Volume 17, Issue 6

November 2016

The Computer Club At Willow Valley

Inside this issue:

The President's Pen by Sid Paskowitz

Membership As of this writing, your Computer Club has 587 paid members including 349 who have signed up as Lifetime members. Please keep your email address current on Club records so we can send you important emails. *Those emails only go to Computer Club members for whom we have a good email address*. Let our Treasurer, Charlie Trumbo, know if your email address has changed or if you don't get a future Newsletter.

Executive Officer Change At the end of 2016 Bob Scala will be retiring as Computer Club Vice President and as chairperson of the Program Committee. Bob has performed superbly in both of those roles and I want to publicly thank him for all of his contributions to the Club. The Computer Club Executive Committee has selected Peter Scott as Bob's successor. We welcome Peter in his new role.

Windows 7 and Windows 8.1 No Longer Available On New PCs The HotHardware website at http://hothardware.com/news/major-oems-no-longer-sell-windows-7-windows-81-pcs-november-1st announced that major computer manufacturers will no longer be selling Windows 7 or Windows 8.1 personal computers after November 1st. The Computer Club recommends Windows 10 on new computers so that should not be an issue.

Scams I keep hoping I don't have to remind folks to beware of scams, but we keep hearing about Residents being scammed on their phones, their devices and their computers. No one who calls you, emails you or displays a message or your computer or device can tell you your computer or device is infected or running poorly. They have to have been given access. If you haven't provided them with access, you are being scammed. Don't give them access. Hang up. Disconnect. Shut down.

Privacy The November 2016 Consumer Reports publication contained an article on How to Protect Your Privacy. Starting on page 28 were 66 Ways to Take Control. I have personally found the following suggestions to be of particular interest. Those who read the article may also find other suggestions they want to consider implementing.

#4 explains how to find out who is sharing your email address with others when you provide your Gmail address to a website.

#12 tells how to possibly reduce the amount of unwanted mail.

(Continued on page 2)

Coming Programs

November 3
Jim Tracy and Bob Davis, Willow Valley
What's New at WVC (Internet and TV) and IT Update

December 1
Tony Poulos, Willow Valley Resident
Time to Replace Your Computer followed by *Expo*

January 5
Ralph Beedle, Willow Valley Resident
Tax Preparation Software and Skills at WVC

All programs are held in the Theater at the Cultural Center on the 1st Thursday of the month at 2:00 p.m. unless otherwise noted.

President

(Continued from page 1)

#23 suggests using Google Drive to scan suspicious email documents for viruses.

#30 tells you how to "Cloak Your Computer."

#33 recommends using fake information when a site asks for personal data that you don't think they should have.

#43 (my favorite) recommends using separate browsers for important (e.g., banking) and less important (e.g., browsing) websites.

#54 (another favorite) encourages ways to check out web links before you click on them.

#55 discusses the use of data encryption using HTTPS.

#57 and #58 tell you to back up your data and keep software updated.

#62 and #63 offer suggestions on avoiding scam emails and pop-ups.

#64 and #65 tell how to tighten Google privacy.

Lots of stuff, but you may want to add some of them to your repertoire of actions when you are working on your computer.

Please Use Recommended Software PC owners are reminded that they can receive the best help if they use software that is familiar to other Residents who volunteer to provide technical assistance. Recommended applications are CCleaner, Malwarebytes, Defraggler and Windows Defender (or Windows Security Essentials). We recognize there are alternatives; however, problems are more quickly diagnosed and repaired when the applications running on the PC are familiar to the helper.

(Continued on page 3)

President

(Continued from page 2)

Classes We know we need more classes on computer-related topics and we are looking for instructors who can teach those classes. If you can help other Residents with topics such as Word, Wordpad, Notepad, browsers, email, etc., please send me an email at wvcomputerclub@gmail.com. We need your help.

MAC SIG Steve Lynn, head of the Mac SIG group, is looking for suggestions as to how the Computer Club can better support Mac users. If you have ideas that can help Steve formulate a plan for supporting Mac users, please send them to him at slynner15@icloud.com. Information Central has been modified based on Steve's recommendations. In the center column of Information Central is a feature called *For MAC Users*. It contains information applicable to Apple computers. Let Steve know if you have suggestions for other beneficial information links that might be added to the area *For MAC Users*.

Recycling Ed Dahrsnin and his team are accepting working computers and components for recycling, but no CRT monitors. Let Ed know if you would like to help recycle computers. Ed and his team meet on Monday afternoons at Manor North. Working in the recycling effort may also help you when you have problems. Thanks to Ed and his team, the Computer Club has given 146 computer systems to the Lampeter-Strasburg School District for families that cannot afford a computer for their students and two laptops to the Hand Middle School in Lancaster for their Science classroom.

