Bits & Bytes

Arkansas' Premier Computer Club

March 2016

Bella Vista Computer Club - John Ruehle Center

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

Website: www.bvCompClub.org Emailjrc@bvcc.arcoxmail.com

Taxes will be done at Computer Lab

The Board has approved the request to taxes to be done here. *Care Community Center,* Kimberly Porter, will be in charge of the details. She is asking for volunteers and may be reached at **479-903-3217**

Meetings

March 14, 2016

BVCC Board Meeting

5:30 pm

Computer Club Meeting

Community Room at

Highlands Crossing 7 pm

The Bella Vista Computer Club will host Nathan Whisenant, income tax preparer for the AARP/VITA tax service at the 7 pm, March 14 meeting. Information about using the tax service and new tax laws and changes will be discussed. Tax preparation is available at the Computer Club lab on Tuesdays and Thursdays from 10 am to 4 pm, with check in at 8 am. This public meeting is in the Community Room of Highlands Crossing Center (lower level), 1801 Forest Hills Blvd. Bella Vista.

HELP CLINICS

Wednesday, March 2 1-4 pm

Saturday, March 5 9 am -12noon

Wednesday, March 16 9 am-12 noon

Bring your tower, laptop, tablet or smartphone for problem solving.

Classes

Excel March 30 9 am-12 noon

We are in the process of re-vamping our class schedules. Please check frequently on the website for scheduling and re-scheduling.

http://bvcompclub.org/March2016.htm

Be sure to check the class schedules at the meeting and sign-up for the ones you are interested in. There is no charge for classes to Club members.

Genealogy SIG 10 AM John Ruehle Center

3rd Saturday 10-12 am

Is Your Head in The Clouds?

Cloud computing – storing data and using application software "out there" in the cloud of Internet servers – is becoming more and more common. See my related article Eight Free Cloud Services You Should Know About for some examples of popular cloud services. But are they safe? Can you trust some company on the other side of the wire with your business or personal data? Can you depend on software that isn't on your computer to be available when you need it? What are the risks of cloud computing, and how can you mitigate them?

The first risk you run is being cut off from your computing resources by some breakdown in communication between you and them. But that's rather unlikely, really. The Internet was designed to route data around broken communication lines, crashed routers, and other obstacles. Unless you live in a country with a totalitarian form of government, the Internet tends to be self-healing, unlike your desktop computer. So before fuming at your cloud storage provider for going down a whole five minutes, estimate how long it would take you to obtain and install a new hard drive, then restore everything from your local backup. Half a day, at least?

Cloud Storage

Oh, and you DO have a local backup, right? If not, see How I Got Hacked... And Why You MUST Have a Backup! for a cautionary tale, and Hard Drives Are Not Forever to learn more about options for backing up your important files.

Risks of Cloud Storage

Data theft is a second and more serious risk of cloud computing. It's not that cloud-computing providers are sloppy about security. They're more conscientious about it than many large enterprises and most small users. But the bigger the castle, the more barbarians there are at the gates. As more companies deposit their top-secret data in cloud-computing providers' castles, more hackers turn their efforts to breaching those high walls. It's a never-ending battle, but fundamentally no different from you versus a lone hacker -- and most home users are no match for a skilled hacker.

To those who say "I would NEVER put my files out there on some cloud server... they're much safer on my hard drive," I say the following: Does your home have gated perimeter access, 24x7 on-site security guards, and security cameras? Do you have a fire detection and suppression system, backup power generators, and a disaster recovery plan in the event of hurricane, flood or earthquake? Do you have sophisticated network monitoring and intrusion detection software? You can bet your cloud storage provider has all that and more in place to safeguard your data.

Government monitoring and seizure of data is a third issue with cloud computing. The European Union has strict, high standards of privacy protecting citizens against government intrusion into their personal business. Not so in the United States, where the law gives government agents enormous latitude to spy upon and seize personal data, if they can get their hands on it. Did you know that the Electronics Communication Privacy Act passed in 1986 allows law enforcement access to anything you have stored in the cloud for more than 180 days without a warrant?

