



Keeping your Computer Secure (updated)

John Steele

Why are we doing this again?

- **This is an update on a talk about a year ago**
- Security threats evolve
 - We need to keep up to date and aware
 - Even the computer chip microcode has been hacked!
 - Vulnerabilities have been found in our Internet Routers
- We need to be reminded that is is an increasingly dangerous world out there
 - Our homes have additional Internet connected devices
 - Alexa, Echo can listen in to you
 - “Internet of Things” devices can weaken your computer security

Keeping your computer secure

- What are the threats we face
 - Every time we switch the computer on
 - Every time we open an email
 - Every time we access a web site
 - Every time we get “we are from Microsoft” telephone call
- What can we do about them
 - Be alert
 - Technical measures
 - Account management
 - Password management

What are the threats we face

- Clever criminals want to gain access to your assets for their own ends:
 - Steal your identity
 - Steal your money
 - Use your computer for their own ends e.g.
 - To use your computer to crack security
 - Cryptocurrency mining
 - To use your computer to mount an attack on other victims

Steal your identity

- Your identity is valuable
 - Personal details can be used to impersonate you
 - Security question responses can be harvested from hacked sites
 - Passwords can be retrieved from sites that do not treat security seriously
 - One vendor's site recently echoed my user ID and password back to me by email as confirmation of my account creation! I had to change it immediately!

Steal your money

- Accounts can be created in your name
 - I have had credit cards fraudulently applied for (and in one case issued) in my name
- Bank account details can be captured by “key logging” software infiltrated into your computer
- Credit card details can be obtained from web sites and used to make fraudulent transactions
 - I have had one credit card used fraudulently
 - The reissued card was also fraudulently used before I received it!

Attackers can use your computer

- If your computer gets compromised it can be used to attack other computers
 - Generate spam emails originating from YOUR computer
 - Can propagate viruses
 - Can participate in “denial of service” attacks on victim sites
 - Typically commanded remotely and could lie dormant for weeks
 - Etc.
- Run their own programs – cryptocurrency mining

Malware – what is it?

- Malware
 - Malicious software installed on your computer
 - Designed to capture and forward information as you use your computer
 - Scan your computer looking for “interesting” information
 - Lock out you from your computer
 - e.g. Ransomware that encrypts your data and demands money to recover it
- Potentially unwanted programs (PUP)
 - Usually related to targetting advertising and harvesting your browsing history

How does Malware get into your computer

- Exploiting security bugs in programs
 - Often reported and patched
 - Can be exploited through links in web sites or emails
- Tempting links inviting you to click but then installing unwanted software in Web sites, or emails, or in documents sent as attachments
 - You took the action (innocently/unintentionally) to allow it to happen
- **Such exploits are far less likely to happen if you normally use a Standard User account**
 - Software installation needs Administrator privileges

Don't Panic!

- The weakest link in the chain is YOU!
 - Be vigilant and think before you click
 - Is that telephone call genuine
- You can see the target web page in an email if you hover the mouse over the link
 - Does it bear any resemblance to what you would expect?
 - Learn to understand the format
 - Does it point to the domain that the email comes from
- **NEVER use an account with administrator privileges for anything other than deliberately installing software from known sources**

More on Accounts

- Most computers as delivered have only ONE account
 - This must be a highly privileged account to enable software to be installed
 - If you use this admin account for normal work however any dubious software that you unintentionally select can install on your computer
 - If you use a standard user account then Windows will prompt for the admin account password and without this password the software won't install – you remain SAFE
 - **Make sure you have a Standard Account and ALWAYS use it for normal work**

Other precautions – Anti Virus

- Anti Virus (Windows)
 - Must have Anti Virus installed
 - Keep it up to date!
 - Microsoft Defender is better than nothing
 - Avast! and AVG now use the same engine but are free and good enough for most of us
 - Kaspersky (if you feel you need to pay) has a good reputation until recently
 - BUT – there are some hints that the Russians Security do have some control over the company. No longer allowed for USA or UK government systems.

Anti Virus (2)

- Not too keep on the IBM Trusteer software as there are reports of problems with accessing other sites
- It is not recommended to use two AV products on the same computer
 - Microsoft Defender however cannot be removed but it shuts down if another AV product is installed
- Good idea to run a virus scan periodically
- A MalwareBytes scan is worth running from time to time.
 - In my opinion not worth paying for the non-free version

Passwords

- Many external sites require accounts to be created
 - The sites may not all handle your passwords safely
 - If/when a site is compromised your user name and password will be in the hands of the attacker and then in the dark web domain
 - Any other sites that use the same username/password pair will be accessible
 - The attacker will try known username/password pairs
- Conclusion
 - You should use different username/password pairs for EVERY such account to be safe
 - At least for accounts that matter

Passwords - 2

- Many accounts need passwords – how can you remember them
 - Passwords must be “strong” especially when credit cards are used
 - Hackers use “Rainbow Tables” to guess passwords very quickly
 - Simple character substitutions (e.g. l → 1 o → 0) can be easily hacked as the hackers know all of these tricks
 - Rainbow tables contains millions of dictionary words
 - Passwords need to be long to defeat modern computer brute force attacks, around 20 characters are now needed for financial transactions

Passwords - 3

- Password creation
 - Must not be guessable
 - Must not be dictionary words
- Can use tricks like the first letters of a phrase with a mixture of upper and lower case characters
 - but this would be a limited character set and therefore needs a longer password
- Need to record them somewhere and for them to be easy to use

