SEMCO

DATA BUS

Volume 38	June 2013	Number 6

IN THIS ISSUE

The SouthEastern Michigan Computer Organization, Inc. (SEMCO) is a non-profit, 501(c)(3), group dedicated to providing information, education and a forum to computer users (professional and amateur) and other interested individuals. Membership in SEMCO is open to all individuals 18 years or older. Persons under 18 years may become members through the sponsorship of a parent or guardian. Dues of $30/year include monthly DATA BUS and free personal ads.

All SEMCO correspondence should be addressed to

SEMCO - P.O. Box 707 - Bloomfield Hills, MI 48303-0707

Web site: **http://www.semco.org**

E-mail: **semco@semco.org**

General information: (voice) answering device in Royal Oak **(248) 398-7560**

Your mailing label and membership card list the month and year your membership expires. Newsletters will not be sent after the month of expiration. Back issues may not be available. Renew your membership as early as possible.

This publication was created using Adobe InDesign CS2
donated by Adobe Systems, Inc.

It is highly likely that all of the readers of this column have at least some familiarity with Facebook. Facebook has become immensely popular, with over 1.1 BILLION registered users as of March 31, 2013. Facebook has become "the" place to post photos, news, opinions, marketing promotions, commentary, and other content. Once posted, the user can somewhat control who sees his content, primarily by restricting the content to selected individuals, friends, or the general public. Even though users may believe that by restricting access to their postings they are private, nothing posted on Facebook is really private. The simple and very common process of clicking on a "Like" button, or even viewing a new Facebook page, will provide data to Facebook and the people or companies that made the original posts. Facebook compiles this data for commercial purposes as well as to place targeted advertising on every Facebook page that a user views.

The old and often repeated adage, "Don't post anything on Facebook that you will later regret!" has been proven true countless times, as potential employers, law enforcement, pedophiles, scam artists, burglars, private investigators, insurance companies, college admission officers, and many others routinely search Facebook for materials of interest to them. Many people utilize Facebook as a real-time diary, posting their locations and activities as they occur. Law enforcement has warned that people posting that they are on vacation or at a
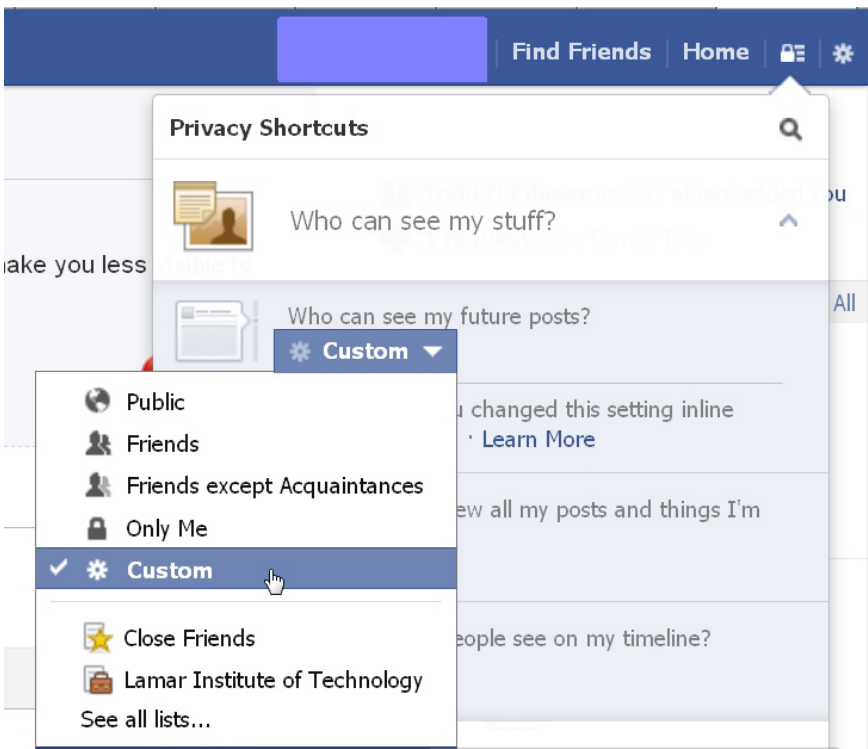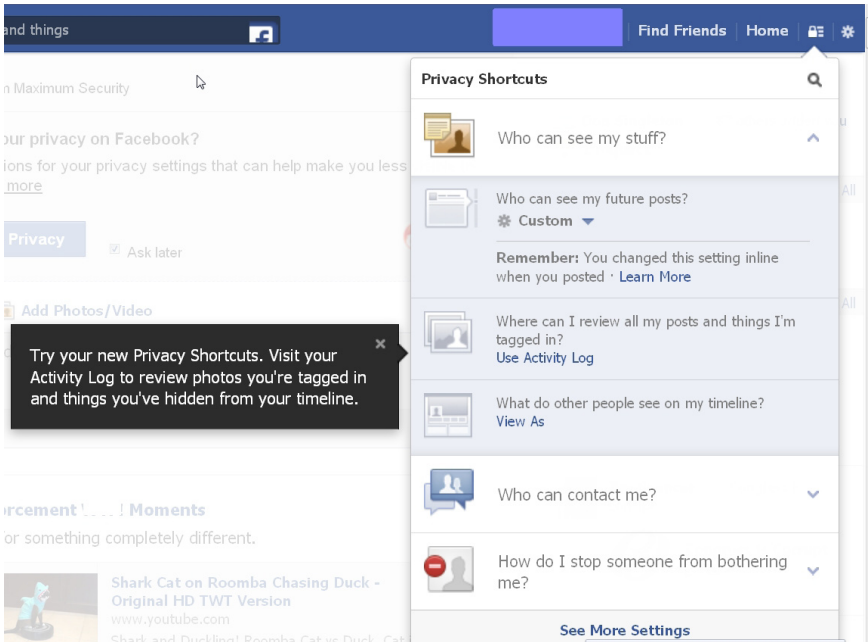
3

movie have returned home to find their abodes burglarized; the crooks found a Facebook posting that the person was away from home at that precise time, making the home that much more vulnerable to the robbers. According to a report " Facebook & your privacy; Who sees the data you share on the biggest social network?" published in the June 2012 issue of Consumer Reports magazine, "Some people are sharing too much. Our projections suggest that 4.8 million people have used Facebook to say where they planned to go on a certain day (a potential tip-off for burglars)." In a "turnabout is fair play," police have been known to create "bait homes" in order to attract the thieves, videoing them in the act of breaking in and robbing the bait house, and then arresting the miscreants at the scene with incontrovertible evidence of guilt. In that same issue of Consumer Reports was a revelation that even liking a Facebook page about medical conditions could create a "red flag" that may be detrimental to the user as, "…4.7 million "liked" a Facebook page about health conditions or treatments (details an insurer might use against you)."

