Interface

Lorain County Computer Users Group
LCCUG.com (or) info@LCCUG.com
Volume 33 Number 2 February 2022

Tuesday
February 8, 2022

Preserving Digital Photos

Presented by

Mark Schulman
Central Florida Computer Society

Using Zoom Only

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

NOTICE: MEETINGS ARE HELD ON ZOOM ONLY UNTIL MAY, 2022

LCCUG Meetings will be happening on ZOOM

No in person meetings at this time.
At a new time: from 10 am. - noon

Please email info@lccug.com if you have any questions or concerns!

2022

Inside This Issue

A Word From Our President

Our February 8, 2022 meeting will be held at 10 am as it has been **but** it will be held ONLY ON ZOOM. Due to the fact that Micky will not be able to attend (he is volunteering for taxes in Oberlin during that time), since he is the only one who has managed the technology for our hybrid meetings that are in person AND online using Zoom. Therefore, we will meet online only.

Join us Feb 8 online in Zoom as we talk about handling your digital photos!

As we continue into the new year, I want to start with thanks to our volunteers that keep us going.

Dennis Smith has been our membership chairman and is taking a break from those duties for a while as he prepares to retire from his "real" job. Hopefully he will be able to return to us in some fashion later in the year. Especially when we were meeting in person, he was a great asset – handling the raffles, prizes and drawings, along with Don. Hopefully we'll see him on ZOOM!

Neil Higgins has been our Education Chairman for years and assistant technology person. Due to health issues, he will not be present in person for a while. He helps keep our Facebook page current with technology stories. Hopefully he will be able to able to join us on Zoom as well. I know I have always appreciated his contributions and I hope he will be able to be more involved again a little later.

Rich Barnett has been our Director of Advertising and Web Page editor. Due to an accident last year, he hasn't been able to attend in person meetings but continues to keep our webpage going!! We're always glad when he can attend the ZOOM meeting. We're happy for his continued improvement.

Pam Rihel dealt with a knee replacement this year but has continued to produce our newsletter! She is another officer that keeps our group going.

Don Hall has been our club secretary for more than a decade. He maintains our minutes and is a big help when we have drawings and raffles. Don is our oldest officer and member at age 93 and has had the best health among us this year!!

Micky is our technology specialist and is handling the technology involved in managing the hybrid aspects of meeting in person and in public. He and Neil have resumed the Problem Solving sessions on the 3rd Tuesday.

LCCUG Officers For 2022

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	**Vacant** membership@lccug.com
Director of Advertising	Richard Barnett advertising@lccug.com
Director of Education	Neil Higgins education@lccug.com

He has been our back up newsletter assistant and website tuner, as well as his duties as Treasurer. He is essential to LCCUG's existence.

Since Micky will be unavailable on Tuesdays for the duration of the tax season, the 3rd Tuesday Problem Solving/Troubleshooting Workshop may be cancelled for the next few months if Neil is not able to host the meetings on his own. If there is interest, Micky is willing to host the workshop on Thursdays instead of Tuesdays. Let us know if you'd like this to happen by emailing us at troubleshooting@lccug.com.

Thanks to this great crew. They make it possible to keep our group together!!

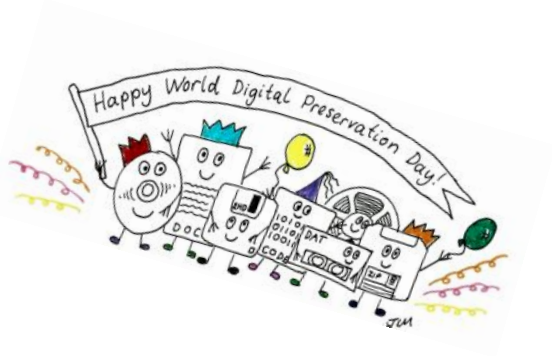
Sandra Ruth
LCCUG President

Tuesday
February 8, 2022

Preserving Digital Photos

Presented by

Mark Schulman
Central Florida Computer Society



Digital photos don't fade with time and can be protected against natural disasters such as fire and floods. That's the theory, anyway. And yet, if you're one of the millions of people with a digital camera, the chances of your great-grandchildren ever seeing your digital photos are very slim. Find out why the odds are stacked against you and what you can do to increase the chances that your family historian 200 years from now will be able to enjoy the photos you're taking now.

zoom

PLEASE NOTE:
THIS WILL BE A ZOOM ONLY MEETING

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 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

John Kolb
secretary@loraincoogs.org

Executive Board Meeting Minutes

JANUARY 4, 2022

The January board Zoom meeting was attended by Sandee Ruth, Don Hall, Micky Knickman, Pam Rihel, Richard Barnett and Neil Higgins.