Passwords - Options

- Many accounts →
 - Many user IDs and Passwords
 - Passwords at least should be unique
 - Each password should not be easily derived from another
- Too many to remember – how do you record them?
 - Notebook or sheet of paper
 - What happens if you lose it or spill coffee on it?
 - Have you kept a copy?
 - Is the copy safe?
 - Is it up to date?
 - Spreadsheet or text document
 - What happens if your computer is stolen or compromised and hence your passwords are no longer private
 - Have you kept a secure backup?
 - There is another way → KeePass

Passwords - KeePass

- KeePass solves most of these problems
 - Passwords are random and can be of any length
 - Generator can be configured to meet specific site length and character limitations (numbers, letters, special characters)
 - Makes it easy to have unique passwords on every site
 - But not easy to type!
 - Autotype solves this problem and makes it very easy to log onto most sites - even easier than typing simple passwords
 - Available for most platforms
 - Windows, iPhone, Android and (with some limitations) Mac and Linux
 - Database is encrypted and can be shared via a cloud service which also provides a backup

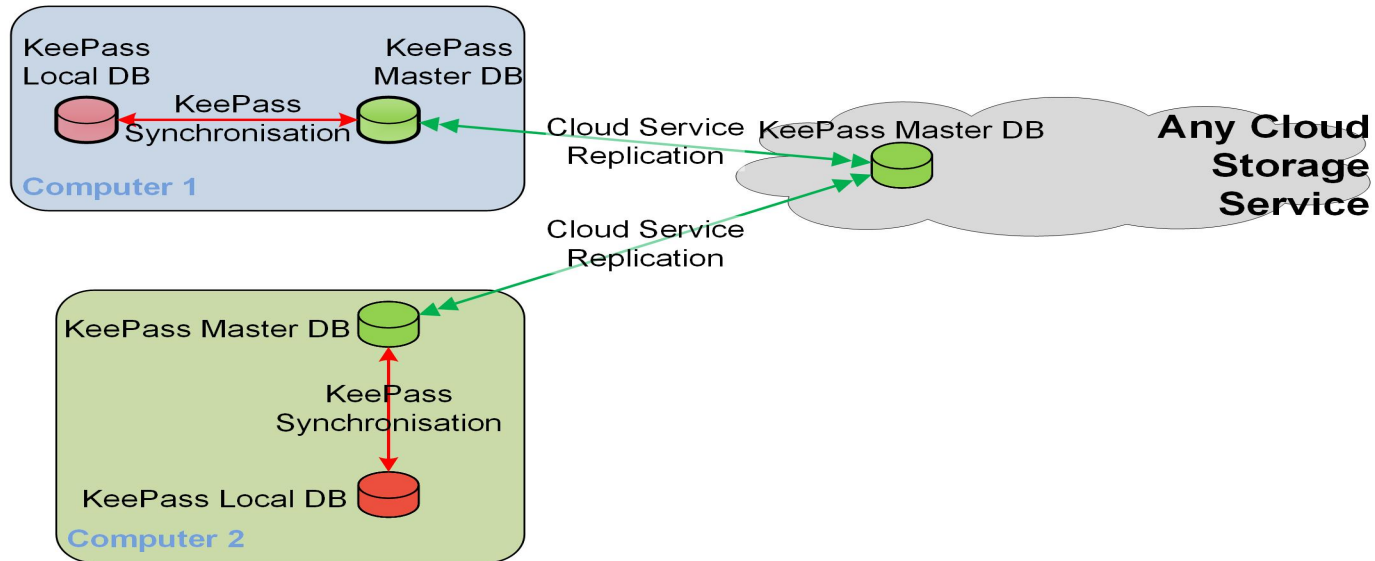
WARNING – Check carefully

- Recently a series of domains was created that looked like KeePass
 - The real KeePass domain is
 - www.Keepas.info
 - The clones included KeePass.fr – there were many more
 - These provided a front end to the KeePass pages
 - Apart from this they may have been innocuous
 - The dangerous one however was
 - Keypass.info
 - **This included a serious malware infection**

KeePass

- Features
 - Database is encrypted with one master key (password or a combination of password and key file)
 - Can safely be stored on a cloud server
 - Can easily be set up to autotype username and password into a web site using CTRL-ALT-A keys
 - Matches Web Page title or shows a list if there is more than one match
 - Database record can hold additional data
 - Such as security questions
 - Attachments (use with care keep them small)

KeePass replication



KeePass Synchronisation

- Synchronising between several computers
 - Local database opened by KeePass using the encryption key
 - Any records may be updated in the local copy
 - Triggers synchronise this with a Master database that is shared via a cloud service e.g. TeamDrive
 - The synchronised cloud database copy is encrypted by KeePass using the encryption key
 - The cloud copy is replicated to all devices that share the cloud database
 - KeePass will replicate any changes to the cloud copy on each device into that computer's local database
 - The end result is for each local copy to contain identical records but does not ensure that the files are identical

Other things you should do

- Which the best defences you may still be compromised
 - Make sure you have a backup that is up to date
 - Should be off-line so that ransomware cannot access it
 - Some evidence that network attached devices are less vulnerable if accessed by a share name //server.... rather than via a drive letter
 - Cloud storage that contains versions cannot be compromised as you can go back to an earlier version
 - TeamDrive provides this feature, not all do

Summary

- Download from sites that you know about, or that there are no adverse reports on the internet
 - Think before you click
- Use a reputable Antivirus product and keep it up to date
- Use different password on all sites (unless you don't care that your password can be accessed)
 - Use a password manager to help with managing these passwords
- Always use a Standard User Account to access the Internet unless you are installing software from a trusted source
 - NEVER use an administration account for normal day to day work
- We try and warn of new threats on the GXCC forum
 - Make sure you have joined!