or table. This promises to be a very informative presentation. Please join us on line via ZOOM beginning at 6:30. A zoom link will be provided via email prior to the meeting

THIS WILL BE A ZOOM MEETING
Please join us via ZOOM. A link to the ZOOM meeting will
be provided in a reminder email to be sent a few days before the meeting.

zoom

The Lorain County Chapter of OGS

is having its next meeting online:

Check our webpage for the next program.
http://loraincoogs.org/events.html

We are having our meetings virtually using bluejeans.com.
To join the meeting on a computer or mobile phone:
https://bluejeans.com/5006724159?src=calendarLink
Also a link will be sent to you before the meeting.

North Ridgeville Library, 35700 Bainbridge Rd. North Ridgeville, Ohio. Meetings are free and open to the public. Social time is at 6:30 PM and the program begins at 7:00 PM. Canceled Until further notice due to Covid-19

Jean Copeland: **jecopeland1975@gmail.com**.

Executive Board Meeting Minutes

AUGUST 3, 2021

Board members Sandee Ruth, Don Hall, Micky Knickman, Pam Rihel, Dennis Smith and Neil Higgins met at the LCCC computer building in downtown Lorain on W. Erie to view the facility as a possible meeting place for LCCUG. Dina Ferrer gave us a tour of the facility which impressed us all. Hours of opening and security were discussed.

After the tour we met at Chris's Restaurant for lunch and the board meeting. It was decided we would like to start using the facility for the October 12 meeting from 10 o'clock AM until 12 noon.

Sandee summarized the advantages of the facility:
Good parking
First floor—no elevators
Several rooms available and a computer lab
Refreshments for sale at Spectrum café
Kitchen available
Public access computers
Lots of spaces
Convenient restrooms
Rooms can easily be rearranged as needed
We don't have to use a room with monitors on the tables
Rooms are bigger than we had been using

Neil moved, Micky seconded the meeting be adjourned.

General Meeting Minutes

August 10, 2021

President Sandee Ruth called the Zoom video meeting to order. A motion to accept the minutes as shown in the August issue of the *INTERFACE* was made by Ron Dix seconded by Cliff Salisbury. Motion passed by voice vote.

Sandee stated the August newsletter was available.
She mentioned the board's visit to the LCCC downtown computer facility and the proposed change to meet there and meeting time of 10 o'clock to 12 noon starting October 12.

Ray Baxter, APCUG President and Treasurer presented his program, "Purchase decisions for printers in 2021". Ray gave a complete rundown on printers, their inks and costs.

Sandee moved, Don seconded meeting be adjourned.

MEMBERSHIP WITH LCCUG:

Yearly dues are now $15.00. For more information contact:

Dennis Smith
Director of Membership,
membership@lccug.com.

Meeting Location:
LCCC Community Center at Lorain High
2600 Ashland Ave, Lorain OH
[illegible] - 10 [illegible]
[illegible] is on the second floor.
Elevator access is available for those in need.

No Meetings at the College

Computer Club News

Don't Forget to Bring in Your Used Ink Cartridges LCCUG is collecting empty ink Cartridges

For every cartridge you will receive a ticket for our special drawing.

Recycle & Help Our Club Too!

LCCUG WORKSHOP Class Ideas?

Neil needs your input into what classes you would like him to present to our members.

Please tell Neil [illegible] of the other officers what you would like to learn and we will be happy to have classes on your subject./subjects.

Neil Higgins Education@lccug.com.

No Meetings at the College

Lorain County Computer Users Group

2021 Calendar of Events

http://lccug.com
email: info@lccug.com

Using Zoom

Meeting opens at 6pm – program starts at 6:30

2nd Tuesday of each month. Changes are announced on the webpage and the newsletter. All meetings are open to the public

January 12, 2021, Avast & PC Security

February 9, 2021 Password Managers by John Kennedy from APCUG

March 13, 2021 The Cloud is Here - Don't Get Left Behind - by Judy Taylour from APCUG

April 13, 2021 TeamViewer and AnyDesk - by John Kennedy from APCUG

May 11, 2021 Back Up Your Stuff - by Micky Knickman and Neil Higgins

June 15, 2021 How Technology Has Changed How We Listen to Music - by Ray Baxter APCUG

July 13, 2021 Digital Asset Estate Planning...

