# THE COMPUTER CONNECTION
## SAUK COMPUTER USER GROUP

MARCH 2024

VOLUME THIRTY -FIVE
NUMBER THREE


INSIDE THIS ISSUE:




**Club Information**

Sauk Computer User Group
PO Box 215
Sterling, IL 61081-0215

Neal Shipley - President
topgun05@gmail.com

*Website* www.sauk.apcug.org

SCUG Email

saukcomputerusergroup@gmail.com

Editor and Printing done by:

Joe Fornero

j4nero@thewisp.net


Member of apcug
An International Association of Technology & Computer User Groups

**Feb. Minutes**
**2/21/2024**

**Open Meeting:** Neal

**Question and answers:** 1) ComEd changing customer account number; 2) Ipass to change from transponder to stickers; 3) CCleaner free version- you may need to occasionally let them know you want to stay on free software.

**Treasurer's report:** Presented by Joe1 and approved by Joe2, 2nd by Glenda.

**Old business: None.**

**New business:** 1) Officer nomination and election- motion made and seconded to let them stand as they are; 2) Web browser (Amazon Silk) can be accessed on non-smart TV with Firestick.

**Adjournment:** Motion made by Joe1.

**Program**: By Joe1-Editing Videos With Free Software:

PatchMyPc.com to download a home updater for any software listed.

4kvideo- video downloader.

NCH- use to edit video.

**Next month's program:** Robert from PCtech2U- smart TV's, password storage and management.

*Respectfully submitted by Tom Rich*

## BOARD MEETING MINUTES FOR FEBRUARY 21, 2024

**Meeting was called to order by:** Neal

**Attending the meeting were:** Joe1, Joe2, George, Gloria, Neal, Tom, Nancy, Diane, and Glenda.

**Treasurer's report was presented by:** Joe1 and approved.

**Discussion Highlights:** 1) Neal requests suggestions for future programs, i.e. MS Office programs or things to do with Windows; 2) How Icloud works, down loading and up loading; 3) Love On A Leash details- renewal cost; 4) New items for drawings from donations.

**Future Programs:** Robert from PCTech2U will be here to give program on password management and smart TV's. Also may do questions and answers.

**Adjournment:** Motion by Nancy, Gloria 2nd.

*Respectfully submitted,*

*Nancy Rich*

## Joke

Where did the computer mouse go to get a drink?

The spacebar

And you know I've been to a couple spacebars before, they're all exactly the same. Great food, no atmosphere.

### New Computer Viruses

The George Bush Virus - Causes your computer to keep looking for viruses of mass destruction.

The John Kerry Virus - Stores data on both sides of the disk and causes little purple hearts to appear on screen.

The Clinton Virus - Gives you a permanent Hard Drive with NO memory.

The Al Gore Virus - Causes your computer to just keep counting and re-counting.

The Bob Dole Virus - Makes a new hard drive out of an old floppy.

The Lewinsky Virus - Sucks all the memory out of your computer, then e-mails everyone about what it did.

The Arnold Schwarzenegger Virus - Terminates some files, then leaves, but will be back.

The Mike Tyson Virus - Quits after two bytes.

The Oprah Winfrey Virus - Your 200 GB hard drive shrinks to 100 GB, then slowly expands to re-stabilize around 300 GB.

The Ellen Degeneres Virus - Disks can no longer be inserted.

The Prozac Virus - Totally screws up your RAM, but your processor doesn't care.

The Michael Jackson Virus - Only attacks minor files

The Lorena Bobbitt Virus - Reformats your hard drive into a 3.5 inch floppy ... then discards it through Windows.

# Do You Know the Preferred Tool of Online Criminals?

**By Bob Rankin**

It's been 45 years since the first spam email was sent, and it's still the favorite tool of crooks and criminals online. A report from security group F-Secure says that spam is the most common method used to distribute malware, phishing attacks, malicious URLs, and scams. Read on to learn the tell-tale indicators of malicious emails, and the true origin of spam...

## Spam: Still Number One With Crooks

You've got software to protect your computer from viruses, spyware, ransomware, and rogue websites. You're careful to keep all your software up to date. Your identity theft spider sense tingles with every suspicious phone call. But then that innocent-looking email pops into your inbox. It appears to be from your friend, your bank, or your favorite online store.

I got one recently that said "A user has just logged into your Facebook account from a Samsung S10 device. We are sending you this email to verify that it is you. Thank you, Facebook Team." It looks very much like the actual account warnings that Facebook does send out. The subject line says "Please respond immediately."

