Password managers

Tom Ryder
tom@sanctum.geek.nz
https://sanctum.geek.nz/

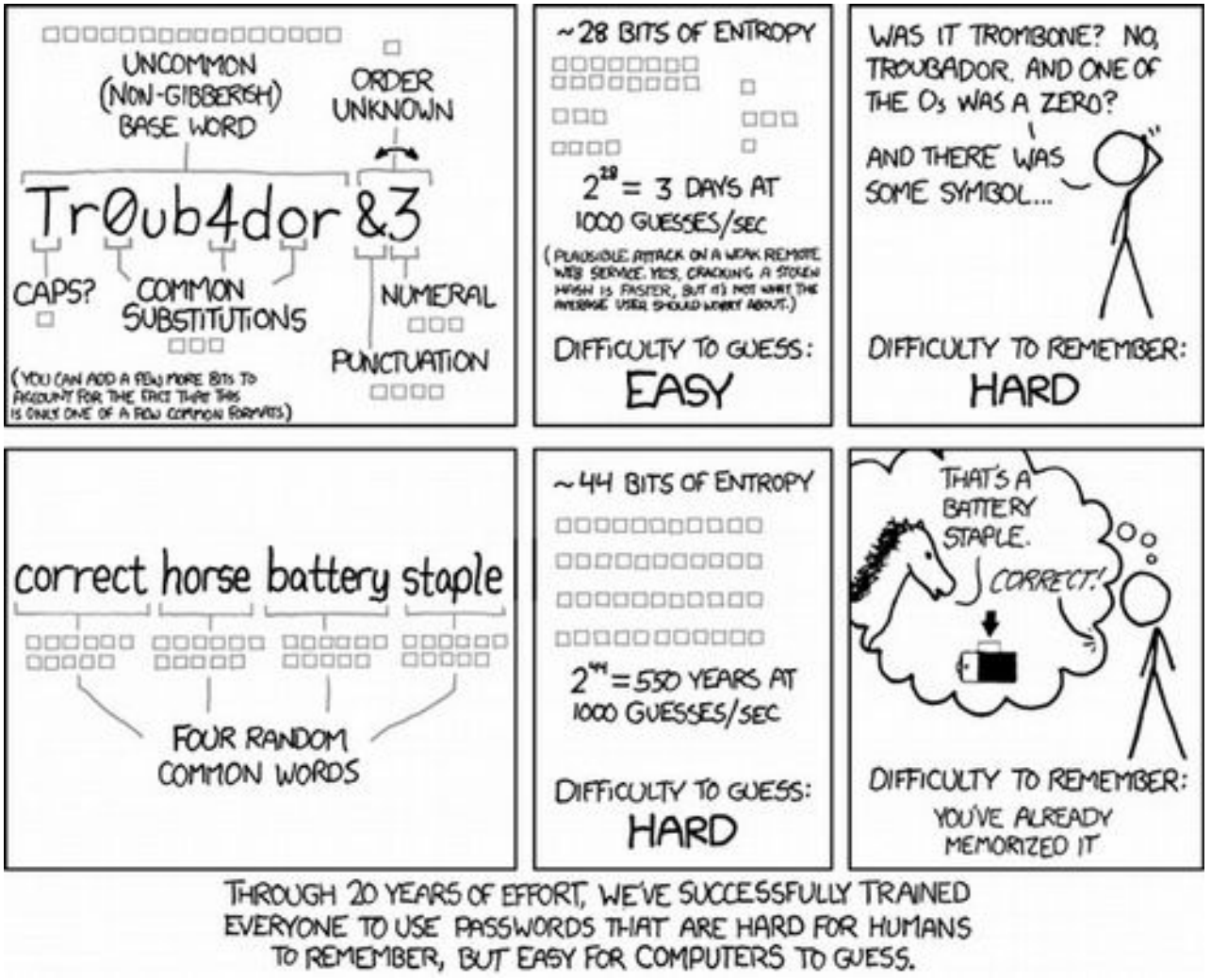
Passwords just won’t die

- We don’t really have a better way yet
- Users **understand** passwords
- Most users *can’t* manage one-time keys
- Most users *don’t* understand public/private keypairs
  - They certainly don’t understand key rotation...
- Biometrics can still be stolen, and *can’t* be “refreshed”
- We might be rid of passwords one day... but for now, we just have to make do.

Good password practices 1/7

- Use a sequence of words, not characters
  - A **passphrase**
  - Easier for humans to remember
  - Harder for computers to guess
- Don’t use quotes from movies or books!
- Not all websites let you do this
- The longer, the better (generally)

Good password practices 2/7



https://xkcd.com/936/

Good password practices 3/7

- Get informed when your passwords are compromised
- Refresh them anywhere you used that password
- Have I Been Pwned: https://www.haveibeenpwned.com/
- Firefox Monitor: https://monitor.firefox.com/
- Be discreet—this is a **privacy grey area**.

Good password practices 4/7

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

GeekedIn: In August 2016, the technology recruitment site GeekedIn left a MongoDB database exposed and over 8M records were extracted by an unknown third party. The breached data was originally scraped from GitHub in violation of their terms of use and contained information exposed in public profiles, including over 1 million members' email addresses. Full details on the incident (including how impacted members can see their leaked data) are covered in the blog post on 8 million GitHub profiles were leaked from GeekedIn's MongoDB - here's how to see yours.

