USER AUTHENTICATION BASICS

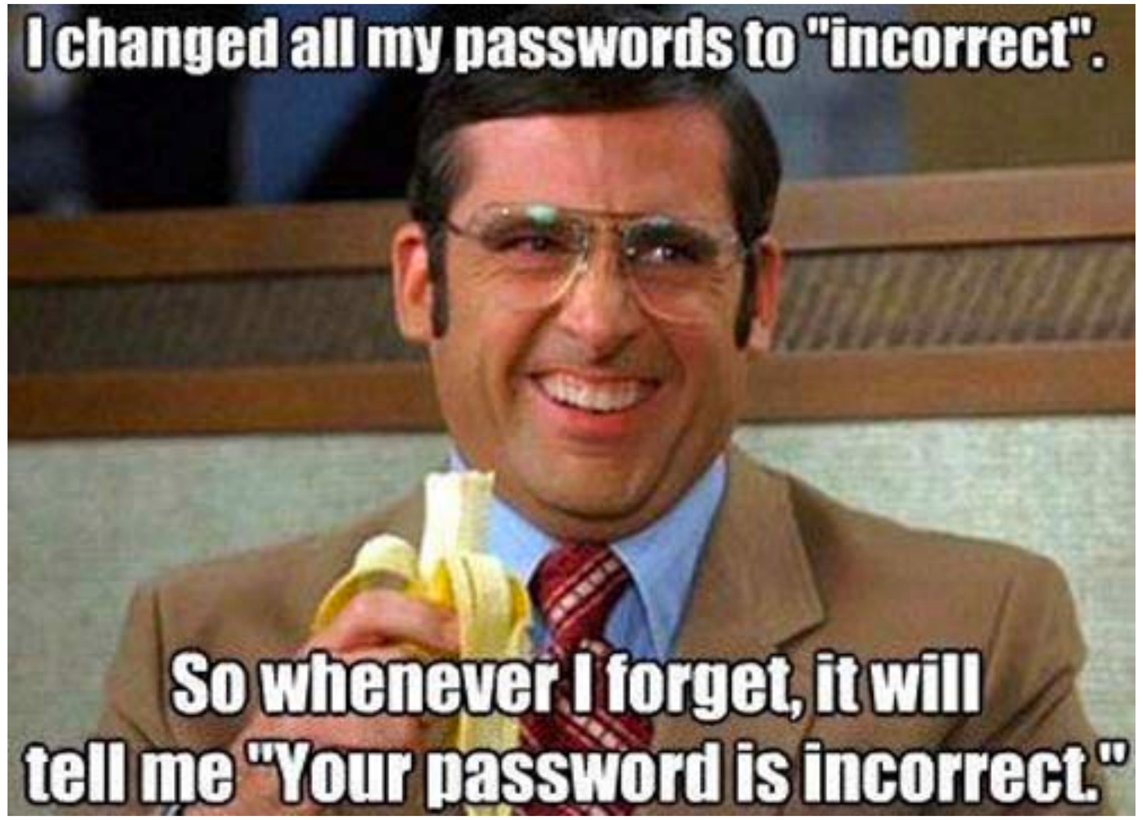
BACKEND-WORKSHOP

Michael Fröhlich - michael-froehlich@cdtm.de

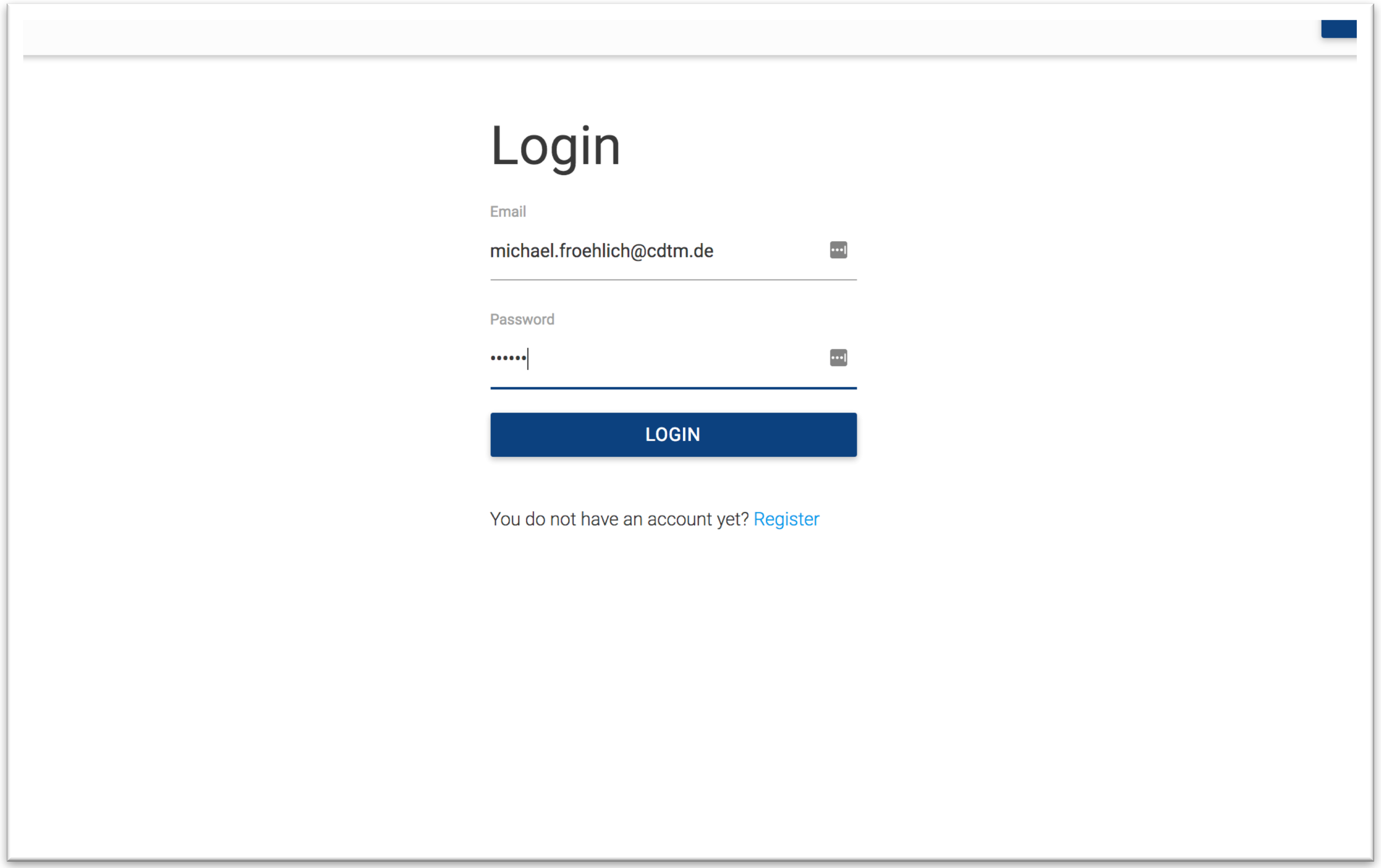
Tobias Dümmling - tobias.duemmling@cdtm.de

USER AUTHENTICATION

- Highly relevant but complex topic
  - Who can read your passwords?
  - How to securely store your user’s passwords?
  - How does authentication work on the web?
  - How anonymous are you really?
- Today we will only give a rough overview ☺


I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."

WHAT HAPPENS IF YOU PRESS 'LOGIN'?

