Bits & Bytes

Arkansas' Premier Computer Club

October 2021

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: October 11, 6pm, in John Ruehle Training Center, Highlands Crossing Center.

General Meeting: October 11, 7pm, "Q & A: Panel of Experts", with Woody Ogden and Pete Opland: an opportunity to submit your computer-related questions to our panel. If our panel doesn't know the answer, someone else in the audience may. Questions are accepted in advance or from the floor; but if research is required to give the best answer, email your question in advance to Q.and.A@bvcomputerclub.org. .

We will meet in-person in Room 1001 on the lower level of The Highlands Crossing Center, 1801 Forest Hills Blvd, Bella Vista, or you may attend the meeting on-line via Zoom. Zoom access information will be published on our website.

Visitors or Guests are welcome.

Because of COVID-19, we recommend observing current masking and social-distancing guidelines as much as possible. Consider attending by Zoom if you or others in your family are in a high risk category.

Genealogy SIG: **No meeting** (3rd Saturday).

HELP CLINICS

October 2, 9am - noon at John Ruehle center
October 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 .

MEMBERSHIP

Single membership is $25; $10 for each additional family member in the same household.

Join on our website at https://bvcomputercub.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)

Wednesday, October 13, 9am -11am. "Data: Where Is It and What To Do With It", with Pete Opland.

Wednesday, October 27, 4pm - 6pm. "Computer Security for Regular People, Part 2", with Justin Sell.

Friday, October 29, 9am -10:30am. "Installing WiFi Printers", with Pete Opland.

Advance sign up required for each listed class (**Maximum attendance 8**): Contact Grace: email to edu@bvcomputerclub.org, text 469-733-8395, call 479-270-1643, or sign up at the General Meeting. Classes are **free to Computer Club members.** Class access information will be emailed to those signed up for the class the day before class.

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

NEW OR RETURNING BVCC MEMBERS

We are pleased to welcome the following new members or members returning to BVCC after an absence since last month's newsletter:

Betty Pierce

SCAMS OF THE MONTH

By Joel Ewing, President Bella Vista Computer Club
president (at) bvcomputerclub.org
Bits & Bytes, October 2021

Scammers now attack on multiple fronts: land-line phone calls, mobile phone calls, mobile phone text messages, email, and even occasionally by regular mail.

Phone land-line numbers, and now also mobile phone numbers, can be added to the Federal Do-Not-Call list at the website: https://www.donotcall.gov/ . Any legitimate business attempting to do telemarketing sales for goods or services is required to honor this list and not to call you with telephone solicitations unless you have authorized them to do so. Political calls, charitable calls, debt collection calls, purely informational calls, and surveys are still allowed, but these calls can't include a sales pitch.

Being on the Do Not Call registry does not stop the most annoying telemarketing solicitation calls, but it does mean that if you receive an unsolicited call with a sales pitch of any kind, from an organization you have not previously authorized for such calls, you know you are dealing with an organization that is either ignorant of your rights or willfully breaking the law, either of which should be sufficient cause to avoid doing business with them or providing them with any personal information.

Some of the more annoying and persistent callers now appear to use "smart" robo call systems designed to make you initially think you are talking with a real person (who might be persuaded to take you off their calling list) when you are actually "conversing" with a machine: it will ask questions in what sounds like a very natural manner and give the illusion of understanding responses; but as soon as you give an unanticipated response it becomes obvious you are conversing with a machine, not a real person.

Some land-line phone providers and mobile carriers do provide services for blocking "known" telemarketers, but unfortunately those methods are based on caller-ID. The most annoying robo-call scofflaws use varying fraudulent caller-ID values and are largely able to bypass those blocks. There may still be some value in reporting such calls at www.dontcall.gov, as they may be able to establish a pattern of abuse that leads to the eventual apprehension of the responsible parties; and each documented offense contributes to the fine.

Some robo calls provide an option to be removed from their calling list. Those options don't have the desired effect. The best action once you've identified the call as an undesired robo call is to either hang up, or put them on

speaker phone and say or press nothing until their equipment times out and hangs up (to maximize the time cost to them of their call to you)

Medicare, IRS, Social Security, etc.

These frauds tend to come in the form of phone calls, where the caller identifies himself/herself with an organization name that claims or implies a connection with a government agency. In the Fall, with medical insurance choices looming, some association with Medicare is the favorite. Nearing tax time, calls purporting to be associated with the Internal Revenue Service or IRS become more common. Calls suggesting some connection with Social Security would be another favorite.

The number one rule to remember here is that unless you have called a government agency and put yourself on a call-back queue rather than wait for an agent, **these agencies DO NOT call individuals**. If they need to initiate communication with you, they always do it via the US Postal Service by an official letter, not by phone or email. If an unexpected caller claims to be from one of these agencies, it is a fraud. If they use an organization name that is not the actual agency name but which suggests an association, that might not technically be fraud, but it is a deliberate attempt to imply an unwarranted association and to deceive.

