Boca Bits

Monthly Magazine of The Boca Raton Computer Society, Inc.

VISIT OUR WEB SITE AT
WWW.BRCS.ORG

Volume 22, Number 10 October 2014

Next General Meeting Wednesday, October 15, 2014 @ 7:30 PM - Q & A Starting @ 6:15 PM

Cyber Security Information

October is National Cyber Security Awareness Month.

In recognition of this important topic, Jerry Naditch will present material from staysafeonline.org and other sources that give up-to-date information on the threats facing computer users.

The focus will be on practical steps we can all take to reduce those threats.

The stakes have never been higher, but mitigation requires mostly simple behavior changes in the way we use our computers.

October 2014 Drawing

There will be a 50/50 drawing this month, 50% of proceeds to the BRCS treasury, and 50% to the lucky winner.

Tickets: 3 for $5, or an arm's length for $10.

Inside This Issue

Membership News & Views

Membership Renewals
As of September 18, 2014

Bruno Chiesa
Zelda & Hershel Fuksman
Greg Glenn
Paul Hirsch
Ken Lassiter
William A. & Molly G. Lipschultz
Donald Ross
Sam Wexler

Upcoming Renewals
Expiring November 1, 2014

Sydelle Apfel
Rudi Aschenbrand
Evelyn Brodkin
Albert Cataldi
Olie Fernald
Neil Garfield
Ron Greenfield
Henry Kurlansik
John W. Lange
Stanley Roth
Alan Schildkraut
Eric Sharenow
Lorraine Zocchi

Membership Incentive

The Board has instituted a new membership incentive.

If you are a BRCS member in good standing and bring in someone brand new who joins BRCS, your membership renewal date will be extended by six months.

Bring in a friend or neighbor so they can see what we are all about.

Get them to sign up and let us know that you are the one who referred them.

SIG News

All SIGs will be at the Patch Reef Park Community Center.

Exit I-95 at Yamato Road. Go West to second left turn after Military Trail (approximately 1/4 mile). Patch Reef Park is on the South side of Yamato Road.

http://www.patchreefpark.org/address-directions

Hardware

First Wednesdays at 1:30 PM. September, October, and November 2014; January thru May 2015.

Windows and the Internet

7:00 PM January 22, and April 23 of 2015

Freeware

7:00 PM October 23, 2014 and March 26, 2015

Potpourri

7:00 PM February 26, and May 28, of 2015

Last Minute Cancellations

Make sure to check the http://brcs.org/sigsopen.html calendar, to make sure there are not any last minute cancellations, before going to the SIG.


Steve Costello

Boca Raton Computer Society President's Message

By Steve Costello, President, BRCS

Communications from the President of Boca Raton Computer Society, regarding important issues and information.

Presentations

September 2014

Richard Miller showed us a Raspberry Pi, gave a presentation explaining some of the things it can be made to do, and gave us a practical demonstration.

October 2014

Jerry Naditch will present material from staysafeonline.org and other sources that give up-to-date information on the threats facing computer users, focusing on practical steps we can all take to reduce those threats.

SIGs

All SIGs will be at the Patch Reef Park Community Center.

Hardware / Software

First Wednesdays at 1:30 PM. September, October, and November 2014; January thru May 2015.

Windows and the Internet

7:00 PM January 22, and April 23 of 2015

Freeware / Open Source

7:00 PM October 23, 2014 and March 26, 2015

Potpourri

7:00 PM February 26, and May 28, of 2015

Member Involvement

Remember BRCS is all about "members helping members".

As was brought up at the May 2014 presentation, to keep the organization going there needs to be more member involvement.

If you have any ideas for Presentations, SIGs, getting new members, or anything else that can help BRCS stay viable, email president@brcs.org, or contact any of the board members with the information.

We Need Help!

BRCS is an all volunteer organization. Get involved and help make this club better than it already is!

Here are some of the positions that need to be filled:

Program Coordinator

We need someone to coordinate scheduling future speakers for our General Meeting programs.

SIG Coordinator

Keeping track of the various special interest groups and meeting places. Making sure the SIG Leaders have access to equipment needed.

Working with the Board in scheduling the meetings for best utilization of meeting space available.

Other

There are many other positions available. Prior experience is not required, and training will be provided. Most positions only involve a few hours a month.

Contact

Please contact Steve Costello at president@brcs.org, or any of the board members (listed under *BRCS Board of Directors* in *Boca Bits*), and offer to help.

Steve Costello
October 2014

Editor's Note

By Steve Costello

This is where the editor communicates with you, the reader.

Here you will find information regarding upcoming changes in format and / or content in *Boca Bits*.

I hope you find something of interest to yourself in this issue.

If there is something in particular you would like to see, contact me and let me know about it, so that I can check about filling your request.

Know someone who writes about technology? If so, have them contact me about publication in *Boca Bits*.

Ira Wilsker Article

A Good Password Manager May Enhance Your Computing Security

As October is National Cyber Security Awareness Month, I decided to include this article about password manager.

Ira sends me an article from his column at *The Examiner*, about once a week with permission for use after the publish date in *The Examiner*.

Ask Leo! Article

10 Steps To Keep From Getting Your Account Hacked

Advice in keeping with National Cyber Security Awareness Month, for keeping your accounts from being hadked.

Allen Wyatt's Word Tip

Printing without Headings

Sometimes you want to use headings to organize your writing, but you might not want them to be printed.

Allen show how to accomplish that using Microsoft Word 2007 and 2010, in three different ways, with a link for a similar tip to do it with previous versions.

APCUG

Two Factor Authentication — Proof of Identity

By Phil Sorrentino, Staff Writer, The Computer Club, Inc., Sun City Center, FL.

Once again, this is in keeping with Cyber Security Awareness Month.

These articles, have been provided through Judy Taylour, via APCUG PUSH/Articles2Go for reprinting, and have not been edited for content, only for styling.

Publication in no way is endorsement, nor agreement with opinions given. A copy of this newsletter has been sent to the author, and/or editor, where possible.

Links

In this online only edition of *Boca Bits*, you should find that all links are live.

They were checked prior the time of publication, however due to the fast changing nature of the internet, some may no longer be valid.

Most modern PDF readers should have no problems processing the links.

The latest versions of Adobe Reader, Foxit Reader, and Sumatra are known to work well. All three are available at Ninite.com, under the Documents column.

