Digital Privacy Salon

Computer security for humans

CIRCL
Computer Incident
Response Center
Luxembourg

TLP:WHITE

info@circl.lu

License: CC-BY-SA 4.0

June 1, 2018

Who we are

CIRCL
Computer Incident
Response Center
Luxembourg

- The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents.
- CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg.
- CIRCL leads the development of **MISP, an open source threat intelligence platform** to support information sharing and analysis in cyber security.

Me

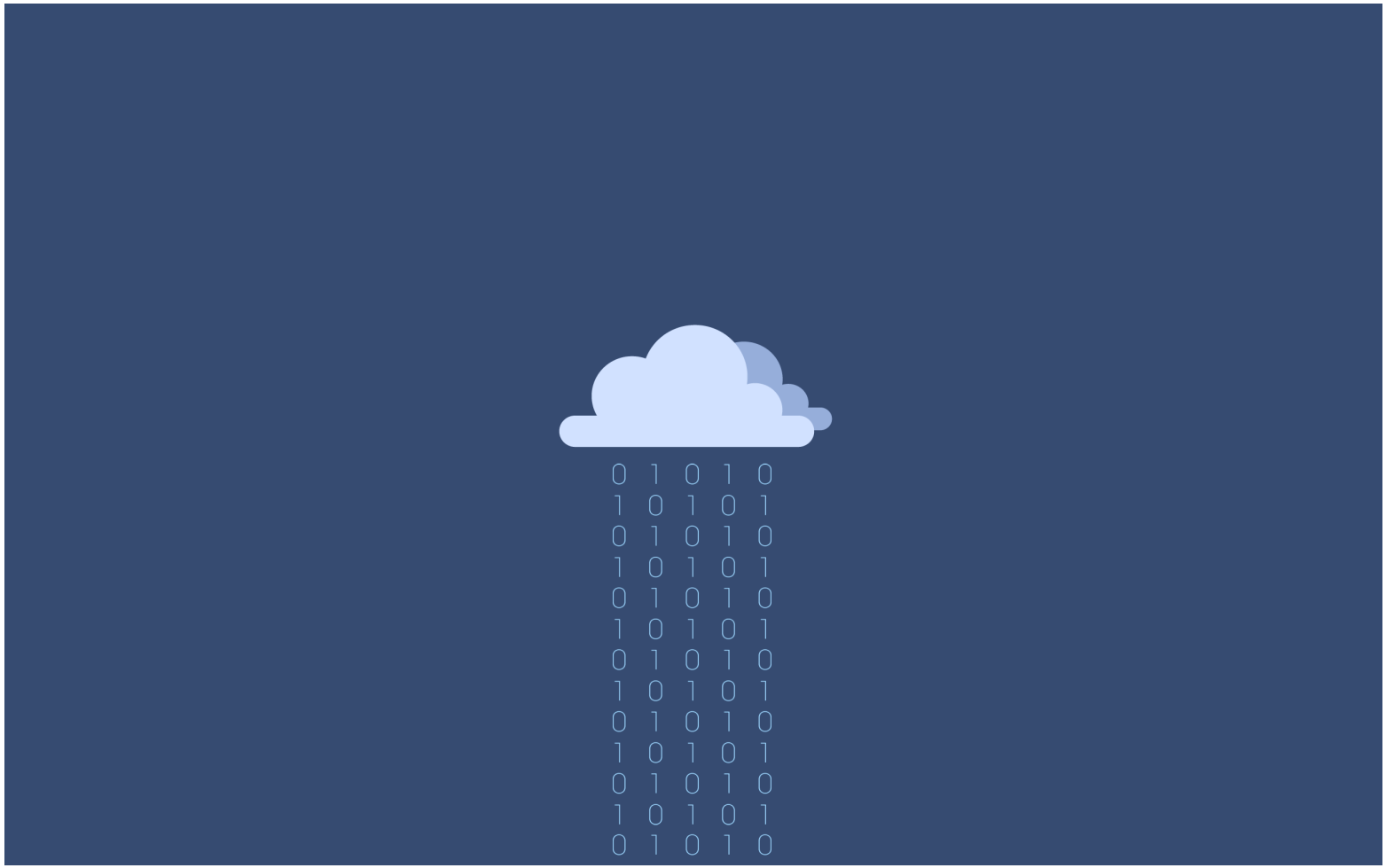
- Raphaël Vinot
- Incident responder, developer, conference co-organizer
- Trainer for technical and non technical audiences
- Bridge between NGOs / civil society and CERT community
- Trainer for communities at risk (journalists, LGBT, ...)