August 10, 2021 Purchase Decisions… By Ray Baxter APCUG

September 14th, 2021 Evernote by Hewie Poplock

Genealogy Tip of the Day

Michael John Neill Genealogy Day 2021 Rootdig.com
mjnrootdig@gmail.com

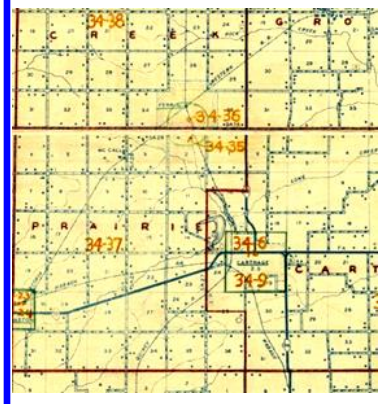
Truncated last Name?

michaeljohnneill, 06 Sep 07:21 PM

Is it possible that the last name you think you have for a person is really a truncated version of the actual name? Could the last half of the name have been "cut off" to avoid sounding a little too ethnic? Could your VanDerWalle relative used the last name of Wall(e) instead?

Census Enumeration District Maps at NARA

michaeljohnneill, 09 Sep 11:52 AM



Census enumeration district maps at the National Archives (1880-1950) are online and can be searched here.

Try searching for "your state your county" or "your state your city" to locate items of interest.

Member of Association of Personal Computer Users Groups

amazonsmile
You shop. Amazon gives.

Thinking of shopping with Amazon? Well you can now go to our **lccug.com** website and just click on the amazonsmile link and start shopping.

Our club gets rewarded for any items purchased from our website. So the more you buy the better it is for our club. SO START SHOPPING.

NEED HELP?

Here's Who to Contact:

Neil Higgins
440-985-8507 - **higgins.neil@gmail.com**
Evenings 6 p.m. -10 p.m. + Weekends
Hardware, Linux & Windows Operating Systems,
Chromebooks, Tweaking your system

Micky Knickman
440-967-3118 - **micky@knickman.com**
Daily 6:00 am to 4:00 pm. Leave message if no answer.
General Software Configuration, Hardware Installation, Basic to Advanced Windows

Richard Barnett
440-365-9442 - **Richard216@aol.com**
Evenings & Weekends
General Software Configuration, Hardware Installation, Basic to Advanced Windows & Web Page Design

Sandee Ruth
440-984-2692 - **sandee29@gmail.com**
Basic Word Processing, Windows, & Web Design
Advanced Internet

Pam Casper Rihel
440-277-6076
6:00 p.m. to 9:00 pm Monday thru Thursday
Genealogy help
prihel1947@gmail.com

Denny Smith
440-355-6218 - **dennis.smith@windstream.net**
Microsoft EXCEL
Leave message on machine if no answer

If any of our members are interested in helping other users with what programs you are adept at, please contact any of our officers with you name, what program or programs you would be willing to give help with, you email address and or phone number and when you would like to have them call you. Thanks

LCCUG Ongoing Workshop

All Are Free And Open To The Public

Problem Solving Workshop

Date: Tuesday - September 21, 2021
Time: 5:30 - 8 pm Instructor: Micky Knickman, Neil Higgins, Richard Barnett
Place: Lorain County Community College @ 2600 Ashland Avenue, Lorain

Canceled

Learn how to repair or update your computer by changing hard drives, memory, CD ROMs, etc.

Members are encouraged to bring their computers anytime before 7:30 pm for assistance from Micky, Neil & others.

Learning About Electronics

Date: Tuesday - September 21, 2021
Time: 5:30 - 8 pm Instructor: Sandee Ruth
Place: LCCC @ 2600 Ashland Avenue, Lorain

Canceled

Learn how use you electronic devices.

Members are encouraged to bring their tablets, iPod, kindles, etc. at 5:30 pm for assistance from Sandee and any other knowledgeable members. The public is welcome to sit in on these classes.

Learn About– Hands on Demonstration

Date: Tuesday– September 21, 2021
Time: 5:30- 8 pm Instructor: Neil Higgins
Place: LCCC @ 2600 Ashland Avenue, Lorain

Canceled

Do you know the specifications of your computer? What is really inside? We'll demonstrate three portable Windows programs (run from a USB Stick) that will tell a computer's storage, CPU, video, and other useful information (including your Operating System Product Key) . This will help determine if your computer will run certain programs, and will help find out what memory or video card upgrade you need.

Please bring a flash drive to obtain software and handouts. If you would like to participate and get copies of the material for this presentation, please let Neil know by sending an email to Education@lccug.com.

ScamBusters.org

SOCIAL SECURITY SCAMS HAVE BECOME AN EPIDEMIC, GOVERNMENT SAYS: INTERNET SCAMBUSTERS #865

Pretending to be from the IRS is getting tougher for scammers -- so they've switched their attention to Social Security.

In fact, Social Security impersonations have moved into the top slots among impostor scams.

We'll explain what the crooks are up to in this week's issue - and tell you about 10 things you can do to avoid the scammers.

Let's get started...