Comments Solicited

Please send your comments and / or suggestions to:

editor@brcs.org

Please include a subject line, that begins with:

Bits Comment

This will enable me to quickly distinguish it from other emails.

A Good Password Manager May Enhance Your Computing Security

By Ira Wilsker
Columnist, The Examiner, Beaumont TX
Radio & Talk Show Host.
iwilsker@sbcglobal.net

Websites:

http://www.techsupportalert.com/best-free-web-form-filler-password-manager.htm

http://www.infoworld.com/d/security/review-the-best-password-managers-pcs-macs-and-mobile-devices-244519

https://lastpass.com

http://keepass.com

https://www.passwordbox.com

http://www.roboform.com

http://splashdata.com/press/worstpasswords2013.htm

With the spread of password stealing malware, password stealing interceptors on jeopardized websites, key logging trojans, and hackers using brute force to determine our online passwords, we all need to practice good password security.

Over the years, I have been promoting password security in this column, yet I still find that many local people are still using simple passwords that are easy to guess.

What may be even worse is that many of those same people who use simple passwords also use the same simple passwords on multiple websites, or use the same simple password on all websites!

This violation of common sense has resulted in countless victims who have had bank accounts emptied, credit cards abused, spam emails apparently sent from our email accounts, problems with eBay and other online sellers, and a variety of other distressing events all because the one password used for all has been compromised.

When the user of a single password for everything has that sole password compromised, then all of their online transactions become vulnerable, often resulting in a massive and expensive case of complex identity theft.

The Need For Complex And Unique Passwords

I have been preaching in this column for many years that we all need to utilize a complex and unique password for each website or other online account that we utilize; in this way if one password is compromised (a more likely occurrence now than in the past), that compromise will only impact that single web service, and not all of the other websites that we visit.

For those skeptics reading this column, multiple evaluations of the passwords stolen in many of the major online data thefts and later published on hacker websites, still indicate that much of the public still have not learned this painful lesson.

(Continued on page 6)

(**Password Managers** *Continued from page 5)*

Earlier this year, the security and password management company Splashdata (splashdata.com/press/worstpasswords2013.htm) published the results of an analysis of millions of compromised passwords, including the 48 million passwords stolen during the October, 2013 data breach at Adobe, which were subsequently posted online by the cyber crooks.

A disproportionally large number of users are still using simple, easy to guess passwords that make their online activities very vulnerable to identity theft. According to Splashdata, the top 10 of the most widely used passwords were (in order of most common and widely used): 123456, password, 12345678, qwerty, abc123, 123456789, 111111, 1234567, iloveyou, and adobe123.

WorstPasswords-2013

The list of most commonly used passwords published by Splashdata was actually much longer, a fact not lost on hackers and identity thieves.

Since usernames and email addresses are very easy to find or deduce, someone wanting illicit access to an online bank account or email account only has to use a purloined username or email address and then sequentially try the most common passwords, which will then possibly give the hacker full access to those valuable accounts.

If you are victimized in this manner, your bank balance is now theirs, not yours.

Password Managers

When I give security presentations, I am frequently told by some members of the audience that complex passwords, consisting of upper case letters, numbers, lowercase letters, and on some websites symbols like $, !, &, and others characters, are too hard to remember, especially for all of the secured websites that they visit.

These people have to make a decision; create, use, and manage different complex passwords for every online service that they visit, or face the high possibility of dire consequences.

This is precisely why one of the most increasingly popular utility categories used online is a password manager. The better password managers can selectively create complex and random passwords, auto-fill usernames and passwords when requested by a webpage, selectively fill common forms with personal information (name, address, phone, etc.), notify the user if a password may have been compromised by a data breach on one of the visited websites, and perform other security services as well.

A quick review of the major websites presents a lengthy list of password managers, but it seems that the same handful keep appearing as among the best in published reviews.

TechSupportAlert

My primary "go to" website when looking for software is Gizmo's TechSupportAlert.com, which has a listing under the heading "Best Free Web Form Filler and Password Manager" (techsupportalert.com/best-free-web-form-filler-password-manager.htm).

Utilizing its widely respected volunteer community of thousands of geeks and nerds, Gizmo's posted ratings and evaluations of software are widely respected and followed.

Gizmo's top rated password manager is LastPass (lastpass.com), available in both free and paid versions ($12/year).

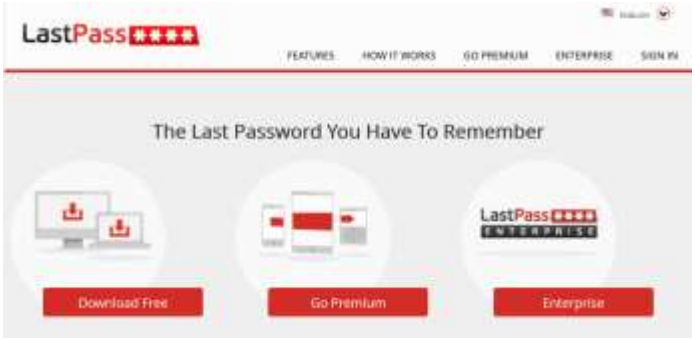
(Continued on page 7)

(**Password Managers** *Continued from page 6)*

LastPass

LastPass was awarded the top rating of 5 out of 5 stars by the community evaluators, and given "Gizmo's Freeware award as the best product in its class!".

To be honest and with open disclosure, I have been using LastPass Premium (the paid version) for several years and have found it indispensable; I have it on my desktop and laptop computers as well as my Android smart phone and my tablet.



LastPassWebpage

The free version of LastPass arguably the most capable and comprehensive free password manager available, and is compatible with most major browsers (Internet Explorer, Chrome, Firefox, Safari, Opera), most contemporary operating systems (Windows, Mac, Linux), and almost all mobile and portable operating systems (Android, iOS, Windows, Blackberry, Firefox OS, Windows Surface RT).

The paid "Premium' version adds a few features such as better multifactor authentication, better access on some mobile phones, enhances sharing, provides priority technical support, allows better form filling on Windows applications, and other enhanced functionality.

Both the paid Premium and the free versions seamlessly and automatically synchronize passwords between the different devices.

My LastPass can also do a security check to determine if any of my usernames and passwords have shown up on any of the listings from compromised online services.

RoboForm

The number two rated password manager on the Gizmo list is RoboForm (roboform.com), which was also awarded a 5 star rating by the Gizmo community.