Bunch of topics

- What's the cloud, and how the internet is built
- Darkweb and other scary buzzwords
- Data at rest, data in movement, encryption
- Browser security, malvertizing
- Mobile devices
- Instant messaging, Slack, ...
- Password, and password management
- Assessing your risks
- Malware, phishing and emails

Network and the cloud

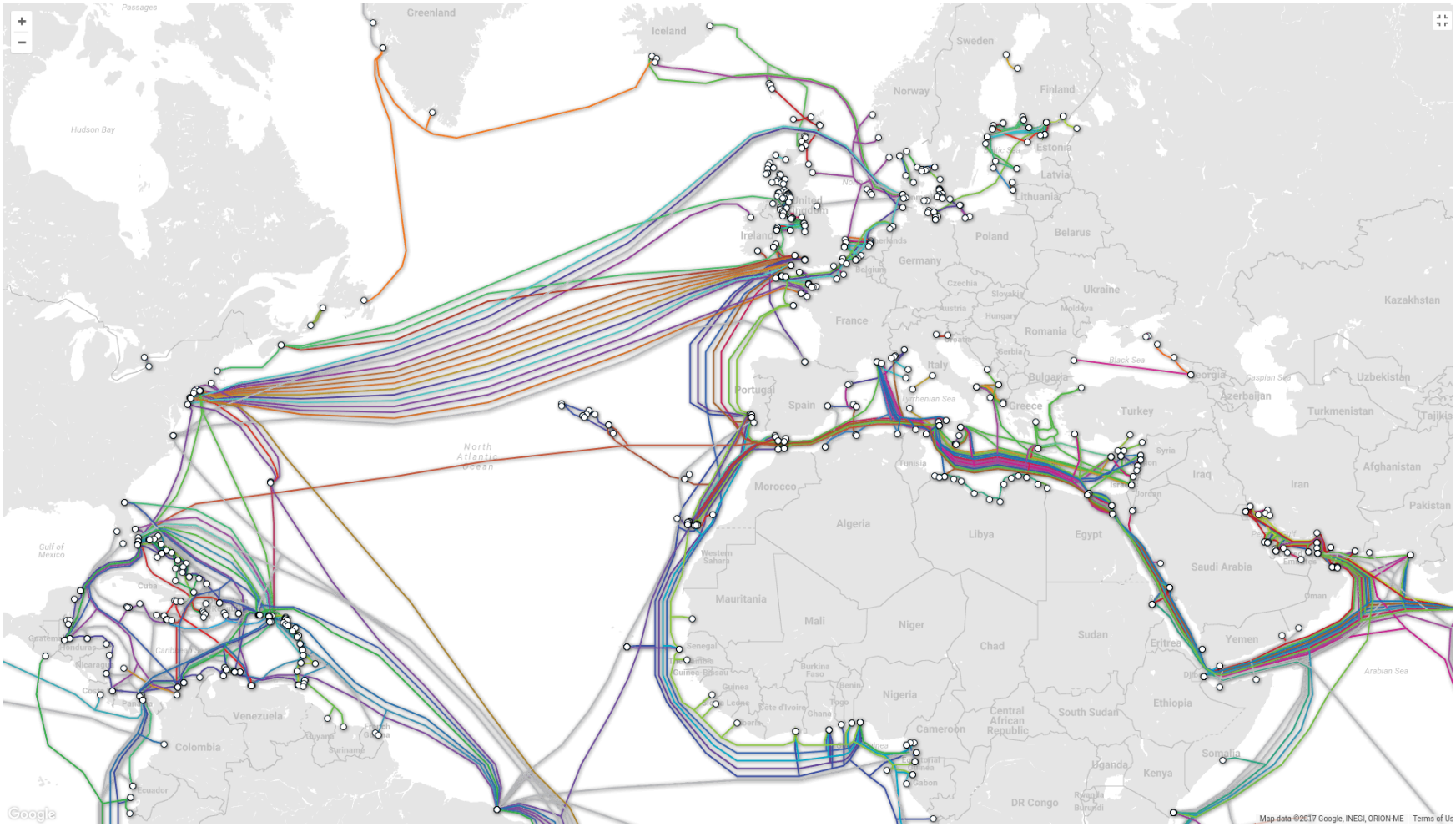
Network and the cloud



Network and the cloud

Network and the cloud

Network and the cloud



Network and the cloud

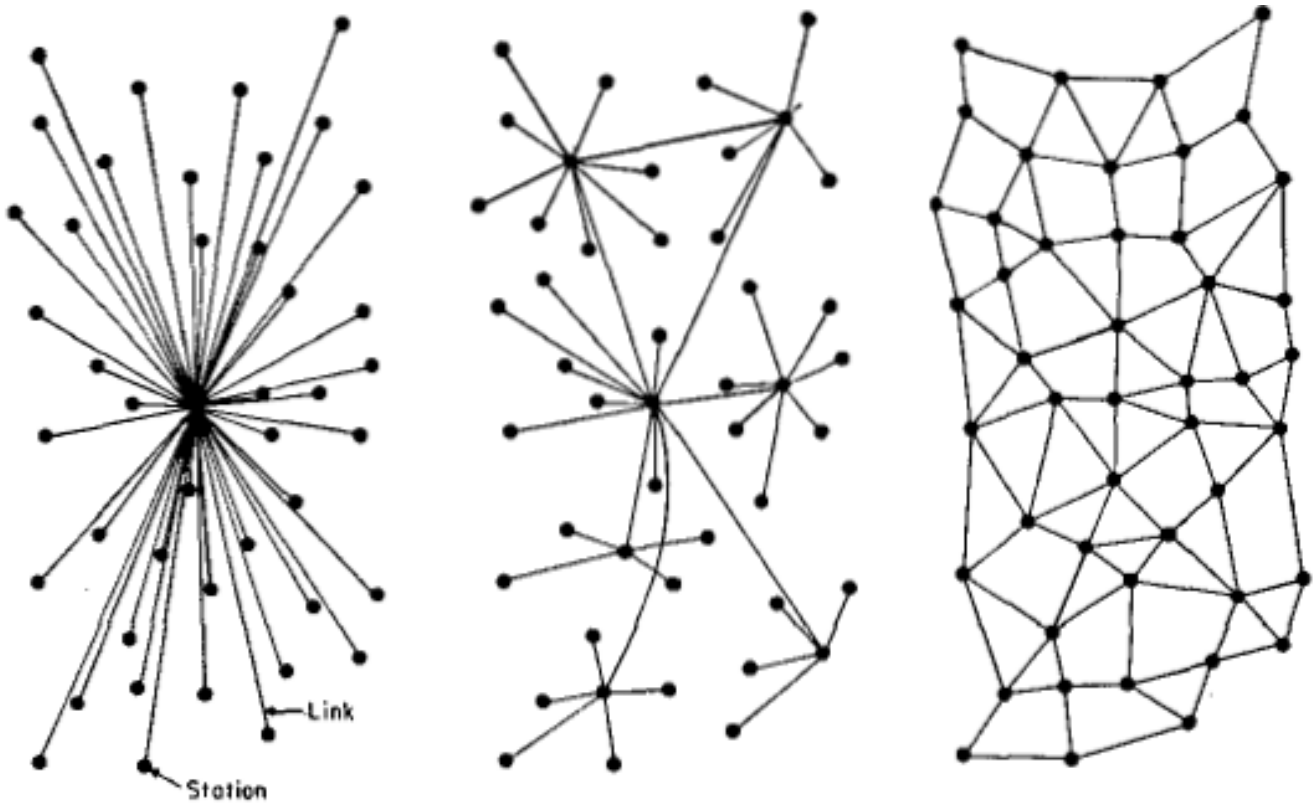


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

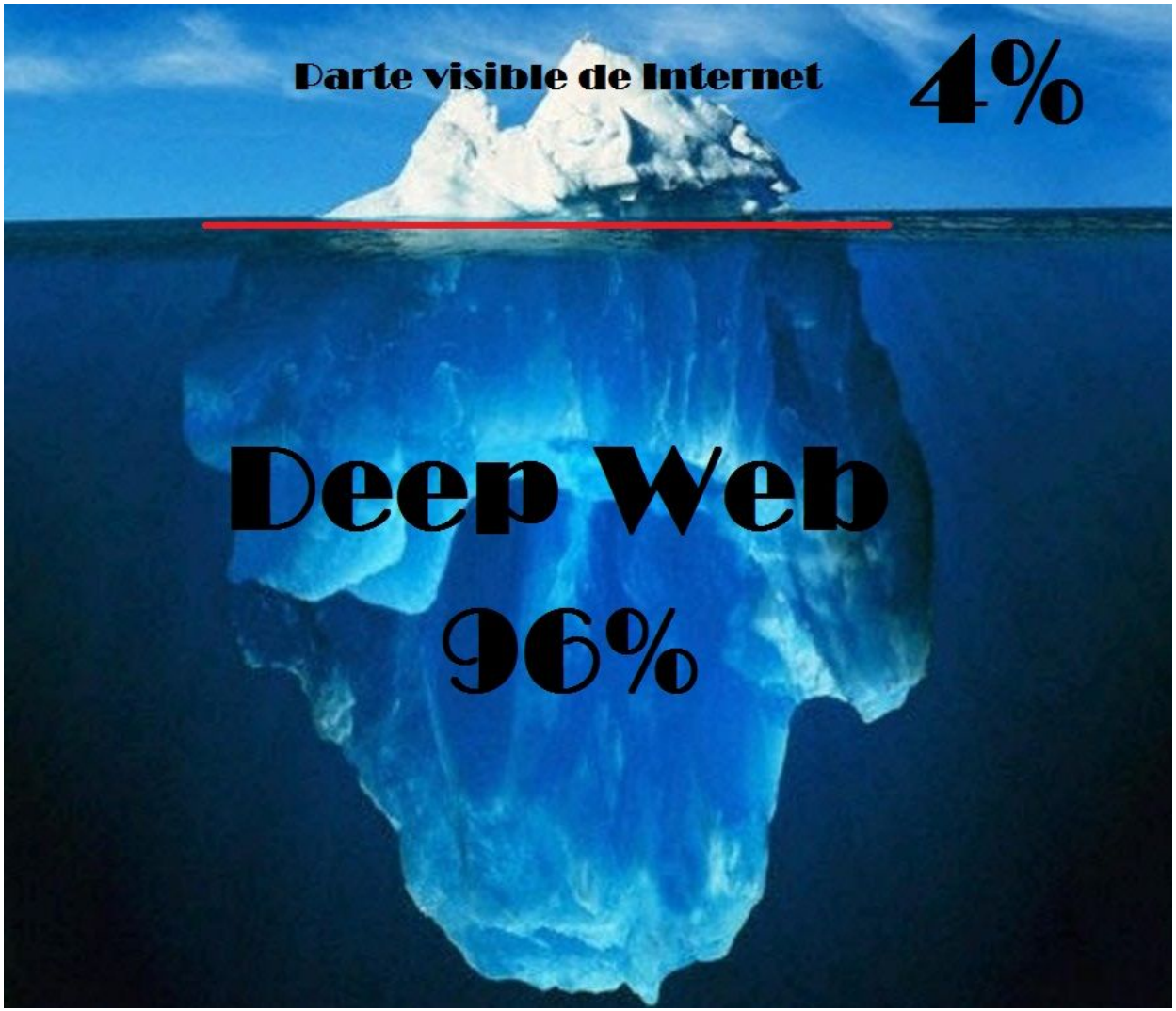