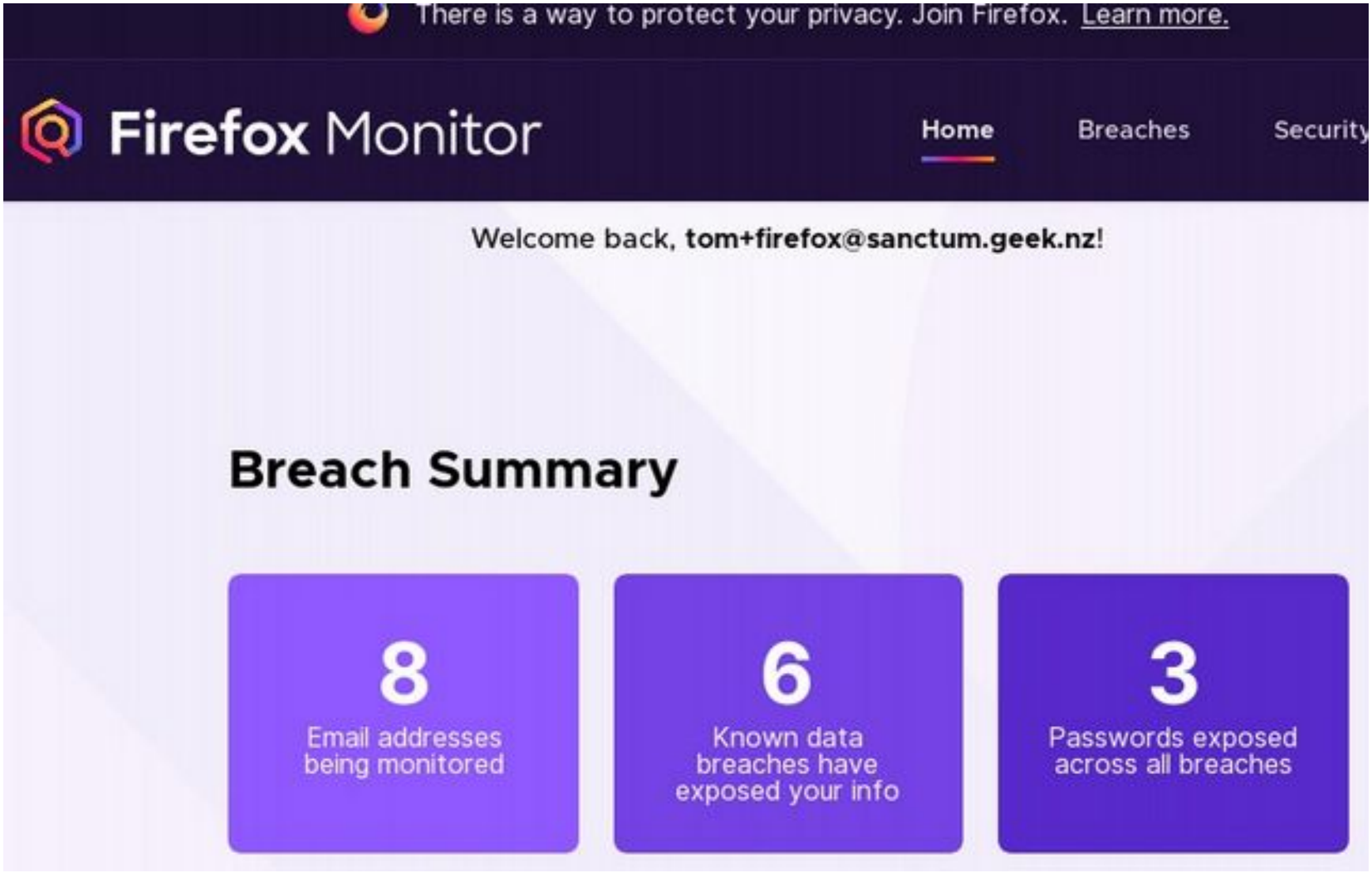
Compromised data: Email addresses, Geographic locations, Names, Professional skills, Usernames, Years of professional experience

Patreon: In October 2015, the crowdfunding site Patreon was hacked and over 16GB of data was released publicly. The dump included almost 14GB of database records with more than 2.3M unique email addresses and millions of personal messages.

