OTTAWA PC NEWS

Volume 35, Number 9 November 2018

MULTI PRODUCT REVIEW

Protecting your passwords

by Chris Taylor

Security experts say you should use unique, complex passwords for each service you use. My memory was good enough for me … up until about 6 or 7 different services. I now have dozens and I can’t remember them all.

A password manager stores all your passwords in an encrypted vault. You just have to remember one password to open the vault. As long as you use a unique, long, and complex password for the vault itself, all of your passwords inside are secure. There are lots of password managers to choose from. This article is not intended to be all-inclusive. I am not even saying I think these are your best options. It’s about how I chose a password manager.

Proven cryptography

Cryptography is very easy. *Good* cryptography not so much.

Bruce Schneier, a highly-respected cryptographer and security pro wrote, “Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can't break. It's not even hard. What is hard is creating an algorithm that no one else can break, even after years of analysis.”

Here I simply have to trust others; I am not a cryptographer. I did web searches to see if lots of others believe a given password manager uses a proven encryption algorithm and has implemented it properly. An open source solution is highly desirable; maybe others who understand encryption will look for flaws in the source code.

Features

I then looked at features. My shortlist; free; not locked into a service run by a provider who may start charging or go out of business; portability (ability to run without installation); a notes field to add related information; and multi-platform (Windows and Android) so I could access my passwords from all my computers and my phone.

Password Safe

Password Safe
Simple & Secure Password Management

Password Safe (https://pwsafe.org/) is a free open source password manger that uses the Twofish encryption algorithm. Designed by Bruce Schneier, I trust the encryption is implemented properly.

Password Safe can generate random, strong passwords for you. It can autofill web page logon screens to save you typing. The Windows clipboard is securely cleared afterwards, but only when Password Safe is closed or you click a button on the toolbar. There is a *Notes* field where you can store information related to a password entry.

Password Safe automatically locks the database if you have not used it for 5 minutes, helping keep secrets secret.

(Continued on page 6)

Inside this issue:

Calendar / Coming Up / Raffle	2
Protecting your passwords	1, 6
December Auction for The Food Bank	3
Nominations for 2019 OPCUG Board	3
Motion to reduce membership fees	3
Safely Removing a USB Drive in Linux	4
Security—it’s all about layers	5
OPCUG Free Software Guide—Part 83	7
Contact Information	8

Next Meeting: WEDNESDAY, November 14th, 2018

November Raffle

This month's raffle prize is the **Case Logic LoDo Satchel**.

The thickly padded laptop compartment fits laptop with up to 15" screen size. It also includes a protective space for a 10" tablet. The unique wide-mouth opening provides easy access and visibility to gear. It has a cotton canvas exterior with leatherwrapped handles and zipper pulls and an adjustable shoulder strap. Two easy-access external accessory pockets have magnetic snap-closure. The removable shoulder strap adjusts for a custom fit. Two interior pockets keep your gear neat and there are two exterior water bottle pockets.

Tickets are $1 for one, $2 for three, or $5 for ten.

Coming Up…

➔Wednesday, November 14, 2018

Topic: #PasswordPhrasing, the Easy, Silly, Secure & Safe Technique for the People
Speaker: Lawrence Patterson; IT Manager / ISSO / ITIL & ordinary computer guy

#PasswordPhrasing, is all about making it easier for individuals to manage their passwords. Lawrence will review the changing landscape of keeping our lives secure by evangelizing our individualism, showing how typing the same set of characters can be bring an inner smile as well as thoughtful techniques that'll focus less on the complexity and more on how we each think.

Acknowledging that the password advice has varied significantly in last couple of years and expecting to change further in the coming months / years, Lawrence will explore the challenges and discuss why #PasswordPhrasing importance to all of us. All the while making the connection between passwords and footwear.

Lawrence's decades' experience supporting, planning, implementing technology from the perspective of the help-desk to management, continues to be passionate about keeping day to day technology practical to everyone needs.

