Interface

Lorain County Computer Users Group
LCCUG.com (or) info@LCCUG.com
Volume 33 Number 3 March 2022

2022

Inside This Issue

Tuesday
March 8, 2022

The Pros and Cons of BACKUPS

Recording by

Ron Brown

Tech Savvy Senior

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!

A Word From Our President

ZOOM meetings are back for the near future! No in person meeting option.

If you aren't comfortable using this online tool, please let me know and I'll do a session with you and show you how easy it is!

Our February meeting was a ZOOM program on preserving your digital photos- link to this recording is at

Preserving Digital Photos
https://www.youtube.com/watch?v=O8ujuA9pjr8
(Thanks to Mark Schulman, Member, Central Florida Computer Society for the nice recording)

The March 8 meeting will be:

Should you back up your hard drive in 2022? Recording by Ron Brown.

We have heard over and over again that we should back up – backup backup! Ron Brown gives the position that maybe that's not the case anymore.

We will also look at the Weekly online program, "Tech for Seniors". This is something I like to sign onto every Monday or watch the recording of the show afterwards on Youtube. I think our members would enjoy learning about this.

As time allows, we'll chat among ourselves like we did last time for those who want to stay. Come and enjoy!

Reminder – we are having a membership sale!!

Pay $15 and you will be a paid member for 3 years. What a deal!

Send your membership to:
LCCUG
PO Box 792
Amherst, OH 44001

Sandra Ruth
LCCUG President

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

Interesting Internet Finds

December 2021

By Steve Costello

scostello@sefcug.com

How To Disable The Smart Compose Feature In Gmail
https://techviral.net/disable-smart-compose-gmail/

I keep the Smart Compose feature turned off because I distrust the AI figuring out what I want to say. So if you have not turned this feature off in your Gmail, I suggest you do it now.

Is Charging Your Phone Overnight A Bad Idea?
https://www.online-tech-tips.com/smartphones/is-charging-your-phone-overnight-a-bad-idea/

This question pops up from time to time. The people at Online Tech Tips answer this and some other questions regarding battery charging.

Tuesday
March 8, 2022

The Pros and Cons of BACKUPS

Presented By

Ron Brown

Tech Savvy Senior

We have heard over and over again that we should back up – backup - backup! Ron Brown gives the position that maybe that's not the case anymore.

We will also look at the Weekly online program, "Tech for Seniors". This is something nice to sign onto every Monday or watch the recording of the show afterwards on YouTube. We believe our members would enjoy learning about this.

zoom

PLEASE NOTE:
THIS WILL BE A ZOOM ONLY MEETING

Woohoo!

Your renewal dues have been changed from $15.00, To 3 years for $15.00. When everyone else is raising their prices our Computer Club is lowering their dues, so tell your friends to come and Join in the fun and learn computer information.

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

FEBRUARY 1, 2022

The board Zoom video meeting for February was attended by Sandee Ruth, Don Hall, Micky Knickman, Pam Rihel and Richard Barnett.

Neil is recovering from an illness and Dennis is on hiatus.
Micky will not be available for February, March and April meetings. The Problem Solving workshops could be held on Thursdays in place of Tuesdays for those months if there is interest.
Preserving Digital Photos will be the program next week.

Micky moved, Don seconded meeting be adjourned.

General Meeting Minutes

FEBRUARY 8, 2022

President Sandee Ruth called the Zoom video meeting to order. A motion to accept the minutes as shown in the February issue of the *INTERFACE* was made by Bill Schubmehl seconded Pam Rihel. Motion passed .

Sandee announced next months program will be Backing Up Your Computer.

Mark Schulman presented his video "Preserving Digital Photos".
His program told of the limited life of the many backup systems: thumb drives, CDs, DVDs and electronic hard drives. He suggested gold DVDs and spinning hard drives for the longest life.
He recommended not writing on CDs and DVDs to prolong their life.

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, Joel Ewing, Kurt Jefferson, David Kretchmar, Scambusters, Ask Leo, APCUG, Google images, Microsoft Office art online, https://computercpr.com/computer-facts/

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 - Geeks on Tour: Hodgepodge of Tech Tips, with emphasis on Google Lens

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.

https://computercpr.com/computer-facts/

Interesting Computer Facts

Here's a list of the top 20 computer facts you might not know:

- The First Computer Weighed More Than 27 Tons. ...
- About 90% of the World's Currency Only Exists on Computers. ...
- The First Computer Mouse was Made of Wood. ...
- About 70% of Virus Engineers Work for Organized Crime Syndicates. ...
- The First Known Computer Programmer was a Woman.