Some pedophiles have found Facebook to be a fertile ground for victim acquisition. According to Facebook rules, children under the age of 13 may not register for an account, yet according to a May 2011 survey by Consumer Reports, there were 7.5 million children under the age of 13 who had Facebook accounts, with 5 million children under the age of 10 with accounts, a clear violation of Facebook's terms of services and policies. According to a Wikipedia article, "On April 15th, 2013 Facebook teamed up the Attorneys General, announcing it's <sic> alliance with the National Association of Attorneys General to help provide teens and parents more information on tools that can help manage profiles on Facebook. The partnership between Facebook and the Attorneys General will take place in 19 states."

Another risk faced by legitimate Facebook users is the fact that many Facebook accounts are outright fraudulent or fake, containing fake or duplicate profiles. In August 2012 Facebook announced that it had identified 83 million fake accounts, which was 8.7% of all Facebook accounts at that time. Many of these fake accounts were used for spamming or other illicit purposes, but many others were innocent violations of the rules by registering accounts in pets' names as well as other non-human monikers.

Much to its credit, Facebook has been making frequent and significant improvements to its privacy and security features. While several third party Internet security products offer to automate Facebook privacy features, Facebook has made it easy for users to set their own privacy settings. On the top-right corner of the Facebook page are two small icons; one looks like a small padlock with three lines on its right, and the other looks like a small gear or star. Clicking on one of these icons opens a variety of menu choices which include privacy settings. The padlock icon opens a menu "Privacy Shortcuts" including "Who can see my stuff?" "Who can contact me?" and "How do I stop someone from bothering me?" At the bottom of that menu is a link for "See more settings" which opens the comprehensive "Privacy Settings and Tools" page.

and things

Find Friends | Home

Maximum Security

Privacy Shortcuts   🔍

our privacy on Facebook?
ions for your privacy settings that can help make you less   Who can see my stuff?   ⌃
more

                          Who can see my future posts?
Privacy   ☑ Ask later   ⚙ Custom ▾

                          Remember: You changed this setting inline
🖼 Add Photos/Video   when you posted · Learn More

                          Where can I review all my posts and things I'm
Try your new Privacy Shortcuts. Visit your   ✕   tagged in?
Activity Log to review photos you're tagged in   Use Activity Log
and things you've hidden from your timeline.
                          What do other people see on my timeline?
                          View As

                          Who can contact me?   ⌄
rcement _..! Moments
or something completely different.
                          How do I stop someone from bothering   ⌄
Shark Cat on Roomba Chasing Duck -   me?
Original HD TWT Version
www.youtube.com   See More Settings

Find Friends | Home

Privacy Shortcuts   🔍

ake you less   isible to   Who can see my stuff?   ⌃

                          Who can see my future posts?
                          ⚙ Custom ▾

🌐 Public   u changed this setting inline
👥 Friends   · Learn More
👥 Friends except Acquaintances
🔒 Only Me   ew all my posts and things I'm
✓ ⚙ Custom
                          eople see on my timeline?
⭐ Close Friends
💼 Lamar Institute of Technology
See all lists...

5

Under the heading "Who can see my stuff?" are options for Friends, Public, Friends except Acquaintances, Only Me, and Custom. Considering my personal privacy, I mostly use the Custom setting for my posts, selecting which of my limited selection of friends can view a particular post. A

Facebook postings by reducing the number of new items displayed, and allows me better control of who can read my posts.

Clicking on the small gear icon on the top-right corner of the Facebook page directly opens the "Privacy Settings and Tools" page. In addition to the "Who
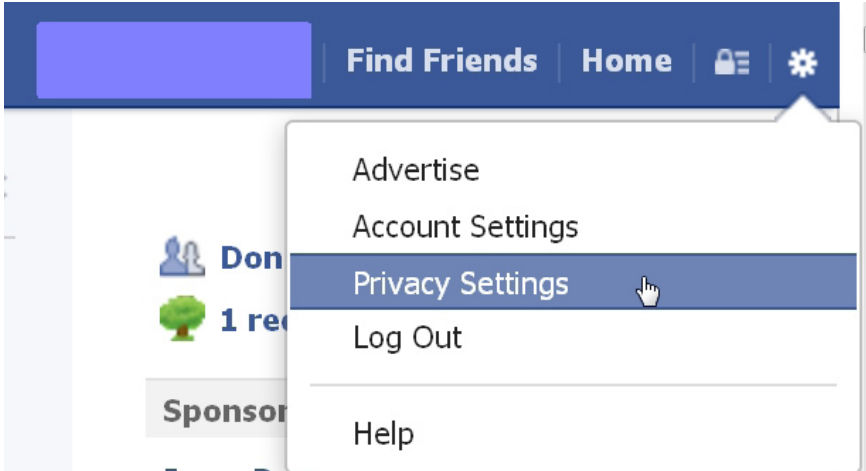
warning to many Facebook users is most appropriate here; while some users believe that having countless friends is a status symbol, it also dramatically increases privacy and security risks as friend requests are blindly honored. According to Consumer Reports (June 2012), 25% of users have falsified some of their personal information for the purpose of protecting their identities. Some unsavory individuals actually create networks of users that are used as references to deceive targeted users into accepting them as friends, as many times a "friend of a friend" is listed as the "bona fides" of a friends' request. Speaking only for myself, other than family, a few coworkers, and a few very close friends, I generally do not accept almost all of the friends requests received and "Likes requested" on Facebook; this makes it easier to read

can see my stuff?" control previously mentioned is a "Who can look me up?" selection. Under this heading are the self-explanatory privacy controls, "Who can look you up using the email address or phone number you provided?" and "Do you want other search engines to link to your timeline?" Since I have tightly controlled and limited my Friends list, I only allow my Friends to look up my e-mail address and phone number. As far as other search engines compiling my information, I selected the "Off" option, not wanting my Facebook information to be included in external search engines. On the left margin of this page are the other Facebook security and personalization controls. Under the Security selection are a variety of options; among the several settings available, I have selected to enable secure browsing.

The other security options easily allow the user to choose an appropriate level of security to meet his personal needs. One important setting to utilize is the "Blocking" selection in the left margin. This is where the user can manage who is blocked from contacting the user, sending invites or apps, and directly blocking unwanted applications (apps). Other personal settings can be accessed from the menu in the left margin.

