Bits & Bytes

Arkansas' Premier Computer Club

October 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 Email: jrc@bvcc.arcoxmail.com

Meetings

October 10th

BVCC Board Meeting

5:30 pm

Computer Club Meeting

Community Room at

Highlands Crossing 7 pm

HELP CLINICS

Open House help clinics will be held Oct. 5 from 1-4 and Oct. 8 and 19 from 9 am to noon. Help clinics are a free service for computer club members.

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

PROGRAM

Combating identity theft and fraud will be the presentation topic at the 7 pm meeting of the Bella Vista Computer Club on

Monday, October 10, 2016.

Mike Whited from Arvest Bank will present the program.

This public meeting is in the Community Room of Highlands Crossing Center (lower level), 1801 Forest Hills Blvd, Bella Vista.

http://bvcompclub.org/october2016.htm

Using Computers with Windows 10 parts 1, 2 and 3 classes will be held Oct. 11, 18, and 25 from 10 am to noon.

Register for classes by calling 579.273.2558.

New officers have been elected but we still need a volunteer for **Secretary.** It is not hard, I did it for two years and enjoyed working with the Board.

Julie Storm

With great regret, the Board has accepted the resignation of our faithful webmaster, Ryan Smith.

Ryan is experiencing serious health problems at this time. Please, let all of us keep Ryan in our prayers.

Welcome New Members

Invite a friend for this meeting!

Genealogy SIG 10 AM John Ruehle Center

3rd Saturday 10-12 am

Yahoo made headlines recently by admitting that it suffered a data breach that may have compromised more than 500 MILLION Yahoo accounts. Here's how to find out if you may have been affected by this (or one of many other) massive data breaches...

Is Your Personal Data Exposed?

The Yahoo breach, which exposed names, email addresses, telephone numbers, dates of birth, and weakly-encoded passwords, happened in late 2014. Incredibly, Yahoo says it didn't even suspect the breach until the summer of 2016, and it didn't advise users to change their passwords until September 22.

While Yahoo may have been "grossly negligent" in its security practices, as two class-action lawsuits already allege, it's worth noting that data breaches go undetected for 201 days, on average. During that time, a lot of damage can be done to users' finances, credit, privacy, and more. That's why it behooves each of us to be constantly vigilant about about our own security.

A savvy reader suggested to me, "You might want to remind your readers to occasionally go to the site Have I Been Pwned and check if they have been "pwned" * at one of the compromised websites. If they had an account (on) those sites, it doesn't necessarily mean that their password has been compromised but it may have been. So it is good idea to change your password at those sites and also at any other sites where you may have used the same password."

(* "Pwned" is gamer slang for "perfectly owned," captured, conquered. In this context, it means a hacker now owns your login credentials, and maybe much more sensitive data.)

Have I Been Pwned (HIBP) collects and analyzes stolen data that it finds online. It then allows users to check their "email address or username" to see if it's on HIBP's "pwned" list. If it is, HIBP displays the information about the source of the data breach, when it occurred, how many accounts were compromised, and if your credentials are known to have been posted on a publicly searchable repository of "pwned" addresses.

I've mentioned HIBP before, but it's worth revisiting, in light of the ever-growing list of websites and institutions that have suffered data breaches. HIBP is the creation of a well-respected security expert, Troy Hunt. According to it-self, HIBP was launched in December, 2013, and as of September, 2016, it receives about 10,000 visitors a day. About 350,000 people have subscribed to be notified if their email addresses turn up on future additions of pwned accounts.

Is It Safe and Effective?

HIBP seems safe and legit. If you learn there that one of your email addresses may have been compromised, by all means change the password for that account, and for any other account where the same password was used. You can also sign up to be notified by email if any of your account information is found in future breaches.

In most cases, when a site breached, the hackers get your email address, and a hashed or encrypted copy of your password. This is why trivial passwords are such a big problem. The weaker your password is, the more likely that the data thieves will be able to decode it.

One reservation I have about HIBP is the timeliness of its data. HIBP harvests published files of compromised ac-counts. Typically, such files are not published until the accounts in them have been thoroughly exploited, sold, and re-sold multiple times. HIBP told me that a MySpace account belonging to me was breached in 2008 but the data wasn't published until 2016. I can't blame HIBP for not knowing about this earlier, but it's little comfort to find out today that my account was pwned eight years ago.

There are cases in which "fresh" data is published. The hackers who breached the Ashley Madison "have an affair" site wasted no time in publishing all the embarrassing data they got on more than 30 million alleged adulterers. (I say "alleged" because most of the accounts turned out to be fakes.) But the overwhelming majority of stolen data will not find its way into HIBP until long after the horse is out of the barn.

"Let's Assume..."