Medicare does not call individuals asking for personal info before sending a new Medicare Card, or in order to send you free equipment.

One call reportedly making the rounds in Bella Vista is a call from "MedicarePlus", from a speaker with a foreign accent.

Calls From Amazon About a Questionable Credit Card Charge

I've been getting several of these a week recently. Supposedly a "questionable" charge between $500 and $1000 has been made in my name at Amazon and they are calling to verify. It's a fraud. Hang up. They are attempting to steal personal information, account passwords or credit card information. Amazon, like any large corporation, does not call individual customers about problems – their business model expects customers to initiate the contact if there is a problem. Out of abundance of caution, the first time this happened I did go to the Amazon website and verified, as expected, that no such transaction had been made or was pending.

Credit Card companies, not retail companies, do employ various techniques to catch questionable credit transactions, like charges that would require your physical presence in two widely separated locations, unusual foreign charges, etc. But if they contact you it will be from a verifiable phone number and they will give you the relevant information, not ask for account information from you – or if you have their app on your mobile device, the verification request may come over that app so you can be certain it's legitimate.

This kind of scam is attempted substituting for Amazon any other large corporation with many customers. They don't have to know you are a customer. They just have to pick a company with enough customers to make the odds favorable that you might be a customer.

Fake Invoices and Bills

I have seen an organization email account that has recently been assaulted (at least 10 in last week) with fake invoices purporting to indicate an annual auto-renewal of a Security product (either Norton 360 or some generic PC Security product) for differing amounts around $200-$300. They provide a phone numbers to "upgrade/cancel your subscription", and will no doubt attempt to steal credit card information if you call to cancel the transaction that doesn't exist. These so far have been very poorly done fraud attempts, coming from different gmail.com accounts (not from norton.com), with numerous grammatical and spelling mistakes typical of non-native speakers of English, text only (no attempt to add easily available Norton logos, etc.), but they are ridiculously persistent considering the general incompetence of the attempt. The organization in question doesn't even own any PC's

A more common fraud attempt for an organization like ours, which has names and email for President and Treasurer available on the Internet, is to send the Treasurer an email that shows the President's name in the From (but with the fraudster's email address) requesting an emergency electronic payment of a bill that requires urgent payment . They hope the organization's procedures will be lax enough that the Treasurer will act without first verifying the authenticity of the request.

Arkansas Unemployment Insurance

I just got my first obvious fraud text message on my smart phone today, which claims:

"Your Arkansas Unemployment Insurance claim account is currently on hold for verification, Please complete your verification by following the instructions in the link below https://tinyurl.com/rry----- (URL partially redacted) to reactivate your account"

I do not have a Arkansas Unemployment Insurance Claim account, so it was obviously bogus, and the sending phone area code was also outside Arkansas. Going to the disguised URL link (from a well-protected system) took me to the actual URL https://ayed.sa/pa/arknet/arkansas/gov/ , which is a web page hosted in The Netherlands, made up to look like it might be the Arkansas Division of Workforce Services (ADWS) and asking for login credentials to ADWS. (If you follow the link on an iPhone, the URL of the actual web page is not easily seen, which makes it more dangerous in that environment). This appears to be an attempt to steal login credentials for the ADWS website.

Auto Warranty Extensions

I get multiple robo calls per month saying my Auto Warranty is about to expire. I first encountered these in 2011 when a new car became two years old, and I knew the calls were bogus because the car had a 6-year extended warranty. Now it's about two years since another new car purchase and I'm getting more of the same calls again. They must have some way to associate phone numbers with two years from the date of a new car purchase and assume you have a two-year warranty. They always say this is your "Last Call" – wish it were true. Supposedly waiting until someone gets on the line and telling them to remove you from their calling list just encourages them. They misrepresent what they are selling as an extension of your existing warranty, and if you buy from them, you don't find out until much later that they have just taken your money and provided no warranty extension. They use forged, different caller-IDs, so there is no way to block their calls. The only recourse you have is to report their calls to the FTC and hope they are eventually found and brought to justice.

At the same time I also get warranty extension offers in the U.S. mail. Many of these I also find suspect because they lack any company name or physical business address and only provide a contact phone number. Doing business with people who want to remain anonymous never seems like a good idea.

OCTOBER – CYBERSECURITY AWARENESS MONTH

By Joel Ewing, President Bella Vista Computer Club
president (at) bvcomputerclub.org
Bits & Bytes, October 2021

Every year since 2003, October has been designated as National Cyber Security Awareness Month. The goal was to at least provide an annual reminder that continuing personal awareness is needed to stay relatively safe and secure from online Cybercrime.