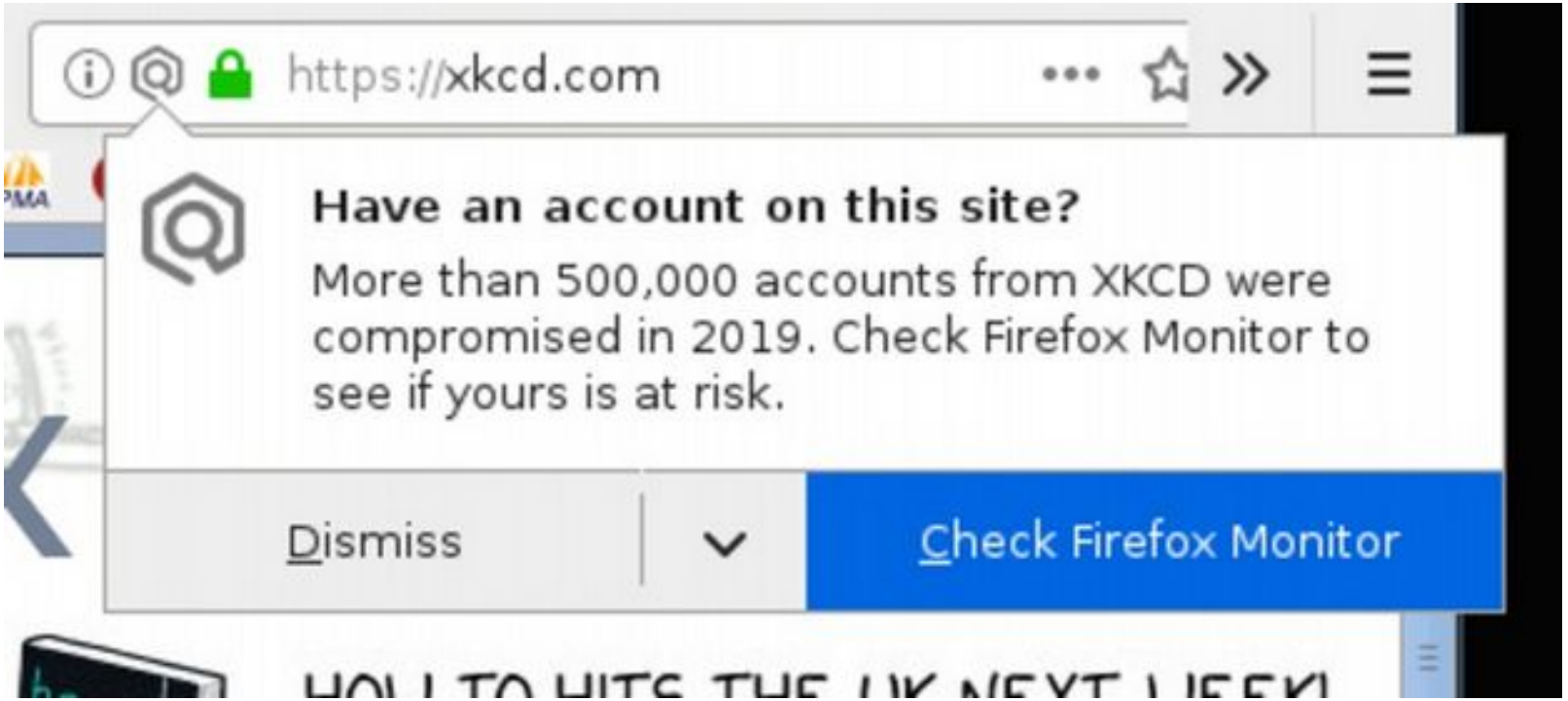
Compromised data: Email addresses, Payment histories, Physical addresses, Private messages, Website activity

Roll20: In December 2018, the tabletop role-playing games website Roll20 suffered a data breach. Almost 4 million customers were impacted by the breach and had email and IP addresses, names, bcrypt hashes of

Good password practices 5/7



Good password practices 6/7



Irony, thy name is xkcd...

Good password practices 7/7

- **Don’t** use the same password or a variant of the same password for multiple sites.
- Really easy to say...
- ... pretty hard to do.
  - password1 ... password2 ... password3 ...
  - password! ... password@ ... password# ...
  - password_gm41l, password_b4nk...

Too many passwords

- This comic is from **1996**.
- Things have got *much, much worse*.