I had used the free version of RoboForm for several years until the free version ceased functioning on Firefox, which led to my switching to LastPass, a change which I do not regret. LastPass imported all of my passwords and other information from RoboForm.

Roboform

While the free version of RoboForm is also compatible with all major browsers and operating systems, as well as smart phones and tablets, the free version is currently limited to storing only 10 forms and passwords, while the much more powerful full version "RoboForm Everywhere for Windows, Mac and Mobile", with unlimited storage of passwords and user information costs $19.95 per year (half-price for the first year).

According to the RoboForm website, the paid version offers "New simplified pricing - one license for all your computers and multiple devices - best value.

(Continued on page 8)

(**Password Managers** *Continued from page 7)*

The RoboForm Everywhere license allows you to use RoboForm software on all your Windows computers, Macs, and other mobile devices, and includes automatic synchronization of all your RoboForm data."

Other Password Managers

Other well rated, but less capable password managers that passed muster on the Gizmo forums include **KeePass** (4 star rating, unrestricted freeware), **Password Safe** (4 star rating, unrestricted freeware), **PINS** (3 1/2 star rating, unrestricted freeware), **KeyWallet** (3 star rating, unrestricted freeware, but not updated for any version of Windows newer than Windows XP), and **Access Manager** (3 star rating, unrestricted freeware).

InfoWorld

Other respected online services have also rated and evaluated the major password managers, and arrived at somewhat similar rankings while including more of the paid password managers.

InfoWorld

A recent posting by InfoWorld Security Central on June 18, 2014 (infoworld.com/d/security/review-the-best-password-managers-pcs-macs-and-mobile-devices-244519), titled "Review: The best password managers for PCs, Macs, and mobile devices", along with a subtitle, "6 local and cloud-based password managers make passwords stronger and online life easier for Windows, Mac, iOS, Android, BlackBerry, and Windows Phone users" somewhat mirrored Gizmo's findings, along with some additional candidates.

LastPass

The InfoWorld evaluations gave LastPass its highest final score of 8.7 out of 10, with a 10 for available features (tied with KeePass in terms of features), and scored or tied the highest in all of the other categories except for value; LastPass was given a score of 9, while KeePass (which is free) was given a 10.

KeePass

KeePass was given the second highest composite score in the InfoWorld testing, with an 8.4 out of 10, faring well when compared to LastPass in each of the items on the scorecard, only beating LastPass on value (free).

KeyPass

Other Password Managers

On this InfoWorld scorecard, **Dashlane** came in third with a score of 8.0, followed by **1Password** (7.9), **PasswordBox** (7.8), and **SplashID Safe** (7.2).

(Continued on page 9)

(**Save Password Managers** *Continued from page 8)*

I am currently experimenting with PasswordBox (passwordbox.com), as they recently had a deal on one of the software daily deal sites offering an unlimited lifetime subscription for the paid version for only $9.99, which was less than a single annual subscription for the full-featured paid version.

PasswordBox

PasswordBox also offers a feature rich free version for Windows, Mac, and most portable smart devices, all of which are immediately synchronized with each other, but the free version is limited to 25 passwords.

I had PasswordBox import my LastPass information, and simultaneously keep both of them synchronized with each other as well as my laptop, smart phone, and tablet.

On a literal side-by-side comparison, my first impression is that my LastPass Premium is more powerful than the paid version of PasswordBox, as PasswordBox has periodically displayed a popup indicating an inability to auto fill the information on some websites that I visit, but also states that they are aware of the problem and are working on a solution.

I will likely stay with LastPass Premium as my password manager, but will continue to give PasswordBox an opportunity to prove itself.

If I wanted a full featured but totally free password manager, I would choose KeePass based on its ratings from Gizmo and InfoWorld.

Conclusion

Create and use unique, complex passwords on each of the websites where you have accounts, and use a good password manager to manage those passwords.

Apple Takes on Levi's
Reprinted with permission:
http://www.chumworth.com/2014/09/12

10 Steps To Keep From Getting Your Account Hacked

By Leo Notenboom

Leo A. Notenboom has been playing with computers since he was required to take a programming class in 1976. An 18 year career as a programmer at Microsoft soon followed. After retiring in 2001, Leo started Ask Leo! in 2003 as a place for answers to common computer and technical questions.

Judging from the questions I receive, hacking accounts seems like a common occurrence. Here are the steps you need to take to prevent losing your account - forever - to a hacker.

My account has been hacked into several times. If I'm able to recover it, it just gets hacked again. Sometimes I can't recover it, and I have to start all over with a new account. What can I do to stop this all from happening?

I don't get this question a lot. But I really, really wish I did.

(What I get over and over and over again is the related "I've been hacked, please recover my account/password for me!" (Which, for the record I cannot do, no matter how often, or how nicely I'm asked.)

The only salvation is in prevention, and this applies to email, social media, and pretty much any password-protected account you might have.

So what can you do to make sure your account doesn't get hacked into in the first place?

1: Select a good password

I'm sure you'd be shocked at how easy many passwords are to guess. Your pet's name, your pet's name spelled backwards, your favorite TV character's catch phrase, your boyfriend or girlfriend's name (or "ilove" followed by that name), and so on.

If you think people can't guess it, you are wrong. They can, and will.

"iLoveMikey" is a bad password. "j77AB#qC@^5FT9Da" is a great password. You can see the problem though – great passwords are hard to remember.

So compromise: never include full English words or names; always include a mix of uppercase and lowercase letters and numbers; always make sure that the password is at least 10 or 12 characters long.

"Macintosh" is bad, "Mac7T0sh" might be good, and probably easier to remember. "HondaPrelude" is bad, but "Pre7ood6? might be ok.

Bottom line: pick a random looking password that YOU can remember, but that THEY would never guess – and assume that THEY are always really great guessers.

2: Protect your password

A scenario I see much too often starts with "I thought I could trust my boyfriend / girlfriend / husband / wife / co-worker so I shared my password. Then we had an argument."

How much damage can someone do if they're angry with you, and they have the password to your account? A lot.

It's very simple: Trust no one. I'm serious on this. Your friends are your friends until one day they're not.

Naturally there are exceptions, but if there's the least little bit of doubt, don't reveal your password. Especially if someone is pressuring you to do so.