The board agreed on "Favorite / Useful Websites" for the January 11 program along with tips and tricks. Sandee also has some 5 minute videos.

Preserving Digital Photos is a program planned for February.

There was $124 raised from the 50/50 raffle for Second Harvest. The board approved an additional $76 to make the donation $200.

Pam moved, Neil seconded the meeting be adjourned.

General Meeting Minutes

JANUARY 11, 2022

President Sandee Ruth called the meeting to order. A motion to accept the minutes as shown in the January issue of the *INTERFACE* was made by Micky Knickman, seconded by Cliff Salisbury. Motion passed by voice vote.

Sandee announced that next months program will be "Preserving Your Digital Photos".

Micky and Sandee presented a program "Useful Websites and Utilities" The many websites shown were both entertaining and informative with many questions from the attendees.

Member of Association of Personal Computer Users Groups

Newsletter Editor: Pam Rihel using Microsoft Publisher, 2016

This Month's contributors: Micky Knickman, Sandra Ruth, Pam Rihel, Don Hall, Neil Higgins, Michael John Neill, David Ketchmar, Kurt Jefferson, Scambusters, Ask Leo, APCUG, Google images, Microsoft Office art online,

Newsletter is now Online at:

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

Computer Club News

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

Recycle & Help Our Club Too!

MEMBERSHIP WITH LCCUG:

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

LCCUG
Director of Membership,
membership@lccug.com.

Meeting Location:
At a new time: from 10 am. - noon
in a new location: LCCC facility at
201 W. Erie, Lorain

Our meeting space is on the first floor – easily accessible – larger – refreshments available! Please email info@lccug.com if you have any questions.

Lorain County Computer Users Group

2022 Calendar of Events

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

Using Zoom

Meeting opens at 10 am – program starts at 12 pm

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

January 11, 2022 - Useful Websites and Utilities presented by our Board Members and Our members

February 8, 2022 - Preserving Digital Photos By Mark Schulman

March 8, 2022 - The Pro's and Con's of BACKUPS; introducing "Tech for Senior"

April 12, 2022 - To Be Announced

May 10, 2022 - To Be Announced

June 14, 2022 - To Be Announced

July 12, 2022 - To Be Announced

August 09, 2022 - To Be Announced

September 13, 2022 - To Be Announced

October 11, 2022 - To Be Announced

November 8, 2022 - To Be Announced

December 13, 2022 - Holiday Lunch

Please check our website LCCUG.com for more updates. If you have anything you would like to know about, PLEASE let up know. We would really like your input.

Genealogy Tip of the Day

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

Out-of-Towners Can Pay Taxes

michaeljohnneill, 22 Jan 03:57 PM

When viewing real property tax records, remember that landowners are the ones who pay property taxes and landowners may not live on the property they own.

Just because you see Nicholas Schnieferdornman paying tax on real property in Amherst County, Virginia, in 1813 does not necessarily mean that he resides in Amherst County at that time. It is possible that he is a non-resident landowner. Individuals who are taxed on personal property in an area are usually residents of that area, but there can always be the occasional exception.

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 Unavailable at this time
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

Most Are Free And Open To The Public

Problem Solving Workshop

Date: Thursday- February 17, 2022 ????
Time: 10AM-12PM Instructor: Micky Knickman, Neil Higgins, Richard Barnett
Place: LCCC @ 201 W. Erie Ave., Lorain, OH

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

Members MUST make an appointment by emailing Micky or Neil at. troubleshooting@lccug.com. This workshop is limited to LCCUG members in good standing. If there are no appointments, this will be cancelled.