https://dilbert.com/strip/1996-02-10

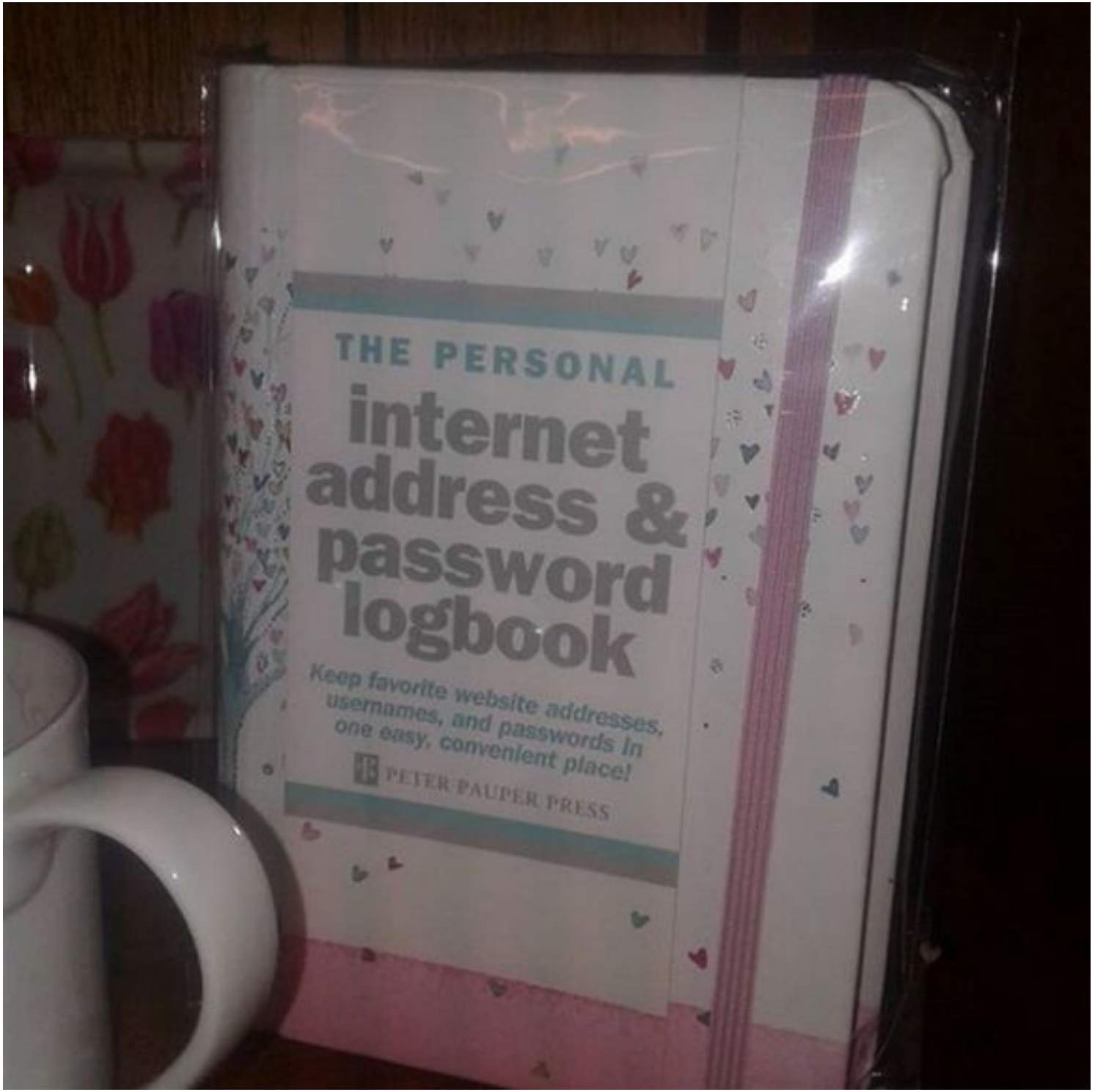
Give up, give in

- It’s so bad, that very many people have **given up**.
- They *don’t even try* varying their passwords.
- They use the same ones on every site.
- More careful users might have a “special” password for their banking and email.
- Can you blame them?

What can we do?

If we can’t *remember* them all...

...we need to *record* them somewhere.


THE PERSONAL
internet address & password logbook
Keep favorite website addresses, usernames, and passwords in one easy, convenient place!
PETER PAUPER PRESS

Not that bad, actually...

CERT NZ
@CERTNZ

Replying to @InternetNZ and @harrismint

Our hot take: if you make sure you've got different passwords for each account, and keep them written down somewhere safe and away from your devices, we reckon it's all good. ¯_(ツ)_/¯ Far safer than using the same password on every account...

11:30 AM · Aug 21, 2019 · Twitter for iPhone

https://twitter.com/CERTNZ/status/1163956588295573505

And if you don’t believe Grandma...

Schneier on Security

Blog | Newsletter | Books | Essays | News | Talks

Blog >

Write Down Your Password

Microsoft's Jesper Johansson urged people to write down their passwords.

This is good advice, and I've been saying it for years.

https://www.schneier.com/blog/archives/2005/06/write_down_your.html

WTF?! 1/2

- It’s a **tradeoff**.
- If a plain text, hard copy password book allows you to use *unique passwords on every site*...
- ... that’s *far* better than using the same password on every site, **no matter how strong that password is**.
- **Don’t trust websites to keep your passwords safe!** Breaches in 2019 are routine.

WTF?! 2/2

- The password book has the *advantage* of being offline by definition.
  - Nobody can read it by hacking your computer or a website you use.
- However, it has the *disadvantage* of being in plain text.
  - Anyone could read it by breaking into your house.

Am I advising you do this?

- **Not really—**there are somewhat better options that we'll explore now.
- But it should encourage us to think carefully about what the actual *threat* is.
- Infosec people call this **threat modelling**.
- **What** are you trying to protect, from **whom**; **how** could they get it, and **how** can you prevent that?

Password manager

- A secure database for password storage.
- We generally mean the **electronic** kind, and not Grandma’s little book...
- We’ll look at least briefly at four examples:
  - LastPass
  - KeePass
  - BitWarden
  - password-store (Tom’s favourite!)

