Online Privacy, Security and Password Management

FOSSASIA Summit 2021
2021Mar18 @ noon
Singapore

der.hans
CDE
Object Rocket, a rackspace company
https://www.ObjectRocket.com/

Yes, we’re hiring :)

ObjectRocket
https://www.ObjectRocket.com/careers/

Rackspace Technologies
https://rackspace.jobs/

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Upcoming Presentations

- List of Some Upcoming and Previous Talks and Publications
  - https://www.LuftHans.com/talks
- Upcoming talks
  - LibrePlanet - Regular expression workshop - 2021Mar20 15:40 local (19:40 UTC) (English)

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Social Media and Fediverse

- FLOX_advocate on Mastodon
  - https://floss.social/@FLOX_advocate
- LuftHans on PLUME
  - https://fediverse.blog/~/LuftHans
- LuftHans on Freenode IRC
  - #SeaGL, #LOPSA, #PLUGaz and #LibreLounge

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

First off,

IANAL

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

And,

Specifically…

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

More Importantly,

IANYL

If you need legal review for any ideas from this talk, please talk to YOUR lawyer

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Why do we need security?

Spectre/Meltdown (again)

— Equifax admin/admin — Heartbleed — Apple SSL — Apple iCloud — Home Depot — Target — Yahoo! x 2 — LinkedIn x 3 — Eharmony — Last.FM — TJ Maxx / Marshalls — Adobe — Nieman Marcus — 7-eleven — Barnes and Noble — TriCare x 2

— Mat Honan — Jennifer Lawrence — Kate Upton — Rhianna

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Cost

> "They could have used my e-mail accounts to gain access to my online banking, or financial services. They could have used them to contact other people, and socially engineer them as well." – Mat Honan

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

What’s really at Stake?

> "more than a year’s worth of photos, covering the entire lifespan of my daughter" – Mat Honan

> "including those irreplaceable pictures of my family, of my child’s first year and relatives who have now passed from this life" – Mat Honan

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Data Collection

- 90% of data ever collected was collected in last 2 years
    - from 2019 Freakanomics podcast

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

First Things First

- Use only trusted software sources!
- Install Security Updates!

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Encryption Example

- Postcard vs Envelope

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

When to Use Encryption

- All the time!
- Every time!
- HTTPS Everywhere browser Add-on from the EFF

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

What to Encrypt

- Log in credentials
- Personal (identifying) information
  - Name
  - Address
  - Phone Number
  - Credit Card Information
  - Medical Information
  - Private Photos
  - Shoe Size

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Password Bleed Over

- Same password at multiple sites?
- One site compromise could quickly expose your data at multiple sites
- Use different passwords for every site!

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Credentialed access

- Credentials are the combination of tokens used for authentication

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Are you you?

- Username, often email address
- Password
- Security Questions
- PIN
- Multifactor Authentication (MFA)
- Body Parts

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Unique

- Every one of those should be unique to every site
- Each item, not just combinational uniqueness
- Some restrictions may apply

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Random String

- Random sequence of text gibberish
- Longer and more random are both better
- Use
  - Letters (upper case and lower case)
  - Numbers
  - Punctuation (`!@#$%^&*.,/:\;`)
- Be cautious of
  - Similar looking characters
  - Underline and dash
  - Spaces and tabs
- Example: `fnYV@tki4M’jj;iTW]21`

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Random Word Salad

- Random sequence of unrelated words
- Longer and more random are both better
- Use multiple languages if you can
- Declension, conjugation, etc.
- Add mid-word capital letters
- Use randomish punctuation
- Example: purPlish lechE verFaehrt sInging liberte
- XKCD Example: correct battery horse staple

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

ERROR: /dev/brain read-write failure

But, Hans, that’s way too much to memorize and it’s not near as interesting as baseball stats…

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Password Managers

- Securely store credential information
- Easy to use for authentication

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Password Manager Requirements

- Free Software
- Hidden Password Entries (* not `hunter2`)
- Locally Encrypted, Operating System Independent File
- Data Liberation
- Automagic Clipboard Entry Clearing
- Easy Copy and Paste
- Configurable Password Generator
- Space For Notes
- Entries Organization

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Password Manager Bonus Features

- Human Readable Password Generation
- Random Word Salad Generation
- Pronunciation Guide
- Random String Generation from Anywhere in UI
- Secondary Key/Value Storage
- Copy/Paste of Secondary Key/Value
- Data Export with Sync
- Site safety verifications
- Automated password changes

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

My Recommendations

- GNU/Linux or BSD Device
  - KeePassXC (keepassxc)
  - KeePassX (kpcli)
- Web
  - Bitwarden
  - Nextcloud
    - WebAppPassword
    - Passman
    - Passwords
- Android
  - KeePassDroid
- Other Desktop
  - KeePass

