KeePass
and other security issues

John Steele

Overview

- Review of security threats
  - Privacy threats
  - Local security on your computer (Windows focus)
  - Internet threats
- Overview of data protection legislation
  - Brexit!
- Steps to minimise your risk
- Password management - KeePass

What are the privacy threats we face

- What are the problems we face?
  - Compromise of your computer
    - Local account management
    - Anti-malware protection
  - Compromise of a supplier computer
    - Access of personal information
  - Identity theft
    - Impersonation – steal your credentials
    - Reputation – damaging personal information being posted
- KeyPass one solution to help protect your privacy

Local security (Windows)

- Much of your local security protection is provided through the optimum use of your local user and administrator accounts
- You obviously do need to be able to install software!
  - There must be a local user account with sufficient administration privilege to do this
    - If you use this highly privileged Admin account for all normal work you are leaving your computer seriously exposed to being compromised
  - For your safety create a Standard user account for all normal work
    - Elevate to your Administrator account only when you need it! This is not an inconvenience. It is vital protection!
- Microsoft have long recommended using Standard/Administrator accounts this way
  - I am not aware of any computer manufacturers however that encourage you to do this or even make it easy to do!

Internet based accounts

- Many Internet services require you to sign up to access their services
  - User id – typically an email address
  - Password with some rules on length, characters and complexity
- Can this be a problem - do you trust their security from hackers?
  - Many hackers investigate weak site security looking for data that can be stolen e.g. user email addresses and password and other personal information → Data Breach
- Attackers use known email addresses to guess passwords for other sites
  - You may have to use the same email address
  - You should avoid re-using the same password on multiple sites

GDPR/DPA 2018 data privacy

- All UK/EU based organisations must implement the privacy regulations enshrined in GDPR
  - GDPR is now incorporated into the UK Data Protection Act 2018 (DPA 2018)
- GDPR requires organisations to take reasonable precautions against data breaches
  - National regulatory authority can fine organisations that fail to adequately protect your data
  - Information Commissioners Office is where you report suspected data breaches in the UK
- Outside Europe the regulatory authority depends on where the organisation is based e.g. in the USA there are both Federal and State data privacy laws which can conflict with GDPR
  - USA has the CLOUD Act and California has its own California Consumer Privacy Act (CCPA)
- In all cases there are legally defined situations where your data can be released to law enforcement and national security agencies
  - You have no right to object and may not even have the right to be informed