SOCIAL SECURITY TRICKS HIT TOP OF SCAMS LIST

Social Security imposter scams have now reached epidemic proportions in the US, outstripping IRS impersonation scams for the first time, according to the federal government.

Some 76,000 complaints valuing losses at more than $19 million were filed in the 12 months prior to April 2019. The comparable IRS sum was $17 million.

But it gets worse. Almost half of those complaints came in the final two months of that period, signaling criminal activity on a huge and growing scale. That can only happen because the scams actually work.

And that $19 million accounts for a tiny 3.4 percent of the complaints. The rest relate to reports of Social Security number (SSN) thefts, which can subsequently be used for identity theft.

Newsletter Editor: Pam Rihel using Microsoft Publisher, 2016

This Month's contributors: Micky Knickman, Sandra Ruth, Pam Rihel, Don Hall, Dennis Smith, Neil Higgins, Michael John Neill, Dick Eastman, Greg Skalka, Kurt Jefferson, Phil Sorrentino, Scambusters, APCUG, Leo Notenboom, Google images, Microsoft Office art online,

Newsletter is now
Online at:

lccug.com/newsletters or **lccug.com**

Woohoo!

Your renewal dues have been reduced from $25.00 to $15.00. When everything else is raising their prices our Computer Club is lowering their dues.

The median or midpoint among individual losses comes out at around $1,500 per victim, which is about four times the amount lost in other types of fraud.

An indication of the scale comes from the 55+ age group organization AARP. Its director of fraud victim services says a massive 94 percent of calls to its Helpline are about Social Security scams.

The current main scam comes in a call from an impostor claiming the victim's SSN has been used in a crime and so it has been suspended. Sometimes, they already have the individual's SSN. If not, they ask for it as "confirmation."

PAY A FEE

Then, in order to reactivate or unfreeze the account, the victim will have to pay a fee, usually in gift cards or a virtual currency like Bitcoin.

Often, crooks also doctor your caller ID so it looks like the call is genuinely coming from the Social Security Administration (SSA).

The calls may also be automated (rob calls) but invite recipients to "press 1" to speak to an SSA official.

This can all seem pretty convincing except for one major factor - the SSA does not suspend Social Security numbers. Period. Nor do they call and demand money. So, if you get one of these calls, you can safely hang up.

Other variations of Social Security scam tricks aimed at stealing your info include calls or emails saying that you're entitled to a refund; you need to "update your account information"; the SSA computers are down; you need to enroll in a new program; they need you to answer some security questions such as giving your mother's maiden name.

It's all about identity theft

SNAIL MAIL VERSION

Another scam even arrives by regular snail mail. It's a letter that offers additional security for your Social Security account - but, of course, there's a form to fill in with all your personal info.

Right now, there's an additional scam threat to Social Security recipients. Due to an oversight, the SSA actually "forgot" to deduct Medicare-related premiums from 250,000 Social Security payments for the first five months of this year. Yes, they really did this.

That means, you may get a bill from a Medicare Advantage or drug plan insurer for the outstanding sums. But because the issue is potentially confusing, scammers will almost certainly use it to try to lever more money out of older folk.

If you get one of these bills, verify that the money genuinely hasn't been deducted from your Social Security

(Continued on page 8)

(Continued from page 7) Social Security Scams….

check. Then download this explanation of what to do from Medicare.

ACTION LIST

Here are some other things to know to avoid falling victim to this scam:

Note that the SSA never emails requests for personal information.

Nor does it visit homes without making a prior appointment.

Never provide personal, financial and other confidential information in response to an unsolicited call. Any such request is a scam.

Don't wire money to someone you don't know, even if they say they're from the SSA.

Don't be fooled by callers who already have your SSN or the last four numbers.

Don't trust your caller ID.

Ignore phone threats. That's not the way government departments operate.

Securely protect and store your SSN and card.

If you're in any way concerned the call might be genuine, call the SSA on 1-800-772-1213 or 1-800-269-0271 -- or contact your local Social Security office.

Stay in touch and learn about the latest tricks from Scambusters - and please share this report with friends and family.

If we're too late with this warning and you already believe you're a Social Security scam victim, file a report at https://oig.ssa.gov/report or www.identitytheft.gov/SSA.

ALERT OF THE WEEK

The 419 Nigerian scam is alive and well. You remember; it's that email from a prince or government official who wants your help to smuggle money out of the country.

The past few months have seen a surge in this scam (which asks you for cash first so the big money can be sent to you).

How Do Websites Keep Passwords Secure? What to look for in every data breach report?

by Leo A. Notenboom

A high-level overview of how websites and services should store passwords security, so next time there's a breach you'll know what to look for.

We often talk about how you and I should keep our passwords secure, most commonly by using a password vault or manager.

