Bits & Bytes

Arkansas' Premier Computer Club

March 2024

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: editor@bvcomputerclub.org**

MEETINGS

Board Meeting: March 11, 6pm, in John Ruehle Training Center, Highlands Crossing Center.

General Meeting: March 11, 7pm. Program: "Tax Software Review", based on a February 10, 2024 APCUG zoom presentation by Tom Burt. Will will also have the drawing for our computer raffle.

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

March 2, 9am - noon at John Ruehle center
March 20, 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 .

Genealogy SIG: March 15, 1pm-3pm, Training Center

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)

Tuesday, March 12, 9am-11am, "Slow PC? Let's Upgrade or Buy New"", with Pete Opland.

Wednesday, March 27, 9am-11am, "Building a Password Manager Using Excel", with Pete Opland

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:

Doug Bowen	Betty Shearer	Bette Powell
Katy Young	Sue Kenny	Gail Wortz
Wilford Wing	Katy Henkel	Bud Henkel

BVCC MARCH 11, 2024 COMPUTER RAFFLE

Once again BVCC will be raffling of a refurbished and customized computer. This time it's a business-type, high-end workstation computer, a Lenovo P520 30BF. For pictures and detailed specs, see our website at https://bvcomputerclub.org/raffle2024.php . The winner will be drawn at the March 11 General Meeting. It is not necessary to be a member of BVCC or to be present at the General Meeting to win. Home setup support will be provided within Benton County, AR.

Tickets may be obtained for a $10 donation each. For additional information on the computer or for tickets, call or text Woody Ogden at 479-966.9357, Pete Opland at 218-753-2353, or Russ Ogden at 360-789-0139.

If you haven't yet gotten your tickets, they will still be available at the March General Meeting before the drawing.

A mouse and keyboard are included, but not a monitor. For those who do not have an existing monitor, BVCC may also have available an inexpensive used monitor. The computer comes with Microsoft Windows 11 Pro and with Microsoft Office 2021 Pro Plus software.

This is a highly-capable computer that would be excellent for any home use application and even for many gaming applications

---

ADDITIONAL INFO ON SCAMS DIRECTED AT SENIORS

By Joel Ewing, President, Bella Vista Computer Club
Bits & Bytes, March 2024
https://bvcomputerclub.org
president (at) bvcomputerclub.org

There are no doubt many websites with information about the scams and frauds that abound today, but since many of our members are seniors, I was particularly interested in scams directed at the elderly. While searching for something else I found a link to web pages of the US Senate Special Committee on Aging, which contains Resources-> Fraud and Scams Resources at https://www.aging.senate.gov/scam-resources .

On that web page you will find some detailed video accounts of of actual cases in which Artificial Intelligence (AI) has been used by scammers, with accounts told by those who were targets of the scam and from others involved. There are general guidelines on what kind of scams to watch for. Some of the video accounts reveal what red flags were potential indicators of a scam.

Areas in which AI is being used to make scams more believable include phishing attacks (imitating genuine communications), family-emergency scams (using AI voice cloning and deepfake videos to impersonate a family member in distress), and romance scans (using AI to operate fake profiles on dating and social media platforms). Scammers may commonly communicate via emails, phone, or text messages, and social media.

Some generic tips to protect yourself include:

- Do not share sensitive information via phone, email, text, or social media.
- Do not transfer or send money to unknown locations.
- Consider designating a “safe word” for your family that is only shared with family members and close contacts.
- Do not provide any personal or sensitive information to an online chatbot.
- Report potential scams to the authorities and the companies involved.

There are a number of red flags that are common indicators of a potential scam:

- Threats of arrest or legal action against you or a loved one unless you agree to pay money immediately.
- Claims to represent a government agency or a business, when the email addresses and supplied Internet links do not go the the official domain name or website associated with that organization; or if the business or agency contacts you on a social media platform rather than personal email. On contacts by phone, caller ID can be forged, but many spammers don't even bother to forge a caller ID that maps to the claimed agency or use a reasonable area code (I have received calls claiming to be from an agency in Washington DC where the caller ID area code indicated it was on the West coast)
- A request for personal information or payment coming in an unsolicited email, text, or phone call
- Pressure to take immediate action
- Asking for payment by difficult-to-recover methods: gift cards, prepaid debt cards, wire transfers, cryptocurrency, or cash
- Offers to move your money to a "protected" account
- A demand for secrecy
- The communication contains incorrect punctuation, spelling, or unusual wording that suggests the writer is unfamiliar with common English usage.