Despite the ready availability and ease of implementing Facebook's privacy and security features, the June 2012 Consumer Reports article indicated that many users have not done much to protect their privacy. "Some don't use privacy controls. Almost 13 million users said they had never set, or didn't know about, Facebook's privacy tools. And 28 percent shared all, or almost all, of their wall posts with an audience wider than just their friends."

With over a billion of us using Facebook, it is inevitable that some less than scrupulous people will be on there with us. By setting our privacy and security settings to a relatively high level, some protection from those who may wish us ill is offered. At the same time, we must also be cognizant that Facebook routinely shares some of our information with others for commercial purposes. Facebook is a wonderful service, but always be aware of who may access your postings, and what others may post on your wall.

WEBSITES:

<https://www.facebook.com/help/privacy>.

<https://www.facebook.com/about/privacy/>.

<http://www.huffingtonpost.com/2013/04/25/facebook-privacy-audit_n_3153801.html>.

<https://en.wikipedia.org/wiki/Criticism_of_Facebook>.

<https://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm>.

<https://en.wikipedia.org/wiki/Facebook>.

<http://techland.time.com/2013/04/04/facebook-privacy-settings-guide/?hpt=hp_bn19>.

Ira Wilsker is a Columnist, The Examiner, Beaumont TX; Program Director of Management Development at the Lamar Institute of Technology, Beaumont TX; and a radio and TV show host. Contact him at <iwilsker@sbcglobal.net>.

Windows Lab
Avoiding Web Ads and Cookies
By Penny Cano

Web advertisements often take up half of the real estate on a webpage. Supposedly, they entice the viewer into buying the products. In actuality, they help to financially support the host website. Cookies, on the other hand, are outwardly invisible. They are put on your computer by websites to identify you. There are good cookies and bad cookies. A secure website (bank, credit card, prescription order, etc.) requires a cookie (good) on your computer to verify your identify. You cannot use the website unless you have their cookie. Public, retail, and other non-secure sites put tracking cookies (bad) on your computer to do things like determine which websites you frequent so they can customize all those ads to what they believe are your interests. Personally, I like to avoid both intrusions. Here is how it can be done on the two browsers I use, Internet Explorer and Firefox.

Firefox is the easiest because there are add-ons you can download and install from. On the Firefox toolbar, select Tools/Add-ons/ Get Add-ons. Mozilla.org/

The two I find most useful are Adblock Plus and NoScript. Adblock Plus doesn't require setting changes other than to be sure the updates are automatic. NoScript installs easily, but it takes some personal interaction to make it work to your advantage. Many ads on websites use Java script, Flash player, or other tools for the animation. NoScript gives you the option to choose which of these scripts you want to allow.

If an unknown script is attempting to execute, there is a yellow warning bar at the bottom of the Firefox window. Pressing the small "S" in the lower right corner of the status bar pops up a menu that allows you to trust (permit) scripts or block them. Usually I make "Untrusted" websites with "ads" (msads.net, adrevolver.com) or "click" (doubleclick.net), etc., in their name. If you make a mistake and block something you need, you can always press the "S" button and go back and "Trust" the script.

The third Add-on I find useful is BetterPrivacy which lets you choose which cookies to accept or deny. The same rule applies in choosing which website's cookies to accept—deny "ads," "track," "click," etc; accept "Discovercard," "Chasebank," and the like. Internet Explorer provides more of a challenge to block ads and cookies. I have not found an Add-on for IE that allows you to choose which scripts are allowed or blocks ads and tracking cookies on a wholesale basis. So it takes more effort on the user's part to accomplish the same thing. Somewhere

in the IE settings there is a check box that says to tell websites you do not want to be tracked. But many of the websites do not honor this.

Also, you can use InPrivate Filtering ("Safety" button under "Tools" on the menu) to block some sites. The most effective way I have found to block ads in IE is not in the IE settings. I use the Parental Control settings in my Virus/ Internet Security suite. I use TrendMicro Titanium Internet Security. Under Parental Controls, I block the general category of "Web Advertisement," but that doesn't get everything.

There is also a section of the Parental Controls that blocks individual websites. The same rule applies here as in Firefox—if the name includes "ads," "click," etc., it's usually a "Block."

Cookie blocking can be done with IE settings under Tools/Internet Options on the menu or the Internet Options icon in the Control Panel. Initially, it is a pain in the neck, but worth it in the long run. On the Privacy tab choose the "Sites" button. If you already know the name of the website whose cookie is to be blocked, you can enter it and choose "Block."

If the website doesn't work right without the cookie, you can always come back and remove the block. The next part can be annoying at first. On the Privacy tab choose the "Advanced" button. Check the box to "Override automatic cookie handling" and mark "Prompt" for First-party and Third-party cookies. Now, each time a website tries to put a cookie on your computer, a Privacy Alert box will pop up. Hit the "Block" button.

They are persistent and may try 20–40 times before the website loads. But if you can do everything you need

to do while denying the cookies, the next time you visit the website and the box pops up, you can check the box that says "Apply my decision to all cookies from this website." Then when you choose block, the website is added to the "Sites" list and you won't get the alert again. If you do this, after a while you will get few alerts and the cookies will automatically be blocked.

Penny Cano <ccnewsletter (at) cox. net> is a member of the Cajun Clickers Computer Club <http://www.clickers. org> and an Instructor for the Dumb & Dumber Workshops. This article first appeared in the November 2012 issue of Cajun Clickers Computer News.

Secure and Keep Track of Your Passwords for Free By Ira Wilsker

Let's face it; most computer users are inherently lazy. In order to make things easy on ourselves we often use the same simple password on multiple websites and devices, or we use the most simple passwords such as "password" or "12345." According to computer security experts who have analyzed millions of purloined passwords, too many of us are using simple passwords that are easy for others to guess, and then access our most intimate or personal data in order to commit identity theft or other forms of computer crimes against us, including industrial espionage.

Last fall, a purveyor of password management and security software, SplashData, published their annual list of the 25 worst passwords of the year, "SplashData's top 25 list was compiled from files containing millions of stolen passwords posted online by hackers. The company advises consumers or businesses using any of the passwords on the list to change them immediately.