3: Set and protect your "secret answer"

Many systems use a "secret question" and its corresponding answer as the key to password recovery or reset. The problem is that many people choose secret answers that nearly anyone can guess. (I'm fairly convinced many services are moving away from this as a security measure simply because so many people gave such obvious and easily-hackable answers)

(Continued on page 11)

(**Keep From Getting Hacked** *Continued from page 10)*

Do people know where you were born? Then they know the answer to that secret question.

Do people know what you're pet's name is? Then "favorite pet's name" is probably a bad secret question for you.

And yet people do exactly that. If your account is repeatedly hacked after you recover the password, I'd guess that your "secret question" isn't that secret after all.

A great approach to this is to realize that there's nothing that says your answer actually has to correspond to the question, or to anything else in your life.

So, pick an unrelated answer that has nothing to do with you. Perhaps your "City of Birth" should be "Crayola", "Chardonay" or "WindowsExplorer". As long as you can remember it it doesn't matter what it is.

An even better approach is to treat it like just another password - a password to your password, for example. Make it long, and obscure, completely unrelated to the "question", and impossible for someone else to guess.

4: Set (and maintain!) an alternate email address

Many services will use an "alternate email address" to mail you a password recovery link if you forget yours.

First, make sure to set that option up, and set it up using an email account on a different system. Create and use a Yahoo account for your Hotmail alternate email, for example.

And second: don't lose the alternate account. For many systems, if you can't access that alternate email account, you cannot get your password back, and you will not be able to recover your primary account.

I've seen too many cases where people lose their alternate email address or let that account lapse, only to be totally out of luck when they find they really really need it to recover their primary account.

5: Set (and maintain!) additional security measures offered

Many services now offer additional security measures such as:

Two-factor authentication – requiring that you prove you have your phone by entering a code texted to you, or a number generated by an authenticator app.

Mobile phone account recovery – similar to using an alternate email address, if you ever do lose your password you can authenticate your recovery attempt by responding to or entering a code sent to your phone.

Trusted friends and family – Facebook in particular allows you to designate other Facebook accounts as "trusted contacts" that can be used to validate that you are you and that you should be allowed access to your account.

In almost all cases these measures need to be set up before you need them, so set them up now, while you're thinking of it. And remember to change them when, say, your mobile number changes, or your friends change.

6: Use a different password on every site

I've written about this extensively: it's important to use different passwords on each of your important sites.

The reason is very simple: if a hacker manages to discover your password on one account they very often will go try your username and password, or email and password, on a multitude of other services. If you used the same password on another service that they happen to try, then that account will quickly be hacked as well.

Password safes like LastPass, Roboform and others are excellent ways to maintain multiple, complex passwords for multiple sites without needing to remember each and every one yourself.

Speaking of your memory….

7: Remember

I realize that "hard to guess" is at odds with "easy to remember", but both are absolutely critical.

(Continued on page 12)

(**Keep From Getting Hacked** *Continued from page 11)*

If you forget your password, and you forget the answer to your secret question or lose access to your alternate email account or some how lose the ability to use any of the password recovery mechanisms provided by the service … well, to put it bluntly, you are severely out of luck.

Don't forget your own password. Don't forget the answer to your own secret question(s). If you must write your information down keep it in a secure place. A sticky note on your monitor under your mouse pad or other, easy to get to place, is not secure. Your wallet might be secure. A locked cabinet or safe might be secure. A properly encrypted file on your computer might be secure.

And once again, a password safe can be used to do the remembering for you.

8: Don't fall for phishing schemes

FROM THE ASK LEO GLOSSARY

You should never have to email anyone your password. EVER.

There are some very common phishing attempts that will threaten you with account closure unless you respond to the email with information about your account. Information like your login name and password. Those emails are bogus. Mark them as spam and ignore them.

Any email that requires you to respond with any information that includes your password is almost certainly a phishing scam.

9: Remember that there is little to no support

The vast majority of the account hacks that I hear of – the hacks where people are ultimately unable to recover their accounts – involve free services with little to no support.

There may be a knowledge base, or a peer-to-peer support forum, but there is rarely someone to email and almost never someone to call.

You are responsible for your own account security. It's often true, and certainly safest to assume, that no one will help you should something go wrong.

That means it's up to you to take the preventative measures I've outlined, as well as keeping your information up to date as things change.

10: Learn from your mistakes

Finally, if looking at this list you realize that:

- the answers to your secret questions are obvious, or
- you no longer have access to your alternate email address, or never set one up, or
- you no longer have access to your old mobile number, or never set one up, or
- your passwords are short and just plain lame and you use the same one everywhere as well

Then fix it! NOW! Before it's too late.

Trust me, if you get hacked and it's for one of those reasons, or you lose access to your hacked account because you never bothered to prepare, you'll kick yourself.

And you may very well lose access to that account forever.

This is an update to an article originally posted : May 2, 2006

Read more:

How do I recover my Facebook login password? If you've lost your Facebook login password, there are a couple of ways to recover access to your account.

I've lost my Hotmail password, can you help get it back? If you have lost your Hotmail password, it's impossible for me to get it back for you. However, there are measures you can take to avoid this situation

I've forgotten the answer to my MSN Hotmail secret question, *and* my password, what do I do? MSN Hotmail actually has three ways to recover your password if you've lost it, but they all require that you have set them up before you run into trouble.

Are free email services worth it? Free email services and accounts are convenient and ubiquitous. But free email services aren't the right place to keep your important information.

Printing without Headings

By Allen Wyatt

Thousands of free Microsoft Word tips can be found online at http://word.tips.net

Lyle uses Word to create essays by putting together an outline and then developing the body of the essay based on the outline. When he is finished with the essay, the outline is important to him, but he does not consider it a part of the essay.

He is wondering how he can print the essay without the outline, which consists of the various headings in the document.

There are a couple of ways that you can print your essay without the headings.

Option 1

One way is to simply delete the headings on the copy you want to print. This is relatively easy for a short document with few headings, and only mildly more complicated if you have a longer document with many headings. (In which case you can use Find and Replace to delete the headings.)

When through printing, simply close the document without saving, and your on-disk version (the last one you saved) still has the headings in place.

Option 2

Another option is to format the headings so that they are white. White text printed on white paper means that they will be invisible on the printed page, but there will still be vertical space left in the document to indicate where the headings really are.

Option 3

The best solution, by far, is to use the Hidden attribute for your headings. Just select the headings (or display the style definition for your headings) and choose Font from the Format menu. Word displays the Font dialog box and you can select the Hidden check box. When you close the dialog box, the attribute is applied to the headings.