Currently Lawrence works for the "The Association of Faculties of Medicine" / AFMC as IT Manger, with certification in ISSO (Information Systems Security Officer), ITIL (Information Technology Library) and has built solutions involving finance, human resources, health & safety, communications, audio visual and facilities.

For meeting updates and additional details, visit http://opcug.ca/regmtg.htm

October Prize Winners

Our raffle for a copy of the Glasswire Firewall software was won by **Tim Hillock**.

And our door prize of a wood paddle to use as a BBQ Grill cleaner went to **Ken Carruthers**.

Have a **CDTT** at Nov's Meeting

November bringing in the chill?

Looking to have a hot beverage while enjoying some down to earth geek talk?

OPCUG has just the thing, as we'll be having **C**offee, **D**ecaf, **T**ea and **T**imbits and we'll see if that'll warm your heart and mind as we try CDTT to see if it's something our members & guests are interested in continuing.

Look forward to sharing a CDTT with you all in November.

2018 CALENDAR

Meetings	Date	Time and Venue
OPCUG General Meeting	Wednesday, November 14th	7:30 p.m. at the Riverside United Church, 3191 Riverside Drive, Ottawa. Parking is free. OC Transpo bus #87 stops nearby. Visit http://opcug.ca/regmtg.htm for directions.
Q&A Session	Wednesday, November 14th	Immediately following the OPCUG General Meeting.
Beer BOF (Wing SIG East)	Wednesday, November 14th	10:00 p.m. (after the Q&A) at the Riverside Pub, 3673 Riverside Drive. Turn left onto Riverside Dr. from the Church.

December Auction for the Ottawa Food Bank

The OPCUG had a backup computer for it's online presence, but now that we have switched to the cloud, we no longer need it and offer it for auction, with the proceeds to go the Ottawa Food Bank.

The computer needs to be picked up at the OPCUG December 12th meeting. If the online winning bidder is not there, then it will be offered to a person in attendance with the highest bid. You must be a member of the OPCUG.

The online auction ends at 5pm, and bidding can continue in person at the meeting until the end of the meeting's presentation.

Online auction bids can be sent to: silentauction@opcug.ca.

Computer specs:

Acer AX3475-ER30P
AMD quad core A8-5500 3.2 GHz with Radeon 7560D graphics
HDMI and VGA ports
8 GB RAM (can go to 16 GB)
2 TB, 7200 rpm hard drive
DVD optical drive
Card reader
7 USB 2 (4 in back, 3 in front)
4 USB 3 (2 in back, 2 in front)
Windows 7 Home Premium
Keyboard
Extreme model JS555 15" LCD monitor

NEWS FLASH!
OPCUG's 2018 Fall Workshop - Computer Tune-up is now being run in partnership with the Ottawa Public Library and, as a result, there will be no cost to attend. Full details are posted at: http://www.opcug.ca/workshop. Note that (free) registration is now being processed through the library's web site.

Nominations for OPCUG Board for 2019

Once a year, the OPCUG holds elections for the 9-member Board of Directors. We are once again coming up to this annual event.

We encourage all members to consider running for a board position or getting involved in some other manner in the operations of the OPCUG.

Nominations can be submitted to nominations2019@opcug.ca or in person at the November and December club meetings

If you want more information about what is involved, please talk to a current or past Board member. Board members are listed on the back page of this newsletter and on the web site at http://opcug.ca/exec.htm.

Nominations must be received by midnight, December 31, 2018.

Please get involved. Please help the OPCUG continue in its role of ***Users Helping Users***!

