Abort, Retry, Ignore...

July 2005	Suggested Retail Price $1.95	**Volume XXI**	**Issue 07**

Simple Password Practices Keep PC and Online Data Secure

By Gabe Goldberg
APCUG Advisor and Columnist
AARP Computers and Technology Website

Password dilemma: We can't live an online life without them, but if they're too numerous to remember, they encourage unsafe practices. What to do?

First, basics. A password is just the key that opens a computer lock. It may gain access to a newspaper's online edition, protect banking records, let you bid on auctions, open a frequent-flyer account, or do anything requiring verified identity.

Some Web sites assign passwords; most allow choosing them. Rules for selecting passwords are easy to find but are often impractical. Don't use easily guessed familiar names or words; use letters and numbers and special characters? OK. Avoid anything related to facts about yourself? Makes sense. Don't share passwords with anyone? Good advice. Change passwords periodically? Oops, it's a memory test
[**http://www.evalu8.org/staticpage?page=review&siteid=8906**].
Use unique passwords everywhere? Hm, that takes a *lot* of passwords. Don't write them down or store them in a computer file? Tilt!

Maintaining passwords is a nuisance. So some people use one password for everything — a bad idea, since sharing or compromising one access opens them all. Password hierarchies are common: use one password for financial matters, another for commerce, and one for trivials such as newspaper sites. That avoids revealing your sensitive e-mail/password combination to junk Web sites.

But don't use a common password for all e-commerce sites
(**http://www.amazon.com** , **http://www.buy.com** , etc.) since they're occasionally hacked. And treat sites like PayPal as financial rather than e-commerce. And don't just guess which password you used on a site; some sites lock accounts after just a

Calendar of Events

TABLE OF CONTENTS

few failed logins.

As passwords proliferate, it's common to store them in a computer file. And having too many site-assigned passwords guarantees the need to record them. But please, don't call the file "passwords.txt" and don't use the word "password" in it. The paranoid and geeky encrypt such files, but that risks losing the file by forgetting the encryption key.

You can print and save registration pages, but that leads to bulky files, cumbersome to search and requiring updating. Some people use an address book or print lists of sites and accounts, then handwrite passwords. But that still needs updating, and can be lost, destroyed, or found by someone untrustworthy.

If you have multiple email addresses, note which you use on a given site, since that's often the key for logging in or receiving password reminders.

Hackers use special software to attack logins, applying dictionary word lists and other guessing techniques. Passwords are described as "strong" (hard to crack) if they have at least eight characters, include upper/lower case and punctuation characters and at least one digit. So even if you use a memory aid for remembering passwords — such as words from a poem — convert them to strong passwords in a way that only you will know.

High-tech devices can add security, but they're usually used only in business settings; they include biometric devices which check fingerprints or eye structure and random logon-key generators.

Software password managers are more practical. These record and secure passwords and then auto-fill online logins. Good ones offer a "don't remember/don't ask" option to avoid recording info about sensitive sites. Encryption is desirable but not mandatory; it should be possible to secure the password manager itself with a master password.

Many managers are free, some are bought, and common software such as Web browsers and e-mail clients often includes it. Google returns many hits related to "password manager" and classy software site Tucows [**http://www.tucows.com**] numbers 300 such tools. Before installing one, make sure it supports your software applications, especially if they're non-Microsoft.

Many people don't secure home computers — but consider cleaners, workers, friends wandering through, perhaps even having permission to use the computer. Suddenly security becomes more appealing. If you handle money online, check banking/financial sites occasionally for unauthorized transactions.

Remember that you may occasionally need access to secure sites while away from your computer. You can copy passwords to a thumbdrive or PDA or simply print them, but remember that they're powerful keys and must be protected. Before traveling, check your passwords so you're not surprised on the road. If you leave your computer running, you can access it remotely via tools such as GoToMyPC.

On business-owned PCs, separate personal from work-related material. Determine whether your office has policies for personal computer use and monitoring of computer activity. Some businesses install keystroke loggers which can capture passwords before they're encrypted. And remember that system administrators can often defeat security measures as part of their job, so you may not want to store sensitive personal material at work.

Work and home PCs both need disaster preparation, so family members or colleagues can access what's needed in an emergency. Work-related passwords and instructions can be stored securely so they're available but can't be secretly used.

