Find your IT-risk culprits!

(your employee)
((and your practices))

Mark Korondi

mark@korondi.ch

KORONDI
CLOUD CONSULTING

/// Agenda

- IT risks – are we affected?
- What is the risk?
- The culprit: your employee
- The culprit: your IT security practices
- Information Security Culture
- Example of stealing a password

/// About me

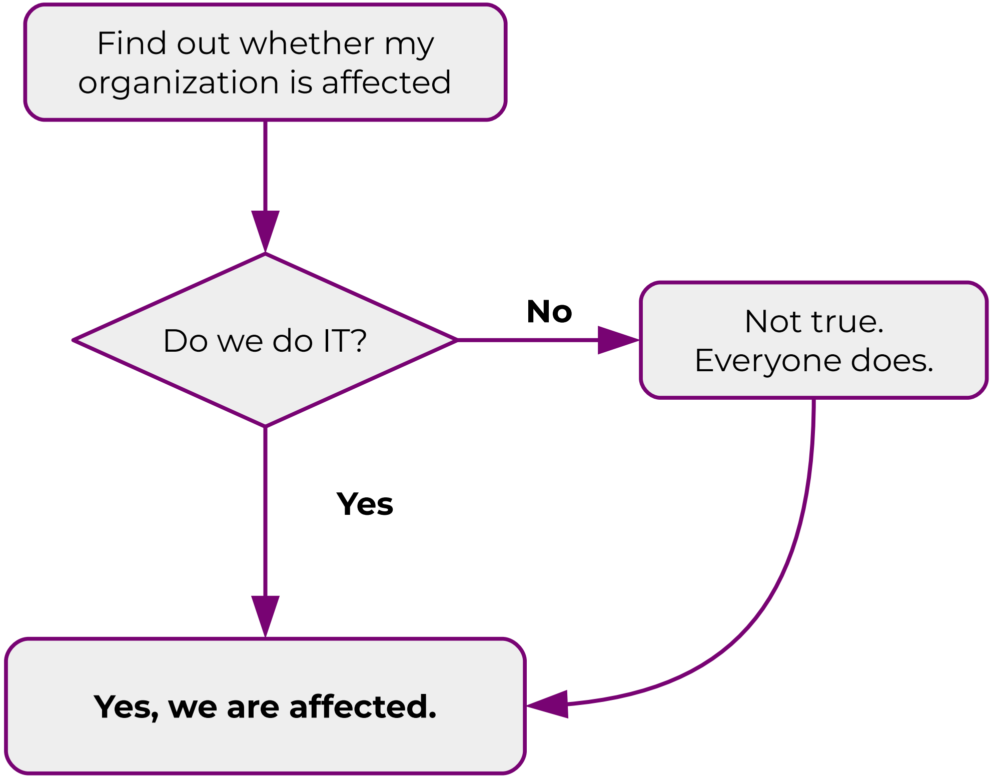
- Workflow evangelist
- Cloud & Storage subject matter expert
- Security / Privacy / Reliable computing enthusiast

- **Past**
  - Deutsche Telekom PanNet
    DevOps / Security / Storage
  - IBM & IBM Research
    Cloud / Security / Storage
  - NNG
    SoftDev / Agile / Embedded

- **Contact**

Email:	mark@korondi.ch
LinkedIn:	markkorondi
GitHub:	kmarc
Twitter:	kmarc

/// IT risks – are we affected?


Find out whether my organization is affected

Do we do IT?

No

Not true. Everyone does.

Yes

Yes, we are affected.

- Customers, peers
  - Website
  - Web / mobile application
  - Web service
- Employees
  - Intranet
  - E-mail
  - VPN

/// IT risks – are we affected?