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

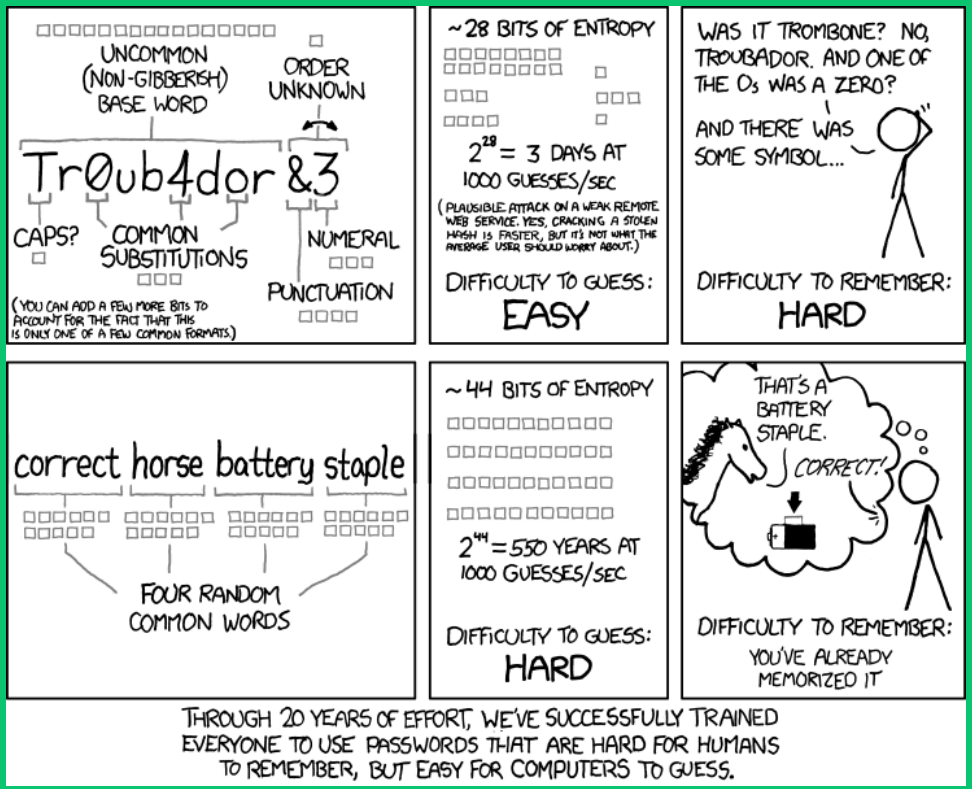
One Password to Hold Them All

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

One Password to Protect Them All

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Passphrases



XKCD: Password Strength - https://xkcd.com/936/

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Pronounceable Strings

- Like Dr Seuss, but make less sense
- Useful for over the phone
- Avoid lookalike characters
    - 1 l
    - 0 O
- Pronunciation guides help
    - werecbyivofejmu (wer-ec-byiv-of-ej-mu)

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

I am me!

Authentication is identifying that you are you

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

How do you prove it?

- 3 types of authentication data
  - What you know
    - Ex: username, password, PIN
  - What you have
    - Ex: ID, smartphone app, physical token
  - What you are
    - Ex: fingerprint, DNA, facial recognition, retina scan

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

4th Element: You’ve been tokenized

- Cookies
- Device ID

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

5th Element

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

ID: Username

- random string: banks, shopping, utilities
    - Ex: `eddyityoz`
- recognizable handle: public and social sites
    - Ex: `FLOX_advocate`

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

ID: Email Address

- Subaddressing
  - `username@gmail.com`
  - `username+randomstring@gmail.com`
- Also great for mail filtering
  - `username+3qkrl-ebay@gmail.com`
- Limited use for social networking
  - Friends and colleagues
    - `I know username@gmail.com, please let us converse`
  - Great for notifications from social networks
    - `username+mastodon@pm.me`

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

ID: Using Subaddressing

- Unique ID and email address for every site
- Use a random token for subaddressing
  - Put site name or other human readable string after the token
    - `username+3qkrl-ebay@gmail.com`
      - account: `username`
      - token: `3qkrl`
      - site: `ebay`
- Don’t reuse that tokenized email address for anything else
- Bonus
  - Filter incoming email to the tokenized email address
  - File fake emails as spam

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

ID: Cookies

- 3rd party cookies can track you on multiple sites
- Lightbeam 3.0 Add-on
- uMatrix Add-on

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

ID: Device ID

- Mobile devices have unique ID

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

ID: Security Questions and Answers

Example: `What was your grandma’s name?+` Example: `What was your first pet’s name?+`
Example: `What is your grandma’s pet’s hairdresser’s shoe size?`