One of the things I noticed in some of the fake "family emergency" scam examples on the above website is that the scam may begin by using common generic relational names like "mom", "grandson", or "granddad" and doesn't volunteer the actual name of either the person they are trying to contact or the person they are trying to impersonate. It's almost as if they are unsure of their skill and are waiting for you to identify by name a family member you think might be calling, so they know if their impersonation is plausible.

If your family members refer to each other by less common names, that alone may be enough to reveal a family-emergency scam. Sometime within the last year I received a phone call that started out with "Grandpa, this is your grandson". I have multiple grandsons, none of them address me as "grandpa", none of them have ever had occasion to phone me on that particular phone number, and if they did, they wouldn't say they were my grandson because they know I have multiple grandsons. It was pretty obvious the call was not legit, so I asked "Which grandson is this?", and they hung up.

I would suggest watching some of the videos on the www.aging.senate.gov website to get a better understanding of how the scammers can appeal to your emotions and pressure you to act quickly, rather than taking the time

think before acting. If you slow down and take time to think, you are more likely to recognize all the inconsistencies in their fabricated story line.

MOST OF US GET IT WRONG:
NOT JUST TEENAGERS DEPEND UPON THE INTERNET

By Kurt Jefferson, Editor, Central Kentucky Computer Society
https://ckcs.org/
lextown2 (at) gmail.com

70% of seniors are now online and using technology, reports the World Economic Forum in July 2019. When it comes to the Internet, the website claims it's – No Longer Just For the Young.

"Young people may roll their eyes at older people who can't use technology as fast as they do, but it's wrong to say that older Americans can't use technology. Remember, a baby boomer, Tim Berners-Lee, invented the World Wide Web, so why should we be surprised that they continue to create, adapt, and use new technology?" reports the World Economic Forum.

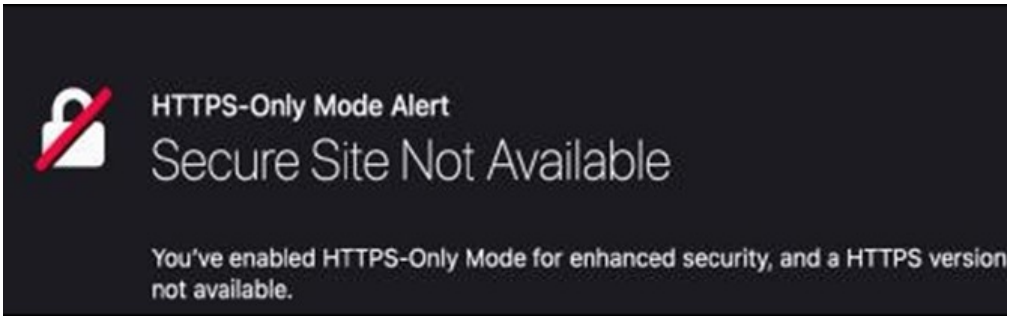
In January 2022, Pew Research revealed its latest technology poll results. It discovered: "When it comes to internet use, virtually all adults ages 18 to 29 now say they use the Internet (99%). A similar share of those 30 to 49 (98%) say the same. And 96% of those 50 to 64 use the Internet, compared with 75% of those 65 and older who report being internet users."

So, if you're over 50 and depend on the Internet, how do you protect yourself against the onslaught of cybercriminals who want your money? Let's start with good advice from Reviews.org.

First off, don't share your information online. I'm amazed at the number of folks who scream to the world on Facebook or Instagram that their baby is due on a specific date. Isn't that an invitation to a burglary? I mean, mom and dad are obviously at the hospital. Who's at home watching the turf? Just don't make major personal announcements on social media. You're visiting New Zealand over the summer? Keep it to yourself. Why in the world would you list your departure and return dates online? Talk about an opportunity for burglars.

Before clicking on a web link, hover your cursor over it. You should see where the link takes you in your browser's status bar. This prevents you from visiting a rogue website disguised as a legitimate one.

Use only secure public websites and a trusted VPN (virtual public network.) Logging onto unsecured Wi-Fi at a motel, restaurant, library, or airport is just crazy. If you must log onto an open wireless network, ensure your VPN is up and running. (I use a VPN even when a Wi-Fi password is required.)



Experts say you should only log onto websites that begin with https:, but this isn't always possible. For example, if I visit a specific school from the home page of the largest school district in central Kentucky, the page won't automatically load on my version of Firefox. I have a Firefox add-on installed called HTTPS Everywhere, which blocks the page and tells me it's not secure.

A button allows me to continue to the http-only site, but the browser add-on is a red flag alerting me to a possible security problem.

There are plenty more basic security tips on the Reviews.org page. Check them out if you want more security suggestions.

Just because you’re over 50 doesn’t mean you have to fall for traps designed to steal your money. Be smart. Be safe. Be vigilant. Scammers are out there, even if you cannot see them.