#	Password	Change from 2011
Presenting SplashData's "Worst Passwords of 2012":		
1	password	Unchanged
2	123456	Unchanged
3	12345678	Unchanged
4	abc123	Up 1
5	qwerty	Down 1
6	monkey	Unchanged
7	letmein	Up 1
8	dragon	Up 2
9	111111	Up 3
10	baseball	Up 1
11	iloveyou	Up 2
12	trustno1	Down 3
13	1234567	Down 6
14	sunshine	Up 1
15	master	Down 1
16	123123	Up 4
17	welcome	New
18	shadow	Up 1
19	ashley	Down 3
20	football	Up 5
21	jesus	New
22	michael	Up 2
23	ninja	New
24	mustang	New
25	password1	New

Even though each year hacking tools get more sophisticated, thieves still tend to prefer easy targets, Slain (SplashData CEO) said. "Just a little bit more effort in choosing better passwords will go a long way toward making you safer online." (Source: <http://www. splashdata.com/press/PR121023.htm>). According to SplashData, the top 10 of the 25 most commonly used passwords (a fact not lost on hackers and crackers) are: password, 123456, 12345678, abc123, qwerty, monkey, letmein, dragon, and 111111.

Despite countless news stories in all of the media about password security, as well as the expanding requirement by many websites that only complex passwords that meet strict standards can be used, millions of users have not learned that painful lesson. In 2009, following a hack at the popular social gaming network RockYou.com, a staggering 32 million user passwords were published. A cyber security company, Imperva Application Defense Center, analyzed these 32 million passwords, and found that users overwhelmingly preferred simple, easy to remember passwords. In the analysis, it was noted that almost a third of RockYou users used short, under six character passwords, a password length that has such a finite list of combinations, it is easy for hackers to use any of several utilities to crack these passwords using a brute force or dictionary technique. In the same study, it was found that about 60% of users had passwords using a limited set of alpha-numeric characters, another easy to crack security problem. Almost half of users used slang, dictionary words, names, or so called "trivial passwords" consisting of consecutive digits or adjacent keyboard keys. The

Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Rank	Password	Number of Users with Password (absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

most common password used, "123456" (used by 290,731 RockYou users), is the same "most common" password noted in other studies of common passwords.

Studies of other massive password thefts, including the six million passwords stolen from LinkedIn, Last.fm and eHarmony revealed a somewhat similar distribution of easy

Password Length Distribution

Source: Tom's Hardware

- Only upper case
- Only lower case
- Only numeric
- Mixed letters and numeric
- Contains special characters

3.81% 1.62%
36.94%
41.69%
15.94%
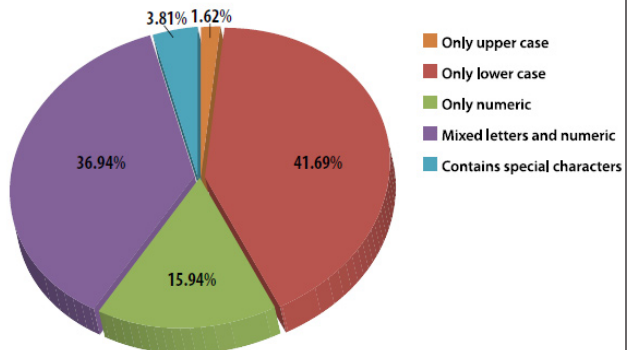
and vulnerable passwords. The security company ESET analyzed these 6 million passwords, and found that the top 5 of the 25 most widely used passwords were password, 123456, 12345678, 1234, qwerty, and 12345. ESET also warned that stealing a common password, especially simple numeric passwords can also open the unknowing victim to a variety of other criminal attacks, including ATM theft (many people use the same four digit password as their ATM PIN), "…digital locks and keypads, handheld authentication devices like an RSA or Digipass token, or a software implementation on a mobile device (such as) authentication via laptops, netbooks, tablets and smartphones."

SplashData, Imperva, ESET, and other security companies and services, have widely published a short list of hints and tips about creating more secure passwords that will be difficult to crack. These security recommendations for secure passwords are substantially identical from the different sources, and generally include the following:

1. Use a password with a minimum of eight characters, including both alphabetical (mixed upper and lower case letters) and numerical characters. Many websites also allow the use of punctuation and other symbols as a part of the password; this makes cracking much more difficult. Some password experts suggest using short words with spaces or characters separating the words and maybe a number, such as "i_lOVe-TeXas!0518". Bruce Schneir, a respected cryptographer, computer security specialist, and writer has proposed this novel idea to create an easy to remember but secure password, "Take a sentence and turn it into a password. Something like "This little piggy went to market" might become "tlpWENT2m". That nine-character password won't be in anyone's dictionary."

2. Never use the same password on more than one website. Hackers and crackers have often found that a user's e-mail address or username and password stolen from one popular website will often work perfectly on other popular websites, making identity theft, financial fraud, espionage, and other malicious activities easy to accomplish. When signing up on a new website, never use an already used password; some scam and phishing (identity theft) websites purposely harvest passwords from new registrants for the explicit purpose of using them on other websites. Bruce Schneir recommends, "If you can't remember your passwords, write them down and put the paper in your wallet. But just write the sentence —or better yet—a hint that will help you remember your sentence."

One of the widely used excuses for not creating complex, hard to crack passwords is that these complex passwords are too hard to remember. Another common excuse given is since most computer users utilize a large number of online services that require usernames and passwords, there are just too many different passwords to remember. In order to have the security of unique and complex passwords for each website along with the convenience of a written password listing, several software authors and publishers have created a class of software generically called "password managers." The

password managers are readily available as both free or commercial products, and are widely available for download or purchase. Many of the comprehensive security suites are now also including a dedicated password manager, as exemplified by TrendMicro's Titanium Maximum Security suite, which includes as one of its components, TrendMicro's "DirectPass" password manager.

Gizmo's popular freeware rating and evaluation service, <http://www.TechSupportAlert.com>, has reviewed and rated many of the password managers and posted the results online at <https://www.techsupportalert.com/best-free-web-form-filler-password-manager.htm>. Gizmo gave its highest 10 Star rating and its "Best Product In Its Class" award to LastPass <https://www.lastpass.com>, the password manager that I have been using for several years. LastPass can safely store passwords "in the cloud" using the same grade of encryption as used by the military (a concern of some users), is accessible from any computer or smart device, works automatically with almost all modern web browsers (Internet Explorer, Firefox, Chrome, Opera, and Safari), and runs on most major operating systems including Windows, MAC, and Linux. For most users, the totally free version of LastPass is feature rich and is totally satisfactory; for those who desire some additional features, including the portable version of LastPass for use on a variety of smart devices including iOS, Symbian, Blackberry, and Android, the premium version of LastPass is $12 per year. LastPass can automatically fill forms with username and password, fill in personal data on applications and delivery instructions,

and provide a host of other services. LastPass will also intelligently capture newly created or changed usernames and passwords from each website visited. Personally, I have been totally satisfied with LastPass.

