

THE C.A.T.S. Eye



PRESIDENT'S CORNER

BRING YOUR LAPTOP WITH YOU TO THE NEXT MEETING!

The Chesapeake Area Technology Society (CATS)

Happy New Year!

We have a **BIG** meeting this Wednesday, January 15, 2014. Best Buy will be sending local representatives to the meeting to demonstrate some of the latest technology available. As we have done the past few meetings, we have some significant raffle prizes that will be demonstrated by the Best Buy team.

Bring plenty of cash! This has become a very popular activity.

Below are the prizes with links for more information on each.

Microsoft Surface Pro 2 (128 GB storage) with Type Cover 2

<http://reviews.cnet.com/microsoft-surface-pro-2/>

Google Nexus 7 tablet

<http://reviews.cnet.com/google-nexus-7/>

Lenovo Ideapad Yoga 11" convertible laptop

http://www.cnet.com/laptops/lenovo-ideapad-yoga-11s/4505-3121_7-35560383.html

Leap Motion controller

http://reviews.cnet.com/input-devices/leap-motion-controller/4505-3133_7-35823002.html

Western Digital My Cloud 3TB

http://www.cnet.com/network-storage/wd-my-cloud-3/4505-3382_7-35828119.html

New meeting location – Broadneck High School Media Center (Map on Page 2)

For those who didn't know, we have had to change our meeting location to the Broadneck Senior

High School, in the 2nd Floor Media Center. The facility is different than what we're used to at Severn River and because of their schedule, we've had to move the main meeting from the 2nd to the 3rd Wednesday of the month. There is an elevator for handicapped use at the end of the corridor for the main (1st entrance) to the school. The custodial staff has been very accommodating to us and will be available to operate the elevator for anyone who needs it on Wednesday.

Upcoming Meeting Topics

At the next few meetings we will have some significant raffle prizes, so bring some cash!

January 15, 2014 – Best Buy representatives (will visit our group to demonstrate some of the latest technology they offer for sale. As the meeting gets closer, we should have more information on the specific demonstration.

February 19, 2014 – We hope to have the local Apple users group, Annapolis Apple Slice, demonstrate the Apple ecosystem to the group. This will show how the laptops, tablets, and mp3 players all work in harmony.

As you can see we have a very full agenda over the next few months. I hope to see you all at the upcoming meetings.

Michael



OFFICERS

PRESIDENT Mike Young.....(410) 551-4411	president@chesapeakepcusersgroup.org
VICE PRESIDENT Mike Regimenti.....(301) 509-6091	vice-president@chesapeakepcusersgroup.org
TREASURER Kathy Walker(410) 266-6317	treasurer@chesapeakepcusersgroup.org
SECRETARY Joyce Shue.....(410) 263-3510	secretary@chesapeakepcusersgroup.org
PUBLISHER/EDITOR Mike Regimenti.....(301) 509-6091	editor@chesapeakepcusersgroup.org

CHAIRPERSONS

PROGRAMS Craig Barlow.....(410) 266-6829	programs@chesapeakepcusersgroup.org
EDUCATION Sam Shepherd.....(410) 647-6077	education@chesapeakepcusersgroup.org
MEMBERSHIP Betsy Fravel.....(410) 703-1425	membership@chesapeakepcusersgroup.org
PUBLIC RELATIONS Joyce Shue.....(410) 263-3510	pr@chesapeakepcusersgroup.org

SPECIAL INTEREST GROUPS (SIGS)

NEW USERS GROUP Sam Shepherd.....(410) 647-6077	
TECH SIG Mike Regimenti.....(301) 509-6091	internet@chesapeakepcusersgroup.org
CRSIG Karl Richmond.....(410) 268-3860	refurbishing@chesapeakepcusersgroup.org
WEBMEISTER Mike DeLucia.....(410) 721-2991	webmeister@chesapeakepcusersgroup.org

If You Think That Your Credit or Debit Card Was Compromised ...

by
Ira Wilsker

WEBSITES:

<http://news.yahoo.com/target-says-data-breach-hit-70-mn-customers-150615694.html>

<http://krebsonsecurity.com/2014/01/target-names-emails-phone-numbers-on-up-to-70-million-customers-stolen/>