Password manager requirements

- **Cross-platform, runs on GNU/Linux—**of course!
- **Free software—**no proprietary code managing my passwords, thanks!
- **Trustable encryption—**modern cryptographic standards, audits of applicable code

Password manager nice-to-haves

- **Multi-factor authentication—**support requiring a code from your phone, or a key, as well as the password
- **Browser integration—**point-and-click to complete passwords
- **Options for cloud storage or local storage—** depending on your tastes—Tom doesn’t like cloud storage

LastPass

LastPass

- Not free software...
- Cloud storage only...
  - Which has suffered several breaches... https://en.wikipedia.org/wiki/LastPass#Security_issues
- **...Next, please!**

BitWarden 1/2

- Better than LastPass, but...err...

BitWarden 2/2

- Uhm...

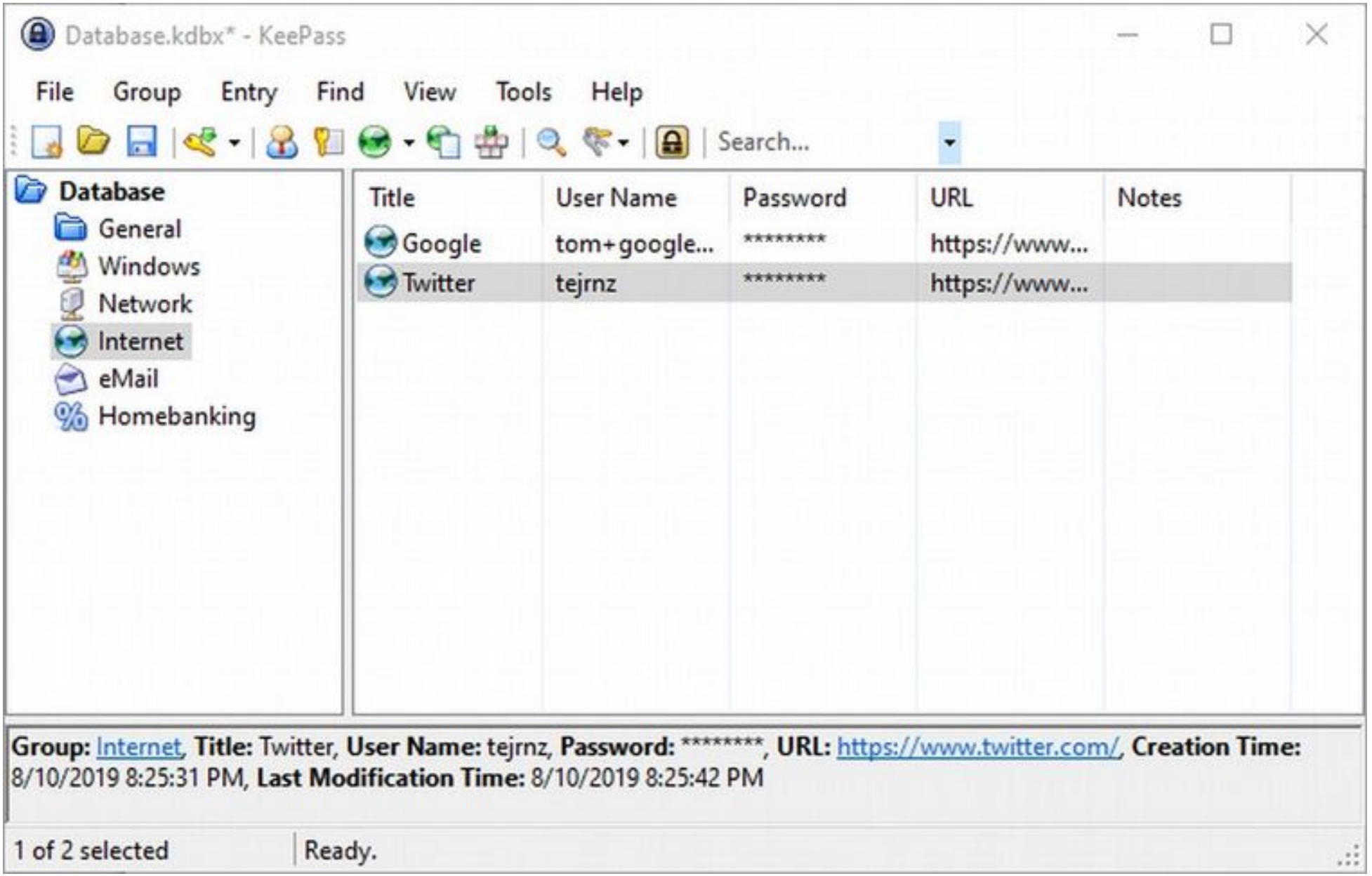
In March 2018, Bitwarden's web vault was criticized for embedding unconstrained third-party JavaScript from BootstrapCDN, Braintree, Google, and Stripe. These embedded scripts could pose as an attack vector to gain unauthorized access to Bitwarden user's passwords.[14] These third-party scripts were removed and eliminated the risk as part of the Bitwarden 2.0 Web Vault update that was released in July 2018.[15]