Gizmo also highly rated the limited free version of RoboForm (only tracks 10 to 30 passwords), and the totally free, unlimited use, password managers KeePass <http://keepass.info> and PasswordSafe <http://passwordsafe.sourceforge.net>. The free unrestricted versions of LastPass, KeePass, or PasswordSafe will each securely store and manage an unlimited number of passwords. Each utility has some different features, as enumerated by Gizmo in the ratings. While all of these will perform a most satisfactory job managing passwords, my personal favorite in the group is still LastPass. **One warning** about any of the password managers, free or commercial; all of them require a password to access the database created by the user. Be absolutely sure to create a unique and complex password to open the password manager, and do not use this opening password in any other manner or on any other website! Using one of these password managers only requires that the user remember a single complex password, negating the excuse that there are too many passwords to remember when using a different password on each website. It would also be a good practice to frequently and regularly perform a security scan with a good quality third-party malware scanner such as MalwareBytes <http://www.malwarebytes.org> or SuperAntiSpyware <https://www.superantispyware.com> in order to verify that no keyloggers have infected

the computer. If a keylogger is detected, it does not matter which, if any, password manager is used, it will become immediately necessary to change all of your passwords.

Creating and using strong and complex unique passwords for each website, and managing them with a good quality and secure password manager will dramatically help to improve our personal level of cyber security.

WEBSITES:

<http://www.splashdata.com/press/PR121023.htm>.

<http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf>.

<http://blog.eset.com/2012/06/07/passwords-and-pins-the-worst-choices>.

<http://www.zdnet.com/blog/security/25-most-used-passwords-revealed-is-yours-one-of-them/12427>.

<https://www.techsupportalert.com/best-free-web-form-filler-password-manager.htm>.

<https://www.techsupportalert.com/content/how-choose-strong-password.htm>.

<https://www.techsupportalert.com/content/how-keep-your-passwords-safe.htm>.

<https://lastpass.com>.

<http://keepass.info>.

<http://passwordsafe.sourceforge.net>.

Ira Wilsker is a Columnist, The Examiner, Beaumont TX; Program Director of Management Development at the Lamar Institute of Technology, Beaumont TX; and a radio and TV show host. Contact him at <iwilsker@sbcglobal.net>.

Q. What are some ways I can customize my Windows 7 computer?

A. Windows 7 provides the greatest number of ways to customize or personalize your computer that Microsoft has given us so far and I will share a bunch of them with you now. Many of the customization options can be reached just by right-clicking on your desktop and selecting the Personalize option.

Q. Change the theme—desktop background, window color, sounds, and screen saver all at once.

A. Right click in a blank space on the desktop of Aero themes (transparent), then click Personalize for a selection of Basic and High Contrast themes. Click on a set of pictures in Aero and there will be an interesting slide show of architecture, art, cartoon characters, landscapes, or nature. You can deselect any of the pictures you don't want to be included in the show. You can also change the length of time between picture change.

Click on Get more themes online to select additional themes. Don't forget to click on Save theme and give it a name.

Q. Change the desktop or select a picture for your desktop.

A. Find the pictures that you want to include in your slide show. All of the pictures must be located in the same folder. Click on one picture, press and hold the Ctrl key on the keyboard and select additional pictures to create a slide show. Select the amount of

13

time between picture changes, the position, and click Save Changes.

Some folks like to set up a series of personal pictures as a slide show and use their computer monitor as a digital picture frame.

Q. Change only the Window colors (borders, Start menu and taskbar)

A. At the bottom of the Personalization window, click the Window Color icon. Click on a color and adjust the Color intensity with the slider bar. If you want to save energy, uncheck Enable transparency. Click Save Changes.

Q. Change sounds.

A. Clicking the down arrow beside the name of a Sound theme lists about 16 different themes. Click on the name, then under Program Events, where there is a speaker icon, there is a sound associated with it. I click on Exit Windows because it has a longer duration, and click the Test button to hear the associated sound. If you don't hear anything, check the speaker icon on the Notification bar to see if the sound is turned down or muted. When you're satisfied, click OK.

Q. Change Screen Saver.

A. Under Screen Saver, click the down arrow to see options. It's no longer necessary to have a screen saver to protect the monitor. Click OK.

Along the left side of the Personalization page are links to more customizations.

Q. Change Desktop Icons.

A. Click on Change desktop icons. The first option lists five icons that you may choose to show on the desktop or NOT. Click the checkbox(es) for icons you want to show. Clicking the Change icon button allows one to select a different icon or browse for a new one. Click OK.

Q. Change Mouse Pointers.

A. Clicking this link opens the Mouse Properties Window with six tabs. The Buttons tab allows two main changes: Right-handed to left-handed and Double-click speed—click & drag the marker on the slider bar and check the speed by double clicking on the manila folder—when it opens, you've used the correct speed.

Tab 2. Pointers, lets one choose a scheme that affects all the pointers or Customize that allows the change of one or more cursors. For a scheme, I most often choose Windows Inverted (extra large) (system scheme). If you want a big red pointer, go to <http://www.philip-henderson. co.uk/R_download/red_right_lrg. shtml.>

Tab 3. Pointer Options, lets one select a Pointer Speed, Snap To the default button in a dialog box, Display pointer trails, Hide pointer while typing, and Show location of pointer when Ctrl key is pressed.

Tab 4. Wheel, sets the number of vertical lines to scroll when the wheel is rolled one notch or one screen at a time, and if the mouse has horizontal scrolling capabilities, how many characters to move at a time.

Tab 5. Hardware, shows what pointing devices (touchpad, mouse, trackball, etc.) are installed on the computer.

Tab 6. Device Settings, allows disabling or enabling of the Touchpad. Click OK.

Q. Change Account Picture.

A. Whether it's an Administrator account or a Standard account, you can change the picture you see when

14

you log in and/or open the Start Menu. Clicking on a picture or Browsing in your Pictures Library and clicking on a picture changes the account picture.

Q. Display.

A. Allows one to change the size of text and other items on the screen by clicking in a radio button: Smaller (100%), Medium (125%), and Larger (150%). Laptops may have only two choices.

Q. Change Taskbar & Start Menu.

A. The Taskbar and Start Menu Properties window has three tabs: Taskbar, Start Menu, and Toolbars. Under the Taskbar tab, Click checkbox(es) for Lock the taskbar (so it stays docked),

Auto-hide the taskbar (so it disappears when you don't need it, but pops up when the mouse pointer is in the area), and Use small icons.

Click on the down arrow to select a different Taskbar location. I keep mine at the bottom.

Click on the down arrow for the Taskbar buttons. Choices are: Always combine, hide labels; combine when taskbar is full; and Never.

I have my computer set to Always combine because it lets you preview the open windows with Aero Peek. (Hover over an icon and thumbnails of the open windows will pop up for your selection.)