<https://www.annualcreditreport.com>

<https://corporate.target.com/discover/article/Target-to-offer-free-credit-monitoring-to-all-gues>

<https://www.creditkarma.com>

<http://news.yahoo.com/factbox-deal-target-39-data-breach-002005721--sector.html>

<http://krebsonsecurity.com/2014/01/hackers-steal-card-data-from-neiman-marcus/>

<http://news.yahoo.com/exclusive-more-well-known-u-retailers-victims-cyberattacks-024345910--sector.html>

http://www.cleveland.com/business/index.ssf/2014/01/after_the_latest_information_b.html

<http://news.yahoo.com/neiman-marcus-latest-victim-security-breach-163741250.html>

<http://news.yahoo.com/changing-card-pin-only-first-step-target-breach-211113764--sector.html>

<http://www.bjs.gov/content/pub/pdf/vit12.pdf>

As I am typing this, the latest number of Target customers who may have had their debit and credit card numbers compromised may have increased to 110 million, according to published sources. In recent days it was reported that an unknown number of Neiman Marcus customers may also have had their credit and debit information stolen by cybercrooks. Now, there are indications that several other unnamed retailers, rumored to have a presence at outlet malls, may also have had their customers' data stolen as well. Despite the massive nature of these data thefts, other than some inconvenience, there is only a small likelihood that any significant number of victims will suffer any material financial losses as the financial institutions issuing debit and credit cards have a "zero liability" policy that holds financially harmless any consumers who may have been the victims of credit fraud, provided the victim notifies the financial institution in a timely fashion.

With well over 100 million likely victims of this massive credit and debit breach, it is probable that many readers of this column

are among those whose debit or credit card information may have been compromised. In December, Target reported that the data stolen included customers' names, credit and debit card numbers, card expiration dates, debit-card PINs and the embedded code on the magnetic strip on the back of cards had been stolen. Subsequent reports also indicate that additional personal information may have been taken as well, including home addresses, email addresses, phone numbers, and other personal information.

These massive data thefts are not just some abstract digital event, but are in reality a massive case of financial fraud and identity theft which may cost businesses and financial institutions hundreds of millions if not billions of dollars. Already, the information from countless thousands of debit and credit cards stolen in the Target breach have shown up for sale on Russian and other eastern European websites already known for selling stolen debit and credit card information. The information for sale includes all of the information on the cards' magnetic stripe,

cont'd on Page 4

3

Compromised? - cont'd

CVV2 security code (three digit security number on the back of credit cards, or the four digit number on the front of American Express cards), expiration date, issuing financial institution, PIN numbers used on debit cards, and enough other information to easily enable dishonest individuals and criminal enterprises to produce counterfeit credit cards. Other crooks can use this same digital information for illicit online purchases, cash withdrawals from ATM machines, financial transfers, and other types of financial crime.

With so many victims of this massive cyber theft, a second wave of related criminal activity has already commenced; many victims have reported receiving “spear phishing” emails (targeted spam emails), telephone calls, and text messages offering to help restore the victims’ credit, recover unauthorized charges, and offer “protection” services. Preliminary investigations indicate that these are predominately scams carefully orchestrated to illicitly obtain additional funds from the victims, and to garner additional personal information in order to enhance the effectiveness of the identity theft. I personally have heard from one local individual who claims to have received a phone call informing him that his credit card information had been stolen at Target, and the caller needed his other credit card numbers, CVV2 codes, and expiration dates, and PIN numbers in order to secure them from additional criminal activity. The person called was told that there was no charge for this service, but what was not said was how the caller would likely use the data provided in continuance of additional criminal activities, by utilizing those additional credit and debit card for illicit financial gain.

There are several steps that the potential victims of the Target, Neiman Marcus, and other data thefts can take to mitigate any potential damage and losses. Almost all of the security

pundits agree that debit card users should contact their financial institutions immediately, and change their debit card PIN numbers to a difficult to guess number. Users should not use street address, birthday, anniversary, last four digits of social security number, or any other identifiable PIN number, but should instead use a somewhat random number for their new PIN.

