http://www.tpcug.org

Bits of Blue

A Monthly Publication of the Tampa PC Users Group, Inc.

March in Tampa

Vol. 28 No. 3 March 2015

Meeting

Windows 10 And Other Things

by William LaMartin

Wednesday, March 11, 2015

6:30 PM

Pepin Distributing Co.
4121 N 50th Street
Tampa, Florida

INSIDE THIS ISSUE

Meeting Preview: William LaMartin will demonstrate Windows 10 Technical Preview plus two other items on which he has been working. Bob LaFave will also conduct the usual Windows SIG for the first 30 minutes of the meeting.

Editor's Comments

By William LaMartin, Editor, Tampa PC Users Group
william@lamartin.com

Dave Palmer is back with another article for the newsletter, for which I am very appreciative. Also, our president, John Witmer has several short comments for the group, and Doug Mullis provided the annual financial report. So there is very little room remaining in the newsletter for me to fill.

The past month for me at the computer has been one of searching and selecting. I have two computer projects that I have been slowly working on for several months. The first consists of compiling a list of old newspaper articles, mainly from the Tampa Tribune and Miami Herald, about happenings in my hometown of Okeechobee. For that project I search the online archive of newspapers at http://www.genealogybank.com, which is a subscription-based site. It is a tedious process since I must consider each of the 17,237 possible items that a search for

Comments.....Continued on page 2

April Meeting: FBI agent to discuss the latest in scams

Bits of Blue is published by the Tampa PC Users Group, Inc., a State of Florida registered non-profit corporation, to provide educational information about personal computer systems to its members. Our mailing address is P. O. Box 3492, Tampa, FL 33601-3492.

However, for business concerning this newsletter, Bits of Blue, please contact the Editor, William LaMartin, at 813-251-3817, or william@lamartin.com.

Technical information found in this publication is not necessarily compatible with your hardware and software, plus other errors or misprints could occur from time to time. Therefore, the use of programs, commands, functions or anything of a technical nature appearing in this publication will be at your own risk.

RENEWING YOUR MEMBERSHIP?

WE CERTAINLY HOPE YOU WILL

MAIL YOUR CHECK AND ANY
ADDRESS OR NAME CHANGES TO:

TAMPA PC USERS GROUP
PO BOX 3492
TAMPA, FL 33601-3492

$25 Individual $35 Family
$60 Corporate = 3 employees + $20 each add'l employee

Go to our web site http://www.tpcug.org and click on the About Us | Join link to join or renew online

Check the address label for your renewal month

Friend of the User Group

We acknowledge
Pepin Distributing Co.
for their support

Affiliations

Florida Association of User Groups

Association of Personal Computer User Groups

Minutes of the February Meeting

By Merle Nicholson, Secretary, Tampa PC Users Group
merle@merlenicholson.com

The Windows Special Interest Group (SIG) opens our monthly meeting. Bob LaFave, the SIG moderator introduces new or little known products and technological developments for discussion by the group. He accepts questions and requests for help in solving problems from attendees. This month in Bob's absence, I was the substitute moderator. The subjects covered were mostly about passwords and the best practices for storing them. Also discussed were the available email clients - particularly Mozilla Thunderbird. The discussion created some lively comments and further questions from the group.

The presentation this month was given by myself, Merle Nicholson, on the subject of Ubuntu Gnome desktop - a variation (officially a "Flavor") of Ubuntu. The demonstration computer is a dual-boot Windows 7 and Ubuntu Gnome, defaulting the boot to Gnome. Navigating around the desktop was demonstrated, as was the menu system, the cataloged download library, updates and utilities. An overview was given of the installed programs and a discussion of WINE, the method to run many of the Windows programs.

I demonstrated and talked a bit about LibreOffice and the reason to never buy Microsoft again for most people. The latest update of LibreOffice has a slightly new look. It is available for Windows users as well. I also displayed the list of useful apps in Google Chrome, all of which are available in Windows, too.

The level of participation during the demonstration was gratifying as was the later feedback from a few members in attendance. ◆

Comments.....Continued from page 1

Okeechobee produces, discarding the vast majority which actually have nothing to do with Okeechobee City and the happenings there. So far I am up to 1926 and have selected around 667 articles. You may view the results at http://www.lamartin.com/OldNewspapersOkeechobeeInfo.aspx. I will mention the second project at the meeting. ◆

Malvertising

By Dave Palmer, Tampa PC Users Group
dkp205@hotmail.com

Just as 'malware' is short for malicious software, 'malvertising' is short for malicious advertising. Like many services on the Internet, online advertising has become highly automated. And like nearly everywhere else on the Internet, cyber criminals have found ways to corrupt that automation to turn a profit.