Click the Start Menu tab to customize how links, icons, and menus look and behave on the Start Menu. Click Customize. Some items such as Computer, Control Panel, Documents, etc. have three options: Display as a link (Opens the specific window), Display as a menu (Lists the files for individual selection), and Don't display this item (Don't show it on the Start menu.) I have selected "Display as a link" or "Don't display this item" for most. Click OK.

Power Button Actions (Same as clicking the down arrow beside Shut down), NOT THE ON BUTTON: Shut down, Hibernate, Sleep, Restart, Lock, Log off, Switch User. I leave mine on "Shut down." Click OK.

Q. Ease of Access Center.

A. The Ease of Access Center is especially helpful for users with vision problems (including blindness) or difficulties using the mouse or keyboard. It includes:

1. A Magnifier that enlarges up to 1600% by clicking the Plus (+) key on the screen. Decrease by clicking the minus (–) sign.

2. A Narrator that reads to you, echoes user's keystrokes, and announces System Messages.

3. An On-Screen Keyboard is used by mouse clicking or touchpad rather than the keyboard.

4. Choose a High Contrast theme for ease of reading.

Q. Side-by-side split screen.

A. With two windows open in un-maximized (restore down) positions, press and hold the Windows key and press and release the Right Arrow key to send one window to the right. Click on the other window and press and release the Left Arrow key to send that window to the left.

Mary Phillips <mary (at) iconusersgroup.org> is Secretary of the ICON Users Group, MO. <http://www.iconusersgroup.org>. This article first appeared in the December 2012 issue of The ICON.

I have been playing with my new ASUS Transformer Infinity TF700 Android (Jelly Bean 4.1.1) Tablet for a few weeks now and love it. I have also been comparing it to my borrowed iPad 2, and functionally I see few major differences. But one difference does show up. The iPad 2 has a 3 row on-screen keyboard that you must toggle to get to the number keys.

The TF700 has a 4 row on-screen keyboard with the numbers always present in the main mode. For me, the 4 row keyboard is a big advantage. It makes entering data and phone numbers much easier. But when I write a longer e-mail or memo, I still long for a real keyboard. Hence, I began a search for a reasonably priced, well rated, lightweight travel keyboard that I might use occasionally.

My first look was the Kensington Bluetooth keyboard and travel folio case for my borrowed iPad 2. That worked well with the iPad 2, and I could also easily mate it to the ASUS TF700. That taught me an important lesson; Despite being marketed as an iPad keyboard, it also worked well with an Android device. I cruised a few websites and determined that this was a fairly general phenomenon. But these are in the $60–$80 range, and given the excellent on-screen keyboard I already had, that was more than I wanted to spend. Also, since the keyboard would only be used occasionally, I did not want the full time weight or bulk of a keyboard built into the carrying case.

My next step was to ask around and do web searches. It appears that the Logitech 920-003390 Bluetooth keyboard is extremely well rated. I saw one at a club meeting, and it looks well built. People seem to really like it, but for my purposes it is large, and also runs around $50.

I also looked at rollup keyboards, but their reviews are poor, and I did not like their typing feel. I looked at the ASUS mating keyboard for my Transformer tablet, but it is expensive and heavy. I could have used a wired USB keyboard (an old USB PC keyboard worked well in a test), but I ruled that out. There are also 2.4 GHz keyboards that use a separate radio dongle, but my tablet has Bluetooth built in, and I did not want to tie up its USB port with another dongle.

Then, as I usually do when I'm stumped, I devoted the better part of a Sunday afternoon to surfing the web looking for alternatives. After a while I began to notice a keyboard that went by several names at several prices, but appeared to be the same device. I even found a YouTube video showing someone installing and using it at <http://www.youtube.com/watch?v=bLYgofpGKHA>.

The reviews I read about it were favorable by a large percentage. Best of all, it was under $20 and available from Amazon. (I usually find that when something is on Amazon and has accumulated a few dozen favorable reviews over a period of months, that there is a good chance that it is not a shoddy product.) Anyway, at under $20 delivered, it was worth taking a chance.

The picture shows the keyboard. As I mentioned, it is sold under various

names including Sanoxy and Anker. Mine was advertised as a Sanoxy Bluetooth Keyboard for iPad on Amazon—at a cost of $13.50. (I have seen it advertised for over $30 on some sites.) Of course, the box it came in had neither name, but it was the same device. The unit is all plastic, but looks and feels like a much higher priced Apple keyboard. It is advertised to have Apple function keys, but I did not test those, since my plan was to use it for my Android tablet.

The keyboard arrived in about 3 days, and worked with my Android tablet directly out of the box. It runs on 2 AAA cells, which I prefer, since I did not want to have to discipline myself to recharge yet another device. (We shall see how long the batteries last, but at least it is easy to carry or buy spares.) The battery box underneath at the rear provides a wedge to hold the keyboard at a good typing angle.

The unit arrived with no instructions, but I just followed the general Bluetooth mating steps for the Kensington unit, and it worked fine. (Especially after I remembered to un-mate the Android Tablet from the Kensington keyboard first!) The keys are well spaced and have a very nice feel to them, with a silent click and a satisfying displacement. They work about as well as my main home computer keyboard. I would say that typing a several page memo on this would not be a chore at all. However, since the on-screen tablet keyboard is quite good for a few sentences of e-mail, this unit will stay in my suitcase most of the time, only coming out when there is a lot of typing to do.

Some of the function keys (meant for Apple) also work on the Android tablet (e.g. home, media player controls,

sleep). Others are still a mystery. As you can see from the YouTube video mentioned above, this keyboard can also mate with a phone.

The picture below (taken away from my cluttered desk) shows the setup I use for heavy typing and spreadsheet work when I travel. It shows the relative size of the keyboard and 10.1" tablet, as well as the tablet case set up in a vertical position.

Most of the time I use the tablet in a "Couch-Pad" mode in the TV room or an airport waiting room to do simple e-mails, web searches, and reading the newspaper. In that case, the on-screen keyboard is fine. But at only $13.50, it is nice to have a second option as well.

This now rounds out my high powered, low cost travel computing system including:

- ASUS Infinity TF700 32 GB 10.1" Android (Jelly Bean 4.1.1) Tablet (Currently $428 on Amazon).
- Included Power Adapter for above
- Poetic Slimbook Leather Case for Above ($12.95).
- Generic Stylus ($1.00).
- ASUS USB Adapter for Tablet ($13.95).
- Bluetooth Keyboard for Tablet (per this article) ($13.50).
- Misc. Cheap Generic Micro SD cards and USB sticks to plug into Tablet.