Some specific examples of different types of Cybercrime include email and Internet fraud, identity fraud (theft & use of personal information), theft of financial or credit card data, theft and sale of corporate data, Cyberextortion (demanding money to prevent an attack or recover from an attack), theft of computer resources (using your computer to launch Cybercrime attacks on others), malicious vandalism (damaging of your data or functionality of your computer system, just because…)

Phishing

The vast majority of successful cyber attacks – 91% according to a study by cofense.com[1] – begin with a phishing scam: emails that mimic messages from someone your know or a business that you trust, designed to trick you into giving up personal information or take an inappropriate action without thinking, like opening a malware attachment or opening a link to a malicious website that downloads malware or tries to trick you into supplying personal or account information. It takes much less effort or skill to trick a computer user into revealing useful information by phishing than to design and deploy malware. And if your goal is to install malware, it is much easier and cheaper to trick a user into installing it himself that to find some software or Operating System "bug" that allows installing the malware outside the user's control.

Phishing emails frequently go hand in hand with website spoofing – a website at a different URL web address that is designed to closely resemble the actual real website, to trick you into supplying your login credentials or other information, thinking it is the real site.

The single most important thing the average computer user can do to protect themselves is to develop the mindset that email cannot be trusted or taken at face value. It is trivial for anyone with minimal technical skill to forge the "From" name on a email and send an email with any name combined with an email address to send a reply to an email account that doesn't belong with the name.

---

1 https://cybernews.com/security/interview-with-cofense-director/

If the object of a phishing email is to trick you into clicking on an attachment or following a link within the body of the email rather than replying to the email, then with a somewhat higher skill level or special applications you can even send an email where the entire From address is completely forged with a valid name and corresponding valid email address, just totally different from the actual sender. If you know what to look for in the raw source text form of the email, you can usually spot inconsistencies that suggest that a totally forged From address is bogus. Just keep in mind that all of the header information you see displayed for a received email (From, To, Cc, Date, Subject) are basically just "comment" lines. It is only the email client app that you use to send an email that enforces the conventions that these fields have actual correct values, and someone using a rogue app to send an email can bypass any or all of those conventions.

If an email is atypical from what you normally receive from an individual or company – bad spelling, incorrect English grammar or usage, has unexpected attachments, asks you to follow unexpected links or take unusual actions, or just asks "are you there" or "do you have a minute" (this makes no sense in an email, which might not be read for hours or days after being sent), then be suspicious.

Some legitimate websites do routinely send emails with embedded links (FaceBook, and Citicard bonus offers come to mind). If the email is expected and your email client allows you to hover over the link and verify that the URL does appear to go to the correct site, these may be OK; but should a "harmless" link suddenly start asking for login credentials when that is not normally the case, close out the browser and go to the website using your known browser favorites, not the email link. It also obviously makes sense to be more paranoid about email links that purport to be associated with financial institutions where you keep significant assets.

These days all commercial and most other websites have now converted to using "HTTPS" secure browser access to make website phishing very difficult or impossible – unless you follow a bad URL link address in a phishing email; but to accommodate older saved URLs in browsers, password managers, advertisements, and search engines, almost all websites will still allow you to start your communication using insecure "HTTP" protocol, and then the website automatically forces the browser to change over to "HTTPS".

Normally there is no problem with beginning a browser web session with HTTP, but there have been rare instances in the past where the Domain Name Servers have been attacked successfully or someone physically intercepts your communications, so that you get sent to a bogus website that pretends to be the intended website. This kind of attack can only work on HTTP access. "HTTPS" access requires the security certificate at the website to match the domain name in the URL, and those can't be forged by someone who doesn't own the actual domain name. If that kind of attack were in progress, an initial HTTP connection to a legitimate URL could be diverted to a bogus site with no visible error and then altered to HTTPS access to a different URL for a plausibly-named but bogus website. It could look normal enough that you might be fooled. If instead you start with an HTTPS connection, if you are being diverted to a bogus address on your initial contact you will be warned by your browser that the security certificate is invalid and that you should not proceed, as the responding site could be bogus.

Although I have not seen this recommended before, it seems like an appropriate 2nd level of defense that would completely eliminate that avenue for attack would be for you to eliminate default initiation of contact with a website using HTTP protocol.

I would recommend going into your browser favorites list, and if you use a Password Manager also into your password manager entries as well, and then manually editing all URL addresses containing "http://" and change them to "https://" – at least for all financial institutions and any other sites you would consider sensitive. You should consider as sensitive any email account sites for email addresses that could be used to reset passwords on sensitive websites.