The Problem Solving Workshop is being held at our new building, LCCC, 201 W. Erie Ave. Lorain, Ohio

You are asked to bring in your computer, laptop and other electronics that you need help with.

Learning About Electronics

Date: Thursday - February 17, 2022 ???
Time: 10AM-12PM Instructor: Sandee Ruth
Place: LCCC @ 201 W. Erie Ave., Lorain, OH

Learn how use you electronic devices.

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

LCCUG WORKSHOP Class Ideas?

Neil may be starting up his workshop soon and he would like some ideas on what type of projects you are interested in learning about. Contact:

Neil Higgins Education@lccug.com.

Bitcoin - the New Gold?

By David Kretchmar, Computer Technician
Sun City Summerlin Computer Club
https://www.scscc.club
dkretch@gmail.com

In March 2021, the total market value of Bitcoin exceeded one trillion dollars for the first time. In addition, each individual bitcoin recently touched a value of over $60,000 before falling back.

Bitcoin's pullback was precipitated by Federal Reserve Chairman Jerome Powell when he made what was perceived as negative comments about Bitcoin. "Crypto assets are highly volatile — see Bitcoin — and therefore not useful as a store of value. Moreover, they're not backed by anything. Instead, they're more of an asset for speculation. "It is essentially a substitute for gold rather than the dollar." Powell also reiterated the IRS's position that sellers and spenders of bitcoins would be required to report capital gains as though Bitcoins were stock.

To put this gold/bitcoin comparison in perspective, the total market value of gold in the world is about 10 trillion dollars, ten times the total market value of Bitcoin.

In this discussion, I'm using the term "Bitcoin" to represent the numerous crypto currencies such as Ethereum and 100 smaller cryptocurrencies, many offering very different features and superior to bitcoin by some measures. Nevertheless, Bitcoin is the most widely known, and Bitcoin's value currently represents almost 90% of the total value of all cryptocurrencies.

Durability

Gold is an inert element that does not oxidize. Bitcoin is dependent on the internet and all of the decentralized participants in its operation. So, if there is some global catastrophe that destroys the internet, then only gold survives. But for anything less than that, Bitcoin and gold are equally durable. A much more likely scenario is the internet suffering some serious but limited issues and being problematic for days or weeks. Without the internet, all financial institutions would have problems functioning. Some theorize that because of its decentralized structure, Bitcoin might emerge as "the peoples" money in the event of an internet meltdown. Bitcoin is currently preferred in nations like Venezuela and other third-world countries, where the fiat currency issued by the government has become virtually worthless.

Transferability

You can trade gold on paper if you are willing to assume third-party risk, which defeats part of the purpose of holding gold. To transfer physical gold, you usually need to move it. Large quantities of gold are heavy and difficult, and expensive to transfer securely. Commissions can be excruciating for small gold transactions.

Bitcoin can be sent to another address controlled by somebody anywhere in the world in seconds, and the transfer is confirmed and permanently recorded in minutes. Thus, Bitcoin is infinitely more transferable than gold.

Divisibility

It is difficult to divide gold, particularly for small amounts. Bitcoin can be subdivided today into 100,000,000 units called satoshis, and the protocol could be extended in the future to support even smaller amounts if that becomes necessary. Bitcoin is infinitely more divisible than gold.

Scarcity

The scarcity of gold is well understood; in the history of humankind, about 6 billion troy ounces of gold have been produced, 90% of which is estimated to exist still. All the gold ever mined would fit inside a 20-meter cube. The world's supply of produced gold increases by roughly 1 - 2% each year, depending on the metal price and discoveries

(Continued on page 8)

(Continued from page 7) Bitcoin - The New Gold

of deposits.

Bitcoin has a limit of 21,000,000 units, including Bitcoins permanently out of circulation due to lost keys. Changing the rules to allow more units of Bitcoin would require a consensus of users. This is possible, but it is very doubtful that the Bitcoin stakeholders would choose a course that would hurt the value of their assets.

Interestingly, both gold and Bitcoin are produced by "mining." Each has been mined to the extent estimated to be approaching 85 - 90% of the total quantity that will ever be produced. Thus, Bitcoin and gold are both scare commodities.