Have you noticed that after you do some online research for a specific purchase that you soon see online ads for similar products on different websites? That's a result of websites leaving 'cookies' on your computer. Cookies don't identify you personally but they can identify you as having an interest in a category of products. In addition, the IP address of your computer provides a general geographic location. When you visit other websites, they read your IP address and any cookies left recently. They also provide this information to an ad network which quickly adds interest-based or location-based ads to the websites you visit. Now advertisers and ad networks know your approximate location and the categories of products you're interested in.

How online advertising works
Ad networks consist of publishers, advertisers and the middlemen who connect the two. Publishers are the owners of the websites you visit. They sell advertising space on their websites. Then there's the advertiser, the individual or business that has a product or service they want to advertise. They buy advertising space on websites.

The sites you visit usually do not play a direct role in choosing the ads you see. Instead, a middleman, a third-party advertising company, manages the ad selection and placement for both the publisher and advertiser. This makes the process more efficient for everyone. The process is highly automated – humans are only rarely involved – usually only at the beginning for initial approval. This business model, advertising supported by ad networks, supports a large portion of the Internet, providing the 'free' information and websites we have come to rely on.

Online advertising can come in many forms. Ads can be a single static image without animation, ads can be animated in one of several different ways, or ads can be video-based. There are pop-up ads, pop-under ads, banner ads and a dizzying array of shapes sizes, styles, formats and technologies involved.

As this advertising business model has developed, ad networks have spread across the Internet. Over time the sheer volume of ads has given rise to a massive and tangled conglomeration of ad networks, ad exchanges and other related businesses that buy, sell, trade and swap ads and ad space constantly as the tides of supply and demand shift constantly. Of course, opportunistic cyber criminals weren't far behind. They soon found many ways to abuse the system for profit.

Delivering the payload
Bad guys may scam the system by posing as legitimate advertisers. They may hack into legitimate but dormant accounts. Either way they gain access to the ad networks. They then create legitimate-looking ads to disguise malware to either deliver malware directly from booby-trapped ads, or to redirect viewers to a poisoned website that delivers the malware payload. In most cases neither the publisher (the website displaying the ad) nor the ad network providing the ad knows the ad is booby-trapped.

One major obstacle to detection of malicious ads is that they are not persistent. Once the user leaves a website or closes the browser, all traces of the ad disappear. In addition attackers take great pains to make their ads hard to detect. They may enable their malicious payloads only after their ads have been approved. They may set the malicious ads to only attack every 10th user. They may set up many different domains and redirect victims many times before the victims reach the poisoned website. These and other practices make detection quite difficult.

Once installed on the victim's computer, malware may look for login information for e-mail, social media, and bank accounts, as well as for identity information.

Malvertising.....Continued on page 4

Malvertising.....Continued from page 3

In some cases the malware can lock the user's computer and demand a ransom.

Click fraud

Another way the bad guys corrupt legitimate advertising is to commit 'click fraud.' Click fraud occurs in pay per click (PPC) online advertising when machines or programs imitate a legitimate user and click on an ad to generate a charge per click without having any interest in the ad itself.

Hackers may use the malware installed by ads to commandeer the victim's computer and add it to the hacker's botnet – a network of hijacked computers used for criminal activities. Botnets (bots) are often used for click fraud. Click fraud sometimes begins when unscrupulous publishers or ad networks hire hackers to boost their numbers or to generate income. Computers in the botnet are instructed to visit various websites and click on specific ads.

Here are a few eye-opening stats from an adweek.com article (http://goo.gl/9zrH7X). Up to 50% of publisher activity is from botnets - automated click fraud. Bots account for 11% of display ad views and 23% of video ads. Of the $43.8 billion in ad revenue, fraudulent activity accounts for $6.3 billion. More than half of traffic from 3rd parties claiming to lift publisher's traffic numbers comes from bots. Click fraud is a major problem in that it raises costs for legitimate publishers, advertisers and ad networks. Click fraud can also be used indirectly to attack legitimate competitors and force them to pay higher advertising costs.

What can be done?