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- March 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 - March 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. Attendees MUST make an appointment by emailing **troubleshooting@lccug.com**. or else the workshop will be cancelled.

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.

Cautionary Tale about Free VPNs

By Joel Ewing, President, Bella Vista Computer Club
April 2021 issue, *Bits & Bytes*
www.bvcomputerclub.org mail-to:president@bvcomputer.org

One of the caveats in the VPN article in the March 2021 *Bits & Bytes*, also mentioned at the March General Meeting, was that free VPN services were not recommended. As if on cue, see the following article recently published by Malwarebytes Labs on "21 million free VPN users' data exposed."

A hack of several free VPN services revealed that not only were some services collecting user activity logs in contradiction of their advertised policy, but some were also collecting email addresses, passwords that were not encrypted, IP addresses, mobile device models, and IDs.

The whole point of using a VPN with mobile devices is to avoid exposing non-encrypted data when using a public Wi-Fi network; but if that data would have been non-encrypted on a public Wi-Fi without VPN, then with a VPN service, it is still exposed non-encrypted within the server of your remote VPN service. In addition, if the service also requires a special app to be installed on the mobile device, then that app will also see any non-encrypted data before it is sent to the VPN service and potentially have access to other data on the mobile device. Thus, a free VPN service is much more likely to be tempted to exploit their access to non-encrypted data if that is their only way to profit from the free service.

One of the reasons for distrusting the security of a public Wi-Fi network is that you can never know whether or not it is supported by secure hardware or whether that hardware is configured correctly to at least make it as secure as possible. Because of the limited number of users on one Wi-Fi network, the motivation to expend much effort to hack that one network is not high. But, if it shares an exposure common to many other Wi-Fi networks using similar hardware, it could be at risk. Furthermore, the users have no way of knowing the details of a particular public Wi-Fi node, so it is wise to err on the side of caution. A VPN service, on the other hand, may have hundreds of thousands of users.

The possibility that a free VPN service may be engaging in questionable behavior and be holding sensitive user data on its servers makes it an extremely attractive target for hackers and data thieves, who can justify spending much time and effort to break in. That makes any collection of sensitive information by a VPN service a more serious concern. One of the suggestions made is that you should look for reviews of a VPN service by known and trusted organizations before deciding on a VPN service. One of the interesting things that this data leak revealed was that there were several differently-named free VPN services that all appear to be run by the same company. These were all supported by mobile apps that were gathering inappropriate data, combined with the attempt to disguise the company's true identity, suggest that this was a deliberate attempt to engage in unethical behavior.

Caveat Utilitor

Genealogy Tip of the Day

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

Disbanded Churches

michaeljohnneill, 04 Feb 10:51 AM

If your ancestor's church disbanded, there are several places the records might have gone:

- the local dump

- the family of the last minister

- a local church of the same denomination

- a regional or national church organization, synod, assembly, diocese, etc.

Contact local historical or genealogical societies, local churches of the same denomination, and regional and national archives (or governing bodies) of the denomination and see if they know what might have happened to the records.

ScamBusters.org

HOW TO SPOT AND STOP A SCAM TEXT MESSAGE

Text messages are a fantastic way to communicate quickly both for business and personal use.

But because they're so popular, crooks are using the short messaging service (SMS) to perpetrate fraud and other scams.

Text messages are rapidly replacing phone calls and emails as the preferred method of brief communication (called a short messaging service or SMS) for many of us -- making it a favorite target for scammers.

Latest available statistics show that Americans lost about $86 million through text-based frauds during 2020. Add to that the frustrations of billions of spam texts sent to our mobile devices every year.
Scammers particularly like them because texts seem to call for an urgent response -- before you have time to think them through.

Many of the SMS tricks are variations of those we're used to in emails or by phone but getting them via texts can catch us unawares.

Let's take a closer look at the five most common text scams:

Smishing: This is phishing via SMS, and it encompasses some of the scams outlined below. Phishing or smishing is an attempt to try to steal personal information from you -- for identity theft or simply to get crooks' hands on your money.

Usually, the message says that one of your accounts at a retailer or bank needs to be updated or reactivated. It includes a link, which takes victims to a fake sign-on page where names and passwords are stolen.
A smishing message might also say you've won a prize or some kind of award or notify you about a supposed package delivery. Or it might offer you a free trial (with a hidden recurring charge).

Don't click on links, phone numbers, or enter website details in the message no matter how believable.

Friend/Relative in Distress: This is a variation of the phone trick sometimes known as the grandparent scam. You receive a text seeming to come from someone you know, saying they're in trouble and asking for money to be wired to them.