Notice of Motion

The club's recent move to a new meeting venue resulted in an increase in annual expenditures of approximately $1000.00. In contrast, switching our web presence to external hosting services, and eliminating printing and mailing costs for the hard-copy newsletter, will reduce expenditures by approximately $2000.00 per annum. The net result of these actions is projected to be an annual increase in capital assets of about $1000.00. Since OPCUG is not-for-profit corporation, the Board of Directors takes the view that we should adjust our on-going fiscal position accordingly by reducing income and/or increasing expenditures. One of the actions that the Board is proposing is to reduce the annual membership dues. Under the terms of our constitution, this requires the approval of the membership at a general meeting. In consequence, the following motion will be presented at the club meeting to be held on December 12, 2018:

Motion: *Resolved that membership dues be reduced from the current level of $25.00 to $20.00 with effect from January 1, 2019.*

Safely removing a USB drive in Linux

by Alan German

I do most of my computing using the Linux side of my dual-boot system but, just occasionally, I use that other operating system! And, one thing Windows does that I find really useful is tell me when it's safe to remove my external USB drive after I click on the icon to "Safely Remove Hardware and Eject Media". Linux Mint 18.2 (Sonya) produced a message indicating that "It is now safe to remove the drive"; however, I sometimes noticed that, even though this message was displayed, the red LED on my USB flash drive was still flashing. This would seem to indicate that disk activity was still underway, and it wasn't necessarily safe to pull the plug. Furthermore, the safe-to-remove message does not occur in Linux Mint 18.3 (Sylvia) – perhaps because it didn't really work?

Of course, I could simply watch the red LED, and wait for it to stop flashing, before removing the drive but, on the particular flash drive I regularly use, the LED is usually hidden by a swivelling metal cover. Rather than always having to fiddle with the drive, I decided to see if I could develop a bash script that would wait for any cached data to be written to the USB drive before indicating that it was indeed safe to remove the external drive. The solution I came up with, after reviewing a lot of suggestions on on-line forums, is the following bash script:

```
#! /bin/bash
# Eject USB drive once buffer transfer has completed
echo "Flushing USB drive buffer"
sync
echo "sync complete"
# Identify the device name for the SILICON16GB USB drive
usblongname=$(lsblk -l | grep SILICON16GB)
usbname="${usblongname:0:4}"
# Unmount the USB drive
udisksctl unmount -b /dev/$usbname
echo "unmount complete"
# Power off the USB drive
udisksctl power-off -b /dev/$usbname
echo "power off complete"
# Script complete
echo "Shell command complete"
read
```

The script undertakes three main tasks. Firstly, it calls the sync command to ensure that any disk writes are complete before proceeding. Sync doesn't return control to the main script file until any/all cached data have been written to the USB drive. Secondly, a combination of lsblk and grep is used to identify the device name for the USB drive of interest. This is necessary since, if multiple USB devices are plugged into the computer, the device name (e.g. /dev/sdg1) may not always be the same. The last four characters in the device name (e.g. sdg1) are saved to a "usbname" variable for use in unmounting and powering off the USB drive. Finally, the udisksctl command is used to unmount the USB drive and then power it off.

Note that the above-noted script has the name of my USB flash drive hard coded as "SILICON16GB". This designator should be changed to suit a different user's system. Also, udisksctl is part of the gnome-disk-utility package so this package should be installed if it is not available by default.

The script is "fail-safe" in that, if there is no USB drive present, it will display errors indicating that the USB device could not be found. If there is no or little disk activity, the script will return the message "Shell command complete" almost instantly. If writing a large file, or a number of smaller files, to the USB drive is in progress when the script is run, the display will pause briefly, after the initial "Flushing USB drive buffer" message, and will then complete normally.

♦♦♦

ARTICLE

Security – it's all about layers

by Chris Taylor

I once heard, "The only secure computer is encased in concrete and dropped in the middle of the ocean. And even then, I am not really sure." There is no such thing as absolute computer security; it's all about layers. If one security layer fails, you hope another layer will provide the protection you need.

In the beginning (i.e. the mid 1980s), personal computer security focused on antivirus. The aim was to block known bad programs from running on your computer. With few personal computers networked, viruses spread slowly. Back then, antivirus signature files were updated about once a month and that actually served us pretty well.