It would also be prudent for everyone to periodically get a truly free copy of his credit report from each of the three major credit reporting agencies; the genuine source of really free credit reports is annualcreditreport.com. Under normal circumstances, individuals are entitled to one copy from each of the three credit reporting agencies each year, but some individuals choose to get a report from only one of the credit reporting agencies, and then ordering another free credit report from another reporting agency four months later, repeating the four month process continuously such that on this staggered basis, credit can be better monitored with triannual reports than annual reports.

Target recently announced that it will be offering a free, comprehensive, credit monitoring service (corporate.target.com/discover/article/Target-to-offer-free-credit-monitoring-to-all-gues) to those compromised in the Target breach. According to the Target corporate website, quoting Scott Kennedy, president, Finance and Retail Services, “The service, which will be available to all guests who shopped our U.S. stores, will include a complimentary credit report, daily credit monitoring, identity theft insurance where available, and access to personalized assistance.” While the signup details have not yet been released by Target as of this writing, signup information should be available shortly, according to Target. Target also announced that there will be a three month window during which Target customers can sign up for the free services when they become available.

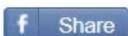
Compromised? - cont'd

For those who may want to start monitoring their credit situation immediately, Credit Karma (creditkarma.com) is also offering totally free credit monitoring services. These free services include credit score reporting, daily monitoring of all three major credit reporting agencies, and real-time account monitoring services.

The Cleveland Plain Dealer newspaper recently published "After the latest on the Target data breach, here are 39 ways to keep you and your finances safe" (cleveland.com/business/index.ssf/2014/01/after_the_latest_information_b.html). In addition to changing PIN numbers, and credit monitoring, 37 other tips are presented to the reader. Among the tips presented are having credit card issuers set daily limit on accounts, have a locking street-side mailbox if appropriate, drop mail in an official mailbox rather than leave it in a private mailbox for pickup, keep a current record of all credit card numbers and issuers, secure your computer, do not open email attachments or respond to spam email, do not carry or display your social security number (SSN), check debit and credit card receipts against monthly statements, do not leave personal information in your car, do not use your actual street address as "Home" on any form of GPS (if stolen could lead the crook directly to your residence), arrange for text alerts from credit card companies and financial institutions, utilize the fraud alert services from the credit reporting agencies, practice good password safety, and several other tasks that individuals should routinely monitor or perform.

Changing card PIN only first step after Target breach: experts

 **REUTERS** By Richard Leong | Reuters – 4 hrs ago



2



By Richard Leong

NEW YORK (Reuters) - Changing the security code for your debit card may be as easy 1-2-3 following a widespread data breach at Target but guarding your personal information from hackers is a longer-term battle, according to experts.

Even though the government protects consumers from this type of fraud, you are not guaranteed the store or bank whose computer system is hacked will tell you about the theft of your personal data.

State laws vary on notifying consumers about such theft.

So it's ultimately up to the consumers to make sure their personal data don't fall into the wrong hands or at least limit the damage if were to happen.

Report unauthorized charges as soon as possible to your credit/debt card companies and monitor regularly your credit activities via the three major credit bureaus, experts say.

cont'd on Page 6

Compromised? - cont'd

According to the Bureau of Justice Statistics (www.bjs.gov), in a report released recently (December 12, 2013), “An estimated 16.6 million people, representing 7 percent of all persons age 16 or older in the United States, experienced at least one incident of identity theft in 2012. ... Financial losses due to personal identity theft totaled \$24.7 billion, over \$10 billion more than the losses attributed to all other property crimes measured in the National Crime Victimization Survey. About 14 percent of victims suffered an out-of-pocket financial loss due to the most recent incident of identity theft. Of the victims who experienced an out-of-pocket loss, about half lost \$99 or less.”

If 2014 has a similar identity theft rate to the rate in 2012 (most recent data available), about one in 14 of us will be the victim of identity theft this new year. With the explosion of the recent massive data thefts in our retail sector, I would not be surprised to see the absolute number of identity theft victims as well as the rate of victimization increase substantially this year. Be proactive; while there is not much that we as individuals can do to protect our data held by major retailers and other institutions, we can still take the steps mentioned above in order to harden our financial protections and reduce the identity theft risks that we all are facing.