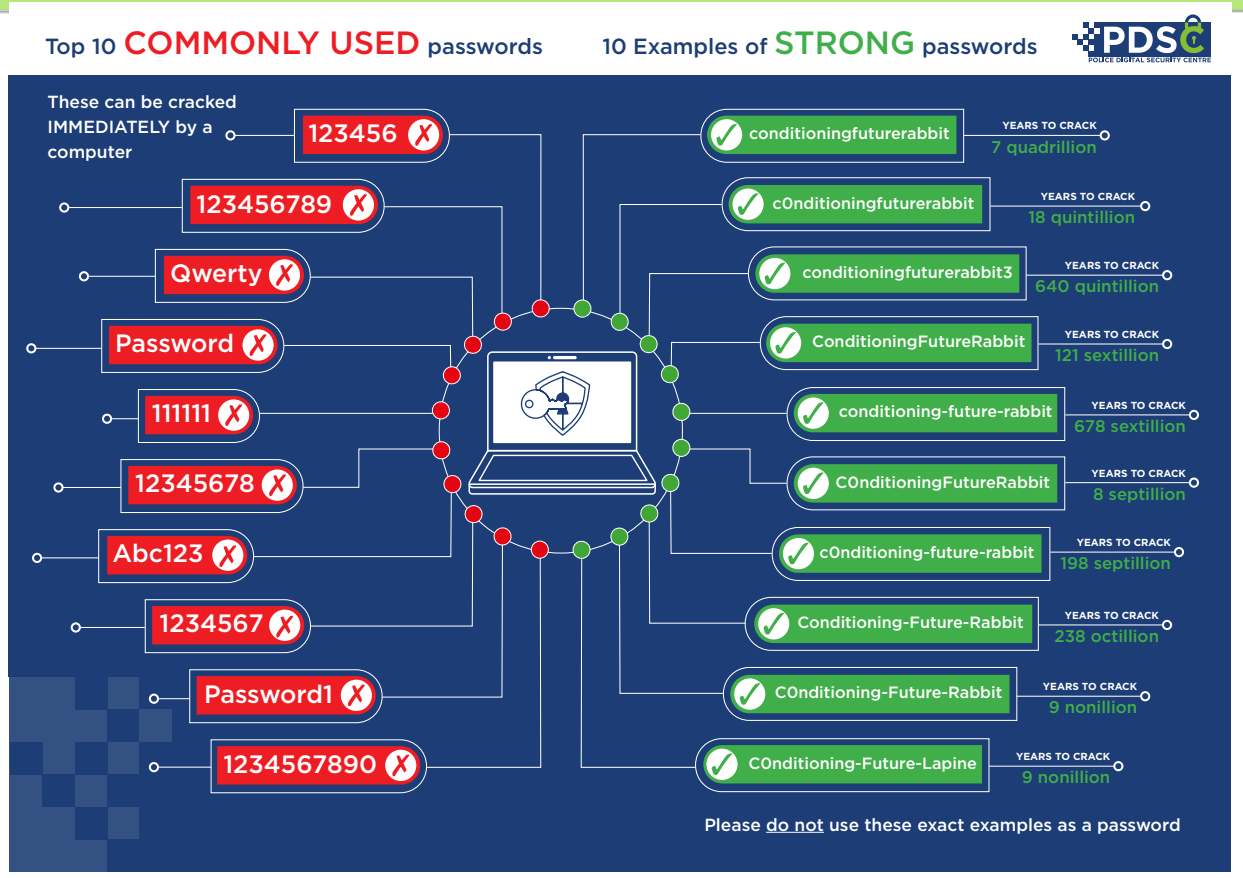
GDPR/DPA 2018 - Data privacy obligations

- All UK/EU organisations are required by law
  - to identify what legal basis they are relying on to store your data:
    - **Consent, Contract, Legal obligation, Vital interests, Public task, Legitimate interests**
  - to publish how your data is used, and whether it is shared with other parties, and how it is protected (which may vary depending on the sensitivity of that data) typically in a Data Privacy Statement and perhaps a Data Processing Statement
- Failure to protect your data adequately can lead to punitive fines
- Organisations must report Data breaches to the ICO
- Individuals can report failure to comply with legal obligations to the ICO
- Be aware that organisations outside the EU and UK do not have to comply and have their own, sometimes conflicting, rules.
  - USA has the CLOUD Act and California has its own California Consumer Privacy Act (CCPA)

What can we as individuals do to minimise risk

- Read the Data Privacy Statements, especially where the organisation is not in the UK/EU, when signing up for an Internet based service
  - If you do not like what they say – do not use the service or take care that your risk is limited
- If possible have a number of email addresses for different types of service
- ALWAYS use a different password for every Internet account
  - If an organisation does suffer a breach then you account data is compromised and if you use the same credentials elsewhere all of those accounts are compromised as well
- Your email address WILL escape into the big bad world. You can check known leaks using
  - https://haveibeenpwned.com/

Password length and complexity vs cracking



How can you manage multiple accounts

- NEVER use the same password on more than one account
  - If you can - use a different user ID and/or email address
    - A unique email address enables you to identify whether your details have been passed to another party
- A strong password must be non trivial, not easily guessed, and not derived from a common pattern and of a reasonable length e.g. more than 12 characters
  - You can get a list of the most popular passwords
    - https://en.wikipedia.org/wiki/List_of_the_most_common_passwords
- Can be entered into password fields on forms easily
- Can be one of many passwords needed – two or three can be remembered
  - What if you have 20 or 100?