This particular scam is hot on WhatsApp right now. It has the advantage over phone calls of crooks not having to impersonate the voice of the individual they're pretending to be. Usually, the trickster will also say they have a new number to avoid arousing suspicion or they may have hacked into the supposed caller's phone

And because victims have no reason to believe a con artist has their number, it's easy to fall for the trick.

But often, as with distress phone calls, the scammer doesn't know the name of the person they're impersonating so their identity is not shown on the incoming text and they use vague phrases like "Hi mom, it's your favorite son."

And even if they do know who they're pretending to be, you can avoid this scam by either asking them a question that only the real person would know the answer to or simply contacting the real person and checking if it's them.

Hack Attack: Sometimes, both for the above scam or simply to get access to a person's phone account, the fraudsters use a clever verification scam.

Victims get a genuine message from WhatsApp with a code that they would normally have (but haven't) requested. Then they get a message from an imposter, posing as a friend saying they accidentally sent their own code to them and asking for it.

They must already have your phone number, since they contacted you. Now they also have a verification code (used for two factor authentication), so they're all set to access your account.

The bottom line on this scam is that you should never share a verification code from any

(Continued on page 9)

(Continued from page 8) How to Spot & Stop A Scam Text Message

source with someone else, even if you think it's someone you know.

Bank/Card Security: This is a widespread smishing scam using a message that pretends to come from your bank or credit card company. It usually says either your account has been compromised, your card has been deactivated, or there's some other problem with it.

You're asked to phone a 1-800 or other number where you'll be asked to confirm your account details, your PIN, or even the three-digit security code on the back of a card. The crook may even request your online password.

Just don't do it. Financial organizations don't operate this way. But even if you think the alert is real, contact them using their listed phone number or the number on the back of a card.

Spam: You're very lucky, you may even be unique, if you've never received an unsolicited text message offering you some kind of deal or requesting certain actions.

Millions of these spam messages are sent out every day at random and using fast-dialing computer systems or networks of compromised machines (botnets).

In fact, many of the scams like those mentioned previously are spammed, that is, transmitted in their hundreds or thousands.

A common trick is to pretend to be a package delivery service like UPS or FedEx or an online retailer like Amazon alerting you to a shipment code. But if you click on the included links, you'll be taken to a fake webpage where you'll be asked for sign-on or other confidential information.

The avoiding action here is to never click on links in unsolicited texts. Go straight to the real source instead and check there. Also consider using a spam-blocking app on your phone.

FINALLY…

Always be skeptical of any text that asks you to take action by clicking a link, phoning a number, visiting a website using an address given in the text, or by emailing. And never rush to action without thinking things through.

Even be wary of keying in the word "STOP" to try to halt unsolicited messages from a particular source. It tells the scammer they've got a hit.

And don't believe that the name or number shown on the incoming text is real. Scammers can spoof or disguise them.

While there's no doubt that text messages are a highly convenient method of communicating, the system is wide open to scammers. Always be on your guard.

THIS WEEK'S SCAM ALERTS

Microsoft warning: The tech giant is warning of new attempts to install malicious software on computers using the firm's Office 365 suite. Victims receive an email seeming to come from Microsoft with an app attachment labeled "Upgrade." Installing this enables crooks to read and write emails in a victim's name as well as the ability to read other files. Microsoft doesn't send notifications like this, so don't install.

How Do I Block Someone from Using My Wi-Fi? The best approach.

by Leo A. Notenboom

Most Wi-Fi access points and routers easily let you block someone from using your Wi-Fi. I'll cover the simple steps.

If I have a Wi-Fi user blocked from using my Wi-Fi, how is it possible that they are still able to be active on my Wi-Fi?

If they're active, you haven't blocked them. Without knowing exactly what steps you took to try to block them, all I can say is those steps didn't work.

(Continued on page 10)

(Continued from page 9) How Do I Block Someone Using My Wi-Fi

Let's look at what you need to do to protect your Wi-Fi connection(s) from abuse.

Blocking Wi-Fi access
The best way to block unauthorized Wi-Fi access is to ensure your Wi-Fi is password-protected and that any open or guest networks are disabled. Then only give the password to those allowed to use the connection.

A caveat about your router
Your router is not my router, and all routers are different.

What that means is that I don't have step-by-step instructions to share with you because whatever I pulled together probably wouldn't work for you and your specific router or access point.

Locate the instructions for your specific equipment to implement the steps below. Fortunately, none of this is esoteric, and most routers and access points make these changes fairly easy.