Steve Baer <baer (at) ieee.org> is a member of the Hilton Head Island Computer Club, NC <http://www.hhicc.org>. This article first appeared in the December 2012 issue of Island Computing.

BOARD MEETING
May 12, 2013
Carol Sanzi

Board Members Present:
President Mike Bader, Vice President Richard Jackson, Secretary Carol Sanzi, SIG-Advice Chairman Franz Breidenich, and Members-at-Large Bob Clyne and Richard Fink. The board meeting was called to order at 12:07 p.m.

Old Business

Carol Sanzi gave the treasury report for Brian Brodsky. The current treasury amount equaled a total of $9,001.45 with $4,240.96 in the checking account and $4,760.49 invested in three Certificates of Deposit. The membership currently is 70. It is time for Dan Diebolt, Keith Kossuth, and Sikander Rashid to renew their memberships.

Bob Clyne stated that the SEMCO meeting was announced on the Internet Adviser radio program. Mike Bader made contact with the station requesting the promotion.

Bob Clyne explained that there has been a problem with the database for renewals. The problem occurred in how the expiration date was entered. Hopefully, the error has been corrected and members will receive a timely renewal notice. Richard Jackson will try to make contact with those members whose membership has expired.

New Business

Bob Clyne requested that the board go into executive session. A discussion took place. The Board exited executive session.

Bob Clyne moved for the approval of the budget as presented. A discussion about income, expenditures, dues, magicJack, and membership took place. Richard seconded the motion and it was carried.

Bob Clyne moved to adjourn at 12:35 p.m. Richard Jackson seconded the motion and it was carried.

SPECIAL INTEREST GROUPS (SIGS)

SIG-COMPUTING
Tom Callow

June 9 1:45 p.m.: Organizing and Protecting Your Hard Drive: In this webinar, presented by Gene Barlow of User Group Relations, two topics will be covered. The first topic is how to better organize your hard drive to make it more beneficial to you. The second topic is how to protect your hard drive from failure and crashes. Finally, a free software product will be given to each attendee that will monitor the workings of their hard drives.

SIG-LINUX
Brian Brodsky

June 25 (Tues.) 6:45 p.m.: Managing Software on Ubuntu & Command Line Interface (CLI) Commands: SIG-Linux chairman Brian Brodsky will discuss how to install software on Ubuntu and how to keep it up to date. Then Brian will lead the group's continuing exploration of command line interface commands. **Where:** At the home of Richard Jackson, 10495 Kingston, Huntington Woods, MI 48070. Call Richard at (248) 546-3694 for Directions.

SIG-TECHNIQUES
Chairman Needed

June 9 3:45 p.m.: Voice Recognition—Is it good enough?: SIG-Computing Chairman Tom Callow will talk about the developments in voice recognition software since 2008 and will demonstrate Dragon NaturallySpeaking Premium 12.

SIG-PROGRAMMING
Richard Jackson

June 15 2:00 p.m.: Visual Basic 2010 Express: Chapters 3 and 4 and the associated programing exercises of the book "Microsoft® Visual Basic® 2010 Step by Step" (held over from May). **Where:** At the home of Richard Jackson. Contact Mr. Jackson for full details: (248) 546-3694.

SIG-ADVICE
Franz Breidenich

June 4 & July 2 (Tues.): 5:30 p.m.: General discussion. At the Madison Heights Library located at 240 West 13 Mile Rd. one block West of John R. The parking lot entrance is off Brush St. The lot and entrance to the library are located on the north side of the library.

Bob Clyne
clyne@mich.com
(to post monthly computer group info)

**CALENDAR-OF-EVENTS
OTHER GROUPS**

COMP (Computer Operators of Marysville & Port Huron)
June 5, 7 p.m. Acheson Community Resource Center, 514 McMorran, Port Huron, MI Jane Wheatly 810-982-1187 or Pam Raisanen E-mail info: <bwcompinfo@gmail.com>. Web: <http://www.bwcomp.org>. Topic: Tech Toys.

DITUG: Detroit IT User Group (Formerly Focus: Hope IT User Group)
1400 Oakman, Detroit, MI. 48238. Web info <http://www.ditug.org/>. See web sites for details. Pre-registration required.

HUG (Holly User Group)
June 8, 9 a.m.–noon (2nd Saturday) Groveland Twp. Fire Hall, 3085 Grange Hall Rd. & Dixie Hwy., Holly, MI. 48442. Ron McCauley 810-629-9683. Topic: TBA.

MacGroup-Detroit
June 30, 3:00 p.m., Birmingham Temple, 28611 West 12 Mile Rd., Farmington Hills. Info: Terry White, <terry@macgroup.org> or 248-569-4933. <http://www.macgroup.org>. SIGs: 2:00 PM. Topic: Adobe Creative Cloud—What's New.

MacTechnics, (MAC User Group)
June 15, See web site for topic, meeting time and location. <http://www.mactechnics.org>. JoAnn Olson at 248-478-4300. Topic: TBA.

MDLUG (Metro Detroit Linux User Group)
June 8. 12, 12:00–3:00 p.m., (2nd Saturday); Check web site for location. Web: <http://www.mdlug.org>. Topic: TBA.

Motor City Free Geek
Every Saturday 1 p.m. to 5 p.m. 1511 Jarvis St. Suite #10, Ferndale, MI 48220. <http://www.motorcityfreegeek.net>. E-mail: <MotorCityFreeGeek@gmail.com>. Recycling & Open Source.

MUG (Michigan User Group)
June 11, 6:30 p.m., (2nd Tuesday): Farmington Community Library-Main Branch, 32737 W. 12 Mile Rd., Farmington Hills, MI. 48334. <http://www.mug.org>. Topic: TBA.

Oak Park Computer Club
Every Fri., 10:30 a.m. at Panera Bread—in the Cornerstone Mall (on the west side of Greenfield, south of Mt. Vernon) just north of Kroger. Including Q&A.

Royal Oak Computer Club
Every Wed., 12:30 to 2:30 PM at Mahany/Meininger Senior Community Center, 3500 Marais Ave., Royal Oak, 48073. Near Crooks & 13 Mile. Guest speakers & regular monthly speakers. <http://tinyurl.com/royaloakcc>.

SHCC (Sterling Heights Computer Club)
June 4, 7:30 p.m. (1st Tues); Macomb Community College South Campus, Bldg. K, 14500 E. 12 Mile Rd. Don VanSyckel <Don@VanSyckel.net>, 586-731-9232; Web: <http://www.SterlingHeightsComputerClub.org>. Topic: Inner Workings of a PC.

SEMCO

Serving the needs of professionals, hobbyists, novices, and prospective computer users since 1976.