But how do websites work? We trust them to do the same: keep our passwords secure from hacking and exposure. How do they do that?

It turns out to be deceptively simple.

When it's done correctly, of course.

Websites should only store what's called a "one-way hash" of your password, not the password itself. The original password cannot be determined from only its hashed value. If a site can tell you your password, they're doing security wrong. When you next hear of a data breach, pay attention to whether the password information is hashed or not. If it wasn't hashed, that implies your password, if included, is out there for anyone to see.

Websites shouldn't store your password

We'll start with the counterintuitive magic: websites shouldn't store your password. Period.

That leads to the question: how do they know you've entered your password correctly if they don't store it somewhere?

What websites should store is called a "one-way hash" of your password. A hash is a complex calculation that generates a large number. A good hash has three very important characteristics:

It is statistically impossible for two passwords to generate the same hash number.

You can create a hash from a password, but you cannot recover the password from the hash.

A small change in the password generates a large change in the resulting hash number, making it impossible to recover "nearby" passwords, even if you know the password/hash combination for some.

That second one is key.

Let's look at an example. I'll use everyone's favorite

(Continued on page 9)

(Continued from page 8) How Do Websites Keep Passwords Secure

password: "password".

One hash1 for "password" is 126,680,608,771,750,945,340,162,210,354,335,764,377. (More commonly expressed in base-16 numbers, aka hexadecimal, as in 5f4dcc3b5aa765d61d8327deb882cf99).

So, if you take password and hash it, you'll get 126,680,608,771,750,945,340,162,210,354,335,764,377.

If you hack a database and get that hash, all you have is 126,680,608,771,750,945,340,162,210,354,335,764,377 — you know nothing. There's no way to take that number by itself and determine what password generated it.

Typing the right password

When you set up or change your password, the site you're setting it with will calculate the hash and store that number. If you enter "password" as your password, then our example site will store "126,680,608,771,750,945,340,162,210,354,335,764,377 " in its database, along with your user ID and/or email address.

Now, days or weeks later you come back to the site and sign in. Here's what happens:

You enter your password ("password", in our example).

The site calculates the hash (126,680,608,771,750,945,340,162,210,354,335,764,377 in our example).

The site compares the hash it just calculated against the hash it stored when you set your password.

If they match, you must have typed your password correctly, since only the exact same password would generate the exact same hash.

If they don't match, you didn't type the expected password that goes with the expected hash.

That's really all there is to it. Aside from some complex math to generate the hash, it's pretty simple.

Telling you your password

I repeatedly used the word "should" above.

A website doing password security correctly should only store the password hash, not the actual password. Since there's no way to go backward — recovering the password from the hash — that means a website using proper security cannot tell you what your password is. They can only tell you that you typed it correctly or not.

Unfortunately, not all sites do security correctly, and there's at least one way to test:

If a website can tell you your password, then they've got that password stored as-is in a database the staff can access.

That's poor security because your password could be exposed in a breach.

Passwords and data breaches

The next time you hear of a large data breach, particularly if it's happened at some online service you use, pay careful attention to the wording describing the information that was exposed.

For example, here's a description of a recent breach from HaveIBeenPwned:

In June 2020, the restaurant solutions provider OrderSnapp suffered a data breach which exposed 1.3M unique email addresses. Impacted data also included names, phone numbers, dates of birth and passwords stored as bcrypt hashes. The data was provided to HIBP by dehashed.com.

(Emphasis mine.) The passwords were stored as hashes. In this breach, passwords were not exposed. While there was other information included in the hack, the most sensitive of all — passwords — had been stored correctly.

Contrast that with this description:

In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services.

There's no mention of hashing at all. This particular breach included actual passwords. Wherever those passwords came from, there was a lapse in security of some sort.

This is what you pay attention to: were the passwords exposed in a breach hashed? If not, change your password on the impacted service immediately. If they were hashed, you can still change your password if you like — and perhaps you should for other reasons — but you can be somewhat less concerned that your password is "out in the wild".

There's more to security than passwords

It's important to note that of course, there's much more to website security than whether or not passwords are hashed. Let's face it: data breaches shouldn't happen, either, but they do.

Hashing is just one (very important) part of website and online service security, which encompasses everything from keeping the web servers themselves secure and malware-free, to using proper database and software security, to ensuring only the proper personnel have

(Continued on page 10)

(Continued from page 9) How Do Websites Keep Passwords Secure

access to sensitive information.

It's a complex world, and easy to get wrong, as every breach we hear about reminds us.

But the next time you hear of yet another breach, now you'll have at least one thing to look at to determine just how security-conscious the service was and how worried you should be.