Unfortunately there's little agreement on who is responsible for addressing these threats. Both publishers and advertisers need to take action to limit malvertising on their networks. In addition a number of companies now exist to validate that ads are being seen by humans. They include WhiteOps, ComScore, Integral Ad Science, The Media Trust and Double Verify, among others. But since consumers are under a serious and direct threat, we must do what we can to protect ourselves.

How to protect yourself

In some cases the bad guys are hoping they can redirect your browser from your intended website to a poisoned website so they can download malware into your computer. For that scenario to work your browser has to: 1) allow the redirect and 2) contain a vulnerability that allows malware to be installed and 3) operate in administrative mode to allow the installation. I've included some instructions below on how to set up the Big 3 browsers to prevent redirects*. In case you still operate daily in administrative mode, Merle wrote an excellent explanation of how to create a standard user account in the Oct 2014 edition of the TPCUG newsletter.

In some cases the ad is booby-trapped with some executable script, often Flash, Javascript, etc. Your protection is to use script-blocking software – NoScript for Firefox and ScriptSafe or Script Blocker for Chrome. Things are a bit more complicated with Internet Explorer. Don't use Internet Explorer unless absolutely necessary. If you're an IE diehard check out the instructions here: http://goo.gl/YTcQpK. Although script blockers are not terribly convenient, removing malware is way beyond inconvenient.

In the end, the threats from malvertising are really no different than other malware threats across the Internet. So the protection advice is no different either.

To reduce the threat from vulnerabilities, first minimize your 'attack surface,' that is, remove programs you're not using. The next step towards minimizing your vulnerability is to keep everything updated – your operating system, browsers, programs, add-ons, plug-ins, etc. Backup your data and system regularly. Use a password manager and strong passwords.

Preventing redirects*

Chrome

To prevent Chrome from being redirected to another site without your knowledge, click the "Customize and Control Google Chrome" button. The button has three horizontal lines on it. Click "Settings." Click the "Show Advanced Settings" link to display more setting options. In the Privacy section, click "Enable Phishing and Malware Protection." Close the browser

Malvertising.....Continued on page 6

Internet Picture of the Month

Colorized Photo by Dullaway

The image is a 1921 photo of an automobile accident in Washington, D. C., which is nothing out of the ordinary. What is of interest is that it is a colorization of an original black and white photo [view the newsletter at our website to appreciate this]. The very subtle colorization was done by Sanna Dullaway. You may view this photo and other of her colorizations at http://mygrapefruit.deviantart.com/gallery/

March's Links

Tampa PC Users Group (that's us)	http://www.tpcug.org
Windows 10 Technical Preview Download	http://windows.microsoft.com/en-us/windows/preview-download
Old Newspaper Search	http://www.genealogybank.com
Digital Photo	http://www.dpmag.com/
Florida Fish and Wildlife Conservation Commission	http://myfwc.com/

Malvertising.....Continued from page 4

window. Google now displays a warning if the browser is trying to redirect you.

Mozilla Firefox

In Firefox, click the "Open Menu" button, which has three horizontal lines. Click the "Options" button in the panel that opens. Click the "Advanced" button and then the "General" tab. In the Accessibility section, check the "Warn Me When Websites Try to Redirect or Reload the Page" box. Click "OK."

Internet Explorer

Internet Explorer doesn't have a way to expressly stop redirects. Instead, you have to limit the whole Internet. Click the "Tools" button, which looks like a gear. Click "Internet Options." Click the "Security" tab. In the Security Levels for This Zone pane, set the slider to "High." This prevents IE from running ActiveX controls, which is how many browser redirects are carried out. However, this might prevent some safe sites from loading correctly. Click "OK."

These steps work for Google Chrome 40, Internet Explorer 11 and Mozilla Firefox 35. Other versions might use different steps.

*The above instructions were taken from: https://www.ehow.com/how_8744477_do-links-redirecting-different-sites.html ◆

Reminder To Use Our Amazon Link; New Board Members

By John Witmer, President, TPCUG
jwitmer@outlook.com

TPCUG has a link to web shopping giant, Amazon, on our website (http://www.tpcug.org) for which the Group receives a small referral commission for all purchases made through this link. It costs you nothing extra to make your purchases by accessing Amazon through this link. Amazon commissions are a valuable source of income to our Group, as seen in the annual Financial Report for 2014, which is included in this March 2015 newsletter. We received income of $427 in 2014, and $688 in 2013. Without this fee income we would have had a $369 operating loss in 2013, and our small 2014 loss would have grown to be $479. Please remember us when you do your shopping on Amazon. We all benefit by keeping our Group's membership fee low as a result of this needed extra income from Amazon.

