Always something to hide

How quickly
can
personal data
be misused?

What is the CCC?

- Founded on September 12th 1981 (tuwat.txt)
- November 16th to 17th 1984: BTX (Haspa) hack
- 1984: first Chaos Communication Congress
- 1987: NASA hack
- 1985 to 1989: KGB hack
- October 2006: Nedap hack
- March 29th 2008: Interior Minister Wolfgang Schäuble’s fingerprint is published
- October 26th 2011: Analysis of new German government spyware
- April 26th 2020: 10 requirements for the evaluation of "Contact Tracing" apps

Today

Hacker ethics

- Access to computers - and anything which might teach you something about the way the world really works - should be unlimited and total. Always yield to the Hands-On Imperative!
- All information should be free.
- Mistrust authority - promote decentralization.
- Hackers should be judged by their acting, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better.
- Don't litter other people's data.
- Make public data available, protect private data.

Breaches in 2023

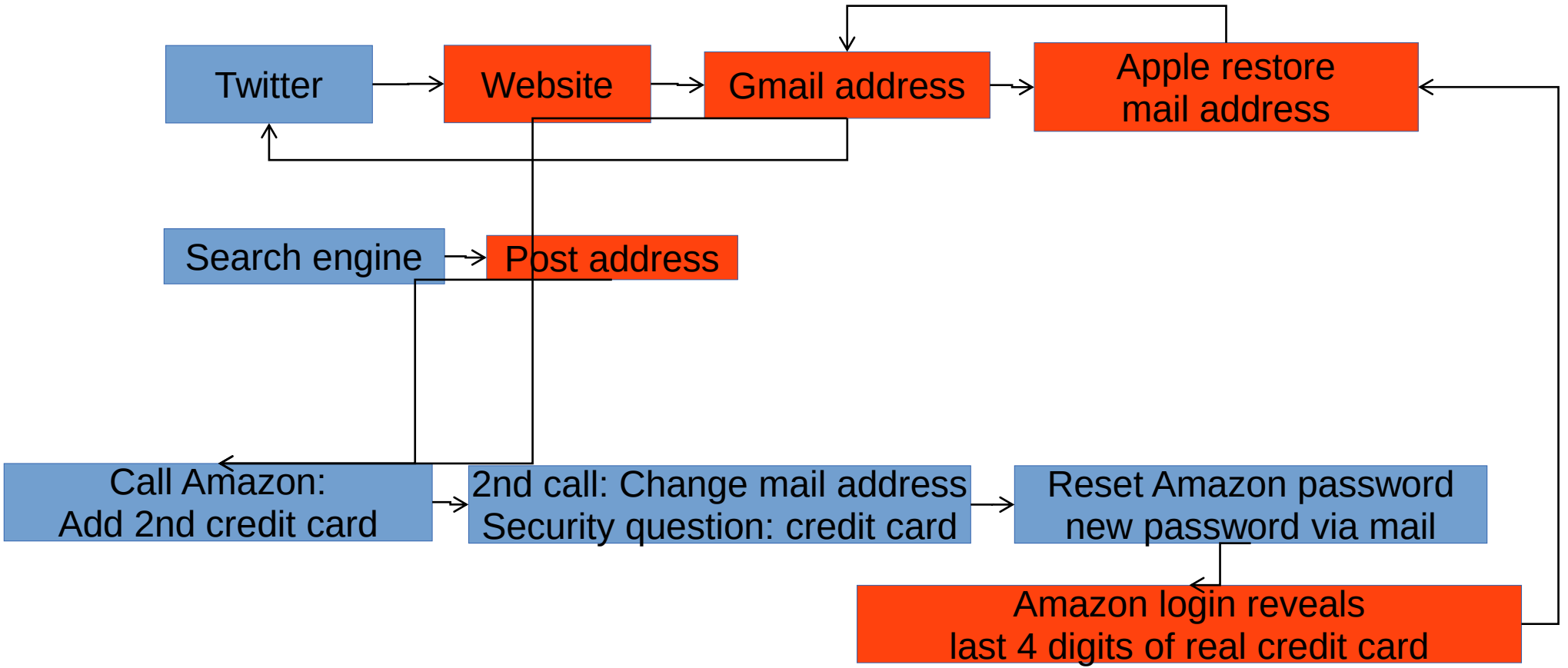
Biggest data breaches

https://en.wikipedia.org/wiki/List_of_data_breaches

Rule of Thumb

There is
no such thing
like
harmless data.