Darkweb*

* The networks chapter is required for the jokes

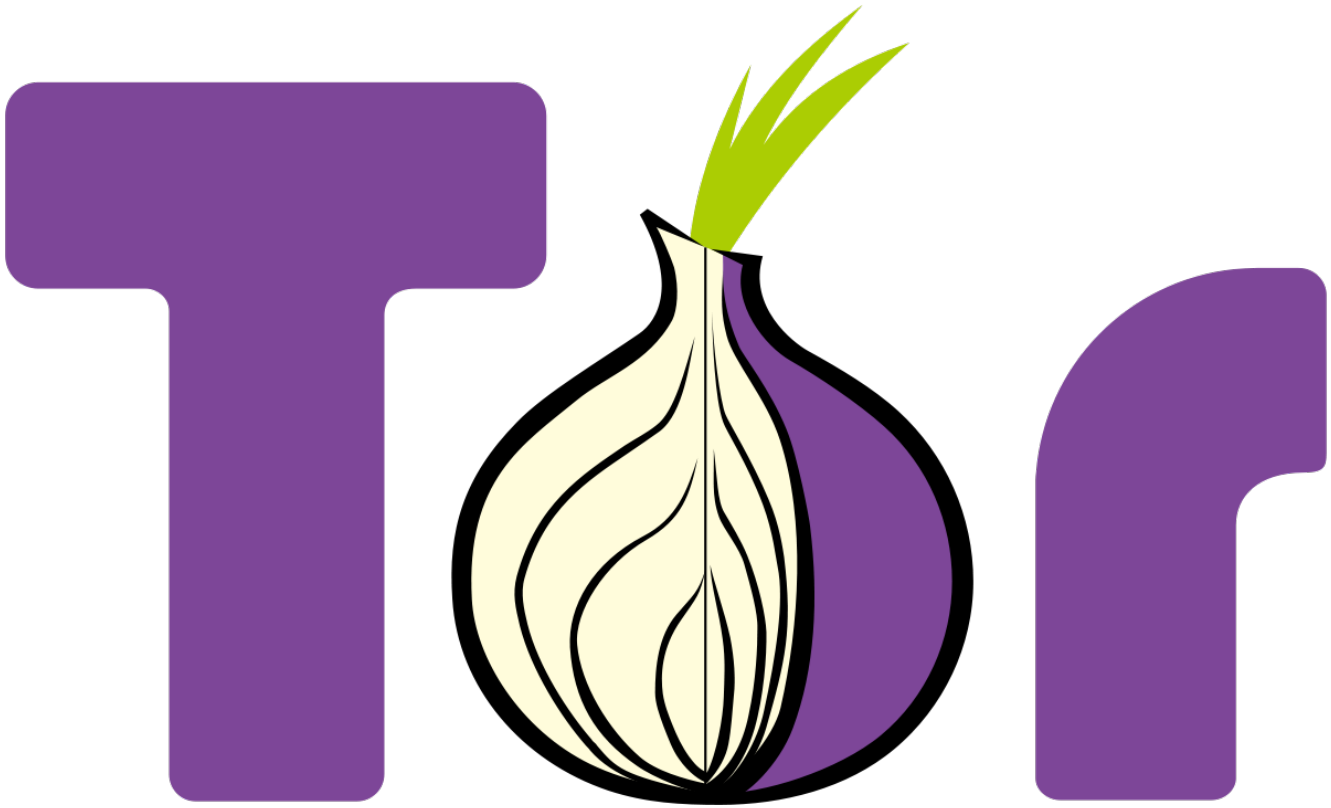
Darkweb


SERVERS
THE CLOUD
AMAZON
WIKIPEDIA
THE WEB SEA
Google
PORN
HACKERS
DEEP WEB
CONTINENTAL
CONTENTS
WIKILEAKS
GOVERNMENT
UNDETECTED
ILLEGAL PORN

Darkweb



... Tor, maybe?



`https://www.eff.org/pages/tor-and-https`

Emails & Phishing

Emails & Phishing

- Very old protocol
- No validation is enforced
- Very easy to impersonate someone (email with your own name?)
- Domain names are cheap
- Relatively easy to create a targeted phish if you know the organisation

What makes a good phishing email?