Update On Officers And Board Members For 2015

I was pleasantly surprised that my annual plea for other Group members to become involved in the leadership of this Group actually produced results for this new year we just began. I am pleased to report that Dave Palmer and Ed Cohen both volunteered their services to be on the Board of Directors for TPCUG, and to add their input and insight into the discussions and decisions affecting the operations and direction this Group faces in the coming year(s). Thanks to you both for stepping up and lending us your help. As most of you know, Dave has also done several great presentations to our Group in the past, including the January presentation on Passwords. ◆

Commentary On 2014 Financial Report

By John Witmer, President, TPCUG
jwitmer@outlook.com

Included in this month's newsletter is the 2014 TPCUG Financial Report prepared by our Treasurer, Doug Mullis. As I looked it over, I was struck by the fact the expenses were greater than the income for the first time ever that I can recall. We spent $55.88 more than we received in income from membership dues and Amazon Commissions. Dues income was in line with past years, and reasonable in amounts, so why the loss this year? It appears the culprit is a combination of lower Amazon Commissions in 2014, and our Newsletter printing costs rising substantially as a result of having to pay a vendor to print all 12 monthly issues this year.

Commentary.....Continued on page 7

TPCUG FINANCIAL REPORT FOR 2014
Submitted by Doug Mullis, Treasurer

TPCUG STATEMENT OF INCOME AND EXPENSES AND BANK BALANCE

2014 INCOME	
Membership Dues (22 Single + 4 Family)	$815.00
Door Prize/Auction Receipts	0.00
Amazon Link Commissions	427.14
TOTAL INCOME	$1,242.14
2014 EXPENSES	
Newsletter Postage	$196.00
Newsletter Printing (12 Mos in 2014)	468.60
FACUG Dues	25.00
APCUG Dues	50.00
Florida Annual Corporate Fee	61.25
Web Site Hosting Fee (12 Months)	181.08
P O Box Rental (fee increase)	78.00
December Holiday Party Costs	204.00
Refreshments (Cookies)	24.99
PayPal Usage Fee (6 Paymts @ $0.85 ea)	5.10
TOTAL EXPENSES	$1,294.02
NET LOSS FOR 2014	$51.88
CASH BALANCE PER BOOKS – START OF 2014	$7,560.86
CASH BALANCE PER BOOKS – END OF 2014	$7,508.98

(No Bank Account Reconciling Items for Beginning or End of Year)

Commentary.....Continued from page 6

Let's consider the newsletter printing cost increase. The Group was fortunate during my employment years with Pepin Distributing that William created the newsletter each month and sent it to me to print on the Pepin copier at no cost other than the cost of a few 8.5x17 reams of paper each year. I was able to print three months of newsletters in 2013 before retirement, so we had to pay for 9 issues to be printed in 2013 using a local printing vendor. In 2014, the Group paid for all 12 months of newsletters to be printed, at a cost of $469. This cost used to be less than $75 a year when I was able to do it at Pepin.

The second item concerning Amazon Commissions is not within the control of the Group, other than reminding the membership to please remember to use the Amazon link on our website before you purchase on Amazon. There is a separate article related to this reminder in this month's newsletter. We do count on these commissions to help offset costs, and it is even more important given the rise in costs of getting the newsletter to our members.

I think we are one of only a few Groups left that still print and mail Newsletters to members, and I know that the members generally prefer to have it that way, like reading a newspaper in hand is preferable to reading it online. So we are not going to propose

Commentary.....Continued on page 8

Tampa PC Users Group, Inc.
P. O. Box 3492
Tampa, FL 33601-3492

First Class Mail

☐ *Member: Your membership is up for renewal*

Commentary.....Continued from page 7

any changes to how you get your newsletter in the mail. The good news is that we have a reasonably comfortable bank balance that can afford to absorb small losses each year for a long time without affecting the financial health of the Group, even in light of declining Amazon commissions if that should happen. And we do not need to raise our dues for membership either as long as the level of membership stays fairly consistent year after year. There are measures that can be taken should our financial situation begin to decline significantly, but I see no indication this is going to happen in the next few years. So sit back and enjoy this newsletter, do your entire Amazon purchasing through our website link, and keep your membership dues paid timely. Your TPCUG should live happily ever after as a result, at least financially. ◆