Identity Theft



c't Security 2013, S. 143ff

Try it yourself

- https://haveibeenpwned.com/ Have I been pwned?
- https://sec.hpi.de/ilc/ HPI Identity Leak Checker
- https://www.abc.net.au/news/2023-05-18/data-breaches-your-identity-interactive/102175688See your identity pieced together from stolen data



Identity Theft Check List

- Use a trustworthy computer. Scan your systems for malware.
- Change all passwords related with the compromised account.
- Keep an eye on your accounts. Check invoices and bookings. Check your send messages folder. Check mail forwarding. Check all mails for personal data that might be valuable for further attacks.
- Block your credit card.
- Inform the police.

Harmless Metadata?

- “How bad can it be if Alphabet (Google, Android), Meta (Facebook, Whatsapp) and the government know when I had communicated with whom as long as they don’t know what we were talking about?”
- Actually they do, at least to a certain degree.
- https://news.stanford.edu/2016/05/16/stanford-computer-scientists-show-telephone-metadata-can-reveal-surprisingly-sensitive-personal-information/

Examples

- A young woman has a several hour long nightly phone call with her sister and calls an abortion clinic the next morning.
- A young man has several phone calls with a cardiologist, a cardiology clinic and a pacemaker manufacturer.
- A young man has several phone calls with a gun manufacturer hotline.

The (Cruesomely Abbreviated) Edathy Affair

- Interpol hands over a list with names of alleged CSAM traders to the German Federal Police (BKA).
- Head of BKA Jörg Ziercke has a phone call with the minister of inner affairs Hans-Peter Friedrich.
- Hans-Peter Friedrich has a phone call with the head of the SPD (German Social Democrats) fraction in the German Bundestag Jürgen Oppermann.

The Imaginary Example of the Alcoholics Anonymous

- The AA chapter meets on every first Monday of a month.
- The chapter’s contact person’s mobile number is publicly known
- Every weekend before the meeting the same 10 Whatsapp users are sending a message to the contact person and get a reply shortly afterwards

Metadata

- Can reveal your
  - Social status
  - Level of education
  - Political views
  - Financial situation
  - Customer interests
  - Sexual orientation
- Some web shops won’t show you certain offers if you are surfing with the wrong operating system.

What does my browser tell about me? Let's find out.

- https://coveryourtracks.eff.org

USER AGENT

Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0

WHAT IS THIS?

A web header that relays information to the web server about your browser and its version.

HOW IS THIS USED IN YOUR FINGERPRINT?

This information can be very specific. *If customized* can single-handedly identify a specific user's browser.

Bits of identifying information: ***7.87***
One in x **browsers have this value:** ***234.59***

How Much Data Does It Take To Create A Fake Video?

- Answer: one minute https://www.npr.org/2023/03/23/1165146797/it-takes-a-few-dollars-and-8-minutes-to-create-a-deepfake-and-thats-only-the-sta
- "I gave it a minute of me talking about some unrelated topic like cheese and then pasted the speech in and it generated the sound file."

Fake News Check List

- Does it stir me up a bit too much?
- Does it confirm my existing point of view a bit too well?
- Look for bad grammar and spelling errors
- Are there reliable sources (i.e. not Sweetie or L0v4B0Y69 on Facebook)? Does the text in a language unknown to me really say what people claim it to say?
- Use Google image search to see whether a photo has been used previously in a different context.

How Can I Recognize AI Generated Deep Fakes?

https://www.foolproofme.org/articles/975-how-to-recognize-ai-generated-images-and-videos-artificial-intelligence

1) Metadata and Source Information
2) Unusual or Unnatural Elements
3) Perfect Symmetry or Flawless Patterns
4) Overly Vivid or Saturated Colors
5) Uncanny Valley
6) Reverse Image Search

Which Face Is Real?

https://www.whichfaceisreal.com/index.php

Other Indicators

- Look at the hands
- Eye reflections say a lot
- A hat or glasses that dissolve into hair or the skin
- Text on clothing can be a sure giveaway

Anatomy of a Ransomware Attack

- Open the gate with an infected email
- Explore and exploit the network
  - Get onto other systems
  - Estimate the value
- Extract data
- Encrypt drives
- Become visible

Typical technical weaknesses

- Outdated operating systems (hospitals running MRT with Windows XP)
- Weak passwords
- Software monoculture
- Backup server in Active Directory
- Backup clients can overwrite backup media
- No backup history
- Full backups that have to be restored completely instead of backups containing only the business critical data

Typical organizational weaknesses

- No or untested recovery concepts
- Understaffed IT department
- Poorly educated staff

Conclusion

- There is no such thing like perfect security
- This is no excuse for giving up
- You won’t fix societal problems with technical solutions

Links

- Net Politics Timeline (En / Ger)
- Digital Self-Defense