Another important consideration is death. What happens to your information stored online in the event that you're no longer around? Everyone should have a plan to pass along important login/password credentials in the event they die. In addition to cloud storage, make sure you think about your webmail, online banking and social media accounts.

And it's always possible that your cloud-computing provider will go out of business. But in the event that a popular, reputable cloud storage provider was planning to shut down their service, they whould provide ample notice and opportunity for customers to retrieve their data. In the unlikely event that a cloud provider suddenly goes dark, what happens to your data in that case? My advice is to keep local backups, or use a second cloud-computing provider for redundancy.

What About Encryption?

Popular cloud storage services like Microsoft Onedrive and Google Drive will encrypt files as they travel between your computer and the cloud servers. So you don't have to worry about some hacker or wifi sniffer peeking inside your spreadsheet as it zips along the information highway. Your files are protected by strong physical security measures, but they're not encrypted while they're stored on the Microsoft or Google servers in the cloud. There are good reasons for that, however. If the files were encrypted in the cloud, you couldn't easily view them over a web interface, share them with other users or do collaborative online editing.

If you want to handle the encryption on your own, my article Encrypt Your Hard Drive discusses TrueCrypt and some other options for encrypting your files. This can work well if you want to use a cloud storage option that doesn't offer encryption. See Ten Free Cloud Backup Services to learn how to access over a terabyte of free online storage.

Dropbox does take the extra step of encrypting user files with SSL (Secure Sockets Layer) and AES-256 bit encryption, once they've been stashed on the cloud server. That gives you the assurance that if Evil Hackers were able to break into Dropbox, they wouldn't be able to read your scrambled files. But the caveat is that Dropbox itself has the decryption keys needed to unscramble the files. This quote from the Dropbox security FAQ explains why:

"We do have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so). But that's the rare exception, not the rule. We have strict policy and technical access controls that prohibit employee access. In addition, we employ a number of physical, technical, and heuristic security measures to protect user information from unauthorized access."

If you're uncomfortable about the lack of encryption for files in OneDrive or Google Drive's cloud storage, or you just don't trust the server-side encryption that services like Dropbox offer, you do have another option. With client-side encryption, you can encrypt the files BEFORE they leave your hard drive, and you control the decryption keys. Most cloud backup services such as Mozy, Carbonite and iDrive offer you the option to use a personal encryption key so that your files are encrypted before sending to the offsite cloud backup, and only you can decrypt them.

Cloud computing is definitely here to stay, and its benefits are compelling. You shouldn't avoid cloud storage services because of imagined or falsely inflated fears, but you should be ready to deal with the real risks.

Courtesy of ASK BOB.. Bob Rankin http://askbobrankin.com

You Can't Take It With You…

Sooner or later, we'll all kick the bucket, buy the farm, or shed the mortal coil. But when you go, what will happen to your online accounts? You may not be content to just leave your Gmail or Facebook account dormant. You may have photos or documents in cloud storage. What if you have money in your Paypal account? And will your surviving relatives have the keys to your online banking or investment portfolio?

The simplest solution is to write down all of your accounts and their login credentials, then give that list to someone you trust. Of course, you'll have to remember to constantly update that document when you change passwords or create new accounts. But what if you don't trust anyone with all of your digital keys, at least while you're still alive?

Back in 2012, I found less than a handful of websites offering digital estate planning services. Now, there are dozens of new players; at least, they're new to the Web - many are offered by established estate planning and legal firms. Much like Turbotax and other tax preparation software, digital estate planning sites walk you step-by-step through the complex process, holding your hand along the way.

Digital Estate Planning

Essentially, all of these services help you make decisions and document them; give you secure cloud storage in which to keep your documents; and provide a mechanism for empowering the people you designate to access the documents and other information they need to carry out your wishes.

Everplans was co-founded by Abby Schneiderman, who experienced firsthand the frustrations of wrestling with her deceased brother's digital legacy when he died in a car accident in 2012. Everplans helps people document their wishes about everything from advanced medical care directives to who gets the pets and grandma's apple pie recipe. Everplans can hold your family photos and your obituary. You can provide information that you want family and friends to learn after you die, and specify who gets what information. Everplans charges $75 per year that your account and repository are active.