Recognizability

Gold can be counterfeited and sometimes needs to be tested for purity. Authentication can be tricky, but not that that difficult for experienced people.

Bitcoin cannot be counterfeited, and it is easy to verify the validity of Bitcoin based on the blockchain, the shared Bitcoin ledger. As a result, Bitcoin is more recognizable than gold, at least among people who understand what a Bitcoin is.

Taxation

Bitcoins are taxed just like stocks, with a maximum 15% or 20% rate on long-term capital gains (assets held for at least a year). That compares favorably with most other alternative investments. But, as Jerome Powell stated, people who use Bitcoin to make a purchase create a taxable event they have to report.

Gold is taxed as a collectible, and sales do not have the advantage of favorable long-term capital gain treatment. When sold, gold gains are taxed at the individual's ordinary income tax rate to a maximum of 28%. Gold buyers may also have to pay sales tax, depending on relevant state laws.

Conclusions

Gold and Bitcoin, as different as they are, both have good investment vehicles and sound money characteristics. As more people grow comfortable with Bitcoin and understand how it works, Bitcoin will replace gold as a store of value. This is precisely what we see happening right now. If this continues, some specialists predict the price of Bitcoin in US dollars should stabilize at $300,000 - $500,000, but it's going to be volatile. Any investment with tremendous upside potential also has massive downside risk.

Price is ultimately determined by supply and demand. Demand comes from widespread recognition, a liquid market, and sustained interest. Bitcoin has been unique, achieving a worldwide network in less than 15 years. Other currencies are acknowledging Bitcoin and even inking their value to Bitcoin. The US and other countries are looking into issuing their digital currencies. Individuals and vendors worldwide are beginning to adopt Bitcoin as a payment mechanism and as stored value.

Bitcoin is becoming a valued currency not by force of government declaration or people's acquiescence but by recognition and widespread acceptance.

Genealogy Tip of the Day

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

Pick A Day

michaeljohnneill, 03 Feb 10:55 AM

Pick a day in your ancestor's life. Try and answer the following questions as of that date:

- Where was my ancestor living?
- Who was in his (her) household?
- What was the ancestor's occupation?
- What was the ancestor's age?
- What was going on nationally on this date (at this point in time)?
- What was going on locally/regionally?
- Were my ancestor's parents alive?
- Were my ancestor's siblings alive?
- Where would he (she) have gone to church the previous Sunday?
- Who were my ancestor's neighbors?

Is a Password-protected Windows Login Secure?

Maybe like a cheap padlock.

by Leo A. Notenboom

Your Windows log-in password gets you surprisingly little real security. I'll look at why that is, why you might still want one, and what I do instead.

I use Windows on two desktops and a laptop. Up until now, I have never bothered using a password when logging on. But recently, I was cautioned to use a Windows Logon password when I bought the laptop. The shop where I purchased it said this was for security, in case someone took it. They also said the use of a password on my home PCs would prevent malware from being automatically installed should I inadvertently download something. Is this true? I ask because a year ago, I tried to close a pop-under ad using the red X button and unknowingly installed malware. I now use Task Manager for such operations, but the bad guys keep changing what they do, so that solution may someday no longer work.

The security provided by a Windows login password is highly overrated.
It doesn't protect you from many of the things that you've mentioned, and it's pretty darned easy to circumvent.

You should probably have one, and with the migration to Microsoft accounts, you'll need one (though you can still log in automatically); just be aware of what it gets you and (especially) what it doesn't.

Is your Windows login secure?

Your Windows login doesn't really protect your computer's contents from theft. While it will keep honest people honest, it's not a comprehensive security tool. Instead, rely on things like physical security, encryption, and other best practices for staying safe.

The biggie: theft

If someone takes your computer, they don't need your password.
There are several approaches a thief can take to compromise your computer and/or steal your data.

- They may be able to set a new administrator password and then do whatever they please. I've Lost the Password to My Windows Administrator Account, How Do I Get It Back? has the technique.
- They may be able to boot from something other than the hard drive, run a different operating system, and then access the contents of your hard disk.
- They may be able to remove the hard disk from your machine and access its contents on another computer.