BLOG ADVI

10 Hackers Steal Card Data from Neiman Marcus

JAN 14



Responding to inquiries about a possible data breach involving customer credit and debit card information, upscale retailer **Neiman Marcus** acknowledged today that it is working with the **U.S. Secret Service** to investigate a hacker break-in that has exposed an unknown number of customer cards.

Earlier this week, I began hearing from sources in the financial industry about an increasing number of fraudulent credit and debit card charges that were being traced to cards that had been very recently used at brick-and-mortar stores run by the Dallas, Texas based high-end retail chain. Sources said that while it appears the fraud on those stolen cards was perpetrated at a variety of other stores, the common point of purchase among the compromised cards was Neiman Marcus.



Advertisement



Recei

Otterbox Cases

Review by George Harding, Treasurer, Tucson Computer Society, AZ

October 2013 issue, TCS eJournal

www.aztcs.org

[georgehardingsbd \(at\) earthlink.net](mailto:georgehardingsbd@earthlink.net)

Here's a company that has grown by providing just what the customer wants. It started with a line of waterproof cases and continued with cases through which the enclosed device could be manipulated. From that point on it was a matter of adapting cases to the continuing flow of new types of devices, still keeping each case waterproof and protective.

Every time I go to a computer show, Otterbox is there and has a new case to give away. I currently have two new cases, the Pursuit and the Armor, which the Company describes as "The toughest case ever made."

The Pursuit is about the width and height of a cell phone, but is a good bit thicker, a bit over an inch. It has a latch that brings the top snugly down to the bottom. The top has a flexible strip just inside its rim, which is what makes the interior waterproof (up to 100 feet deep). Protection also includes crush (up to 1,000 pounds), drop and impact, as well as dust and debris. It's designed to provide super protection for outdoor activities. The exterior of the case has hard plastic "bumpers" on each corner and end. There is a flexible loop attached to make it easy to fasten the case to your belt. Inside, both the top and bottom have semi-rigid pads to help soften impacts.

The Armor is a cell phone case sized for the iPhone 5, iPhone 4 or Samsung Galaxy, but could be used for others as well. The case is described as waterproof, drop proof, dust proof and crush proof.

For Otterbox waterproof is no big deal; all their cases are waterproof! For this case, however, "water proof" means submersion for 30 minutes at 6.6 feet of water. "Drop proof" for this case means protection for drops up to 10 feet. "Crush proof" is probably the most amazing – up to 2 tons! Soft foam on the interior provides a custom fit and cushioning. There is also a screen protector built

in that prevents scratches and damage to the glass display. It's hard to imagine any type of action that would damage your cell phone!

About:

Otterbox Pursuit and Armor cases

Vendor: Otterbox

www.otterbox.com

Price: Pursuit about \$20, Armor about \$100



The article above has been obtained from APCUG with the author's permission for publication by APCUG member groups; all other uses require the permission of the author (see e-mail address above).

Linux Magazines

by

Cal Esneault, Former President and leader of many Open Source Workshops & SIGS,

Cajun Clickers Computer Club, LA

November 2013 issue, Cajun Clickers Computer News

www.clickers.org

[ccnewsletter \(at\)cox.net](mailto:ccnewsletter@cox.net)

Since Linux is not as commonly used as some other computer operating systems, users frequently resort to online sources for instructional information. Although easy to find, typical research often ends with information having a question and answer format focusing on isolated issues. A magazine format can give a broader view without being long or technically complicated. Two suggestions for free, online magazines for users are PCLinuxOS Magazine and Full Circle Magazine.

PCLinuxOS is a PC operating system with a KDE 4 desktop environment that was started by Bill Reynolds (“Texstar”) in Houston, TX. It has an open-source “community” operation that publishes its own magazine. There is a lot of emphasis for new users transitioning from other operating systems. Many technical articles stick to a moderate length, and there is a lot of “fun” content (such as food recipes, screen shots of customized desktops, reader feedback, etc.).