Thank You My thanks to all of you who volunteer your time and knowledge to help other Residents. We need more volunteers! •

Privacy and Anonymity by Al Williams

Some people have told me that they are not worried about privacy because they have nothing to hide.

But is that really true? For example, would they give me their online bank account logon information and tell me to help myself? Would they announce to the world their email account's username and password and say that everyone is welcome to send out spam through their email?

Privacy is about protecting information. To be more specific, it is about protecting the content of communications.

Many of us use Google's gmail for email. But, did you know that Google reads every email? They use that information to target ads for you as you are reading your email.

(Continued on page 6)

What Happened On October 21? by Al Williams

You may have read about the major attacks on the Internet on October 21. The attacks made the news because many people in major cities of the US could not get to major web sites. News articles mentioned that something called IoT devices were being used to make the attacks. What happened and what are these devices?

In the past, attacks have been against individual web sites. Friday's attacks were different; they were against Domain Name Services (DNS), provided by Dyn, a major company in the US with data centers around the world. There are other DNS providers in the US but Dyn is a large provider.

The difference in the attacks is significant because by attacking Dyn, the hackers attacked not just one web site but many major web sites, simultaneously.

Why is DNS vital to the health of the Internet? We know web sites by their names: Netflix, Amazon, Twitter, LL Bean, Lands End, etc. But computers do not work with names, they work with the numeric addresses assigned to the web sites. DNS is similar to a telephone directory. You enter a name such as Lands End into the search box in your browser, your browser gives a DNS provider, such as Dyn, the name of the web site and asks the DNS provider for the corresponding numeric address. Your browser then uses that numeric address to take you to that web site.

The attacks in the US made it impossible for many Internet users from Boston to Washington DC, Chicago, Dallas, Seattle, San Francisco, and Los Angeles to watch movies on Netflix, shop on Amazon, tweet on Twitter and use dozens of lesser known Internet companies.

The attacks worked by sending millions of requests to Dyn's DNS servers asking for the numeric addresses of web sites. Over 10,000,000 devices were asking for numeric addresses. There were so many requests that Dyn's equipment could not keep up and no one's requests were answered.

These devices are part of the Internet of Things (IoT) which are the refrigerators, ovens, thermostats, lamps, door video systems, webcams, and many other seldom noticed things which are connected to the Internet. Hackers have discovered that many of these devices have standard usernames and passwords and are therefore easily instructed to send out queries to conduct DNS attacks. According to *Computerworld*, this attack used cameras connected to the Internet.

Will this type of attack go away? No. Can their effect be reduced? Only by upgrading the firmware in the IoT devices such that they cannot be instructed to send out queries, or by replacing the devices.

Unfortunately, because of the way that the Internet is designed, there is nothing at this time that will prevent attacks like Friday's from continuing. If you would like to see current attacks, google *Akamai real time monitoring,* go to that web site, and then select the *Attacks* tab. While I am writing this article, major outages are occurring not only in the places listed above but also Atlanta, Vancouver, Portland, South Korea, and Japan •

Protect Yourself From Identity Theft by Al Williams

The United States Computer Emergency Readiness Team (US-CERT) has written a basic tip on preventing and responding to Identity Theft. First issued in 2008, the most recent revision is October 1, 2016. An overview of their tip follows. For more information, google *US-CERT ST05-019*.

Computers are not the only way that your identity may be stolen. If someone can gain access to your personal information, including credit card numbers, phone numbers, account numbers, and addresses, by stealing your wallet, listening to your phone conversation, rummaging through your trash, or picking up a credit card receipt that you threw away, that person may be able to impersonate you to purchase items, open new accounts, or apply for loans.

If you shop online, the company you purchase from will have your information in their database. If someone can gain access to that database, your identity may be stolen. You may provide your personal information to other web sites as well, such as genealogical sites or the state division of motor vehicles. Access to those databases also provides information that may lead to identity theft.

As long as you provide personal information to others, there is no way to guarantee that you will not be a victim of online identity theft. But there are steps that you may take to minimize the likelihood.

- Do business with reputable companies
- Take advantage of security features. Passwords are the most obvious but other techniques such as two-factor authentication make it more difficult to steal your identity.
- Check the privacy policies of the web site(s) that you use
- Be careful when posting personal information. If you post on Facebook or on other public forums and you reveal information about yourself, be careful. The US-CERT recommends:
    - View the Internet as a novel, not a diary
    - Be careful of what you advertise (or broadcast) about yourself
    - Realize that you can't take it back. It is said that nothing totally disappears once it is published on the Internet.
    - Use your common sense
- Use and maintain anti-virus software and a firewall. Ever since Windows XP, Service Pack 2, Microsoft Windows machines have had a firewall enabled. With Windows 10, Microsoft's Windows Defender is always enabled. Follow the Computer Club's recommendation to also use Malwarebyte's anti-virus software.
- Stay aware of your account activities. Check your credit report yearly.