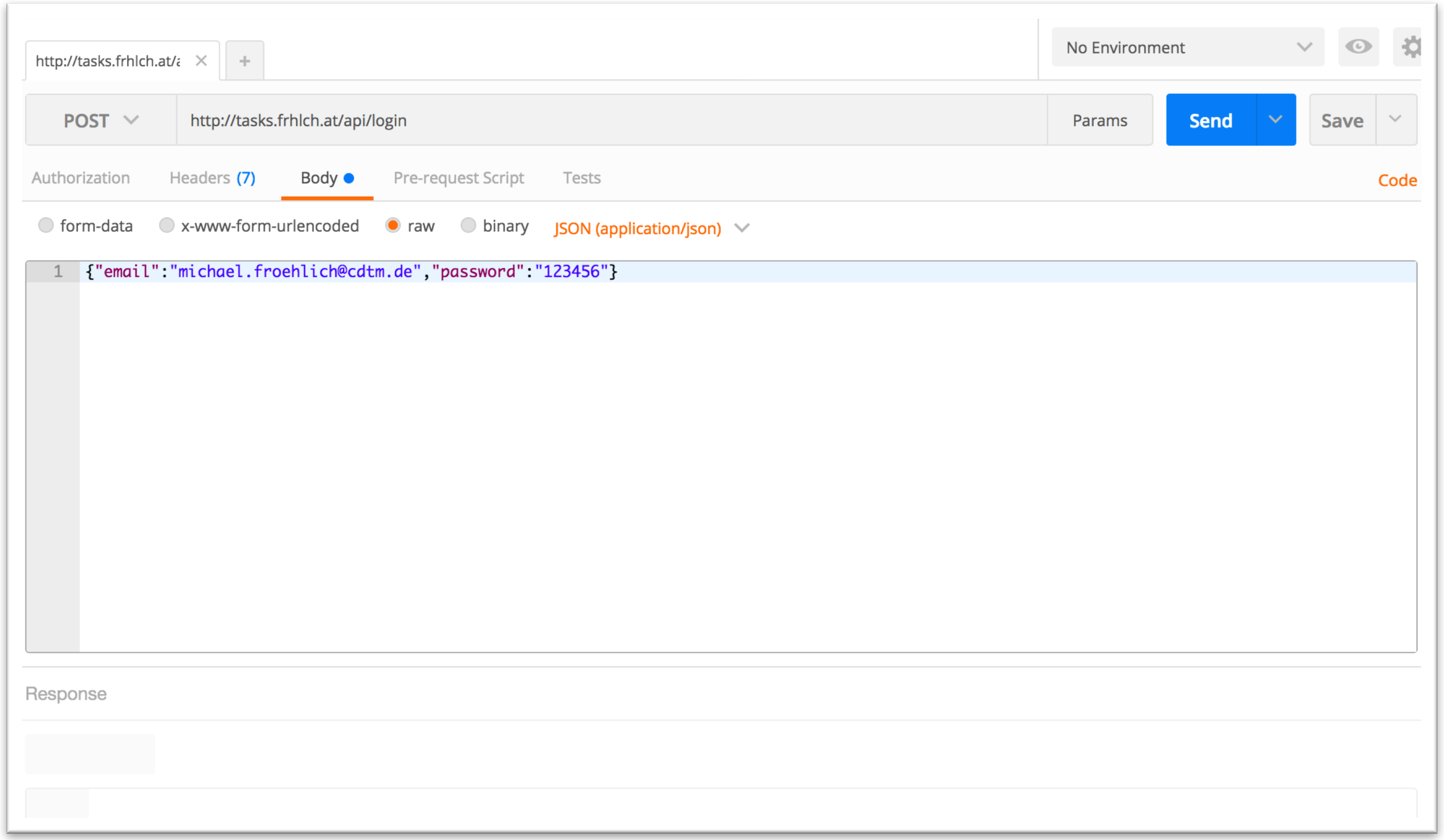


Login

Email: michael.froehlich@cdtm.de

Password: ••••••

You do not have an account yet? Register



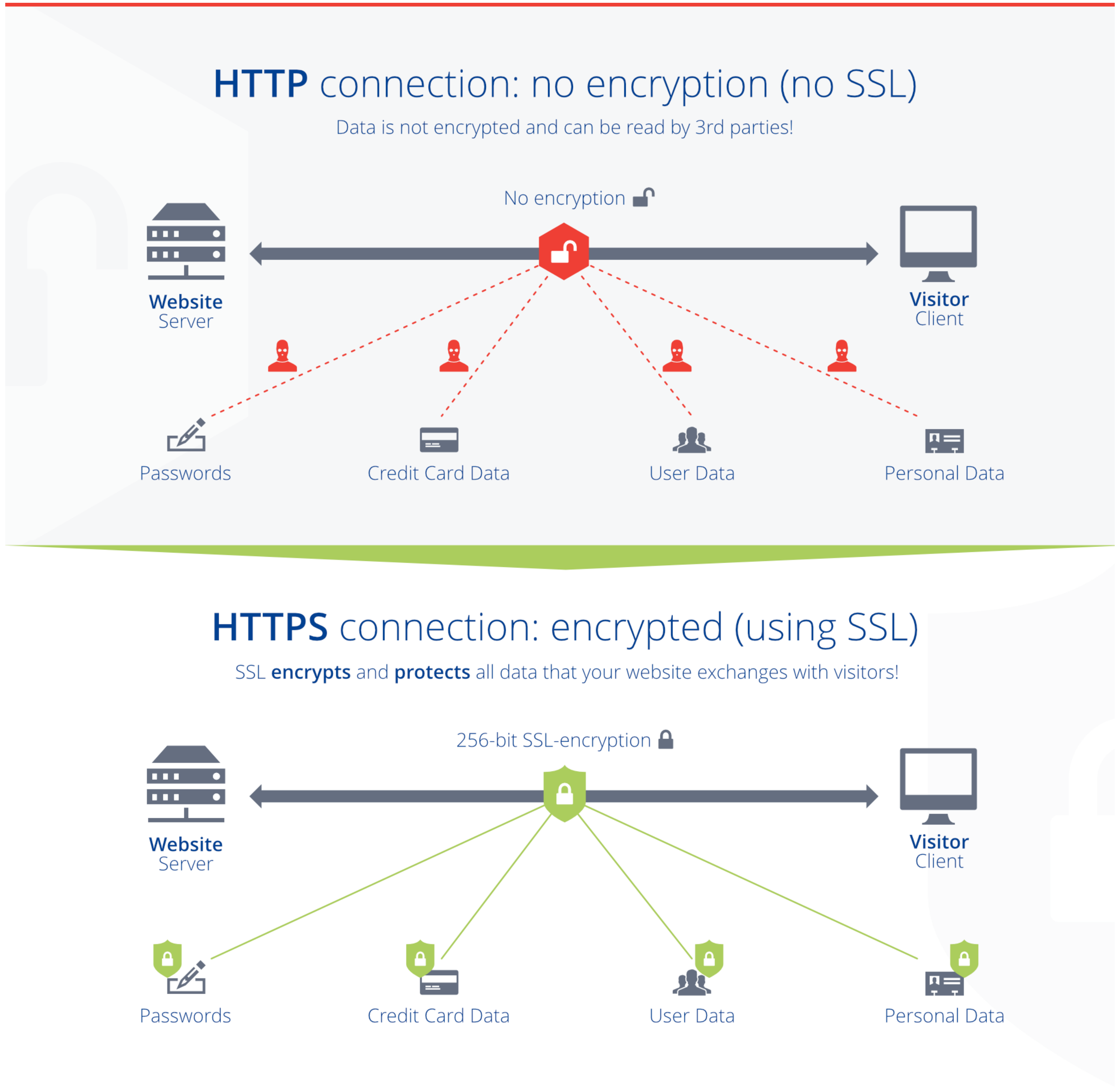
POST http://tasks.frhlch.at/api/login

Body: ○ form-data ○ x-www-form-urlencoded ● raw ○ binary JSON (application/json)

```
{"email":"michael.froehlich@cdtm.de","password":"123456"}
```