For home computers and facilities such as e-mail and finance, remember that many ISPs and companies have privacy policies

prohibiting revealing information to family members, even in cases of illness or death. Instructions and important passwords should be stored with essential family records. Note that changing situations may require special care — for example, a divorce might motivate tight security.

This article appeared originally on AARP's Computers and Technology Web site, [**http://www.aarp.org/computers**]. (c) AARP 2004/2005. Permission is granted for reprinting and distribution by non-profit organizations with text reproduced unchanged and this paragraph included. Please e-mail the author, Gabe Goldberg, at [gabe@gabegold.com] when you print or post it.

There is no restriction against any non-profit group using this article as long as it is kept in context with proper credit given the author. The Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member, brings this article to you.

Another Silent Attack on Our Computers
By Ira Wilsker
APCUG Director
Columnist, The Examiner
Beaumont, Texas' Radio Show Host
Police Officer

WEBSITES:
http://research.microsoft.com/rootkit

http://www.sysinternals.com/utilities/ rootkitrevealer.html

http://www.f-secure.com/blacklight

http://www.f-secure.com/blacklight/ rootkit.shtml

At the recent computer security symposium in Corpus Christi, one of the speakers mentioned something that I was vaguely aware of as a threat. The threat is considered as a silent attempt to invade our computers for the purposes of installing viruses, Trojans, worms, or other malware devices. This silent threat may be used by terrorists to launch a coordinated attack on our infrastructure, steal our personal information, or otherwise wreak havoc. So insidious is this threat that it would sound like the content of an urban legend, yet it is documented as real. Imagine a threat that would be undetected by the current antivirus, firewall, and anti-spyware software, yet be so powerful as to effectively take over our computers, without our knowledge. This threat, formerly considered solely as an unproven concept, is now known to be real. This threat is also now implicated in taking over countless computers. This contemporary threat is known by the innocuous term "Rootkit".

A rootkit is defined on the Sysinternals website as, " ... the mechanisms and techniques whereby malware, including viruses, spyware, and trojans, attempt to hide their presence from spyware blockers, antivirus, and system management utilities. There are several rootkit classifications depending on whether the malware survives reboot and whether it executes in user mode or kernel mode." The security software company F-Secure expands the definition with, "Rootkits for Windows work in a different way and are typically used to hide malicious software from for example an antivirus scanner. Rootkits are typically not malicious by themselves but are used for malicious purposes by viruses, worms, backdoors and spyware. A virus combined with a rootkit produces what was known as full stealth viruses in the MS-DOS environment."

Because rootkits are currently very effective at hiding malware from our antivirus and anti-spyware scanners, it is quite possible or even probable that our computers are infected, despite repeated scans with properly updated software.

Microsoft, and other vendors, have acknowledged the threat and are now beginning to produce software that can detect and destroy the rootkits on our computers. The software is still in its infancy, and lacks the ease of use, automation, and attractive graphical interfaces

that we are used to with our antivirus software. It is inevitable that as word of the rootkit threat spreads, and more computers are identified as having stealthy rootkits hiding viruses and other threats, that the small current crop of rootkit detecting software will improve, and other competitors, probably the major antivirus vendors, will join the fight. If rootkit technology continues to spread, the current crop of generally excellent computer security suites from the likes of Symantec (Norton), McAfee, Panda, TrendMicro, and others will be forced to add rootkit protection to their respective suites, or face competitive obsolescence.

Fortunately for us, there are a few rootkit detectors already available, mostly for free! This first generation of products still needs much refining to enable the average person to scan for rootkits with ease, but they are still a very good first step. There are a few rootkit detectors available which are currently free. One "RootkitRevealer" is from a company known for its excellent and often free software, Sysinternals. This software uses a patent-pending technology to detect rootkits, and is currently available for download at **http://www.sysinternals.com/ntw2k/freeware/ rootkitreveal.shtml** . RootkitRevealer will run on almost any Microsoft operating system, NT4 and later, which includes Windows 2000, and XP.

Another rootkit detector is from F-Secure, a well-known computer security company headquartered in Finland, with offices in the US and elsewhere. F-Secure's product is "Blacklight", available as a free beta (pre-release) version until July 1. Blacklight can be downloaded at **http://www.f-secure.com/blacklight** .