So you click, and you've been had. Because of the sense of urgency created by this message, one might ignore the fact that it was sent from "ebxjwwptsoqwvbbqjivcqpoduuxdur.com.au" (clearly not Facebook HQ) and that there were 50-odd sketchy addresses in the Reply-to header.

Spam is still the most effective attack vector for hackers and online criminals, according to research from F-Secure. They reported that phishing, spam, and other email threats were the source of 51% of all attempted malware infections. Hopefully you were not in the 51% Club.

Cybercriminals capitalized on fear and confusion during the Covid-19 pandemic, and continue to use malicious email attachments containing infostealers – malware that steals passwords and other sensitive information. Facebook, Chase Bank, Microsoft, PayPal, and Bank of America were the most frequently spoofed brands. As usual, cybercriminals are taking their cue

## Do You Know the Preferred Tool of Online Criminals? (cont.)

from water -- by traveling along the path of least resistance.

Here are some of my tips for staying safe from phishing attacks. First, see my article How Hackable is Your Password? to learn how to **maintain strong, unique passwords** for all accounts and change them regularly.

**Enable two-factor authentication** wherever possible. See [DIGITAL LOCKDOWN] Authenticator Apps Protect Your Accounts. And **keep your software and systems up to date** by following my advice in Keep Your Software Updated (or else...).

F-Secure says these phishing campaigns are effective because users are already accustomed to receiving notifications... failure of delivery emails, alerts for hitting storage limits, requests for reactivation, or package delivery notifications, and 'update your password' emails.

Keep in mind that spam and phishing can take the form of text messages as well as email. I wrote about bogus "account services" and package delivery scams in [SCAM ALERT] Smishing is Getting Worse (what you need to know and do).

As software vulnerabilities are closed and anti-malware suites grow more capable, spam becomes relatively more effective compared to hacking and exploitation of software vulnerabilities. Spam still is infinitely scalable, too; it costs nearly nothing to blast out millions of spam emails from a compromised machine, and spambot networks of thousands of slave machines are commonplace.

While success still depends on spewing out millions of spam emails to get a handful of "bites," spammers are constantly refining their techniques and improving their batting averages.

**Why Do People Click?**

According to F-Secure, here are some clues as to what makes phishing spam successful:

- The probability of a recipient opening an email increases 12% if the email claims to come from a known individual
- Having a subject line free from errors improves spam's success rate by 4.5%

## Do You Know the Preferred Tool of Online Criminals?

(cont.)

A phishing email that explicitly states in its call to action that it is very urgent gets less traction than when the urgency is implied

Most users have finally learned not to click on email attachments sent by strangers, or any attachment that comes unexpectedly. So more phishing emails include URLs instead; people are still conditioned to click on links to see where they go, especially if the link says “click on this link...”
The link often does not lead directly to a malicious site, but to an innocuous site that redirects traffic to a malicious site. That way, the bad guy avoids detection by automated analysis software that previews links and compares them to known malicious URLs. Here are some of the most common phishing tactics:

- The Fake Tech Support scam: An email arrives with a warning that your computer has been compromised with malware, and directs you to click a Norton or McAfee link to scan your computer, or call a bogus Microsoft Tech Support phone number.
- The Suspicious Activity scam: An email claiming to be from your bank says there is suspicious or unusual activity on your account. It may ask you to respond with your username and password.
- The HR/IT scam: You get an email that appears to be from your employer's Human Resources or IT department. You may be directed to update employee information, or download an app.
- The UPS/FedEx/ USPS scam: An email or text advises you that a package cannot be delivered due to incorrect shipping information. You are urgently advised to click a link or your package will be returned or discarded.
The Amazon/Apple scam: A message informs you that you've ordered some expensive item from either Amazon or Apple, and asks you to login and confirm the purchase.

In every case, a careful examination of the sending address, or a phone call to verify the sender will reveal that it's unwise to continue. Never trust the phone number or email address provided in the message.

## Do You Know the Preferred Tool of Online Criminals?
(cont.)

Another technique I've seen lately is a quick email asking "Sorry to bother you, do you order from Amazon n?" If you engage with this scammer, he or she will spin a tale of how they had a problem buying an Amazon gift card for a sick friend's birthday, and ask if you would kindly do so, with a promise that you'll be reimbursed. I can't imagine who would fall for that obvious scam, but apparently there really is a sucker born every minute.

**A BIT OF HISTORY:** I mentioned in the opening of this article that the first spam message was sent over 45 years ago. That happened in May 1978 when a marketing executive for Digital Equipment Corporation sent an unsolicited email to 397 ARPAnet addresses, with an invitation to a product demonstration. The term "spam" was not applied to unsolicited messages until April 1993, and according to Wikipedia, is thought to derive from a Monty Python comedy sketch "in which a group of Vikings sing SPAM, SPAM, SPAM... at increasing volumes." It was adopted to refer to "unsolicited commercial electronic mail sent to a large number of addresses, in what was seen as drowning out normal communication on the internet." So now you know.

