Bits & Bytes

Arkansas' Premier Computer Club

May 2025

The Bella Vista Computer Club - John Ruehle Center

Highlands Crossing Center, 1801 Forest Hills Blvd Suite 208 (lower level), Bella Vista, AR 72715

Website: http://BVComputerClub.org **Email: BVCCeditor@bvcomputerclub.org**

MEETINGS

Board Meeting: May 12, 2pm, in John Ruehle Training Center, Highlands Crossing Center.

General Meeting: May 12, 3pm. Program: "A Collection of Short Topics from AskLeo.com".

We will meet in-person in John Ruehle Training Center, Highlands Crossing Center, lower level, 1801 Forest Hills Blvd, Bella Vista, or you may attend the meeting on-line via Zoom. Zoom access information is published on our website.

Visitors or Guests are welcome.

Consider attending by Zoom if you are unable to attend in-person.

HELP CLINICS

May 3, 9am - noon at John Ruehle center
May 21, 9am - noon at John Ruehle center
Members may request Remote Help on our website at https://bvcomputerclub.org at menu path Member Benefits ►Remote Help .

MEMBERSHIP

Single membership is $30; $15 for each additional family member in the same household.

Join on our website at https://bvcomputerclub.org at menu path Get Involved ►Join/Renew, by mailing an application (from the web site) with check, or complete an application and pay in person at any meeting.

CLASSES

(At BVCC Training Center)

"Introduction to GIMP", Thursday, May 14, 1pm-4pm, with Joel Ewing.

"Introduction to MS Excel" in two parts, Tuesday May 20, 1pm-3pm, and May 22, 1pm-3pm, with Joel Ewing.

Advance sign up required for each listed class: For reservations: email to edu@bvcomputerclub.org, or sign up at the General Meeting. Classes are free to Computer Club members.

Check the monthly calendar and announcements for any last minute schedule changes at https://bvcomputerclub.org .

NEW OR RETURNING BVCC MEMBERS

We are pleased to welcome the following new members or members returning as BVCC members after an absence:

Judith Lisenby
Tom O'Neal
Barbara Berner
Shirley Gilbert
Michael Nickles
Diane Standefer
Sue Kenny

LENOVO LAPTOP RAFFLE WINNER

The winner of the April 14 raffle for the Lenovo IdeaPad 5 laptop was Maxine Olson. Maxine is a relatively new BVCC member, having joined in early February 2025.

Our annual raffle is one of our major fundraising activities that helps to keep us solvent. The net proceeds from this year's event was just over $1,118. Our thanks to everyone that participated.

MALWAREBYTES WARNING ON ATTACKS USING ZOOM

In an April alert, Malwarebytes described how attackers are luring victims into participating into a Zoom video call and tricking victims into accepting a "Remote Control" request, allowing the attacker to take over their PC, with the object of installing malware and gaining access to their accounts and assets.

Remote Control is a feature in Zoom that enables a trusted remote person to use the Internet to take over your PC to resolve some problem. That level of access should never be granted to an unknown or un-trusted 3rd party.

In this new scheme, the attacker changes their Zoom screen name to "Zoom" so that the victim sees a notification that says "Zoom is requesting remote control of your system". Someone unfamiliar with the remote control feature of Zoom may approve this request thinking it is some Zoom app requirement for Zoom to continue to work, when in reality they would be giving the remote attacker total control over their PC.

Remote control of your system should never be granted while using Zoom unless you have initiated the Zoom contact and have an independent means to verify the identity of the party at the other end of the Zoom connection, and would trust them sitting at your PC controlling your keyboard and mouse while your back is turned. Keep in mind that a person's Zoom Screen Name is whatever text characters they choose to type -- Zoom makes no attempt to restrict the value or verify that it is a name the actual account holder would be entitled to use.