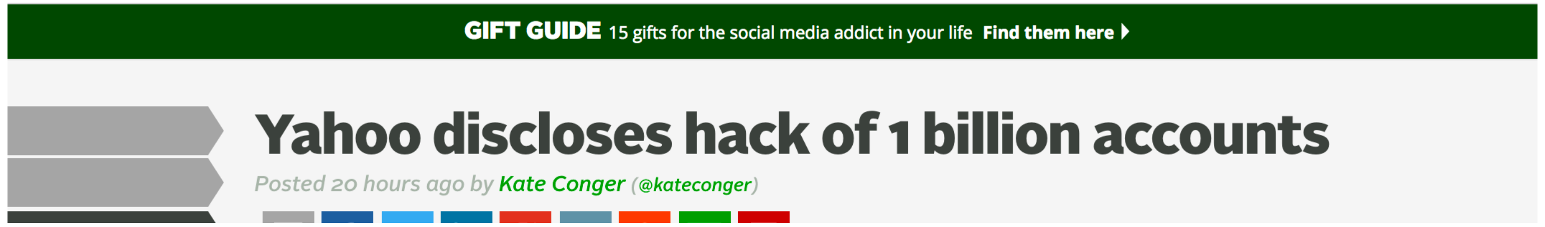
HTTP VS HTTPS

- Transport Layer Security
- Benefits
  - Encryption
  - Authenticity
  - Confidentiality
- Bonus
  - Higher SEO ranking


HTTP connection: no encryption (no SSL)
Data is not encrypted and can be read by 3rd parties!
No encryption
Website
Server
Visitor
Client
Passwords
Credit Card Data
User Data
Personal Data
HTTPS connection: encrypted (using SSL)
SSL encrypts and protects all data that your website exchanges with visitors!
256-bit SSL-encryption
Website
Server
Visitor
Client
Passwords
Credit Card Data
User Data
Personal Data

WHY TO NEVER STORE CLEAR TEXT PASSWORDS

- Doing so puts your users at risk
- Data Leaks or being hacked can loose your users trust and destroy your business
- You don’t need your users passwords to authenticate them

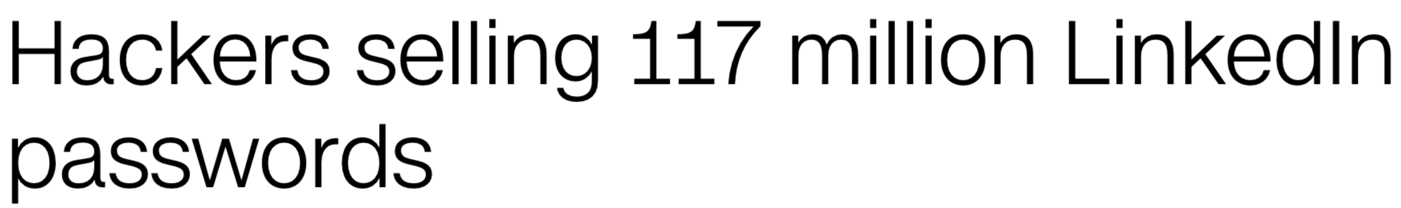


GIFT GUIDE 15 gifts for the social media addict in your life Find them here

Yahoo discloses hack of 1 billion accounts

Posted 20 hours ago by Kate Conger (@kateconger)