A quick note to pedants

Since this type of overview tends to bring out those with an eye for excruciating detail and minutia, one small caveat:

This is only a high-level overview to make the concepts accessible to more people. Of course, password management implementation details can get very complex. If you're about to comment with a complaint that I didn't discuss different hashing algorithms (ugh), or that MD5 shouldn't be used for passwords (I agree), or that password hashes should be salted (ditto), and why didn't I talk about rainbow tables (hoo, boy) . . . don't.

Those concepts were never the point.

Related Questions

Can a website owner see my password?

Website owners can possibly view your password in either of two ways. One, they can watch your keystrokes as you type in the password when signing in to their site; or, if they actually store your password in plain text in their database, they can also view it there. Note that the latter is considered bad security since anyone with access to the database would be able to view your password.

Where can I keep all my passwords safe?

The best way to keep all of your passwords safe is to use a password vault. These utilities store your passwords securely encrypted and accessible only to you. Many include additional features, such as automatic password entry, password generation, and in some cases, notification if an account is compromised or if a password you're using is not secure for any reason.

NEW!!!

$5.00 given away to members joining our meeting. If your name is called you will receive the full amount, no matter how many names we pull before someone is at the meeting.

In 2021, vow to start using a password manager

By Kurt Jefferson, Editor, Central Kentucky Computer Society
January 2021 issue, CKCS Newsletter
www.ckcs.org lextown2@gmail.com

I keep telling students in my CKCS classes that they need to start using a password manager. You should be using a password manager on your iPad, iPhone, Mac, Windows PC, and Linux PC. Seriously? Yes.

With a good password manager, you only need to remember one password. That's right. You don't need to remember the one you use when you buy from Amazon. And the password you use to pay your water bill. And the one you use to log into your bank account.

Password managers are apps that securely keep track of your passwords, allow you to create private notes, automatically log you into your password-protected websites, and more.

Some of the best include:

- 1Password
- Dashlane
- LastPass
- Keeper
- NordPass
- RoboForm
- Sticky Password
- bitwarden
- RememBer
- Enpass

If you're reluctant to use a password manager, wired.com says you've got company.

"Password managers are vegetables of the Internet. We know they're good for us, but most of us are happier snacking on the password equivalent of junk food," writes Wired in an article headlined, "The Best Password Managers to Secure Your Digital Life."

As I read that I said to myself, "Ain't that the truth." I know plenty of really smart people who are committed to their habits, who are stub-

(Continued on page 11)

(Continued from page 10) IN 2021 Vow to start using a password manager

born, and who simply cannot change. They don't use password managers. You probably know your web browser will save your passwords automatically for you. The website Tech Republic says this is a bad idea.

Why you should never allow your web browser to save your passwords shows others can see your passwords. The article describes step–by–step procedures that someone can use to view your saved passwords in Google Chrome, Firefox, and Safari browsers.

The article concludes: "Don't allow your browser to save your passwords. None of them. Not one. If you do, those passwords are vulnerable. All someone has to do is have access to your computer (remote or physical) and, unless you use Safari or the Master Password feature in Firefox, those passwords are available for anyone to see. If you absolutely must have your browser store your passwords, and you're not using macOS, make sure to use Firefox and enable the Master Password feature. Use Chrome at the peril of your passwords. In place of having your web browser store your passwords, make use of a password manager."

If you use a Mac, you might avoid using Apple's built-in keychain system and opt instead for a password manager. Glenn Fleishman, who writes about security issues for Macworld, gets into the details and digs deeper into this if you're interested.

Tom's Guide spoke with several digital–security experts. While some are not fond of password managers, plenty of others use them, trust them, and rely on them.

Cybernews writes, "You really should use a password manager. Yes, they have their flaws and vulnerabilities. But it's still better than re-using the same weak passwords and writing them down as a note on your smartphone that becomes a playground for your kids after work."

LCCUG

Windows 10, S-Mode – What's that? Do I need it? Do I want it? Apps and Applications – Mobile and Desktop

By Phil Sorrentino, Newsletter Contributor, Sarasota Technology Users Group
December 2020 issue, STUG Monitor
www.thestug.org philsorr@yahoo.com

Recently I needed a very inexpensive, low-end Windows 10 laptop. I intended to stream movies from one of my main computers, located across the house, to this new device and then show the movies on a big screen TV. From a performance point of view, I may have been able to use a Chromebook, a Tablet, or even an old phone but I wanted the device to be able to be part of a Windows network. So I decided I needed a low-cost Windows 10 computer. Keep in mind that nowadays, even low-cost laptops come with pretty decent performance, capabilities, and features. I've bought a few computers in the past and I've found that the important things to consider have always been, CPU, display, RAM, Hard drive (electronic drive in some), Networking (Wi-Fi), and Input/Output ports.