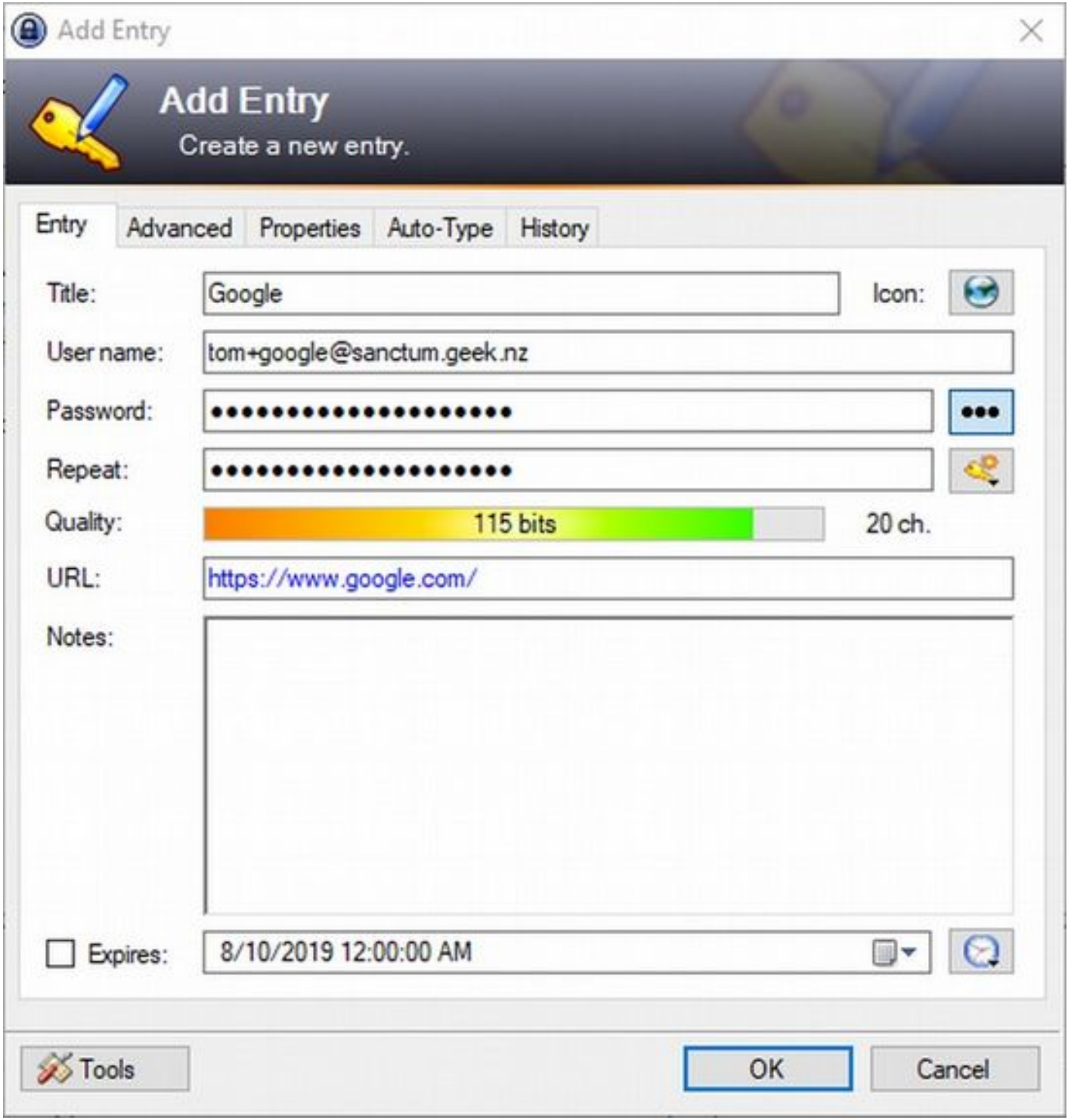
...Web vault? JavaScript from **Google?** As the kids say, "***oof****..."*

KeePass

Now *that's* more like it.

- Free software
- Local storage
  - **Master password** or **key file**
- Modern crypto standards (AES)
- Application-independent input
  - "Autotypes" your password
- Plugin support


Database.kdbx* - KeePass
File
Group
Entry
Find
View
Tools
Help
Search...
Database
General
Windows
Network
Internet
eMail
Homebanking
Title
User Name
Password
URL
Notes
Google
tom+google...
****
https://www...
Twitter
tejrnz
****
https://www...
Group: Internet, Title: Twitter, User Name: tejrnz, Password: ********, URL: https://www.twitter.com/, Creation Time: 8/10/2019 8:25:31 PM, Last Modification Time: 8/10/2019 8:25:42 PM
1 of 2 selected
Ready.


Add Entry
Add Entry
Create a new entry.
Entry
Advanced
Properties
Auto-Type
History
Title:
Google
Icon:
User name:
tom+google@sanctum.geek.nz
Password:
Repeat:
Quality:
115 bits
20 ch.
URL:
https://www.google.com/
Notes:
Expires:
8/10/2019 12:00:00 AM
Tools
OK
Cancel

KeePass
Password Safe

Home
- Home & News
- Forums
- Feature List
- Screenshots

Getting KeePass
- Downloads
- Translations
- Plugins / Ext.

Information / WWW
- Help
- FAQ
- Security
- Awards
- Links

Support KeePass
- Donate

KeePass Plugins and Extensions

Information about the plugin framework (installing plugins, security, ...) can be found on the help pages 'KeePass 1.x Plugins' and 'KeePass 2.x Plugins'.