I have recently tried both products, and I personally found Blacklight the easier to use. It seemed effective at detecting and eliminating rootkits.

Microsoft will shortly be making available its rootkit detector, the "Strider GhostBuster", details at **http://research.microsoft.com/rootkit** .

Persons unknown who wish to do us harm, either at a personal level such as stealing our account information and committing the crime of identity theft, or the impersonal level, such as cyber terrorists intent on shutting down our critical infrastructure, may use the rootkit technology to bypass our otherwise necessary defenses.

Until such time as the integrated computer security suites catch up with this threat, I will now have to add a rootkit detector to my recommended list of essential computer security utilities, alongside antivirus software, a good firewall, and a spyware detector. It is also imperative that all four of these utilities be frequently updated to ensure a reasonable degree of personal security. We will also have to add rootkits to our vernacular of cyber threats, along with the now ubiquitous terms "virus", "spyware", and "hacker".

I shudder to wonder what may be coming down the pike next.

There is no restriction against any non-profit group using this article as long as it is kept in context with proper credit given the author. The Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organization of which this group is a member, brings this article to you.

Another Success!

We would like to thank all of you for attending the picnic. It was very successful and everybody contributed to our big free raffle. We had all kinds of items both computer and non-computer stuff. There was more than enough food available. If you missed it, there is always next year. We all had a good time.

Roger Kinzie
Mike Goldberg
Picnic Chairpersons

The Board would like to thank the Picnic Chairpersons for a job well done.

Lamp Post 64
July 16, 2005
By John Spizzirri

The nanny-state is alive and well in the European Union (EU). As television (TV) moves to the Internet the EU wants to regulate content. The Sunday Times reports (**http://business.timesonline.co.uk/article/0,,9071-1690352,00.html**) that most TV on the Internet follows existing rules for TV broadcasters but there is no law that regulates the new media. What the article tells us is that some Internet TV producers MIGHT do something the government does not like so 'there ought to be a law' before someone does something. Oh yeah, that makes a lot of sense.

It's been a while since I've done a short tutorial about how to store documents or programs. For those of you who have seen this before, skip on to the next item. Storing documents is what a computer does well. First, we need to define terms. A document is any file that contains information. You may have created it with a word processor, spread sheet program, camera, sound recording program, or some other program. You may have downloaded it from the Internent. You may have gotten it off the CD of the Month (CDOM). Where does the computer store these documents? Generally, they are stored on hardware devices such as hard drives, CD's or DVD's. There are subdivisions on the hardware that allows for catagorizing files that are similar to one another. The main problem associated with storing documents is remembering where you put them. Using the subdivisions of the hardware effectively will make remembering much easier. One subdivision of a hard drive is called a partition. Different partitions are known by different drive letters as are additional hard drives (under Windows). Thus, if your machine has a C: and a D: drive, they may be separate hard drives or they may be two partitions on the same hard drive. Another subdivision is called a folder. You create folders directly using the operating system (Windows). Some folders are provided for by the operating system (My Documents, My Music, and My Pictures). Here is were the problem starts. When you create a text document and save it to the My Documents folder, it is at the same level or holds the same place as any other document that is in the My Documents folder. It also has the same level as the My Music and My Pictures folders. When you have more than 20 documents in the My Documents folder, finding a particular document starts to become difficult. There is an easy method of simplyfying your search. You can create a word processing folder inside the My Documents folder. If you have very few (less than 20) word processing documents finding a particular document will be easy as clicking on the My Documents folder and then clicking on the word processing folder for a list of all the documents you have stored there. If you are like me, you have many word processing documents that deal with a wide variety of subjects (like Lamp Post articles). I make a folder for each type of document. For instance, I have a folder specifically for letters I write to Henry Hyde (my Congressman). Because I write to various politicians, I have created a folder called politicians in the word processing folder. Inside the politicians folder I have a state folder and a national folder. Here is a diagram of how it looks.