In the 1990s, Internet connectivity grew exponentially, as did security threats. Even Microsoft understood (albeit a little late) that more than just antivirus was needed and introduced a firewall in Windows XP SP2 in August 2004.

> ***"The only secure computer is encased in concrete and dropped in the middle of the ocean. And even then, I am not really sure."***

In January 2003, the SQL Slammer worm spread to 90% of all vulnerable hosts world-wide in the first 10 minutes after release. It exploited a vulnerability for which a patch had been available for 6 months. Vulnerability management was born in the realization that few users would, or indeed *could reasonably be expected to* keep all their software up-to-date with security patches.

The fundamental concepts behind antivirus, firewalls, and patch management have not changed over the years. But each has become more complex.

Blocking "known bad" with antivirus signature files is arguably essential. But now, with more than 10 million new malware variants per month (https://www.av-test.org/en/statistics/malware/), it is not enough. Antivirus programs use heuristics to catch unknown malware. More and more are using real-time blocking techniques to stop new malware before you get updated virus signature files.

To this day, the firewall built into Windows (now called *Windows Defender Firewall*), is aimed solely at blocking unsolicited inbound connections. While this is extremely helpful – indeed essential – from a security point-of-view, Windows Defender Firewall eschews more advanced capabilities, such as blocking outbound connections unless you authorize them. While members of the OPCUG are more likely to be able to handle issues regarding computer security than the average member of the general public, Microsoft does not want to deal with even a very small fraction of their billions of users not being able to figure out if some program should be permitted to access the Internet.

Vulnerability management has evolved. Microsoft's Windows Update service has matured since it was introduced with Windows 98. While not problem-free, Windows Update is remarkably robust. Other vendors have added self-updating capabilities and most are quite reliable. Unfortunately, a lot of vendors don't include automatic updating capabilities. I should add that my biggest concern is about patching security vulnerabilities, not feature updates.

Secunia Personal Software Inspector, which was bought a number of years ago by Flexera, was a wonderful vulnerability management program. PSI tracked over 20,000 programs for security vulnerabilities and patches. Unfortunately, that program went end-of-life in April, 2018. I have yet to find a good replacement for PSI. Some former employees of Secunia are building a new vulnerability management program (https://vulndetect.com/), so hope remains.

Computer security goes well beyond these technical safeguards, but I think antivirus, firewalls, and vulnerability management represent the bedrock of computer security. Every computer user should embrace all three and watch for advancements in each to keep ahead of the latest threats.

Passwords *(Continued from page 1)*

There is a Windows installer version, a portable version, and a free, unofficial Android port.

As an aside, Schneier's newsletter *Crypto-Gram* (https://www.schneier.com/crypto-gram/) and blog *Schneier on Security* (https://www.schneier.com/) are well worth reading.

KeePass

KeePass
A lightweight and easy-to-use password manager
Brought to you by: dreichl

KeePass (https://keepass.info/) is well-known, free, and open source. It supports the Advanced Encryption Standard (AES) and the Twofish algorithm to encrypt its password databases. Both are highly regarded.

KeePass includes measures to protect against dictionary and guessing attacks. Process memory protection keeps your passwords encrypted while KeePass is running, so they are not revealed even when Windows dumps the KeePass process to disk. There are protections against keyloggers.

There are lots of convenience features. It can generate complex passwords. Usernames and passwords can autofill web logon screens and information it puts on the clipboard is automatically cleared after a user-defined time period. There are many options including the ability to automatically lock the vault after a user-defined period of inactivity.

A *Notes* field allows you to store other sensitive information such as your Social Insurance Number. Entries can even store file attachments, such as a photo of your passport or birth certificate.

There's a Windows installer version and a portable version. Even the installer version does not write outside the program directory, other than to create the program directory and Start menu icons. KeePassDroid is an unofficial, open source Android port.