I/O & Synchronization

IOProtocolExt
Adds support for SCP, SFTP and FTPS.
SftpSync
Adds support for SFTP and SCP.
KeeAnywhere
Adds support for online storage providers.
KeeCloud
Adds support for online storage providers.
KeePassSync
Synchronize using online storage providers.
KPDataSave (Dropbox)
Save your database in Dropbox.
KPGoogleSync
Synchronize using Google Drive.
KeePassOneDriveSync
Synchronize using OneDrive.
KeePassMasterSlaveSync
Synchronize specific entries only.

Utilities

AdvancedConnect
Allows to specify applications for direct connections.
AlternateAutoType
Adds hot keys for alternative auto-type sequences.
AutoTypeCustomFieldPicker
Allows to pick a custom field during auto-type.
AutoTypeSearch
Provides quick searching as enhancement to global auto-type.
AutoTypeShow
Shows an entry after auto-typing.
AutoTypeSplitter
Splits auto-typing into distinct parts.
CheckPasswordBox
Prevents auto-typing passwords into wrong places.
ColoredPassword
Allows to use different colors for password characters.
Custom Icon Dashboarder

Integration & Transfer

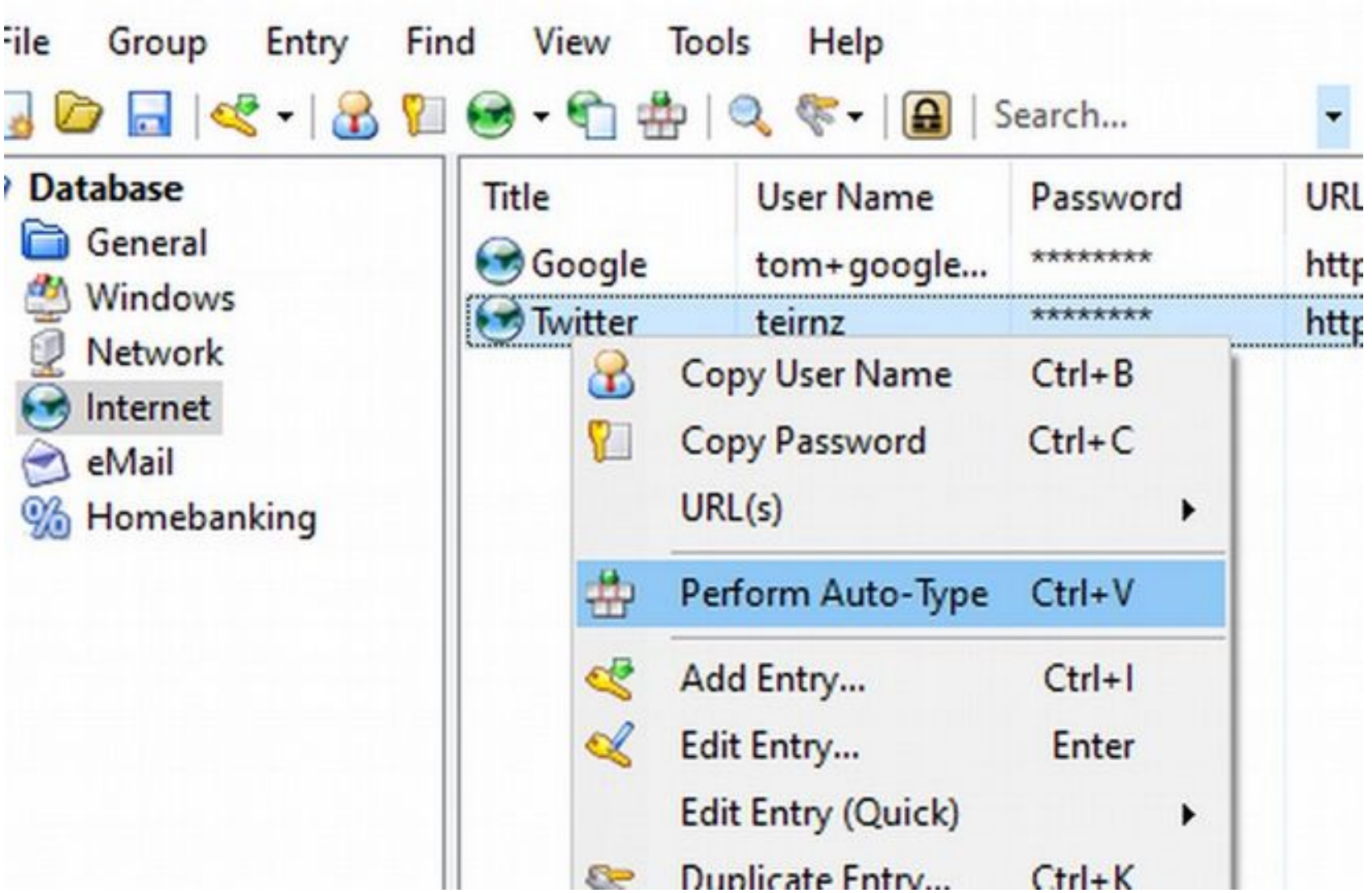
KeeForm
Opens websites and fills in the login data automatically.
Kee
Bridge between KeePass and web browsers.
Passafari
Integrates KeePass and the Safari browser.
URL in Title Bar
Browser extensions that show the current URL in the title bar (for multiple browsers).
KeePasser
Allows auto-typing into webforms based on URLs (Internet Explorer and Maxthon).
KPFloatingPanel
Displays an always on top KeePass floating panel.
KeePassHelper
Browser extension that retrieves credentials from KeePass.
WebAutoType
Allows auto-typing into webforms based on URLs (multiple browsers).
RDCAutoTypeAndTCATO
RDC auto-type support and improved TCATO selection.
TCATO Placeholder
Allows to enable/disable TCATO per auto-type sequence.
HotKeyEnabler
Allows to define custom sequences of keys system-wide with auto-type functionality.
KeeOtp
Generates TOTP authentication codes.
Tray TOTP
Generates TOTP authentication codes.
Character Copy
Allows copying individual characters from entry strings.
Password Change Assistant
Helps to change passwords.
QrCodeGenerator
Displays passwords as QR codes.
KeePassQRCodeView
Displays entry fields as QR codes.