F-secure includes tips for security-conscious people in its security blog. Some recent topics include ransomware, stalkerware, and account takeover. F-Secure predicts that the use of phishing tactics as a lure, using office documents as an infection vector, and the use of cloud services to host malicious content, will likely continue.

The good news is that with education and software, we have eliminated or limited many malware attack options to spam. The bad news is that spam still works. My best advice: Think twice before you click.

From the website of Bob Rankin,

https://askbobrankin.com/

do_you_know_the_preferred_tool_of_online_criminals.html.

# Learning Technology Today
## By Jim Cerny

In the ancient computer days, ten or so years ago, learning technology was very different than it is today. Before the dreaded COVID days of isolation, classroom settings were very popular for learning technology. Classrooms had individual computers, and the subjects were on general and basic topics everyone needed to learn. Most people then purchased their own computers for the first time and needed to know how to use them. Do you remember having to learn how to use a mouse? How about changing the size of a window on your screen or searching the Internet? In those days, these things were new to most people.

Now technology training (not just "computer classes") has dramatically changed. The big jump off the cliff into something new in learning was the massive changes that COVID brought about. You know the story – training went to online classes, and in-person meetings were all but eliminated. Now that the COVID epidemic is over, have we returned to "normal" learning? I think not. Many of these changes will remain with us. So how do we adapt, and what do the "tech learning classes" look like today and in the future?

I advise searching the Internet for the specific training you want or need. Here's why:
1. More and more everyday devices will use more and more technology – refrigerators, cars, TVs, doorbells, and toilets. Can you imagine attending a class on how to use your refrigerator? No, I can't either, no matter how cool it would be! If there was a class, how many attending would have the same refrigerator with the same controls or options?
2. There are too many options, and no one uses all of them. I am still learning my car's options and have been driving it for four years! A word-processor app like Word has options I am not even aware of and will probably not use anyway but may be very useful for a few people.
3. Use of multiple devices – cell phones, TV adaptors, tablets, laptops, etc. Now you can get your email,
watch a movie, or do your banking on different devices –each one will have a slightly different way of doing the same thing. Likewise, teaching even the same topic or app can be used differently on other devices.
4. We tend to have specific needs from our technology. Do any of these questions sound familiar? -- "How do I put text on a photo?", "How do I read my email on my cell phone?" or "How do I get the sports channel I want on my TV?". Our needs and wants are now getting much more specific. A class on a specific topic and device would be attended by only a few people wanting that specific knowledge.
5. We don't want to waste time learning things we will probably not use or already know. In any class, people come with different and unequal levels of experience and knowledge.
6. People are used to "convenience learning" when they have time and do not have to travel. Many colleges provide "at home" learning using the Internet.

All this is to say that the Internet is probably the best source for learning a specific task for a particular device. Ask Google, "How do I ..." and be very specific. Enter the name, model, and year of your car, the make and model of your refrigerator, or your phone or tablet. Google loves specificity. Demonstration videos and text instructions will magically appear for you on any topic. It is truly a learning gold mine of knowledge – give it a try!

*Jim Cerny, 1st VP, Education Chair, and Forums Coordinator*
*Sarasota Technology Users Group*
*https://thestug.org/*
*jimcerny123 ** gmail.com*

## Zoom Sessions

**Neal is hosting a weekly evening Zoom; (Each Friday) @ 7:30 PM Central Time**

https://us02web.zoom.us/j/3975898877?pwd=RjF5ZTM3R25qNXhHRjdWRVAzQ1M2Zz09

Meeting ID: 397 589 8877 Passcode: 4ukxAh

Phone users:

Dial by your location +1 312 626 6799 US (Chicago)

Meeting ID: 397 589 8877 Passcode: 936460

*You're welcome to check in and visit, or ask a question, maybe even get an answer.*

**Scanning this QR code should take you to our web page.**

There will be a Question & Answer. Bring any questions you have about your computer or problems you may be having. It will be conducted by:
**Robert**

The next meeting of the Sauk Computer User Group will be

March 9, 2024

Question & Answer : 1 PM

Presentation: 2 PM

Business Meeting : 3 PM

Place: **Whiteside Senior Center**
**1207 West 9th Street**
**Sterling, Illinois 61081**

**ROBERT FROM PCTECH2U WILL BE DOING THE Q&A AND DOING THE PRESENTATION ON SMART TVS AND PASSWORD MANAGEMENT**