With the Hidden attribute set, there are two ways you can instruct Word to treat the text:

You can control whether hidden text is displayed on-screen, and you can control whether it is printed.

These settings are separate from each other, and in this case you probably want the headings to be visible on-screen, but invisible when printing.

Follow these steps:

1. Choose Options from the Tools menu. Word displays the Options dialog box.
2. Display the View tab. (See Figure 1.)

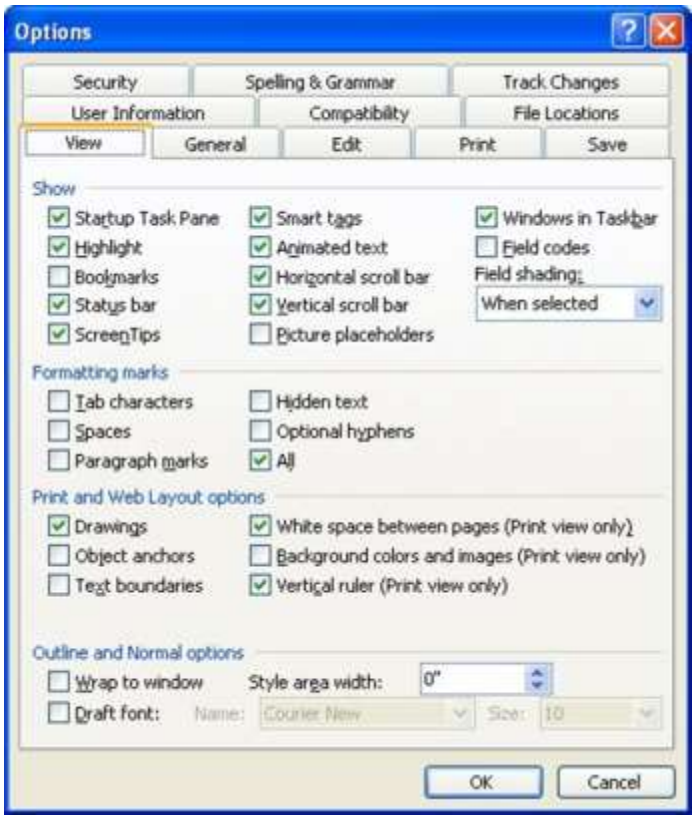


Figure 1. The View tab of the Options dialog box.

(Continued on page 14)

Printing without Headings *Continued from page 13)*

3. Make sure that either the Hidden check box or the All check box is selected. Either of these settings will make sure the hidden text appears on-screen.
4. Display the Print tab. (See Figure 2.)
5. Make sure the Hidden Text check box is cleared. This setting controls whether hidden text is printed or not.
6. Click OK to close the Options dialog box.

WordTips is your source for cost-effective Microsoft Word training. (Microsoft Word is the most popular word processing software in the world.)

This tip applies to Microsoft Word 2007 and 2010.

You can find a version of this tip for the older menu interface of Word here: Printing without Headings.

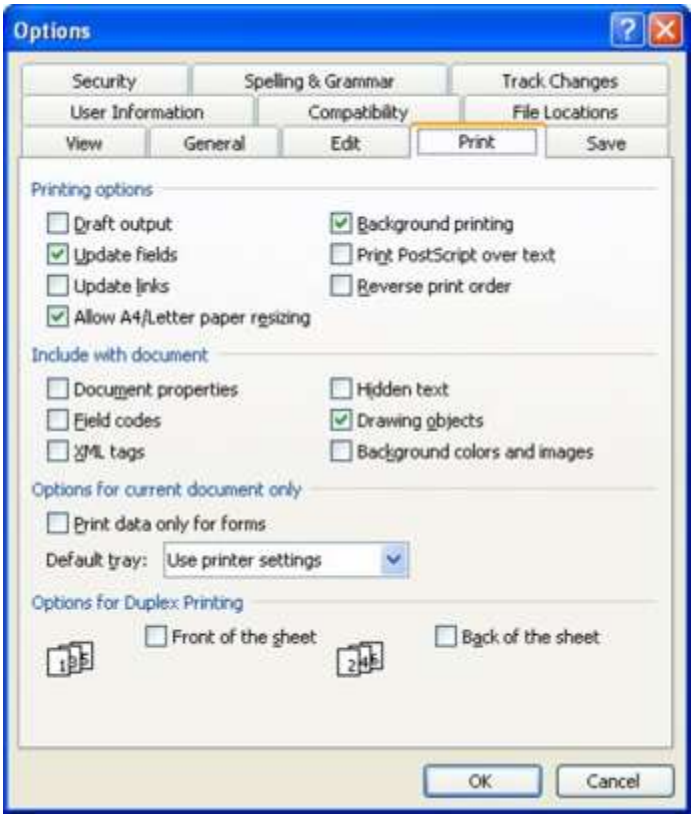


Figure 2. The Print tab of the Options dialog box.

Links To Some Other Microsoft Word Tips

Word 2003

Wavy Underlines, Double Underlines, and More
http://tipsforwordprocessing.com/word_2003_0028.html

More Underlining Tips
http://tipsforwordprocessing.com/word-2003-underline-keyboard-shortcuts.html

Word 2007

Microsoft Word 2007 Tip Sheet (PDF)

http://itsweb.lsu.edu/USS/images/item3473.pdf

Word 2010

Turn a Picture Into a Watermark

http://blog.knowledgewave.com/msoffice/pc-tip-of-the-week-microsoft-word-2010-3.html

Two Factor Authentication — Proof of Identity

By Phil Sorrentino, Staff Writer, The Computer Club, Inc., Sun City Center, FL

March 2014 issue, The Journal
www.scccomputerclub.org/

philsorr (at) yahoo.com

Introduction

When you walk up to a teller in a bank and request information about your bank account, the teller may ask you to authenticate yourself by providing a picture form of identification.

But if you have been going to this bank for many years and she is familiar with you, she may just give you the information. In truth, your face and her knowledge of you have provided the necessary authentication for her to respond to your requests.

Authentication is much easier in the real world than it is in the software and computer-network world.

Authentication is the act of proving one is really who one says he or she is. In the computer world, we all experience this every time we sign on to one of our accounts or websites.

Typically we are asked for a User Name and a Password. The correct User Name and Password combination proves, to the software requesting these items, that we are who we say we are.