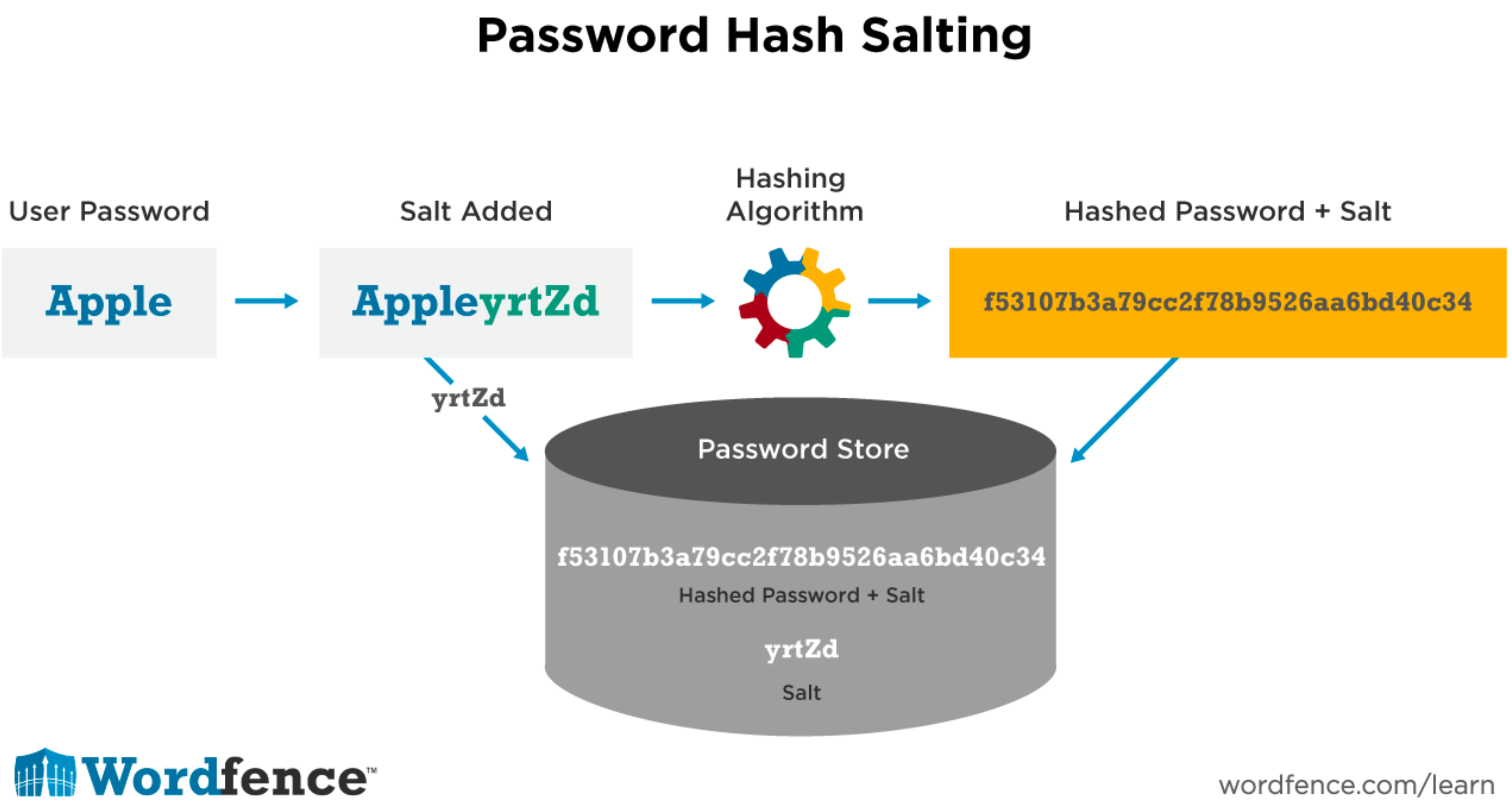
Sony Promises All PlayStation Services Will Return This Week (Again)



Hackers selling 117 million LinkedIn passwords

Dropbox hackers stole 68 million passwords - check if you're affected and how to protect yourself

STORING PASSWORD HASHES



Password Hash Salting

COOKIES & SESSIONS

- Cookies are text files saved on your computer on the request of a webserver
  - The Webserver can then read and write from and to this file *(on your computer)*
  - E.g. shopping cart items, preferences, authentication, session ids
- Sessions
  - A *server-side* storage of information that is desired to persist throughout the user's interaction with the web site or web application.
  - Instead of storing large or sensitive amount of data in a cookie (*client side)* just a session identifier is stored, so the server can retrieve the session storage