I've been using KeePass and KeePassDroid for many years and am very satisfied with both.

I store my KeePass vault in a local Google Drive folder, which is automatically synched between all my computers and phone. The KeePass portable program files are also on my Google Drive, so I can access my passwords from any internet-connected Windows computer.

Standard Notes

Standard Notes

If you don't want to mess with setting up your preferred cloud storage to store your password vault and configuring all your devices to access the vault from that location, *Standard Notes* (https://standardnotes.org/) is an interesting free & open source note manager. It is not designed as a password manager, so don't expect it to generate passwords, enter your password into web sites, etc. But it can be used to manage any text-based information, including passwords.

Standard Notes uses AES-256 for encryption with a password-stretching algorithm (https://en.wikipedia.org/wiki/Key_stretching) with over 100,000 iterations.

Beyond being secure, what I like about Standard Notes is that a free account allows automatic database synchronization between all your devices. If you worry that the vendor might go out of business, you can self-host the synchronization back-end.

Standard Notes is available for Windows, Android, Linux, iOS, and Mac. You can also access your notes through a web site (https://app.standardnotes.org/)

A puzzling default

Standard Notes assumes your operating system has been adequately secured; to the extent that, once you open your vault the first time and provide the password, it will never ask for your password again if you are logged into the OS.

If the operating system's security is adequate, why bother with a password manager at all? Many people treat their overall Windows experience in a low-security fashion with a weak or even no password. Then they want to treat specific sensitive information in a more secure fashion. Fortunately, Standard Notes does have an option, which I highly recommend, to add a password requirement every time you open your vault.

♦♦♦

OPCUG Free Software Guide—Part 83

Compiled by Alan German and Micheline Johnson

This guide features an annotated list of free computer programs. The software mentioned has not been reviewed (except where noted) nor have any tests necessarily been conducted. Consequently, no guarantees are provided that the individual programs will perform as described. Rather the list of available software is provided for the information of our members who may find one or more of the programs useful.

Qihoo 360 Total Security
Five anti-virus engines in one product! Integrating award winning engines from 360 Cloud Scan Engine, 360 QVMII AI Engine, Avira and Bitdefender to provide you with the ultimate in virus detection and protection capabilities.
Web Site: http://www.360totalsecurity.com/

Folder Size Explorer
This simple and very fast disk space analyser is similar to Windows Explorer but it calculates folder sizes as you browse them, and allows you to quickly identify directories on your hard drive or network that are consuming the most disk space. It can also calculate checksums (MD-5, SHA-1, SHA-256 and SHA-512) of all your files, and will save file and folder lists to CSV files for viewing in external applications like Excel and Notepad.
Current Release: Version 2.0
Web Site: https://www.folder-size-explorer.com

Just Basic
Remember BASIC from the good old days? Just BASIC is based on the classic BASIC programming language. It is easy to learn, and it has been extended with structured programming facilities and easy-to-use GUI commands so you can create your own Windows programs without needing to learn all the underlying details of the Windows operating system.
Current Release: Version 1.01
Web Site: http://justbasic.com/

Encircle
Conveniently add items that you own to an inventory, ensuring that you have the necessary information if you ever need to file an insurance claim. Create your inventory room-by-room by simply taking photos with your Android smartphone or tablet.
Web Site: http://tinyurl.com/zpjmotc

IncrediMail
Have fun sending E-mail! Share photos right in your email. Decorate messages with backgrounds. Share funny emoticons and animations. Send fantastic animated E-cards.
Web Site: http://www.incredimail.com/en

Krut
Capture movie files, including sound, playing on selected parts of your screen. Krut records separate files for audio (wav) and video (mov), which allows for easily transforming the results to any movie format using an external encoding program. The program runs on Windows with Java installed.
Current Release: Version 0.9.3
Web Site: http://krut.sourceforge.net/