Below are a few of the article topics covered in the last three issues of the PCLinuxOS magazine:

Xfce User Tips and Tweaks (Parts 1,2, & 3)
Password Security Revisited
OpenVPN: Other VPN Services
LibreOffice Tips & Tricks (Parts 1,2, & 3)
Inkscape: Holiday Tree; Torn Paper Effect
Undo Gmail’s Latest “Enhancements”
Backup Your Gmail Account With getmail
GIMP Tutorial: Masks Explained
Game Zone: Sacred Citadel

Linux vs. Windows

Testimonials from veteran PCLinuxOS users

Gramps genealogy program

Screenshot Showcase

Full Circle Magazine covers Ubuntu and its derivatives (Xubuntu, Lubuntu, Edubuntu, etc.), but it is not associated with Canonical Ltd, the commercial sponsors of Ubuntu. It has many recurring feature topics (news, ask the new guy, software reviews, command line skills, etc.) and usually has more than 50 pages of content. For the most part, it relies on volunteer writers, There is also an associated podcast available. Note: the title Full Circle is in reference to the Ubuntu logo.

This magazine also carries well detailed multi-part articles about a few of the more popular software titles. Examples include LibreOffice, Inkscape, Blender, Python, and GIMP. There are sometimes special editions of concentrated compilations of these articles.

Examples of special issues are three special issues for LibreOffice, two special issues for Inkscape, and 6 special issues for Python (see the September 2013 main magazine issue for details). Since most of the software with multi-article coverage is cross-platform and can run on most operating systems (Linux, Mac OS, Windows OS), these articles should be of interest to almost any computer user.

Linux Magazines - cont'd

Both magazines are published monthly. PCLinuxOS Magazine started in September of 2006 and is now at issue 80. Full Circle Magazine started in May of 2007 and is now at issue 77. Both can keep you up to date on news, software, and hardware related to Linux. In addition, you can get any of the past issues in PDF format from their archives without cost. These archives provide a huge resource of detailed information written in a style friendly to the average user.

These magazines are excellent examples of the way the open-source community works to share the knowledge about free computer software. Even if you do not currently use a Linux OS, browsing these magazines will give you a quick view of what open source software is all about.



This and the following articles have been obtained from APCUG with the author's permission for publication by APCUG member groups; all other uses require the permission of the author (see e-mail address above).

808 Headphones

Review by George Harding, Treasurer, Tucson Computer Society, AZ

www.aztcs.org [georgehardingsbd \(at\) earthlink.net](mailto:georgehardingsbd@earthlink.net)

Our mobile devices usually play sound, especially music. Most cell phones and all MP3 players come with earbuds, which are convenient and easy to carry.

But cords often get so tangled that using them is too much trouble.

The earpieces may not be the right size or may be irritating to one's ear. An elegant solution to these problems is a set of headphones, but the best ones are quite expensive.

808 Headphones are reasonably priced and give you all the advantages over earbuds. They are elegant in design, being smooth in appearance. They fit snugly over your ears, so there's no problem with fit or irritation. The earpads are very comfortable. Each earpad is adjustable so as to fit different head sizes and shapes.

Probably the best feature is the sound quality. You get very good bass response as well as treble (although my ears are too old to benefit from those high notes!). The rated frequency response is 20 – 20K Hz. The power capability is 20mW, 60mW maximum. The headphones come in a very nice flexible case with a zipper closure.

One of the earpads folds in so as to fit compactly in the case. There are two cables supplied with the headphones, stowed in a net pocket inside the case. The company describes them as “tangle-free,” and they appear to be so. One is a plain cable with 3.5 mm plug on each end. The other is a flat cable with a control for play/pause, for those devices that permit that. A 6.3mm adapter is also supplied.

These are really nice headphones and are reasonably priced.

Vendor: 808 Headphones

www.808headphones.com

Price: About \$90



The Jeopardy Answer Is...What?

by Linda Gonse, Editor & Webmaster, Orange County PC Users' Group, CA

www.orcopug.org [editor \(at\) orcopug.org](mailto:editor@orcopug.org)

The final question on Jeopardy on its September 26 episode was based on the category “Internet.” The question was “The animal for which this computer program is named is actually a red panda.”

Do you have any idea what that program is? When I tell you the answer, you will shake your head — as I did — and you will say “What? That’s not right!”— just as I did.