Of course, we could give our User Name and Password to a friend, something we rarely want to do because then he would be able to authenticate himself as the owner of our account.

"Hacking" occurs when someone or some software program attempts to guess your Password after acquiring your User Name: maybe from some public information source.

(Remember, User Names are available all over the internet.) This is a form of brute force "hacking" of an account. And unfortunately, there are many other, more sophisticated, ways of hacking into an account.

So, more formally, "Authentication is the act of confirming the truth of an attribute of a datum or entity, which might involve confirming the identity of a person or software program, or ensuring that a product is what it's packaging and labeling claims to be."

In other words, Authentication involves verifying the validity of at least one form of identification. As it turns out, practically, there can be three forms of authentication, called factors.

Now, two-factor authentication requires the use of two of the three authentication factors. These factors are:

- • Something only the user knows (e.g., password, PIN, pattern);
- • Something only the user has (e.g., ATM card, email account, mobile phone); and
- • Something only the user is (e.g., biometric characteristic, such as a finger print).

(These factors are so important for authentication that they are identified in government documents in the standards and regulations for access to U.S. Federal Government systems.)

(Continued on page 16)

*(**Two Factor Authentication** Continued from page 15)*

Some security procedures now require three-factor authentication, which involves possession of a password, and a physical token, used in conjunction with biometric data, such as a fingerprint, or a voiceprint, or a retina scan.

Two Factor Authentication

Two-factor authentication is not a new concept.

ATM Example

When a bank customer visits a local automated teller machine (ATM), one authentication factor is the physical ATM card that the customer slides into the machine ("something the user has").

The second factor is the PIN the customer enters through the keypad ("something the user knows"). Without the corroborating verification of both of these factors, authentication does not succeed.

Credit Card Gasoline Purchase Example

Another example is when you use your credit card for a gasoline purchase and you have to enter your ZIP code to confirm the charge.

You must provide a physical factor (something you own), the card, and a knowledge factor (something you know), the ZIP code.

Factors

These examples show the basic concept of a two-factor authentication system: the combination of something the user knows and something the user has.

Knowledge Factor

"Something only the user knows" is termed a Knowledge factor and is the most common form of authentication used.

In this form, the user is required to prove knowledge of a secret in order to authenticate, typically, a password, PIN, or a Pattern.

All of us are familiar with the password which is a secret word or string of characters.

This is the most commonly used mechanism for authentication.

Many two-factor authentication techniques rely on a password as one factor of authentication.

A PIN (personal identification number), is a secret series of numbers and is typically used in ATMs.

A Pattern is a sequence of things, like lines connecting the dots on the login screen of a cell phone or tablet.

Possession Factor

"Something only the user has" is termed a Possession factor. A key to a lock is a good example.

With today's computer systems your email account or your phone or a swipe-card is used as a possession factor.

Inheritance Factor

"Something only the user is" is termed an Inheritance factor.

Historically, fingerprints, a biometric method, have been used as the most authoritative method of authentication.

Other biometric methods such as retinal scans are possible, but have shown themselves to be easily fooled (spoofed) in practice.

More Two Factor Authentication Information

Two-factor authentication is sometimes confused with "strong authentication", but these are fundamentally different processes.

Soliciting multiple answers to challenge questions may be considered strong authentication, but, unless the process also retrieves "something the user has" or "something the user is", it would not be considered two-factor authentication.

Two-factor authentication seeks to decrease the probability that the requester is presenting false evidence of its identity. The more factors used, the higher the probability that the bearer of the identity evidence is truly that identity.

(Continued on page 17)

*(**Two Factor Authentication** Continued from page 16)*

These systems ask for more than just your password. They require both "something you know" (like a password) and "something you have" (like your phone or email account).

After you enter your password, you'll get a second code sent to your phone or email, and only after you enter it will you get into your account.

It is a lot more secure than a password only, and helps keep unwanted snoopers out of your accounts.

Two Factor Authentication Systems

Many well-known systems employ two-factor authentication.

Some of these are:

- Amazon Web Services
- Dropbox
- Facebook, Google Accounts
- Microsoft/Hotmail
- Paypal/eBay
- Twitter
- Evernote

The two factor authentication will typically be employed when you are using a different computer, or a computer from a different location, when trying to access one of your accounts.

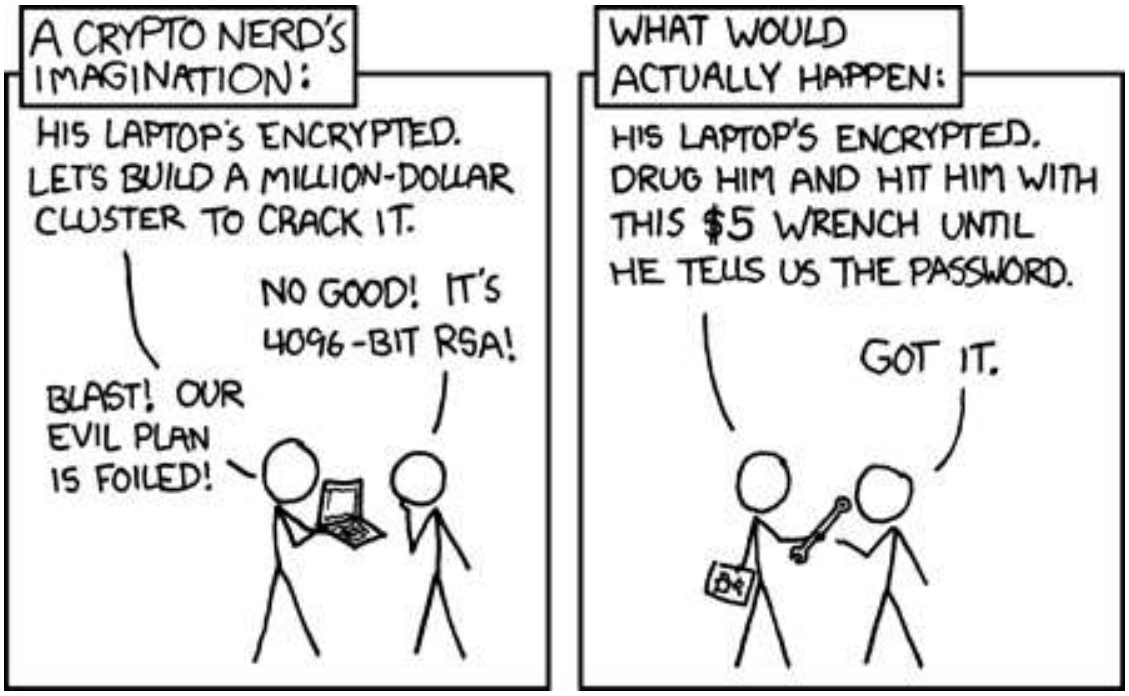
Most of these two-factor implementations send you a 6 digit code via a text message for you to input when you receive it.