Folder   *Folder*   *Folder*   *Folder*
My Documents --> WordProcessing --> Politicians -->National -->

Folder   *Word Processing Documents*
HenryHyde --> (letter documents to Henry Hyde)

Now if I need to look at a letter I wrote to Henry Hyde, I double click on My Documents then

WordProcessing then Politicians then National then Henry Hyde. I have named the letters by the subject I wrote Hyde about. Windows automatically time and date stamps each file so I can sort the files alphabetically by subject or chronologically by date. Under the WordProcessing folder I have general folder names with each succeeding folder name becoming more specific until I get to the actual document. This helps keep the number and variety of items in any one folder small and manageable. By creating folders in this way, I can rapidly navigate to the document I want to view. I do not have to search through hundreds of files to find that letter I wrote to Henry Hyde 4 years ago about a particular piece of legislation. The method I use to create a folder is to double click on My Documents. I right click in an open area on the right side of the window. Select New from the menu and then select folder. Enter the folder name and press enter. To create a folder inside the one I just created, I double click that folder and repeat the process. My Documents folder appears on the desktop or the start menu. That is not its actual location. It is always on the C: drive under users name in the Documents and Settings folder. If there is more than one user of the machine, each has there own My Documents folder. Security settings may prevent you from looking at someone else's My Documents folder. Let's get back to the My Documents folder, I have also created a spreadsheet folder, presentations folder, downloads folder, text folder, zips folder and a pix folder. The text folder is for downloaded snipits of text that I keep only for a short time. The zips folder is for zipped files that I have downloaded for a short period of time. The pix folder is for pictures I have downloaded for a short time period. If I determine that I want to keep something for a longer period, I transfer that file to another folder for longer storage. The download folder is used for temporary storage of files that may be added to the CDOM. Here is an article that more simply explains this process: **http://www.stevenelliott.co.uk/artman/publish/printer_49.shtml** .

Mozilla's (**http://www.mozilla.org/**) FireFox browser (**http://www.mozilla.org/products/firefox/start/**) and Thunderbird e-mail programs have been updated with security patches. Both are on this month's CDOM.

Claria (**http://www.claria.com/**), formerly known as Gator, is an Internet advertising company that spreads the following products: Dashbar, Gator, PrecisionTime, and Weatherscope. Microsoft Corporation (MS **http://www.microsoft.com/**) has indicated that they may be interested in purchasing Claria. MS is part of the Anti-spyware Coalition (**http://www.antispywarecoalition.org/**) whose job is to define what spyware, adware and malware is so it can be eliminated by programs such as MS's antispyware beta program. Well after MS started showing interest in Claria, they changed their antispyware beta program to exclude Claria from its definition of spyware (**http://www.techweb.com/wire/security/165701104**) and (**http://www.securitypipeline.com/165701157**). I guess when money is involved... You know the rest. CNet also has a report at **http://news.com.com/Group+delivers+definition+of+spyware/2100-1029_3-5783926.html** .

MS has issued three serious (what other kind are there?) security patches for Windows XP and Word. The full story is at the Security Pipeline article: **http://www.securitypipeline.com/165701875** .

I occasionally receive phishing e-mail. I recently got one purportedly from ABN AMRO LaSalle Bank. I right clicked on the provided link so that the link would open in a new tab (in Firefox). The link read like the actual link to LaSalle Bank (**http://www.lasallebank.com/**). When the link opened the lasallebank.com address was replaced in the address box by a TCP/IP number

sequence. The page was asking for my name, ATM/Debit card number, PIN, password, and account number. When I clicked on View/Page Source, the source opened but would not stay displayed - it kept minimizing without any action on my part. By the way, I do not have a LaSalle Bank account of any kind. I closed the tab and Googled LaSalle Bank. I clicked on the LaSalle Bank link. The LaSalle Bank home page came up and the URL remained **http://www.lasallebank.com/** instead of the TCP/IP numbers. On the page there is a consumer alert about e-mail fraud. I will reprint it here for your enlightenment. The actual link to this warning is **http://www.lasallebank.com/privacy/spot.html** .

Spot a Fraudulent Email

It's often hard to detect a fraudulent email. That's because the email address of the sender often seems genuine (such as support@LaSalleBank.com), as do the design and graphics. However, there are telltale signs for spotting fraudulent emails.