The lesson is simple: having a password on your Windows login gets you zero security should your computer be stolen.

Or put the way I usually put it: if your computer's not physically secure, it's not secure.

What a Windows log-in password does get you

Not much.
I view the Windows login as a cheap padlock. It keeps honest people honest and prevents a few mistakes, but is not much of a deterrent to someone who's really intent on breaking in.

I don't see how it slows down malware infections since those happen when you're already logged in, using a password or not. The only scenario slightly impacted might be malware trying to get administrative privileges. If there's no administrator password, perhaps it could. But that scenario seems rare, especially given that the true "Administrator" account is disabled by default and UAC is enabled for all other accounts.

Login passwords are useful, and perhaps even required, for some things:

- Preventing unauthorized access to your files by other computers on your local network.
- *Allowing* authorized access to your files when using other computers on your local area network.
- Signing into your desktop computer remotely.

My Windows machines all have log-in passwords for two reasons:

- I now use Microsoft accounts for all, which requires a password.
- I want to be able to log in using Remote Desktop.

(Continued on page 10)

(Continued from page 9) Is Password Protected...

- On machines I don't expect to travel with, I typically have automatic login turned on so I still don't have to enter the password.
- I do not password my Windows login for any serious security.

Do this

So if the Windows login doesn't make your data secure, what does?

Particularly for portable computers you take with you, the most important things you can do are:

- Enable BitLocker whole-disk encryption.
- Do *not* enable automatic login.

You might also consider those steps for desktop machines where you can't control physical security. If anyone can walk up to the machine, they can do anything.

For all machines, then, staying secure comes back to our common list of best behaviors:
Have good security software.

- Keep all your software — security, applications, and operating system — as up to date as possible.
- Be skeptical and on guard. That means not opening attachments you don't expect and learning to recognize and not fall for phishing attempts.
- Back up religiously.

But definitely don't assume that the Windows login really helps.

And while you're at it, subscribe to Confident Computing! More tips like this, less frustration, and more confidence, solutions, and answers in your inbox every week.

ScamBusters.org

MASTERCARD SECURITY ALERT: SPECIFIC THINGS YOU CAN DO TO PROTECT YOURSELF FROM CREDIT CARD FRAUD AND IDENTITY THEFT

The largest security breach to date occurred late last week when 14 million MasterCard and 22 million Visa credit card numbers were hacked. Up to 40 million credit card users may now be at risk of fraud from their MasterCard, Visa and other credit cards.

The security breach took place at CardSystems Solutions, a third-party transaction processor for merchants and financial institutions.

It appears that the breach was caused by a hacker who gained access to CardSystems' database and then installed a virus-like script that captured customer data. The F.B.I. is investigating the security breach.

According to MasterCard, names, credit card numbers, expirations dates and the three or four digit credit card security codes were stolen. Social Security numbers, birth dates or other highly sensitive personal data were not part of the security breach.

MasterCard said that only 68,000 of the 13.9 million MasterCard holders were at "a higher level of risk."

MasterCard, as well as some other credit card providers, have zero-liability policies, so consumers who find unauthorized charges made on their credit cards will not be responsible for paying for the charges.

This security breach is simply the latest, albeit the largest, in a long line of breaches reported this year. Security breaches or lost computer tapes have been reported this year by ChoicePoint, LexisNexis, Citigroup, Bank of America, Stanford University, United Parcel Service, and many others.

(Continued on page 11)

(Continued from page 10)

Since there has been a relentless string of security breaches -- both online and offline -- this year, we offer 7 specific suggestions of things you can do to help protect yourself from credit card fraud and identity theft:

1. Check all your credit card and bank statements very carefully. If you have access online to your credit card charges and/or bank accounts, we recommend you check your statements frequently so you can spot problems as early as possible.
2. If you find any unauthorized charges on any of your credit cards, notify your card issuer immediately.
3. If you discover a problem, follow the advice in our article: "What to Do if Your **Credit Card** or Wallet is Stolen."
4. Consider using one-time use credit card numbers, called "controlled payment numbers" or "virtual account numbers," for your online purchases. Controlled payment numbers help protect your privacy and your security. They are substitute numbers that let you shop online without using your real credit card number. Typically, controlled payment numbers expire after one use (although their use can be extended for repeating monthly bills). These substitute numbers link back to your credit card number without you ever having to reveal your actual credit card number when you shop.The benefit is that if the substitute credit card number is stolen, such as in this case of the 40 million MasterCard and other credit card numbers, the substitute number would be worthless and your real credit card number would not be compromised. Currently, we know of two credit card issuers who offer this service: Citibank and Discover Financial Services. MBNA Corp. and others may also offer this service (however, we could not find a public link).For more info, visit:

Citibank (Virtual Account Numbers) **Discover Card** (Discover Deskshop).

5. Consider purchasing a credit monitoring service. These services typically offer periodic copies to your credit reports so you can monitor your credit file, email alert notifications of key changes in your credit reports, identity theft insurance, and personal customer service help.All three major credit reporting companies offer these services. They are not inexpensive. The service we now personally use is **Equifax Credit Watch Gold**. (Please note that this is an affiliate link, so ScamBusters does earn a commission if you purchase this service by clicking on this link. This means you are helping to financially support Internet ScamBusters with your order.) Note: Some people have very strong negative feelings about these services. They believe these services should be free to everyone, and that having to pay for them is completely unfair. We respect that opinion. Our belief is that regardless of whether or not these services *should* be free, the fact is that they aren't. So, we believe the more practical question now is whether or not these services provide sufficient value to you to be worth the not inconsequential cost. Personally for us, because of all the security breaches this year -- both online and offline -- the answer is now that it is worth it to us. It may or may not be for you.
6. Consider putting a 'fraud alert' on your credit file with the major credit card bureaus as a precautionary measure. A fraud alert is an alert that the three major credit reporting companies attach to your credit file that alerts creditors that your private financial information has been, or may be, compromised. This free service alerts creditors to use additional steps to verify your identity before opening new accounts in your name. When you place a fraud alert with one of the three major credit reporting companies, they will automatically notify the other two companies on your behalf, so you don't need to place the alert with all three. In addition to flagging your account with a fraud alert, your name will also be removed from prescreened offers for credit cards and loans. And, you may well be able to receive free

(Continued on page 12)

(Continued from page 11) MasterCard Security Alert

copies of your credit report from all three major credit monitoring companies. Placing a fraud alert does not damage your credit. You can remove the alert by calling the number on the credit reports you receive.

There are certainly drawbacks to placing a fraud alert, including that getting new credit cards and other credit may be more difficult. For example, a fraud alert may limit your ability to get instant credit for in-store purchases.

Creditors are asked to call you at a designated phone number before opening new accounts, and you may be required to show additional identification when opening new accounts.

Another drawback is that a fraud alert may not prevent a scammer from opening a new account in your name. Creditors are asked to call and verify all credit applications made in your name before they open any new credit account or grant any new credit. However, creditors are not required by law to contact you. In other words, fraud alerts can legally be ignored by creditors.

Placing a fraud report is done by an automated system -- it is almost impossible to speak to a human being. Here are the three agencies and their phone numbers:

Equifax: 1-800-525-6285
Experian (formerly TRW): 1-888-397-3742
Trans Union: 1-800-680-7289
For more information, visit the **FTC** website.

7.Reread our article called "**Credit Card Fraud**: 21 Tips to Protect Yourself," and follow the advice.We highly recommend that you seriously consider each of these items involving your MasterCard and other credit cards, and take action on all that make sense for you to protect yourself from credit card fraud and identity theft.

The Anatomy of a Scam: Ransom for My Files

By Kurt Jefferson, Editor, Central Kentucky Computer Society
https://www.ckcs.org lextown2@gmail.com

In mid–February, I checked my Gmail account as I do several times a day. Lurking in my Junk folder was a mysterious email message that appeared to come from Germany.

The email address used to send the message might be stolen or forged. But the subject is clear:

Payment for your account.

This is a new form of what's called "ransomware." It used to be that criminals would install software on a user's computer and encrypt all the files – basically locking them so the user can't read them. The victim would get his or her data back after meeting ransom demands.