(Continued on page 6)

Protect Yourself From Identity Theft

(Continued from page 5)

How will you know if your identity has been stolen? Here are examples:

- Unusual and unexplainable charges on your bills
- Phone calls or bills for accounts, products, or services that you do not have
- Failure to receive regular bills or mail
- New, strange accounts appearing on your credit report
- Unexpected denial of credit card purchases

What can you do if you think or know that your identify has been stolen?

- Contact companies and banks where you have accounts. Contest unauthorized transactions. Close accounts to prevent further use. Send a letter to create a record.
- Contact the main credit reporting companies—Equifax, Experian, TransUnion—and put fraud alerts on your credit reports to prevent new accounts being opened
- File a report with the local police
- File a complaint with the Federal Trade Commission
- Contact other agencies as necessary. For example, the Social Security Administration and the Pennsylvania Department of Motor Vehicles. •

Privacy and Anonymity

(Continued from page 3)

They state that they do not sell personally identifiable information. They do, however, present ads from companies when they know that you are likely interested in those products. They make a lot of money from those ads. The ads are why gmail and the other Google products are free. Can they do this legally? Yes. It is in their Terms and Conditions that you agree to when you sign up to use gmail.

It isn't just Google. No email through the major email providers – gmail, aol, yahoo, etc., is private unless you take steps to protect the contents.

Anonymity is being unknown to other people. It is also about remaining unknown.

Anonymity is much harder to achieve on the Internet. That's because all communications are addressed to someone. You've probably heard the word meta-data. When talking about email, that word refers to the data that go along with emails and specifies from whom the email is coming and to whom it is going.

It isn't just email, other means of communication such as payments and file transfers also reveal who you are. It is possible, however, to have communications with someone else where both of you remain anonymous and the communications are private. •

The Equipment Corner by Ed Dahrsnin

Refurbished Systems

System 478: HP ProBook 6560b, Windows 10 Pro

System 479: HP ProBook 6560b, Windows 10 Pro

System 490: HP ProBook 6560b, Windows 10 Pro

System 495: HP ProBook 6560b, Windows 10 Pro

System 496: HP ProBook 6560b, Windows 10 Pro

System 497: HP ProBook 6560b, Windows 10 Pro

Miscellaneous We have 3 volt CR2023 batteries (suitable for motherboards to keep the system clock running) and a variety of CD-ROM's, floppy disk drives, keyboards, 2-button mice, various power supplies, and assorted cables. Please contact Ed Dahrsnin at 464-6591.

Donations We continue to accept printer cartridges and laptop computers *with* power adapters. We accept *only* working printers *with* drivers and documentation. Also, we accept *only* working monitors. Cathode Ray Tube monitors are *not* acceptable. Stand-alone scanners are *not* acceptable. Bring the items to Manor North's recycle closet on the fifth floor of 'J' building on Monday only, from 1pm to 1:30pm. •

The Mission

The Mission of the Willow Valley Computer Club is to:

- Provide the means to educate beginners or interested non-users on how to use a computer.
- Arrange for speakers to talk to the Club about subjects that would be of interest to those with some background and experience in computer use.
- Provide a forum for interchange of computer information among members.

For more information about the Club, contact Sid Paskowitz at 464-2127 or wvcomputerclub@gmail.com •

The Leadership

Officers

President: Sid Paskowitz

Vice President: Bob Scala

Secretary: Marge Schmieder

Treasurer: Charlie Trumbo

Community Representatives

Manor: Larry Gallagher

Manor North: JoAnne Phillips

Lakes: Gene Simasek

Providence Park: Peter Scott

Committee Chairpersons

Program: Bob Scala

Training: Ralph Beedle

Equipment: Ed Dahrsnin

Technical Support: Tony Poulos

Website: Sid Paskowitz

Publicity: Wally Gordon

Newsletter: Al Williams

Mac Interest Group: Steve Lynn

Computer Room Coordinators: Gene Simasek Lee Wermuth

Microsoft Liaison: Ed Dahrsnin

Past Presidents

Larry Gallagher

Reviewer Acknowledgment

The following individual kindly reviewed this issue:

Sid Paskowitz

Tony Poulos

Thank you,

Al Williams

Interested in reviewing the Computer Club newsletter before it goes to press, providing advice about the content, or writing an article? Please contact:

Al Williams at atwilliams136@gmail.com