Emails & Phishing

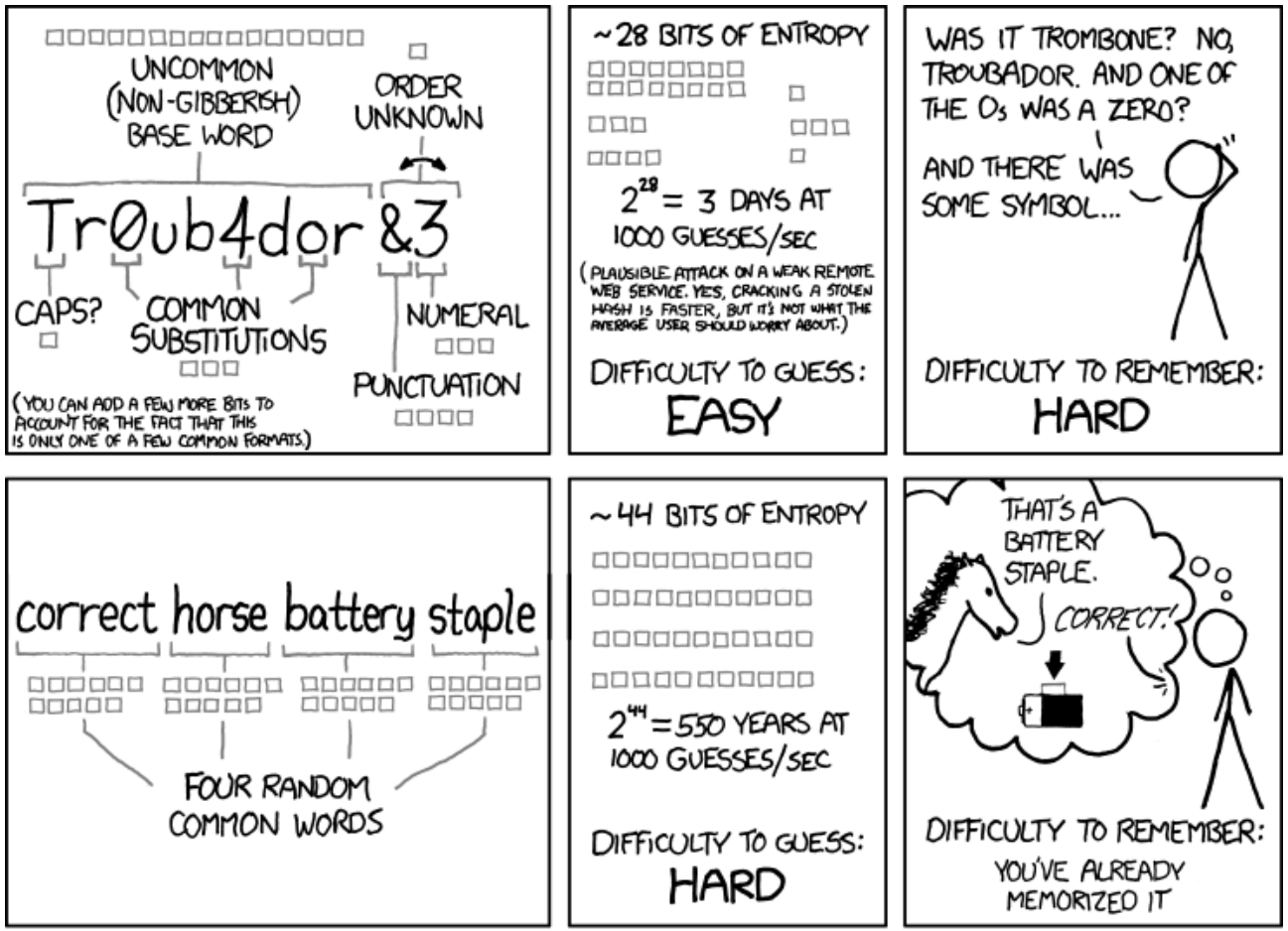
- Someone having an email address in the organisation
- A good domain name
- A valid email format (firstname.lastname@company.com)
- A target whose job is for a good part to receive and open attachments (HR, finance department)
- Someone scared to ask the IT department, or is new (linkedin)
- Someone who doesn't know the management (big organisations)

Emails & Phishing

- Someone having an email address in the organisation
  - `http://www.XXXX.com/about-us/board-of-directors`
  - `http://www.XXXX.com/about-us/management`
- A good domain name
  - `https://shop.gandi.net/en/domain/suggest?search=XXXX.com`
  - `https://shop.gandi.net/en/domain/suggest?search=XXXX-finance`

Passwords

Passwords


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Passwords & passwords manager

- Unique password for each website.
- Context matters: throw away passwords/accounts are fine
- Password Manager:
  - Mac OSX: Keychain
  - Windows: Browser based
  - Paper

Browser security

Browser security

- Legitimate websites get compromised
- Ad networks are extremely intrusive
  - `https://www.eff.org/privacybadger`
- HTTPS everywhere
  - `https://www.eff.org/https-everywhere`
- uBlock
  - Firefox: `https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/`
  - Chrome: `https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm`

Contact

- info@circl.lu
- https://www.circl.lu/
- OpenPGP fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5
- Found suspicious documents? Do you need a custom training for your teams? Don't hesitate to contact CIRCL