* Learn more about computing in an informal, non-academic setting.
* Get honest answers to computer questions without commercial bias.
* Meet and interact with other computer users. Personal and electronic networking.
* Gain access to members willing to provide help in response to a phone call or e-mail.
* Receive monthly newsletter with informative articles.

MAY REFRESHMENT DONORS
Coordinator: Richard Jackson
Donors:
Bob Clyne
Carol Sanzi
Ken Phillips

COMPUTER RESOURCE PEOPLE

This is a list of people willing to be resources for other members to call when they have hardware or software questions.
Are you willing to help members learn?
Which software programs are you familiar enough with?
It is not necessary to be an expert, but just have some familiarity with the program and be willing to help someone starting to learn it. Please give this some thought and volunteer at the next group meeting.

Almost Anything: Vander-Schrier	**MS Office for Windows:** Callow
AutoCAD: Comptois	**MS Word:** Clyne
Genealogy: Cook	**Networking:** Callow
IBM PC Hardware Issues: Clyne, Yuhasz	**Novell Netware:** Yuhasz
Operating Systems: Callow, Clyne, Yuhasz	**Quicken:** Clyne
MAC Hardware and OS Issues: Yuhasz	**Geocaching:** Cook
Security: Bader	**Relational Database Programming**: Lis

Bader, Mike—586-447-6683, 9am–8pm................... mdbader@flash.net
Callow, Tom—248-642-5770, 9am–5pm................. tcallow@monaghanpc.com
Clyne, Bob—810-387-3101, 9am–10pm .... clyne@mich.com
Comptois, Jerry—248-651-2504, anytime
Cook, Stephen—313-272-7594, eves....................... scook48227@ameritech.net
Lis, Bernie—248-669-0101, 10am-8pm .... BerlLis@comcast.net
Vander-Schrier, Jack—586-739-7720,12–8pm .... jvanders@comcast.net
Yuhasz, Steve.. Help@yuhasz.org

21

SEMCO CALENDAR
Engineering Society of Detroit
20700 Civic Center Dr., Suite 450, 4th Floor
Southfield, MI. 48076
42° 29' 7" N by 83° 14' 29" W

June 9—SUNDAY (Meet 2nd Sunday)

**SEMCO Board Meeting at 12:00 noon. For Officers and SIG Chairpersons.
Other members are invited to attend.**

SEMCO General Meeting at 1:30 p.m.

Special Interest Groups (SIGs)

SIG-COMPUTING, 1:45 p.m.: Organizing and Protecting Your Hard Drive: In this webinar by Gene Barlow of User Group Relations, two topics will be covered: (1) How to better organize your hard drive. (2) How to protect your hard drive from failure and crashes. A drive monitoring program will be given to each attendee.

SOCIAL PERIOD, 3:15 p.m.: Refreshments! (Reminder: Keep it neat & tidy.)

SIG-TECHNIQUES, 3:45 p.m.: Voice Recognition—Is it good enough?: SIG-Computing Chairman Tom Callow will talk about the developments in voice recognition software since 2008 and will demonstrate Dragon NaturallySpeaking Premium 12.

SIG-PROGRAMMING, June 15 (Sat.) 2:00 p.m.: Visual BASIC 2010 Express: Chapters 3 and 4 and the associated programing exercises of the book "Microsoft® Visual Basic® 2010 Step by Step" (held over from May). **Where:** At the home of Richard Jackson. Contact Mr. Jackson for full details: (248) 546-3694.

SIG-ADVICE, June 4 & July 2 (Tues.) 5:30 p.m.: General discussion. At the Madison Heights Library located at 240 West 13 Mile Rd. one block West of John R. The parking lot entrance is off Brush St. The lot and entrance to the library are located on the north side of the library.

SIG-LINUX, June 25 (Tues.) 6:45 p.m.: Managing Software on Ubuntu & Command Line Interface (CLI) Commands. Where: At the home of Richard Jackson, 10495 Kingston, Huntington Woods, MI 48070. Call Richard at (248) 546-3694 for Directions.
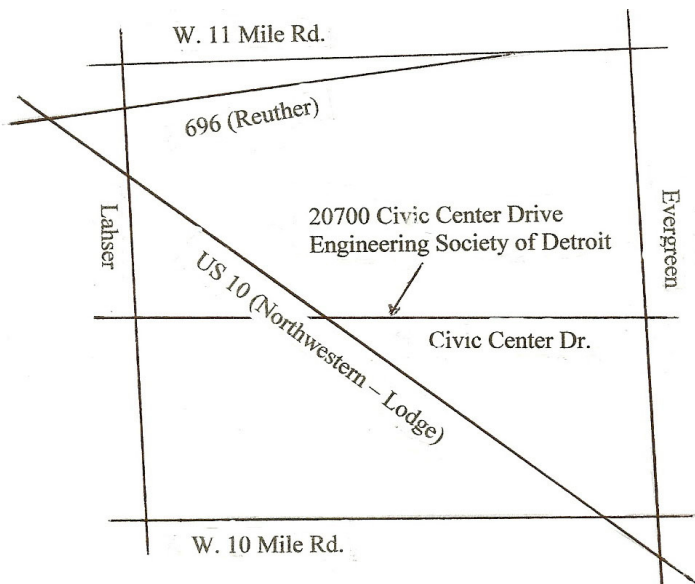
July 14—SEMCO Sunday.

http://www.semco.org
PUBLIC INVITED
22

SEMCO Meetings at [Engineering Society of Detroit](#)
20700 Civic Center Drive, Suite 450, 4th Floor
Southfield MI 48076.
42°29'7" N by 83°14'29" W

From I-696 exit at Evergreen. Take Evergreen south to Civic Center Drive. Civic Center Drive is about halfway between I-696/Eleven Mile Rd. and 10 Mile Rd. Turn west, right if you are coming from the north, onto Civic Center Drive. Follow Civic Center Drive, watching the number signs on the right. When you get to the 20700 sign turn right, north, and follow the drive until you arrive at the southwest corner of the brown building with the Engineering Society of Detroit sign near the top. Turn right, east, and go past the front of the building. When you reach the end of the building, turn left, north and go to the back of the building and turn left, west, again. The parking lot will be on your right. The entrance is in the center of the building. Park in back of building. Enter the rear door. The ESD office is on the fourth floor.

THE ENGINEERING SOCIETY OF DETROIT®
FOUNDED IN 1895
Affiliate Society

APCUG
Member of

SouthEastern Michigan
Computer Organization, Inc.
P.O. Box 707
Bloomfield Hills, MI 48303-0707

SEMCO (future meetings)
June 9
July 14

SEMCO: A Community Organization
Helping People for the 21st Century