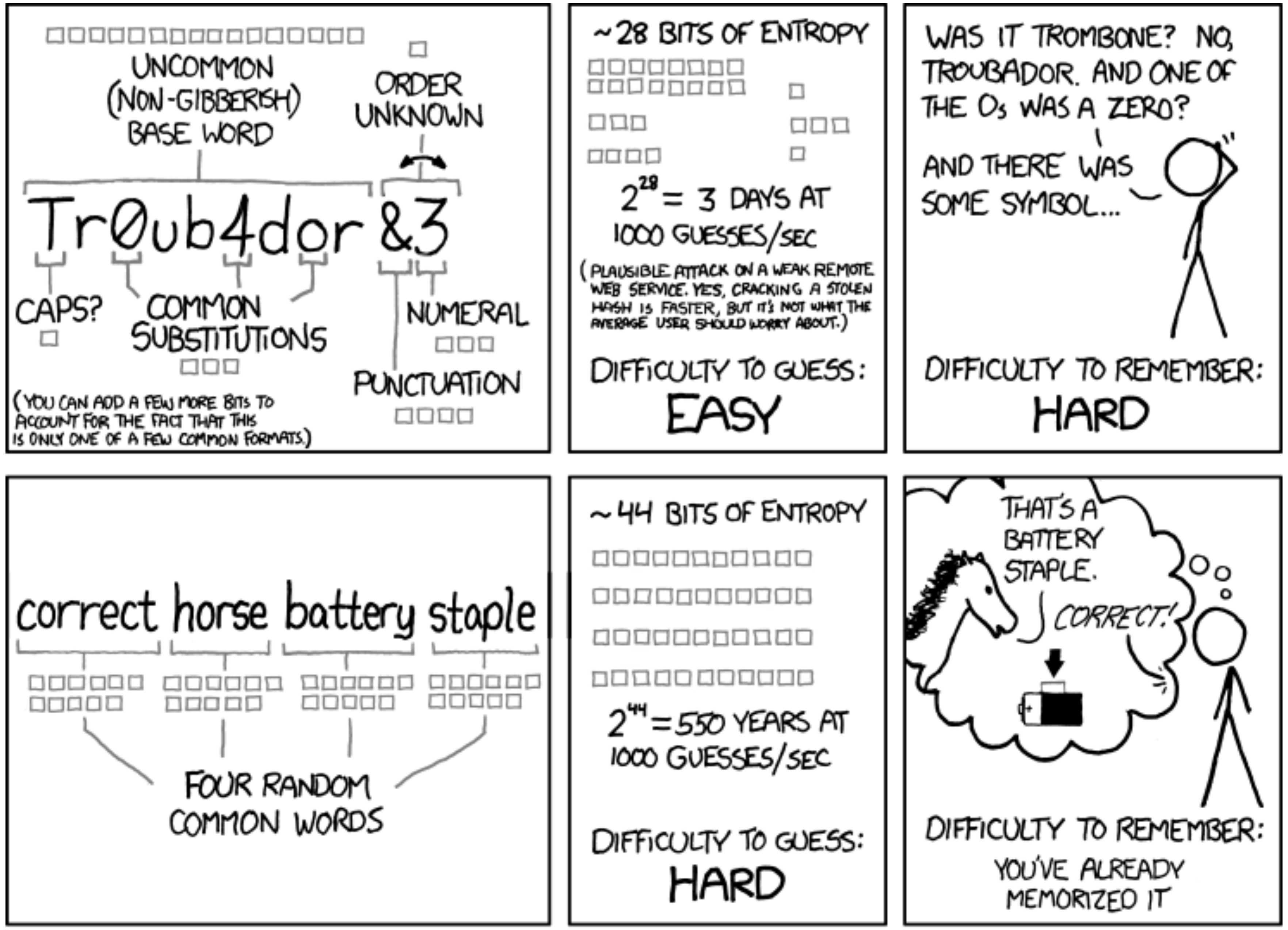
What is a cookie? (Video) https://www.youtube.com/watch?v=I01XMRo2ESg

Introduction to Cookies: https://code.tutsplus.com/tutorials/an-introduction-to-cookies--net-12482

PASSWORD STRENGTH

- Complexity < Length: http://i.imgur.com/zFyBtyA.gif
- Password-Strength: http://password.social-kaspersky.com/en

(don't enter your real one)


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.