HIBP is a free service, and at the very least provides a wakeup call for password vigilance. There's an old saying that to ASSUME "makes an ASS of U and ME." But when it comes to your online accounts, the opposite is true. Given the fact that many popular websites, online stores, health insurance companies and even banks have suf-fered embarrassing data breaches, it makes sense to assume that you HAVE been affected.

Things You Should NEVER Share Online

Two major trends are in conflict on the Internet. “Security” is big these days; it’s more important than ever to protect yourself against ever-increasing cyberthreats. “Sharing” is equally big, thanks to companies like Facebook and Twitter which make money when you share your thoughts, experiences, and other life-stuff with strangers. But security and sharing do not mix well. Here's what you need to know...

Are You Over-Sharing?

Look at airline boarding passes as an example. People excited about going on vacation often post pictures of their boarding passes on social media. (I guess they fear their “friends” won’t believe them without proof.) Unfortunately, those boarding passes may contain all the information an identity thief needs.

Delta Airlines’ boarding passes include the E-Ticket number, booking reference, frequent flyer number and even how many bags you have checked in. Go toDelta’s site and you’ll find the “manage existing trips” option. All you need to login there is the passenger’s name and E-ticket number or booking reference. That allows anyone with that info to change your seating assignment, change the date of your return flight, or even cancel your tickets. That's just one example; most airlines have the same type of barcodes and online passenger portals.

In some cases, the barcode on an airline ticket contains also the passenger’s phone number, date of birth, frequent flyer number, payment information, passport data, names of others in your party, and where you'll be staying upon arrival. Few passengers realize that, so even the security-conscious fail to cover it when taking a photo. Barcode readers are cheap, and many cybercrooks have them.

Tickets to concerts and other events should not be posted online until after you have used them. Tickets bear all the info necessary to create useable counterfeits. Many people have been disappointed at the box office to learn their tickets have already been used. If you must have bragging rights, Ticket Master has a helpful page on theDo’s & Don’ts of Sharing Ticket Pics Online.

Of course, you should never post a picture of a check online. See my article, “Paper Checks Can Lead to Fraud”.

You should never tell the world that you are or soon will be on vacation or away on business. You might as well put a sign on your lawn that reads, “Nobody home, rob this house.” Use private messages to inform people who really need to know that you’ll be away for two weeks. Wait until you get home to share vacation photos and anecdotes with everyone.

Is Your Slip Exposed?

Going on a date to someplace expensive? Muggers would love to know that. Throwing a bridal shower where there will be a heap of expensive gifts? A home invasion is possible if you post the place and time online weeks in advance. Your social life is full of opportunities to get ripped off, or even physically harmed. Don’t share it with strangers.

Linking one of your social networks to another may prove embarrassing, at the least. When you link a Facebook account to a LinkedIn account, suddenly your professional colleagues know your personal life. One guy got fired this way; he called in sick at work and then bragged on Facebook about putting one over on the boss. His boss saw that and fired him.

Parents and grandparents love to post pictures of children, and they rarely consider the long-term effects on their offspring. A recent story making the rounds tells of an 18-year-old Austrian girl who is suing her parents because they refuse to take down 500+ "potty pics" and other embarrassing baby photos posted on Facebook.

Aside from causing possible embarrassment, a photo can reveal sensitive info about kids, and enables a creep to recognize a child. Mentioning the child’s name enables a creep to say, “Hey, Jenny, Grandpa So-and-So sent me to take you to his house.” Don’t mention anything about children on social media that can help perverts find and trick them. Remember, they’re kids, who trust easily.

More Facebook Faux Pas

I am constantly amazed by Facebook users who share their phone numbers and even home addresses with everyone. Ditto for users who leave location services enabled on Facebook or Twitter. I had to tell one single mom, via Twitter direct message, that her phone was broadcasting the street address of her home to the whole world. She had a major panic attack.

Facebook reports that 40 percent of its users leave their entire profiles open to the public. That means everything you post is available to 1.2 billion people! Take the time to get familiar with Facebook’s privacy settings and lock down your profile. Then be careful to make “friends” only of people who are friends in real life. The rest are strangers, and you don’t know what they might do with your personal info.

Even close friends and spouses should not have your passwords. Breakups happen, and before they happen someone often sneaks a peek at someone else’s social media accounts. Facebook has become a divorce attorney’s best friend, saving thousands of dollars on private investigators.

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!

The **Bits & Bytes** will be updated as new information comes.

Please check often!

Club Officers:

Sylvia Hill- President

Bob ShewmakeVice-President:

Secretary:

Treasurer: Joel Ewing

Board Members:

Marie Herr, Ken Nelson, Marilyn Russell

Committee Chairs:

Jim Prince, Membership

Julie Storm, Newsletter Editor

John Reese, Programs

Earl Cummings, Librarian

Nancy Jones, Public Relations

Ryan Smith, Webmaster

Marie Herr, Education

Bob Shewmake, Genealogy Liaison

Thank you for supporting Bella Vista Men's Chorus

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***