Will Your Data Outlive You?

FinalRoadmap gives special emphasis to end-of-life care instructions. Its planning protocol gets into details that are often omitted from paper-based advanced care directives and wills, right down to what specific medical interventions you want or don't want, and even who will be permitted in your presence while you're dying. Yes, the questions are uncomfortable, but it's better for you to answer them now than to leave family agonizing over what you would want them to do. FinalRoadMap charges a one-time fee of $249.

Similar services include The Digital Beyond, PlannedDeparture.com, AfterSteps.com and PrincipledHeart.com. Shop around for one that offers the services most important to you, and whose approach makes the most sense.

For do-it-yourselfers, Google offers a free digital estate planning service dubbed Inactive Account Manager. It's intended to deal with your Google assets (email, Drive, Photos, Google+ page, etc.) but you can also leave instructions about anything else in an email that will be sent to your trusted contact(s) if you don't log into your Google account for a specified period of time.

There's also Deadmans Switch which lets you send emails after you die. An email to your executor, for instance, might contain a list of accounts and passwords or a full-blown digital will and testament. The service sends a check-in email to you every so often; you confirm that you're still alive by clicking on a reply link. If you don't reply within 60 days, you are presumed to be dead and your stored emails are sent. The free version supports up to two recipients. For a one-time fee of $20, you get up to 100 recipients and the ability to customize the check-in intervals and reply deadline.

Final Wishes for Your Data

Generally, survivors are left to deal with the corporate policies of multiple online services when someone dies. There is no federal law empowering executors or designated representatives to access a decedent's digital assets. Only 9 States have enacted such laws, and their provisions vary widely.

The Uniform Law Commission, which drafts model legislation that States generally adopt as-is for the sake of uniformity (e. g., the Uniform Commercial Code), approved the Uniform Fiduciary Act in 2014. One of its main provisions is that a fiduciary who has access to a tangible asset will have access to digital assets of a similar type. So if your executor is given control of your business, the online portions of that business and online records associated with the business would be available to the executor, too. But so far, only Delaware has adopted the UFA.

What do you want done with your email after you die? Many people want a relative to login and send a message to all contacts with their news of their passing. Should your Facebook page be closed or converted into a "memorial page"? How about your digital photos stored on Flickr? Do you have a blog or website that may need to be closed down? Any paid online services you need to cancel? These and many other questions are worth answering before you go.

Courtesy of ASK BOB.. Bob Rankin http://askbobrankin.com

WELCOME NEW MEMBERS

Doris Allen

Sherry Burch

Valerie Ennis

Louise Hendrix

Cleta Stanley

Mark White

Sally Peterson

Reminders

Be sure to check the class schedules at the meeting and sign-up for the ones you are interested in. There is no charge for classes to Club members.

Check your Membership to see if it is renewal time. We value each one of you!

Club Officers:

Bob Shewmake: President

Rich Clark: Past-President

Vice-President: Sylvia Hill

Secretary: Joe Tropansky

Treasurer: Joel Ewing

Board Members:

Marie Herr, Ken Nelson, Sylvia Hill, Marilyn Russell

Committee Chairs:

Jim Prince, Membership

Julie Storm, Newsletter Editor

Marilyn Russell, Programs

Earl Cummings, Librarian

Nancy Jones, Public Relations

Ryan Smith, Webmaster

Marie Herr, Education

Chuck Billman, Training Center Admin.

Bob Shewmake, Genealogy Liaison

Kathy Clark, Genealogy Communications

As a Courtesy to our Club Members

We are happy to list your computer related articles

that you wish to sell.

There is no charge, but it will be on space available.

Classes and open house clinics are free to Computer Club members. Club membership fee- $20; ½ price additional family member. Classes and help clinics are held at the John Ruehle Center located in the Highlands Crossings Center, 1801 Forest Hills Blvd., Suite 208, Bella Vista. Class descriptions at ***bvcompclub.org***