(I won't even need a mouse with this computer; the touchpad will do just fine.) Most laptops, these days, have pretty nice screens, though the price seems to go up as the screen gets bigger. I wasn't going to use the screen for watching the movie so I decided to look for a small screen. The CPUs were all from Intel or AMD, not top of the line but more than capable enough. Most had 4 GB of RAM. Hard drive capability varied but because I wasn't going to use the laptop to store much this wasn't a big concern. I did establish that I wanted a minimum of 64 GB if the laptop used SSD (Solid State Drive) memory rather than a hard drive. (In the past I had one with only 32 GB and I had trouble updating the Operating System when it was necessary.) Wi-Fi was a necessity because of the location of the laptop with respect to the movie streaming computer. Also, I wanted at least two USB ports, one for extra memory, should the need arise, and one for a mouse, should the need arise. With that minimal description, I started my search.

There are plenty of name-brand laptops out there like HP, Dell, Microsoft, and Lenovo, but I wanted a very low-cost device, so I widened my search to other

(Continued on page 12)

(Continued from page 11) Windows 10 S-Mode….

brands like LG, ASUS, Acer, and Toshiba. I even considered "refurbished" laptops but I never found one for the right price. My search ended when I found an 11-inch ASUS Vivobook laptop model L203M at what I thought was an incredible price, $294 at Walmart. (Recently, I have seen it for about $10 less.) As I became familiar with the laptop features, I realized it had Windows 10 S-Mode. I knew there were a few different versions of Windows 10 like Home and Pro for home use and Enterprise for businesses, but I wasn't familiar with S-Mode.

You will probably only come across the S-Mode version of Windows 10 if you are looking at the low end of Windows laptops. (I found laptops from all of the name brands that had Windows 10 S-Mode installed, even Microsoft has one, but the ASUS was about the lowest when I was looking to make the purchase.) In a nutshell, Windows 10 S-Mode is a version of Windows 10 that is streamlined for security (I guess, hence the S) and performance, while providing a familiar Windows experience. To increase security, it allows you to get and use Apps only from the Microsoft Store and requires you to use Microsoft Edge for browsing. All other versions of Windows 10 have the option to install applications from third-party sites and stores like Google, Yahoo, and hundreds of others. Because many people prefer Chrome to Edge, this could become a pivotal issue, but if you can live with Edge as your browser this may be a good choice. Part of its improved security may be a side-effect of the inability to install Apps from other websites not approved by Microsoft since viruses tend to hide in dubious internet downloads. One interesting feature of S-Mode is that you can convert from S-Mode to the standard Windows 10 Home (or Pro) version, but it is a one-way conversion. It's as easy as going to the Microsoft Store and Opting out of S-Mode. Once you convert you have to stay there, you cannot go back to S-Mode, though I've seen indications that this might change in the future. (Microsoft used to charge a fee for this conversion, but now it is free.)

Windows 10 S-mode has been around since 2017. It is a lightweight version of the Windows 10 Operating System. Published statistics indicate it has been installed over 825 million times, so there are a good number of users. It is more protected than other versions and streamlined so it can run fast even on budget CPU devices. Even with its limitations, Windows 10 S-Mode still includes File Explorer, as we all know, the keys to the kingdom. It is aimed at the Education sector of the computer business where a certain amount of control, and possibly limitation, is needed. This puts Windows 10 S-Mode in direct competition with Google's Chromebooks which have enjoyed unprecedented success and popularity in this education sector. The literature indicates you can find Windows 10 S-Mode laptops starting at about $200, but the lowest price I found in my search was just under $300. (Microsoft probably subsidizes the cost of the OS to hardware manufacturers, so you are probably only paying for the hardware.

So when all is said and done, is Windows 10 S-Mode right for you? Could be if you have minimal needs, that could be met by even using a Chromebook.

How Reliable is Reliable Enough?

by Greg Skalka, President, Under the Computer Hood User Group
www.uchug.org president@uchug.org

Google defines reliability as consistently good in quality or performance; able to be trusted. We all want our technology to perform well, as we depend on it more and more in our lives. In placing a call, turning on our lights, driving to the store, checking our bank balance, or taking a commercial flight, we all want (and perhaps expect) 100% reliability in our experiences with technology. Nothing can be completely dependable, however, and no matter what we expect, tech failures happen. Reliability can be regulated by government agencies, specified by standards, or simply provided "as-is" by the manufacturer. In the end, it is up to each of us to decide if the reliability levels we get meet our needs.