This 6 digit code becomes the second factor to be used with the original password.

This definitely adds an extra step to your log-in process, and depending on how the account vendor has implemented it, it can be a minor inconvenience or a major annoyance.

(And it also depends on your patience and your willingness to spend the extra time to ensure the higher level of security.)

But in the long run the use of a two-factor authentication improves the security of your private information, no doubt something we all want.



Reprinted with permission:
http://imgs.xkcd.com/comics/security.png

Interesting Internet Finds

Steve Costello, Boca Raton Computer Society
editor@brcs.org

http://ctublog.sefcug.com/

In the course of going through the more than 300 RSS feeds, I often run across things that I think might be of interest to other user group members.

The following are some items I found interesting during the month of September 2014.

Is USB safe?
http://askleo.com/is-usb-safe/

Leo Notenboom tells us about the "BadUSB" flaw, what it is and what is known about the implications.

What Does Airplane Mode Do, and Is It Really Necessary?
http://www.howtogeek.com/194421/what-does-airplane-mode-do-and-is-it-really-necessary/

Have a device with airplane mode? HowToGeek explains what it does, and why you should use it, even if you are not on a flight where it is required. I know I use it whenever I don't need to be connected, or when I can not get any connections, like on my last vacation in Vermont when my wife had service and I didn't.

Beware the Fake Tech Support Scam
http://askbobrankin.com/beware_the_fake_tech_support_scam.html

Bob Rankin talks about the fake tech support scams, that are prevalent in different areas and times. He talks about how to recognize them, and avoid them, as well as what might happen if you fall for one of them.

3 Things to Do to Make Your Internet Life More Secure
http://www.maketecheasier.com/make-internet-life-more-secure/

Interested in making you internet life more secure? If so, check out these three things you might not be doing already.

How to set up two-factor authentication on your Google account
http://www.greenbot.com/article/2605221/how-to-set-up-two-factor-authentication-on-your-google-account.html

This post explains how to set up two-factor authentication on your Google account. If you haven't already set it up, you should to keep it more secure.

Online Identity Theft: Prevention and Protection
http://www.thewindowsclub.com/online-identity-theft

The Windows Club explains what online identity theft is, and how to prevent it and protect yourself.

****

Most Fridays, more interesting finds will be posted on the *Computers, Technology, and User Groups Blog*:
http://ctublog.sefcug.com/tag/interesting-internet-finds/

Computers, Technology, and User Groups Blog

Steve Costello has started the above referenced blog. It is at http://ctublog.sefcug.com.

You can subscribe via RSS, or email, to receive the latest updates.

Posts

This blog has posts related to specific user groups, and things related to computers and technology in general.

Normally there are no more than three posts per week. However, there could sometimes be more.

Posts are under a Creative Commons license, and as such you can use them, provided you attribute the work as shown in the license.

There is a specific page for the BRCS Freeware SIG at http://ctublog.sefcug.com/about-the-brcs-freeware-sig/.

Information

For more information about the blog check the about page at http://ctublog.sefcug.com/about-this-blog/.

http://ctublog.sefcug.com/contact/ is the URL for the contact page, should there be any other questions.

Boca Raton Computer Society, Inc

BOARD OF DIRECTORS

OFFICERS

President
Steve Costello
754-200-1531
president@brcs.org
http://ctublog.sefcug.com/

Vice President
Jerry Naditch
561-865-1253
gnaditch@brcs.org

Treasurer
Sherman C. Potter
561-495-6797
shermp@brcs.org

Secretary
Robert Koehler
561-278-6163
bobkoe@comcast.net

DIRECTORS

Greg Glenn
561-395-3316
glenngga@cs.com

Richard Miller
561-393-5813
RMiller@genesis-one.com

Arthur Shebar
561 266-3800
ashebar@comcast.net

Marty Troum
561-736-4843
mtroum@comcast.net

Stanley Warshaw
swarshaw@brcs.org

BRCS Member's Help Line

This help line is for BRCS members who need answers to technical questions, but cannot wait for the monthly meetings.

Help-line volunteers offer their time to assist BRCS Members only!

Note: Some volunteers will answer questions only by email.

If you would like to become a Help Line volunteer, contact:

info@brcs.org

Digital Photography

Jerry Dinerman..... gerald@dinerman.com

Freeware

Steve Costello (email only)..... editor@brcs.org

Skype (Telephone via the Internet)

Luis Sanchez.....561 483-6771

Spanish Interpreter (Will relay questions)

Luis Sanchez.....561 483-6771

PLEASE REMEMBER:

When you call the help-line, the people who answer are volunteers. please treat them courteously.

Helpline contacts are not paid employees.
They are fellow club members, who have volunteered to try to assist you. *Please interact with them as such.*

Computer Help At Your Home From a BRCS Member

These club members make house calls. They have different skill levels, areas of expertise, and will charge different rates.

The listing of any name does **NOT** constitute a recommendation by BRCS of the person providing the service.

Call, or email, them for pricing, and to make appointments.

Richard Miller	561-393-5813
Lee Reynolds	954-755-8541
Leon Tanenbaum	561-302-2936

PERSONAL ADS

We are happy to run a personal ad, free of charge, and subject to space availability, for members of BRCS.

Items must be computer related hardware or software.

Send information, with a subject line beginning with the words BRCS Personal Ad, via email to:

editor@brcs.org

Get Published!

- Do you like to write?
- Do you have a favorite piece of software, or hardware, you want to let others know about?
- Are you passionate about technology?
- Have some interesting websites others should know about?

We are always looking for some home grown articles for the newsletter. You do not have to be an expert, and you don't have to be an experienced writer.

Submit your article, review, commentary, etc., to:

editor@brcs.org.

If anything needs to be corrected, or edited, you will be advised of the changes before it would be published.

The deadline for the newsletter is the Saturday following the general meeting, by which time the edition is pretty much filled, so allow for it being published at least a month after that.

The earlier a submission is received the better, as time is needed for editing, for content, as well as space.