Hospitals and other health care facilities have been targeted in recent years, and these attacks have escalated.

Now scammers are sending emails containing ransom demands – even without installing any software.

That is the gist of the email I received in my Gmail account. So, it appeared on both my Macs and iPad.

I'm sharing the message with readers of this newsletter to alert you – should you receive a similar threat.

Payment for your account
Feb. 17, 2021 at 4:33 P.M.
From: webmaster@dreirad*******.de
To: Kurt

Greetings!

I have to share bad news with you. Approximately few months ago I have gained
access to your devices, which you use for internet browsing.

After that, I have started tracking your internet activities.

Here is the sequence of events:

Some time ago I have purchased access to email accounts from hackers (nowadays, it is quite simple to purchase such thing online).

Obviously, I have easily managed to log in to your email account [email account name deleted].

Obviously, I have easily managed to log in to your email account [email account name deleted].

Continued from page 12) The Anatomy of a Scam...

One week later, I have already installed a Trojan virus to Operating Systems of all the devices that you use to access your email.

In fact, it was not really hard at all (since you were following the links from your inbox emails). All ingenious is simple. =)

This software provides me with access to all the controllers of your devices (e.g., your microphone, video camera and keyboard).

I have downloaded all your information, data, photos, web browsing history to my servers.

I have access to all your messengers, social networks, emails, chat history and contacts list.

My virus continuously refreshes the signatures (it is driver-based), and hence remains invisible for antivirus software.

Likewise, I guess by now you understand why I have stayed undetected until this letter…

While gathering information about you, I have discovered that you are a big fan of adult websites.

You really love visiting porn websites and watching exciting videos, while enduring an enormous amount of pleasure.

Well, I have managed to record a number of your dirty scenes and montaged a few videos…

If you have doubts, I can make a few clicks of my mouse and all your videos will be shared to your friends, colleagues and relatives.

I have also no issue at all to make them available for public access.

I guess, you really don't want that to happen, considering the specificity of the videos you like to watch, (you perfectly know what I mean) it will cause a true catastrophe for you.

Let's settle it this way:

You transfer $950 USD to me (in bitcoin equivalent according to the exchange rate at the moment of funds transfer), and once the transfer is received, I will delete all this dirty stuff right away.

After that we will forget about each other. I also promise to deactivate and delete all the harmful software from your devices. Trust me, I keep my word.

This is a fair deal and the price is quite low, considering that I have been checking out your profile and traffic for some time by now.

In case, if you don't know how to purchase and transfer the bitcoins - you can use any modern search engine.

Here is my bitcoin wallet: (Bitcoin wallet deleted)

You have less than 48 hours from the moment you opened this email (precisely 2 days).

Things you need to avoid from doing:

*Do not reply me (I have created this email inside your inbox and generated the return address).
*Do not try to contact police and other security services. In addition, forget about telling this to you friends. If I discover that (as you can see, it is really not so hard, considering that I control all your systems) - your video will be shared to public right away.
*Don't try to find me – it is absolutely pointless. All the cryptocurrency transactions are anonymous.

*Don't try to reinstall the OS on your devices or throw them away. It is pointless as well, since all the videos have already been saved at remote servers.

Things you don't need to worry about:

- That I won't be able to receive your funds transfer.
- Don't worry, I will see it right away, once you complete the transfer, since I continuously track all your activities (my trojan virus has got a remote-control feature, something like TeamViewer).
- That I will share your videos anyway after you complete the funds transfer.
- Trust me, I have no point to continue creating troubles in your life. If I really wanted that, I would do it long time ago!

Everything will be done in a fair manner!
One more thing... Don't get caught in similar kind of situations anymore in future!

My advice - keep changing all your passwords on a frequent basis

---

So there you have it. Obviously, I'm not about to pay a ransom. And my files have not been locked.

Hucksters are sending out these emails worldwide, hoping someone will be terrified and meet their demands. It makes the Nigerian email scams and pleas for help via email (please send money now – John or Mary has been hurt while visiting London or Paris or Sydney or Madrid or…) seem rather tame, doesn't it?