Backup

Another Backup Plugin
Creates backups of databases.
DB_Backup
Creates backups of databases.
DataBaseBackup
Creates backups of databases.
KPSimpleBackup
Creates backups of databases.
SimpleDatabaseBackup
Creates backups of databases.

Import

1P2KeePass
Imports 1Password 1PIF files.
AnyPassword Import
Imports CSV files exported by 'AnyPassword'.
CardFileKPPlugin
Imports CRD files created by 'Cardfile'.
CodeWallet 3 Import
Imports TXT files exported by 'CodeWallet 3'.
CodeWallet 6 Konverter
Converts TXT files exported by 'CodeWallet 6' to importable CSV files.
eWallet Import
Imports TXT files exported by 'eWallet'.
eWallet Data Liberator
Export data from 'eWallet' and import it into KeePass.
eWallet2KeePass
Migrate 'eWallet' data to KeePass.
KeePassBrowserImporter
Imports credentials from various browsers.
KeePassFirefoxImporter
Imports passwords from Firefox.
MSDN/TechNet Key Importer
Imports MSDN/TechNet key files.
OnePIF
Imports 1Password 1PIF files.
Oubliette Import


File
Group
Entry
Find
View
Tools
Help
Search...
Database
General
Windows
Network
Internet
eMail
Homebanking
Title
User Name
Password
URL
Google
tom+google...
****
http
Twitter
teirnz
****
http
Copy User Name Ctrl+B
Copy Password Ctrl+C
URL(s)
Perform Auto-Type Ctrl+V
Add Entry... Ctrl+I
Edit Entry... Enter
Edit Entry (Quick)
Duplicate Entry... Ctrl+K

Too complicated!

- KeePass is the best of all the GUI-friendly ones I've seen.
- But this is all so *complicated*. It's storing, tracking, listing, and displaying small strings of text in files.
- Why do we need a whole new app for that?

Why, indeed?

password-store

- A tree of **plain text files**...
- Encrypted with **GnuPG**...
- With a small **Bash script wrapper**...
- Tracked in a **Git repository**
  - If you want...
- **...that’s it.**

password-store: Install

```
$ sudo apt-get install password-store
```

password-store: Generate key

```
$ gpg --gen-key
```

password-store: Start new store

```
$ pass init user@example.com
mkdir: created directory
'/home/user/.password-store/'
Password store initialized for 1F8F4292
```

password-store: Make password

```
$ pass generate example.com 25
(ry_^rpCw@l%1Q`:RjVk\}P!/
```

Err, can I have it without the awkward characters...?

```
$ pass generate example.com -n 25
iQSP33ojhb93Qy7GG6OzCqM48
```

password-store: Retrieve password

```
$ pass example.com
iQSP33ojhb93Qy7GG6OzCqM48
```

Err, do you have to show it on screen...?

```
$ pass -c example.com
# It's in your clipboard!
```

password-store: List passwords

```
$ pass
Password Store
├── aa.co.nz
│   └── tomryder
├── academia.edu
│   └── tom+academia@sanctum.geek.nz
├── accounts.wizards.com
│   └── tyrefire
├── activeglobal.com
│   └── tom@sanctum.geek.nz
├── addons.mozilla.org
...
```

password-store: Track passwords

```
$ pass git init
Initialized empty Git repository in
/home/tom/newhome/.password-store/.git/
[master (root-commit) 680f3be] Add
current contents of password store.
```

Caveats

- If your password database is stolen, you've got time while they crack it (which they won't—threat models, remember?)
- If your *computer is hacked*, and you're being screen-scraped and/or keylogged, it can't help you.
- Passwords are disposable and dispensible...

"Don't let yourself get attached to anything you are not willing to walk out on in *30 seconds flat* if you feel the heat around the corner."

—Heat

Questions?

- **CERT NZ password manager advice**
- **KeePass**
- **password-store**

Email: tom@sanctum.geek.nz
Website: https://sanctum.geek.nz/
Social: @tejr@mastodon.sdf.org