What is a Password manager

- Simplifies use of many complex passwords – only one password to remember
- Stores user ID and password in an easy to find/searchable store
- Provides easy way of automatic typing into the target site
- Typically includes a random password generator must allow you to
  - Choose valid character set – not all characters may be valid on a site
  - Choose patterns e.g. at least one letter number and punctuation
  - Set password length
    - Minimum length should be at least 12 characters
      - including Upper and Lower case, digits and special characters and not contain any “dictionary” words
      - Substitutions, e.g. figure 0 for letter o or O, are well know to cracking programs
      - May need to comprise if you ever need to type especially into a phone or a catchup service on a smart TV

My Password Manager choice – KeePass V2

- Local application – does not depend on Internet Access
- Data is stored in a local file not on a web server
- Data is strongly encrypted (except when being accessed in computer memory)
  - Unlocked with a single password or a Key file or both
    - Composite password is passed through a one way hash function multiple (configurable) times typically to take about 2 seconds
    - Deliberately slow to foil password guessing attacks
      - Hence safe to store copy in the cloud and on removable storage
- Can store any additional data fields associated with the site
- Can store related files as attachments

Automated logon in many cases

- Initiated by a (configurable) key combination
  - Default = Alt + Ctrl + A
- Autotype matching on Window Title
  - Fully configurable to cope with special cases
  - Many options to allow for differing security approaches
    - e.g. Pick 4th 5th and 1st character from password
- Not restricted to Username and Password
  - Custom fields can be created e.g, for security questions

Pre-requisites before installing

- Should have a well protected computer
  - Malware can install “key loggers” that can capture keystrokes or targeted attacking programs that can detect KeePass and access potentially passwords
  - Run as Standard User, never routinely as Administrator
  - Have a well regarded AntiVirus program
    - There are some dubious products about
    - Check with known good AV comparison sites – see GXCC support site
- Download Password manager only from the author’s site
  - Here is the genuine KeePass link https://keepass.info/
  - There have been fake sites that provided KeyPass with “added extras”
    - See keepass.com and several similar sites – why take the risk!

Installing KeePass

- Download KeyPass only from the author's site
  - https://keepass.info/
    - Recommend V2 over V1 as it has greater flexibility
      - Both versions are actively maintained by the author
    - Open Source Donation ware
- All support is via the KeePass forum – KeePass Author, Dominic, actively participates
  - My forum UserID is steelej and I contribute regularly
- Installation on platforms other than Windows - Look at links on Download page
  - Most are "third party" ports and are not directly supported by the KeePass support forum although they do offer help or point you to the right place
  - KeePass2Addroid is the best port for Android devices
  - KeePassXC is a cross platform port but does not have all of the features.

Installing KeePass - recommendations

- You will be shown options to use a KeyFile when you create a database
  - This is any file that can be used as well as, or instead of, a password
    - KeePass can create one for you
    - It is up to you to back it up and ensure that NO changes whatsoever are made.
      - If it is a text file even opening it and saving without any visible change will probably change it and make it IMPOSSIBLE to open your password database.
    - Do not select this option unless you are very confident you know what you are doing!
- You will be shown an option to use your Windows account
  - **NEVER use this option – it can be very dangerous unless you are an expert.**
    - Your will probably loose all of your data if your computer crashes or Windows needs to be re-installed

KeePass Features

- Custom fields can be added to each entry e.g.
  - Bank contact details
  - Credit card number
  - Bank address
  - Etc.
- Notes
  - Use for free text notes, create new fields for any data to be typed as a data entry
- Attached documents
  - Use with care – can make database large
- Entry history (limit configurable)

KeePass extensions

- KeePass is designed to be extensible through plugins
  - I only recommend and use one for general use = KPEnhancedEntryView
    - https://keepass.info/plugins.html#kpenhentryview
    - This provides a convenient view for additional fields
  - Installation of Plugins varies with the plugin
    - In general you need to login to your administrator account to gain write access to the Plugin folder
    - For example KPEnhancedEntryView
      - Delivered as a ZIP file containing a
        - .PLGX file – this is the plugin
        - Readme file telling you how to install it

Demo time 1

- Using Main KeyPass basics
  - KPEnhancedEntryView has been installed
- If time available show installation in VM of KeyPass and KPEnhancedEntryview

Autotype fields

- Autotype placeholders
  - https://keepass.info/help/base/autotype.html
  - https://keepass.info/help/base/placeholders.html
-