The most important thing is …

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Nonsense Is More Secure

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Reminder

IANYL

If any of my suggestions go against local laws requirements please consider your legal liabilities

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

ID: Security Questions and Answers

- Random answers
- Random questions
- Use pronounceable strings
- Key/Value Store

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Multi-Factor Authentication (MFA)

- TOTP - Time-Based Tokens
- HOTP - Hash-Based Tokens (HMAC)
- Message - SMS
- Message - Push Notification
- Email
- Phone Call
- Body Part

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

MFA: TOTP (Application or Token)

- Time based tokens
- Site does not need phone number
- Use your device like a hardware token
- Time sync
- Backup/offline numbers
- OneTimePass, andOTP and more in F-Droid repo
- my recommendation

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

MFA: HOTP

- Each code used only once
- Must be kept in sync
- Client to server auth
- Server to client auth

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

MFA: Requires Phone Number

- SMS
  - MitM
- Push notification
- Phone call
  - Who is calling?
  - Alternative: Nextcloud Video Verification

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

MFA: Email

- See SMS :)
    - Spam rather than sales calls

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

MFA: Body Part

- Hard to change credential

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

ID: Birthdate

- Lie when you can
- February 31 no longer works :(
- One liner for randomish date
    - `date -d @$RANDOM*24*3600/2-500000000 +%Y%b%d`
    - # Random day between 1954 and 1999

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

ID: PINs

- some PINs can be 5 or 6 digits

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Backups

- Make regular backups
- Make offsite backups
- Deletion
    - Clouds are forever

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Going Forward

- Use long, random strings
- Use subaddressing
- Use multifactor authentication
- Ask vendors to encrypt email

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Nicht Vergessen!

Please use unique credentials for every site!

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Glossary

- Credentials
  - Anything used to identify you for authentication
- Passphrases vs passwords
  - Essentially the same
  - passphrases implies they are longer and it’s OK to use special characters and spaces
  - try code snippets as KeyPassXC passphrases
- Subaddressing delimiters
  - Often a '+', but doesn’t have to be
  - Depends on your mail provider

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Other Privacy Talks and Tools

- The Privacy Tax: How tracking and hacking affect disabled people, and what we can do about it @ Linux.Conf.AU
- Cover Your Tracks / Panopticlick browser fingerprinting test
- The Elephant In The Background: Empowering Users Against Browser Fingerprinting @ rc3

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Resources

- Linux Journal (2017Jan): Online Privacy and Security Using a Password Manager
  - https://www.LuftHans.com/LinuxJournal/Online_Privacy_and_Security_Using_a_Password_Manager
- My talks and publications
  - https://www.LuftHans.com/talks/
- Mat Honan Wired article
  - http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/
- Subaddressing list at Wikipedia
  - http://en.wikipedia.org/wiki/Email_address#Address_tags
- XKCD "Password Strength" explained
  - https://www.explainxkcd.com/wiki/index.php/936:_Password_Strength
- Nextcloud Video Verification
  - https://nextcloud.com/blog/unique-sharing-security-video-verification/

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Obtaining Software

- KeePassXC
  - https://KeePassXC.org/
- KeePassX
  - https://www.KeePassX.org/
- FDroid
  - https://f-droid.net/
- Bitwarden
  - https://bitwarden.com/
- Nextcloud
  - https://Nextcloud.com/
    - WebAppPassword
    - Passman
    - Passwords

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Privacy Enhancing Firefox Add-ons

- Lightbeam 3.0 from Principia
    - forked from Mozilla by former Outreachy intern in Berlin
- uMatrix from Raymond Hill
- NoScript from Giorgio Maone
- uBlock Origin from Raymond Hill
- uBO-Scope from Raymond Hill
- Decentraleyes from Thomas Rientjes

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Credits

- XKCD by Randall Munroe
  - http://XKCD.com
  - Password Strength XKCD 936
- Freakonomics Radio
  - America's Math Curriculum Doesn't Add Up (Ep. 391)

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Bonus Rounds

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Data Escrow

- Use a different KeePassXC file to store other important information
  - Bank account info
  - Life insurance info
  - Government citizen numbers
  - Passphrases for GPG keys
  - PDF copies of contracts and other documents
  - Use multiple different files

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Tips

- Don’t use links in email to login
- Use application-specific passwords
- Don’t use Internet Explorer
- Don’t use Outlook

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/

Getting Help

- Free Software Conferences (CLT, FOSSASIA, SeaGL, SCaLE, OLF)
- Local user groups
- Tech Support Fastlane XKCD 806

© 2007-2021 der.hans | https://floss.social/@FLOX_advocate | https://www.LuftHans.com/talks/