Winyl
A free digital audio player and music library application for Windows. Listen to music and radio, rate your favorite tracks, create playlists, browse song lyrics, and tag music files.
Current Release: Version 3.2.1
Web Site: http://vinylsoft.com/

Future Pinball
Future Pinball is a real time Pinball Development System. It allows you to design and play your very own pinball simulation in True real time 3D. It uses Advanced Physics to provide the best possible Simulation of a true to life pinball machine.
Current Release: Version 1.9.1.20101231
Web Site: https://futurepinball.com/

OTTAWA PC NEWS

Ottawa PC News is the newsletter of the Ottawa PC Users' Group (OPCUG), and is published monthly except in July and August. The opinions expressed in this newsletter may not necessarily represent the views of the club or its members.

Member participation is encouraged. If you would like to contribute an article to Ottawa PC News, please submit it to the newsletter editor (contact info below). Deadline for submissions is three Sundays before the next General Meeting.

Group Meetings

OPCUG meets on the second Wednesday in the month, except July and August, at the Riverside United Church, 3191 Riverside Drive, Ottawa. Parking is free at the church. OC Transpo bus #87 stops nearby. Details at http://opcug.ca/regmtg.htm.

Meetings are 7:30–9:00 p.m. followed by a Q&A Session until 10 p.m.

OPCUG Membership Fees:	$25 per year
Mailing Address:	3 Thatcher St., Nepean, Ontario, K2G 1S6
Web address:	**http://opcug.ca**
Follow us on Facebook:	**https://www.facebook.com/opcug**
Follow us on Twitter:	**https://www.twitter.com/opcug**

President and System Administrator	**Chris Taylor**	chris.taylor@opcug.ca	613-727-5453
Meeting Coordinator	**Bob Herres**	meetings@opcug.ca	
Treasurer	**Alan German**	alan.german@opcug.ca	
Secretary	**Gail Eagen**	gail.eagen@opcug.ca	
Membership Chairman	**Mark Cayer**	mark.cayer@opcug.ca	613-823-0354
Newsletter	**Brigitte Lord** (editor/layout/e-distribution)	brigittelord@opcug.ca	
Public Relations	**(vacant)**	info@opcug.ca	613-366-7936
Facilities	**Bob Walker**		613-489-2084
Webmaster	**Brigitte Lord**	webmaster3@opcug.ca	
Privacy Director	**Wayne Houston**	privacy2@opcug.ca	
Special Events Coordinator	**(Mr.) Jocelyn Doire**	jocelyn.doire@opcug.ca	
Director	**Lawrence Patterson**		

How to get the OTTAWA PC NEWS by e-mail

Here's how to get the OPCUG newsletter by email:

Create a Google Account

Any valid email address can be used as a Google Account. Pick an email address you want to use and browse to **https://accounts.google.com**. Click *Create account* and follow the instructions.

Make sure your new Google Account is functioning properly by going to **https://accounts.google.com** and signing in.

Sign up for the OPCUG Google Groups

Browse to **https://groups.google.com**. If you are not signed into your Google Account, click the *Sign in* button at the top.

1. In *Search for groups or messages*, type *OPCUG*. The top of the search results will show Groups matching OPCUG. Click on *See all 3*.

2. Click on *OPCUG-Newsletter*, then click the *Join group* button. In the resulting dialog box, you can opt to change some preferences, such as;

    a. If *My display name* shows as your email address you can change this to something like *firstname lastname*

    b. Email preferences can be changed to only send daily summaries or not email you at all when new postings are made (meaning you must manually check at the web site to see if there are any new postings)

3. Click the *Join this group* button.

4. You will then see the list of postings that have been made to the group. Click on any entry to see the actual posting.

More detailed instructions on how to join this and other OPCUG Google Groups are found here:

http://opcug.ca/public/GoogleGroups.html

There are no issues of the newsletter published in July or August.