1. Use a password
The single most important thing you can do is make sure your Wi-Fi access point is configured to use WPA2 (or WPA3) security. Among other things, that means you'll assign it a password or network key. Only individuals who know the key can then access your Wi-Fi.

Give that password to anyone you want to allow to connect, and don't give it to anyone else. It's that simple.

Unfortunately, it's also not that difficult for the password to "leak".

For example, anyone with physical access to your Wi-Fi-enabled machine may be able to view the Wi-Fi password used to connect. If you're in a situation where someone is motivated to do so, then you'll want to ensure that your machines are properly secured as well.

2. Disable guest or open Wi-Fi
Many routers and access points now provide two separate Wi-Fi connections:

- The "normal" connection you use and secure with your WPA2 password.
- An "open" Wi-Fi connection that could be used by your guests without a password.

The two are isolated from each other so your guests can't access your equipment or spread malware to your machines.

But they would still be using your Wi-Fi and your internet connection.

Open hotspots like this are easy to find, and anyone within range could connect and start using — or abusing — your network. The only real solution is to turn this feature off completely.

3. A word about MAC address filtering
One of the common responses I get on this topic is to enable MAC address filtering.

Each computer's network connection, including Wi-Fi, has a theoretically unique MAC address. By configuring your access point to allow connections from only certain MAC addresses, you can, theoretically, exclude everyone else.
Theoretically.

The problem is twofold:

- MAC addresses are not necessarily unique, and can even be changed to specific values in software.
- The MAC address is transmitted in the clear.

A motivated individual need only listen in to a Wi-Fi connection already established with your access point, make note of the MAC address being allowed through, and then change their computer's MAC address to be one of those allowed.

In practice, it's a fine approach, mostly because motivated individuals with the knowledge to perform those steps are not common. But it's important to realize that it could happen.

Do this
If you truly want to prevent unauthorized use of your Wi-Fi, I recommend you:

- Set up WPA2 or WPA3 on your Wi-Fi.
- Disable any open or guest network.
- Secure all computers using that Wi-Fi to prevent the password from being exposed.

It's Called Clickbait, and You Need to Learn to Avoid It

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

I was eating yogurt as I was reading stories about one growing danger on the Web: Clickbait. What I read made me pause and put down my spoon.

It turns out that plenty of us are clicking on email links or Facebook postings sent to us from unknown senders. Unfortunately, this can lead to malware and Trojan horses infecting your computer.

The practice is called clickbait. Someone you don't know sends you an email or a Facebook posting. It contains a link. You click on it.

Catchy and provocative headlines are usually a dead giveaway that you're being targeted by clickbait.

Clickbait often contains these qualities:

- Headlines that appeal to your strong emotions, such as humor or outrage
- Headlines designed to grab your attention, leaving you wanting more information
- Headlines that tell you nothing about the content of the article
- The headline is too good to be true
- Content that encourages you to share the item with someone else on Facebook
- Funny images or video

Examples of clickbait headlines include:

87–Year–Old Trainer Shares Secrets to Losing Weight

When You Read These Shocking Food Facts, You'll Never Want to Eat Again

Stop Eating Chicken Breasts Immediately

Here's the scary part. A study of 7,804 students by the Stamford Historian Education Group revealed that more than 80 percent of middle school students believed an ad was an actual news story. This, despite the fact the ad was clearly marked with the words, "sponsored content."

The point is to teach people to recognize clickbait and to avoid it. It's not worth your time.

Free IQ tests and credit score checks often ask you to fill in personal information. Unfortunately, you don't know that the website collects your personal details to build a profile on you. Once you submit this information, you'll be subjected to scams and even more links to dangerous websites.

Clickbait links open the door to more spam and potential malware, adware, spyware, viruses, worms, trojan horses, and the real possibility that someone could take over control of your computer. Just say no by refusing to click on links you aren't sure about.

Genealogy Tip of the Day

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

Scan the Whole Thing First

michaeljohnneill, 05 Feb 11:09 AM

This post is not about digitally scanning documents. This one is about actually using your eyeballs.

I first worked on my children's Belgian ancestors years ago. When using the vital records from the 19th century, I used them the way I had other European records from the same time span. I looked in the "book" for and read through the entries for the years I thought included the person's birth date. Then, if I had the correct person and had the names of the parents, I scanned the years before and after the birth to locate siblings.

Imagine my surprise when I found indexes interspersed in the records. I had never encountered those before. While indexes are not perfect, they would have saved me a great deal of time.

The first time you use any "new" record, familiarize yourself with the whole thing first, don't assume that it is like every other one you have ever used.