Most large companies now use an ISO 9000-based quality management system to demonstrate their ability to provide quality products and services that consistently meet their customer's needs. The basics boil down to 'say

(Continued on page 13)

(Continued from page 12) How Reliable is Reliable Enough

what you do' and 'do what you say'. Unfortunately, for the customer, the issue is often that not enough is said, and the only standard the customer has is their expectations about quality and reliability; these usually wind up being different from the vendor's.

I have a lot of smart home devices. Many companies make and support products and systems to remotely control lights and devices in your home. You can control them remotely through an app on your smartphone or tablet, or through an Amazon Alexa or Google Home Assistant device. In addition to immediate control, your items can be programmed to turn on and off in a scheduled manner. The manufacturers portray these smart devices as simple and easy to use, so the consumer might assume they are reliable. Unfortunately, they are fairly complex and sometimes not so reliable.

I'm typically up and out of the house to work well before my wife is awake. To make my workday mornings easier (and safer, especially in the darker mornings of winter), I program lights downstairs to come on just before I would come out of our bedroom. This gives me a little bit of light to help me see when going down the stairs before dawn. I use a Belkin Wemo smart plug, with a family room lamp plugged into it, to give me some of that light. I've programmed the ON time in the Wemo app so that at my selected time the Belkin servers send a message over the internet and through my Wi-Fi to the smart plug to turn on. Once I get downstairs, I turn the light off manually with our Amazon Echo Show as quietly as possible, using the screen icons rather than voice control. In this case, the OFF command is sent from my Show over the internet to Amazon's servers, and then passed to the Belkin servers and back over the internet to my Wemo smart plug.

This seems like a lot of complex communications, but it has worked very reliably over the four months since I set this up. Last week, however, it didn't do so well, failing to turn off correctly on two different days. On the first day, Alexa could not turn the light off; I had to go into the Wemo app to do it. On another day, even the Wemo app could not turn the light off, as the smart plug appeared as inactive in the app. I finally had to resort to pressing the button on the smart plug to shut it off. In both cases, everything worked fine again after a short time. I was happy to see it working, but was reminded of the engineering saying "Problems that go away by themselves can come back by themselves."

Though I was not happy that the smart plug worked unreliably those two days, was there anyone I could blame? Perhaps not, as Belkin and Amazon had said I could control my light in this way, but they didn't say it was guaranteed to work 100% of the time. That it had worked reliably all but two days in four months is in reality pretty good, considering the plug cost only $20 (and the Echo Show cost $50).

This brings up one key factor in the reliability equation: high reliability generally costs more. The successful landing of the NASA Perseverance Mars rover last week was a tremendous technical achievement, but it came at a cost of around $2.5 billion. That kind of money can buy a lot of reliability, however. The NASA Opportunity rover, launched in 2003, cost $400 million and had a planned mission duration on Mars of around 90 days, yet it continued exploring and communicating until 2018. NASA's Curiosity rover has been operating on Mars for the last 8.5 years, far exceeding its original 2-year mission life. Hopefully, Perseverance can demonstrate a similarly high level of reliability.

Money can't buy total reliability, however. Since its inception in 1958, NASA has spent over $650 billion (perhaps $1.2 trillion after inflation). It has had many great successes, putting 12 men on the moon, exploring all our system's planets with robotic probes, and currently has put five rovers successfully on Mars. It has had some tremendous reliability successes, such as the Voyager 1 and 2 probes that are still providing communications

(Continued on page 14)

(Continued from page 13) How Reliable is Reliable Enough

as they leave our solar system. It has also endured tragic failures, the worst of which are the losses of crews of the Space Shuttles Challenger and Columbia, and Apollo 1.

Not everything needs to be as reliable as a spacecraft, but many things, especially where failure would involve loss of life or a high economic loss, require high reliability. Structural items such as buildings, bridges, and tunnels, and transportation items like aircraft, trains, ships, and cars, all need higher safety and reliability standards. You may sit in both, but you justifiably have greater concerns and expectations about safety and reliability for your automobile than for your La-Z-Boy recliner.

One way to mitigate risks when reliability and safety are not deemed sufficient is through back-up systems. Hospitals may add back-up power generators to compensate for a power grid that is not totally reliable. There probably are measures that should have been taken (and now likely will) to harden the Texas power grid against the extreme cold weather it experienced recently.

Our computers hold information internally in rotating magnetic platter hard drives and SSDs, but these are not immune to failure, so prudent users back up that information. Automobile tires can fail for a variety of reasons, so automakers offer several back-up systems, including a spare tire and changing tools, puncture sealant, and run-flat tires. Tire pressure monitoring systems are now required for all automobiles, as a safety backup.

We have continued to add safety features to motor vehicles over the years to reduce the number and severity of accidents. Safety glass, power steering and brakes, seat belts, airbags, energy-absorbing bumpers, and rear back-up cameras all add safety to cars through technology. Despite these enhancements, however, over 16500 Americans died in motor vehicle traffic crashes in 2020. Now automakers are looking to add self-driving technology to our highways; will it be safe and reliable enough?