About The Boca Raton Computer Society

Since 1983, members of the PC User Group of Boca Raton, now the Boca Raton Computer Society, Inc., have been helping one another use and learn about computers.

We have over 150 members, including computer professionals, business owners, home users, and novices.

We welcome hundreds of visitors to our meetings each year. Network with others who share your interests!

GENERAL MEETINGS
(OPEN TO THE PUBLIC)

General meetings are held on the third Wednesday of each month, at the South County Civic Center, 16700 Jog Road in Delray Beach, Florida.

The Civic Center is on the east side of Jog Road, between Clint Moore Rd. and Linton Blvd., opposite Morikami Park.

The general meeting begins at 7:30 p.m., with most meetings featuring presentations by outside speakers including Microsoft, IBM, Adobe, Corel, etc.

Q & A SESSIONS
(OPEN TO MEMBERS ONLY)

At 6:15 p.m. several **QUESTION** and **ANSWER** sessions are held to offer assistance to those seeking help with various computer topics. These sessions are staffed by club members.

BOARD OF DIRECTORS
(OPEN TO MEMBERS ONLY)

The **Board of Directors** meets on the second Monday of each month, at 7:00 p.m., at Patch Reef Park on Yamato Road, just west of Military Trail, in Boca Raton. Members are welcome to attend.

SERVICES

BRCS members receive our monthly newsletter, ***Boca Bits***, which provides information about meetings, SIGS, and includes articles by prominent writers, about current computer-related topics.

Special Interest Groups (SIGs) are smaller meetings which explore specific topics in greater depth, such as Graphics, Hardware, Software, Windows, Scanners, email and Internet, to name a few.

Although we support the sharing of Public-domain and user-supported software, the BRCS strongly opposes illegal distribution of copyrighted software.

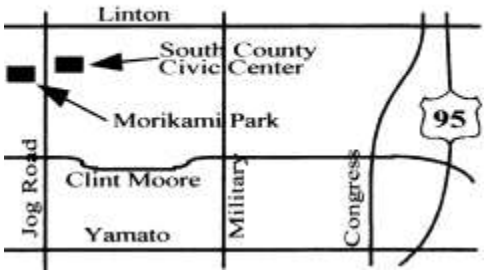
From time to time, the BRCS arranges group purchase discounts on major hardware and software items.

DUES (U.S. address only)

Membership is $45 per year and includes the monthly newsletter, Help Lines, attendance to SIG meetings and more.

Dues may be paid at the general meetings or mailed to the address listed below.

GENERAL MEETING SITE



Visit the Boca Raton Computer Society's Web Page on the Internet
http://brcs.org

Boca Bits Activities Calendars

October 2014

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

DAY		MEETING	TIME
Wed	1	Hardware	1:30 PM
Wed	15	Question & Answer Tables	6:15 PM
		General Meeting	7:30 PM
Sat	18	Boca Bits Submission Deadline	1:00 PM
Thu	23	Freeware SIG	7:00 PM

Be sure to check the BRCS website at
http://brcs.org
for locations, cancellations or changes, prior to the SIG or meeting you plan to attend.

November 2014

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

DAY		MEETING	TIME
Wed	5	Hardware	1:30 PM
Mon	10	Board Meeting	7:00 PM
Wed	19	Question & Answer Tables	6:15 PM
		General Meeting	7:30 PM
Sat	22	Boca Bits Submission Deadline	1:00 PM

Boca Bits Staff

Editor

Steve Costello editor@brcs.org

Contributing Authors

Thank you to the following, for contributing articles for *Boca Bits.*

Ira Wilsker iwilsker@sbcglobal.net

Leo Notenboom leo@ask-leo.com

Allen Wyatt allen@sharonparq.com

Phil Sorrentino philsorr (at) yahoo.com

http://www.chumworth.com/

http://xkcd.com/

About Boca Bits

Boca Bits is published monthly by the Boca Raton Computer Society, Inc. (BRCS) 5030 Champion Blvd., G-11 #202, Boca Raton, FL 33496-2473. The BRCS is an independent, not-for-profit user group and is not affiliated in any way with any vendor or equipment manufacturer.

Disclaimer

No warranty, expressed or implied, is made by the Boca Raton Computer Society, the Boca Bits editorial staff, or the individual authors or contributors. This disclaimer extends to all losses, incidental or consequential, from the use or inability to use any and all information in any issue of this publication. Unless specifically stated otherwise, the opinions expressed in any article or column are those of the individual author(s) and do not represent an official position of, or endorsement by, the Boca Raton Computer Society.

Copyright

Submission Format

Any word processor or text editor capable of producing straight ASCII text files may be used to write your article. We'll make it as easy as possible for you, just don't do any formatting like use of the Tab key, Italics, Bold, etc. Use the Enter key on your keyboard just to separate paragraphs. If you would like to include your formatting, please send a second file that can be used as a reference. Include your name and telephone number so we can contact you if we have questions.

Transmission

Please send your article, or advertising copy, by email to editor@brcs.org, or via postal mail to: BRCS 5030 Champion Blvd., G-11 #202, Boca Raton, FL 33496-2473, Attention: Editor.

Deadline: Deadline for each issue is 12:00 p.m. on the Saturday following the General Meeting.

Advertising

Non-commercial classified ads for computer-related merchandise are published, subject to space availability, at no charge to Boca Raton Computer Society members.

"Members Helping Members" since 1983

BRCS Boca Raton Computer Society

MEMBERSHIP APPLICATION

Boca Raton Computer Society, Inc.
5030 Champion Blvd., G-11 #202
Boca Raton, FL 33496-2473

Membership is $45.00 per year and includes the monthly Newsletter, Help Lines, attendance at SIG meetings, and more.

First Name _____ **Last Name** _____
Address _____ **Home Phone ( )** _____
City _____ **Work Phone ( )** _____
State _____ **Zip** _____ **My Email Address** _____

We depend upon volunteers to maintain the quality and efficiency of the organization. Your participation will not only help the club, but help you become more proficient on the computer.

Please let us know your fields of interest.

1._____

2._____

3._____

4._____

Other Computer Clubs that you belong to:

For office use only
Membership Number _____ Renewal Date___/___/___ Check No._____ Recommended By _____

Member of
Association of Personal Computer User Groups

Member of apcug An International Association of Technology & Computer User Groups

Member of:
Florida Association of Computer User Groups

FACUG