The DealDash (Penny Auction) Scam

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

If you watch much TV or surf the internet, you've seen ads promising products as much as 95 percent off retail at DealDash.com or other penny auction sites. DealDash advertises itself as offering fair and honest auctions, but is it really? Millions of people have signed up for a chance to buy items at penny auctions at a fraction of the retail price. Who wouldn't want to buy a new iPad for $30? But think about it; who would want to sell that iPad for $30 when it cost several hundred dollars wholesale? It is worth noting that the "penny" in penny auctions refers to the bid increments, but your actual cost could be many dollars.

Consumers are buying more items online every year and appreciate the convenience, selection, and often substantial cost savings. So, these penny auctions would appear to be an extension of that money-saving online buying concept.

Most consumers are familiar with online auctions at sites such as eBay, where interested individuals bid up the price of an item until time expires. The high bidder at the end of the auction wins the item at the winning bid price.

However, another form of online auctions, internet penny auctions, has expanded in recent years. While some of these sites are *technically* legitimate, many of their business practices are questionable, and most consumers would be better off avoiding them altogether.

How penny auctions work

In some ways, online penny auctions are internet bidding sites that share some similarities with legitimate auction sites like eBay. However, the BIG difference is that consumers who bid on penny auctions must pay for each bid they make regardless of whether they win or lose the auction.

Generally, anyone interested in bidding in a penny auction must pay a registration fee before gaining access to bidding. While not required by all penny auction websites, this fee is often described and charged in what many consider an underhanded way. For example, it is typical for a consumer to make a query regarding online penny auctions. If the consumer provides credit card information, that credit card is immediately charged $60 - $99 as part of the registration process. Often consumers provide credit card information without realizing they are authorizing any payment.

An Auction Example

(Continued on page 13)

Continued from page 12) A Deal Dash (Penny Auction) Scam

As stated above, the penny auctions' business model immediately charges anyone furnishing them a credit card number of at least $60, which buys 100 bids.

Most new bidders bid on one or two auctions, lose their 100 bids ($60), and quickly realize getting a bargain wasn't as easy as it looked. These sites count on the addictive nature of *almost* winning an auction, maybe losing by a penny or two, to encourage a percentage of bidders to buy more bids. Sometimes a substantial discount is offered - i.e., if you sign up right now, you can get 200 bids for the same $60.

Penny auctions usually allow losing bidders to apply at least part of the money spent on bidding towards buying the product at *their* retail price. However, penny auction sites, including DealDash, often substantially overstate the retail price of items, so buyers are usually either overpaying or perhaps getting completely ripped off.

How the Auction Works

The bidding for an item typically begins at $0 and then increases by one cent each time someone bids. There is a countdown clock that restarts every time someone places a new bid. Some websites even allow users to set up automatic rebids if they are outbid. The total price of the item "won" is determined by the number of bids, so you could end up paying well over the retail value of the item you're bidding on. Generally, you have also lost the money spent on the used bids if you lose the bid.

Let's say the auction is for a new computer with a stated retail value of $599. The bidding starts at $0, increases in 1 cent increments, and one "lucky" bidder "wins" the computer for $30. The winning bidder is given credit for the bids he has "spent" at $0.60 each. It is not unusual to see individuals bidding hundreds of times, so if the winner in this example bid 300 times, that winner paid $180 for their 300 bids, if each bid cost $0.60. Still, this does not seem like a bad deal for the winner; $180 for a $599 computer, even if it is a system you could get on Amazon for $399.

If a penny auction item sells for $180, the auction site has received 18000 incremental 1 cent bids, which cost the bidders as much as $10,800! Penny auction sites often promote themselves as "social media" buying and stress the social nature of their sites. What they don't advertise is how addicting these sites can be. $10 gift cards can go for over $20 when bidders' egos apparently overrule all common sense. And I can virtually guarantee that YOU will not get that computer for $180.

An individual cannot determine which penny auction sites are "legitimate." Some state attorney generals have found that some penny auction websites use "shills" that automatically outbid people, making it virtually impossible to win items at a reasonable price. Some of these shills are software programs that show a fake username to persuade consumers that they are bidding against a real person. As a result, several penny auction sites have disappeared, never shipping items won. Other sites have sold financial information about users or put additional charges on credit cards without permission.

Conclusion and Recommendation: Avoid Penny Auctions

While online penny auctions may sound like an attractive deal at first, consumers should be very wary before handing over any money or credit card information. It is doubtful that consumers will save any money by using the service to purchase goods, and much more probable they will be ripped off.