Sometimes reliability is not as important as other factors, such as cost or convenience. Often new technologies are not as reliable initially, but in time may improve (or wind up being shunned by consumers). I like my Amazon Alexa devices, but I don't always get the responses I expect. Considering the complexity of the system, low cost to me and less than a critical need for the information, a less than perfect performance is acceptable. Alexa may not always provide the information I'm looking for, but I'm easily able to recognize this and so am not really harmed by her "incompetence".

Some kinds of unreliability are more acceptable than are others. If your smart home lock is unreliable, it might be better if it occasionally fails to unlock when you get home, rather than sometimes not locking when you leave. It is the same with computer security; it is better to err on the side of being too restrictive than too permissive. Users can put up with only so much in unreliable access, however. New technologies such as fingerprint scanning and facial recognition for login, though more convenient than passwords, won't gain wide acceptance if valid users are not reliably recognized. If the convenience difference is great enough, however, users might be willing to accept having to scan multiple times for access.

Reliability in our technology is important, but the need for it varies with the product and the potential downsides. Our sensitivity to quality issues should be greater for a Boeing 737 MAX airplane than for a wireless router. We as individuals and as a society will have to weigh the cost, quality, and risk trade-offs to determine in each case how much reliability is enough.

Pam Rihel prihel1947@gmail.com
Dick Eastman
http://www.eogn.com.

Millionth Item Digitized and Made Freely Available via Bodleian Libraries Website

The University of Oxford's Bodleian Libraries has reached a significant milestone, with the millionth digitized version of an item held in its collections now having been uploaded for free public access anywhere in the world.

Launched in 2015, the Digital Bodleian website is a free resource providing unfettered access to a vast array of items housed in the institution's wide-ranging collections.

The digital archive of images has steadily grown throughout the six years since its launch, with an original notebook belonging to poet Jenny Joseph, a former student at St Hilda's College, now having become the one millionth item digitized and made available for public access.

"Whether you are a student, a researcher or someone who has a personal passion, we are delighted to be able to make our collections, built up over the last 400 years, for all to be able to view, download and use," says Richard Ovenden, Bodley's Librarian at the Bodleian Libraries.

"We invite everyone to explore the diversity, interest and sheer beauty of these manuscripts, books, archives, photographs and paintings. Many of the collections we have digitized were gifted to the Bodleian, and the costs have often come from generous donors and funding bodies who share our desire to make these materials widely available."

Having blazed a trail by digitizing content as far back as the early 1990s, the Bodleian Libraries was the first library outside the USA to partner with Google as part of their ongoing mass-digitization programe.

You can learn more at https://advisor.museumsandheritage.com/news/one-millionth-item-digitised-made-freely-available-via-bodleian-libraries-website/.

The Bodleian Libraries and Oxford college libraries web site may be found at: https://digital.bodleian.ox.ac.uk/.

Genealogy Tip of the Day

Michael John Neill Genealogy Day 2021 Rootdig.com
mjnrootdig@gmail.com

Be Willing to Change

michaeljohnneill, 05 Sep 05:14 PM

Part of genealogical research is evaluating what you have and altering conclusions when new and more reliable information warrants. Early in our research when we are inexperienced, it can be tempting to rely too much on family information. It can also be easy to rely on incomplete information–especially before we learn that "official" records can be incorrect or inconsistent.

And sometimes DNA and other information will cause us to re-evaluate what we thought was true even when we had a number of records and completely analyzed them.

My children's great-great-grandfather (father of their great-grandmother) has morphed through many iterations over the nearly thirty years that I have researched him–always because I have located new information:

- a Greek immigrant to Chicago, Illinois, born in the 1880s–turned out he was the great-great-grandmother's second husband and not the biological father of any of her children;
- a man born in Chicago in the 1880s (first husband of the great-great...Read More

Preparing for the 1950 Census Release

michaeljohnneill, 05 Sep 04:49 PM

We've still got room in our prepping for the 1950 census release webinar. Ordered recordings will be available after the session on 9 Sept 2021 and can be viewed at the purchaser's convenience. Details on our post.

Analyzing Each Statement

michaeljohnneill, 30 Aug 11:34 AM

Records contain many statements and each of those statements can either be true or false. Analyze each statement separately, thinking about who likely gave the information, how likely they were to actually know the information, and the circumstances under which they were giving the information. It's also helpful to think about whether the person might have any motivation to give incorrect information and whether there would have been any penalties for giving false information.

It's also worth considering if more than one person could have been involved in giving the information and how publicly that information was given.