Tips for spotting a fraudulent email:

* Frequently these emails make some form of urgent appeal to provoke you to take action immediately. For example, stating that your account may be closed if you fail to confirm, verify or authenticate information immediately.
* There are embedded links that look legitimate because they contain all or part of a real company's name. These links take you to fraudulent sites (or pop-up windows) that ask you to enter, confirm or update sensitive personal information. Sometimes the emails instruct the recipient to enter the information into the body of the email.
* There may be obvious spelling or grammatical errors.
* The writing may be awkward or inappropriate.
* The visual or design quality may be poor.
* Fraudulent emails typically will not provide alternative methods for communicating the requested information (i.e., telephone, mail, and physical locations).
* Fraudulent emails often provide a general greeting and don't identify you by name.
* Fraudulent emails may contain attachments asking you to install software so that fraudsters can use it to record your keystrokes and online activity.

LaSalle Bank does not:

* Send urgent or time-sensitive emails that ask you to provide, update or confirm sensitive data like your Online User ID or Password, Personal Identification Number (PIN), Social Security Number, ATM/Debit Card or account number, credit card number or expiration date, or mother's maiden name.
* Require you to enter anything other than your Online User ID and Password to login to LaSalleOnline.
* Send you an email that tells you to provide personal information because it's for your own security.
* Send you an email with input fields that ask you for sensitive information.
* Send emails without providing alternative methods of communication.
* Send email with attachments asking you to install software.

Paul McDougall wrote an article for Security Pipeline outlining why outsourcing Information Technology (IT) functions to Arab countries would defeat Al-Qaeda. Check the article for yourself at

http://www.securitypipeline.com/165701882 . I think he does not have a good grasp of reality.

Podcasts are becoming the next big fad. IPod is Apple Computer's small music player (**http://www.apple.com/ipod/**). Apple sells music for the IPod. Other audio content is available at various Web sites (**http://www.podcastalley.com/** , **http://www.podcast.net/** , and **http://www.odeo.com/**). This content includes radio programs - like Rush Limbaugh (**http://www.rushlimbaugh.com/**). Some of this content is free (not Rush). If you own an IPod, you may want to check out those sites. Some of these programs will also run on MP3 players.

Between you, me and The Lamp Post that's all for this month.

Computer Hysteria: Crash!
by Berry F. Phillips
Member of the Computer Club of Oklahoma City
and a regular writer for the CCOKC website and the
eMonitor bfpdata@gbronline.com

Crash! Crash! That was the sound of Stephen King's sledgehammer bashing the car that hit him while jogging. Perhaps he thought Christine from his earlier horror novel had come back to haunt him!

Crash also strikes terror in the hearts of computer users. According to the Pew Internet and American Life Project approximately two thirds of Americans use the Internet and about 87% of them through connections in their homes. While there is no research data on the number of computer users that cannot master their computers, there is evidence of anger and frustration with computers that could escalate into what one psychologist calls "computer rage."

University of Maryland Professor Kent Norman says, "Men and women are taking out their frustrations on the computer and unfortunately, sometimes misdirecting it to other people." Norman, who directs the Laboratory of Automation Psychology and Decision Processes at the University, conducted an online survey where twenty percent of the respondents admitted they dropped a computer on the floor out of anger. They described smashing, microwaving, and cursing their computers. One claimed he threw his laptop in a fryer and several claimed to have shot hardware. The study further suggested computer users were most annoyed by: e-mail snafus including spam, waiting while a computer completed a simple task, having to redo something because of a glitch and having to upgrade obsolete programs. Microsoft ranked high on the list of objects of ire. With the increased popularity of wireless networks, DVD players, and game systems, the possibilities of irritations are almost endless.

You can lower your cyber blood pressure by taking some preventative medicine. Increase your knowledge to make yourself a more-informed user. Join the Computer Club of Oklahoma City and network with other computer users

and learn from their experiences (misery loves company!). Do NOT go on the Internet without a regularly updated and weekly-maintained complete computer security system including antivirus, anti-spyware and firewall software. (Not having the money for commercial applications is no excuse as there are several excellent freeware security software programs available online. Often forgotten is a good registry and unnecessary-file cleaner that has automatic backups, which can substantially reduce your crashes. Defrag weekly if needed and scandisk at least once a month. Do not forget to make an emergency boot disk.

Finally, in case of a crash, do not panic. Write down what you did immediately prior to the crash, and any instructions you receive from your computer. Make sure you have been taking fruit to lay at the feet of your computer guru or lay money on your friendly computer tech. The life you save may be your own computer. SOS stands for Save Our System!