ANOTHER VARIANT OF THE SEXTORTION EMAIL FRAUD

Because some of our BVCC email accounts are published on our website, they eventually become targets for criminal SPAM. One of the periodic recurring scams that has been around for over a year is known as the Sextortion scam. This is the one that claims some Trojan malware has been installed on your system to track your keystrokes, that they have infiltrated and monitored your PC for months, have compromised your email and contacts, and will publish compromising videos from your webcam and screens of the porn sites you have been watching unless you pay a large amount in Bitcoin. They never provide any evidence of any private data obtained from your PC or email account, because all their claims are false.

They spam the same fraud emails to multiple email account addresses that are in lists accessible to criminals. Those email accounts are most likely known because they have appeared in some context on websites, not because your own PC or email account has been compromised. They send the same fraud emails to email accounts that are only accessed from a computer that doesn't even have a webcam! Their requested method of payment obscures not only their identity but also the identify of any person paying their extortion; so there is no way they could delete all the videos they claim to have on you upon payment of their extortion -- unless no videos actually exist. They are just hoping their random emails will reach a few recipients guilty of the suggested actions, who might be spooked into paying without considering whether their claimed exploit is plausible.

Previous versions of this fraud were sent from different servers around the world and from random forged email addresses. So far this is the only version that has reached our published BVCC email accounts. The newest variant forges your own email as a From address in an attempt to "prove" they have indeed compromised your email account. Forging an email From name is trivial, and even forging a From email address is not that difficult for spammers with the right tools. Actually hacking some specific email account is very difficult by comparison, so it is not a cost-effective attack approach when simple forging of email addresses is an easy alternative.

PRIVATE BROWSING: IS IT ALL IT'S CRACKED UP TO BE?

By Chris Taylor, President
Ottawa PC Users' Group, Ontario, Canada
https://opcug.ca
Published in Ottawa PC News (November 2023)
Editor: brigittelord (at) opcug.ca

For well over 10 years, web browsers have offered ***private browsing***, designed to keep your browsing —well—private.

Google Chrome calls it an ***Incognito window***, Firefox, Opera & Brave call it a ***Private window***, and Microsoft Edge calls it an ***InPrivate window***. The easiest way to get there is to right-click the browser's icon on the taskbar and choose the appropriate ***New…*** item from the pop-up context menu.

When in a private browsing window, browsing history, cookies & site data (such as images and contents of webpages), and information entered in forms are not saved to your computer. Other users on your computer will not be able to see your web browsing activities. When browsing, web servers won't automatically recognize you as a returning user, and you won't be automatically signed into websites.

When you close a private browsing window, the browser discards site data and cookies created during that session. Note that you need to close the private browsing window to remove traces. Until you do, a simple click on the back button will return you to the previous page visited in that window.

Private browsing deactivates extensions. You can enable extensions in private browsing windows if you need them. For example, in Google Chrome, click the kebab menu (⋮) at the top-right of the window. Choose ***Settings***. Find the extension you want to allow in Incognito windows and click ***Details*** under that extension. Toggle on ***Allow in Incognito***.

Private browsing is not a panacea

It does not prevent all tracking. While websites do not have the luxury of using cookies to track you, there are many other means of tracking. For example, a web server can know your operating system, browser version, extensions you have loaded, screen resolution, IP address, and more. These data items can be used to fingerprint and track you.

Private browsing does not prevent ads. It does not prevent malware. It does not hide where you are browsing from your ISP or employer.

As Gizmodo reported in October 2022, ***Even Google's Own Staff Thinks 'Incognito Mode' Isn't All It's Cracked Up to Be*** - https://gizmodo.com/google-incognito-mode-google-chrome-1849648071

Where is private browsing useful?

If you are using a computer at a public kiosk, it will prevent the next person using the computer from easily seeing where and what you browsed.

If you use multiple accounts on a single website, a private browsing window can help you keep things separate.

If you are using another person's computer, it can be helpful in making it less likely you leave traces behind.

Strangely, I have encountered shopping sites that required private browsing for the checkout process to work properly. I guess they didn't want to sell things to me all that badly.

For more information about private browsing, see https://en.wikipedia.org/wiki/Private_browsing.