Malware

Windows Defender under Windows 10 and later now provides adequate defense against typical malware. No virus detection software is 100% effective against Day 0 attacks by new malware, but your odds of encountering that are low. One important defense against malware for most users is timely installation of Windows updates to Windows Defender and to the Windows Operating System itself, so that known software security issues are resolved. It is equally important to remember that no anti virus program can protect you if you intentionally introduce the malware by making a habit of installing software of questionable merit from unreliable sources. A computer system that you depend upon to be functional for specific purposes should not also be loaded up with extraneous programs or applications that do not contribute to that function.

The best defense against some of the more destructive forms of malware, like ransomware, is to make frequent image backups of the computer and to retain multiple older backups. If ransomware makes your data inaccessible, the only certain way to recover your data is to find a backup that was taken before the ransomware infection occurred.

Passwords

One person may easily have over 100 different online accounts. Your choice of passwords for on-line accounts is something you can control, and your choices greatly affect how secure your on-line accounts will be.

Typically a website will use an email address as the username and combine that with a password. You hope the website using that account is well managed, but with enough different website accounts, there is always the chance one could get hacked and expose your account information and password.

Typically the same email address will be used with multiple website accounts. This makes it extremely important to use a unique password for each website. The first thing a criminal will do after acquiring a compromised username/password for one website is to see if the same combination will work on many of the commonly used websites. Using the same password on multiple websites risks turning a minor inconvenience of changing or recovering control of one hacked website into a major disaster with many compromised accounts and much greater chance of financial loss.

The only practical way to keep track of a large number of good unique passwords for many websites is to use a Password Manager application and only have to remember one unique password for the password manager database. Obviously that makes that password manager database and its password critical information that must be securely backed up and stored where it could be accessed by your representative should you become incapacitated.

What makes a password secure? Many websites require passwords to be a mix of uppercase and lowercase letters and digits. Some also require the presence of at least one special character. What's of almost greater importance

is a sufficient number of characters. In some cases passwords with as few as eight characters will be accepted, but a password that short can potentially be cracked in a few hours. With current technology it could easily take several hundred years to crack a 12-character random password, but improvements in technology make that time shorter every day. Some now recommend a minimum password length of at least 16 random characters.

A Password Manager program makes it easy to generate and use random passwords of any length. You do however need a password to access the password manager database itself that is both secure yet easy for you to memorize. A pass phrase (a series of words strung together) is one way to create a longer password that can still be easily remembered, but it does need to be longer than a random password to have the same level of security. Another simple technique to create a long password that appears random but is yet easy for you to remember is to base it off the first letter of words in a phrase from a book, poem, or quote that is very familiar to you. When using a pass phrase, be careful to avoid obvious words, like names of family members, that someone who has researched your personal information could easily guess.

Some sites also allow you to set up Multi-Factor Authentication (like requiring a code that is sent to your smart phone). This is indeed much more secure, but be careful that there are some alternatives that can be used as backup authentication. You don't want an authentication procedure that will make it impossible for you to access your account if you lose your smart phone, or make it impossible for anyone acting on your behalf to gain access if you are incapacitated.

Protecting Sensitive Information

If you choose to post your sensitive information in inappropriate public or quasi-public places, you don't have to be a victim of phishing or malware to put your identity at risk or to compromise your on-line accounts.

Be cautious about what you post on social media. It's amazing how much personal information you can deduce about family relationships, names, and birthdays, place of residence, etc. from a person's social media presence. Too much public personal information could put you at higher risk for identity theft. Posting detailed online information about planned absences from your home could also inform criminals of the ideal time to break into your house if they can deduce your address.

You should also not assume that email is secure. Your emails exist for an unknown length of time in un-encrypted form on on both the servers of your email provider and those of the email recipient's email provider. All email is being scanned by applications that try to determine whether or not it is SPAM email, and if one of those servers were compromised, one could scan for other "useful" information. You can also expect technicians to occasionally read random emails to try to diagnose problems with email delivery. Or, a court order could require your Internet Provider to produce copies of all your emails.

Unless you regularly use encrypted email (it exists, but is not simple and rarely used by ordinary people), you should assume that your email may be read by others. Avoid sending in the body of an email complete account login information, Social Security Numbers, financial account numbers, other sensitive financial information, or personal identifying information that would be useful for identity theft or financial fraud.

Sensitive information can be sent by email as an encrypted attachment, provided the encryption key is sent to the recipient by a different means (telephone call, regular mail, or direct in-person communication). The current

versions of both MS Word and LibreOffice Writer (and the other applications in those Office suites) have Security options to encrypt documents, although for historical reasons both call the encryption key a "password". There are also various other free applications that can be used to encrypt and decrypt any arbitrary file. It is important to know that the document is actually encrypted, not just password protected. A mere access password can be easily circumvented; but if the file is encrypted, then the actual data has been altered in ways that are practically impossible to recover without the encryption key, unless a trivial key were used.