There is no restriction against any non-profit group using this article as long as it is kept in context with proper credit given the author. APCUG

CAEUG OFFICERS & CHAIRPERSONS

President	Mike Goldberg
V.P. (Programs)	Frank Braman
Secretary (& donuts)	Dean Holste
Treasurer	L. Johnson
Newsletter Editor	Kathy Groce
Membership Chairperson	
& Circulation Manager	Pete Nicchia
CAEUG COD Coordinator	
& Publicity	Terry Moye
Software Reviewer	Brian Noon
Webmaster	
& Technical Consultant	John St. Clair
Coffee Service	Joan Thompson
Picnic Chairpersons	Mike Goldberg
	Roger Kinzie

Reminder: You'll get better, faster service if you use CAEUG in the subject of your e-mail.

ABOUT THE NEWSLETTER:

This printed version of our newsletter was laid out using **Adobe's Pagemaker Version 7.0** for Windows.

The opinions expressed in this newsletter are not necessarily those of the CAEUG Officers, members or other contributors. CAEUG, its officers, newsletter editor, authors or contributors are not liable in any way for any damages, lost profits, lost savings, or other incidental or consequential damage arising from the use of the information provided herein. Every reasonable effort has been made to confirm the accuracy of the contents of this newletter, but that accuracy is not guaranteed.

Permission is granted to reproduce any or all parts of this newsletter for personal use. Also granted is permission to reproduce for publication any part of this newsletter provided that a copy of the publication is mailed to CAEUG, immediately following publication and CAEUG is given credit.

The CAEUG newsletter is published eleven times annually. Contributions by members are encouraged and will be gratefully acknowledged in the newsletter. We have a policy of exchanging newsletters with other users groups across the nation. Several CAEUG member articles have already been picked up and reprinted.

MEMBERS HELPLINE

Any member with a specific expertise can volunteer to be on the Members Helpline.

Beginner Helpline . . . . Billy Douglas

Beginner hardware problems .Dick Fergus

QuickBooks, Turbo Tax, IBM Lotus, MS Excel, Corel's Quattro Pro . . . Terry Moye

Hardware problems, Win 9x, 2K, XP & Linux . . . . John Spizzirri

NEW Money Saving Offer for CD of the Month
Pre Order + Prepay = SAVE $$

The club will offer the CD of the Month on a pre order, prepaid basis. The charge will be $70.00 a year for 9 months. This is $20 annual savings over buying them for $9 each month. Lynn Johnson, the treasurer, will keep track of anyone placing a 9-month order.

Beginner's SIG

Ask questions and discuss computer experiences with this group.
Such as:
1. New to Computers? (basic topics)
2. How to use the Web or download information
3. How to install hardware/software
4. Discuss how to troubleshoot hardware conflicts, learn boot up emergency tricks
5. What do you want to know??

SIG meets before regular meeting from 9:05 to 9:45

Membership Costs.....

	First Yr.	Renewal
Individual	$25.00	$20.00
Family	$30.00	$25.00
Corporate	$30.00	$25.00
Associate	$20.00	$15.00

CAEUG
P. O. Box 2727
Glen Ellyn, IL 60138

FIRST CLASS MAIL

Meeting place and date information:

The next REGULAR meeting will be held at the
Glenside Public Library in Glendale Heights
starting 9:45am on
Saturday July 23

The library is located. Please park at the West side of the lot, away from the building. Thank you. The meeting(s) are not library sponsored and all inquiries should be directed to Mike Goldberg at MikeGold60137@yahoo.com. Individuals with disabilities who plan to attend this program and who require certain accommodations in order to observe and/or participate in the program are requested to contact CAEUG president, Mike Goldberg at MikeGold60137@yahoo.com, at least five (5) days prior to the program, so that reasonable accommodation can be made for them.

CONFIRMED Meeting dates for 2005 at Glenside Public Library:
July 23, August 27

NEW CD OF THE MONTH FORMAT: Is now available in **two** (2) flavors. The **Basic CD** will be packed with the standard items, while the **CD of the Month** will have NEW and updated items. Both are available at the meeting.

Presentation for July will be about Web Ads

CAEUG website has a new home.
Remember to change your bookmark to the new address at   http://www.caeug.net