Are you ready? The answer is “What is Firefox (the internet browser)?”

“Fire fox,” in Chinese, is another name for the red panda.

In fact, Mozilla launched a website called “Firefox Live” in November 2011 to educate

and raise awareness of the endangered red panda species.

Live videos of three baby red pandas, Bernadette, Dolly, and Winston, that were sheltered at the Knoxville Zoo, were streamed on the Firefox Live website until March 2012. When the babies reached maturity they were sent to breed and become part of the animal families at the Virginia Zoo (Norfolk, Virginia) and the Zoo Boise (Boise, Idaho). Subsequently, the Firefox Live website was retired.

If you'd like to find a red panda in a zoo near you, go to http://redpandanetwork.org/red_panda/find-a-red-panda-near-you/

from the Secretary's Desk....

The Board of Director's Meeting was held on Wednesday, January 8, 2013. The meeting convened at 7:00 pm.

In attendance were the following: Mike Young, Joyce Shue, Betsy Fravel, Karl Richmond

Upcoming Meeting Topics

Tentative schedule of meetings topics. The meetings are subject to change or rearrangement:

- January 15 – Best Buy will present the hot items that were sold during the holiday season. We will have at least 2 representatives from Best Buy at the meeting and possibility 4. Matthew Norman who did the presentation last January will be doing it again this January. There will be several raffle items based on their presentation.
- February 19 – A presentation on Apple products and raffle items will include a Mac Book Pro, iPads and an iPad mini.
- March 19 - A presentation from the Apple Slice Group
- April 9 - (NOTE- this is the 2nd Wednesday) - Topic - TBD
- May 21 - Topic - TBD
- June 4 - (NOTE- this is the 1st Wednesday) - Topic - TBD

SIGs

- CRSIG – An application for a \$5,000 grant from The Rotary Club was submitted. This upgrade is to start upgrading the electrical system and purchase 2 air conditioning units at the CRSIG location. Karl Richmond (new CRSIG chairperson) is seeking a donation of a 4 or 8 port KVM switch. There are presently 8 computer ready. A new application is being developed and will be posted on the web site for individuals and non-profits seeking refurbished computers in the near future. The SIG is still in need of hard drives that are at least 80 GB SATA and/or IDEs. They are also in need of PS2 and USB keyboards.

Finances

No Financial Report

New Business

- Joyce will start using Meetup.com within the week.

The meeting was adjourned at 8:45 pm.

*Respectfully Submitted,
Joyce Shue, Secretary*

The Next Regular Meeting will be at
The Broadneck Senior High School

Wednesday
January 15th, 2014

Meeting will be held in the 2nd Floor Media
Room at BSHS.

It starts at 7:00 P.M. with club business
and a short discussion period.

You're invited to a presentation
the Latest & Greatest
Technology Products
by the folks at
Best Buy

Members and their friends are welcome to
come, ask questions and become enlightened.

How to Find: Broadneck Senior High School

BSHS is close to Cape St. Claire, MD. From Annapolis and points south, take Rt. 50 East towards the Bay Bridge. Take Exit 29 B (cross over Rt. 50) at the light, turn **LEFT** on College Parkway, at next light , then **RIGHT** on Greenholly Drive. At the first light, turn **Right** on to the road that leads to the school and the Broadneck Public Library. BSHS will be ahead and slightly to your left. (Of course, if you are coming from points North, you could turn left onto College Parkway) and follow it 4.1 miles & turn **LEFT** on Greenholly. The first entrance you see, is the **Main Entrance, the left door has been open at 7 pm.** Go through the second set of doors and follow the corridor to the staircase. The Media Room is on the second floor, just off the stairs. Signs will be posted to direct you to the **MEDIA ROOM** where we will be meeting.

**The meetings are held at the BSHS in the
Media Room.**

The Chesapeake Area Technology Society



1783 Forest Drive #285
Annapolis, MD 21401

FIRST CLASS

INSIDE THIS VERY ISSUE!

President's Corner

Credit Card Compromised?

Secretary Desk

Linux Magazines

Otterbox Cases

THE FIRST ALL DIGITAL ISSUE!

.... and a little bit more!

Proudly Affiliated with