- You are **dependent**

  (not an option not to have)

- You **transform**

  (or others disrupt)

- You **complicate**

  (more tools, more interfaces)

- You **pose new risks**

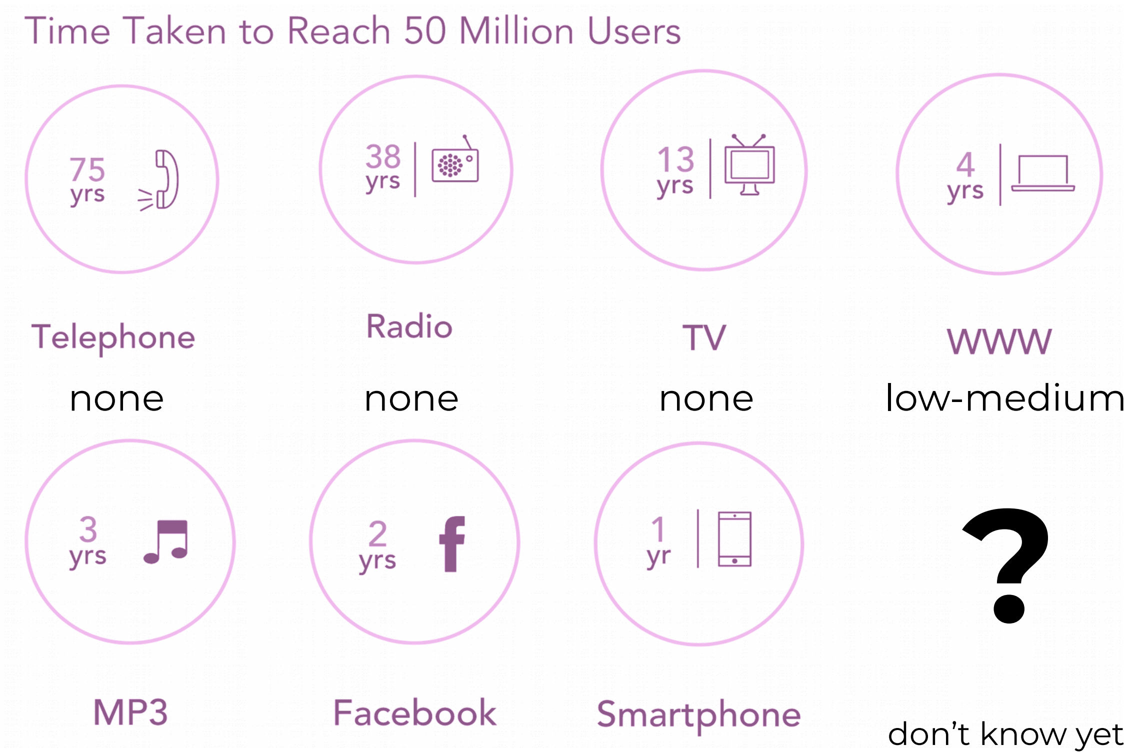
- Number of email users will rise to 2.9 billion by 2019.
  (Source: Statista, 2016)

- *“companies unable or unprepared for [digital transformation] changes will quickly fall to the bottom of the pack.”*
  (Source: Forbes, 2017)

- IT spending grows by $500 billion between 2016-2022.
  (Source: Gartner, 2018)

- Known software voulnerabilities grew from 900 to 15,000 between 1999-2017
  (Source: CVEDetails, 2018)

/// IT risks – are we affected?



IT Risk:	none	none	none	low-medium

?

don't know yet

IT Risk:	low-high	medium-high	high	probably high

Source: KPMG. https://www.iif.com/system/files/32370132_insurance_innovation_report_2016.pdf

/// IT risks – are we affected?

Yes.

/// What is the risk?

*Risk = Threat * Vulnerability * Asset*

*Risk = ((Threat * Vulnerability) / CounterMeasure) * AssetValueAtRisk*

- Example – payroll
  - **Threat:**
    - employee to learn other’s salaries
  - **Vulnerability:**
    - old CMS with no security patches
  - **Counter measure:**
    - password login
  - **Asset value at risk**
    - salary database

- Example – any SMB
  - **Threat:**
    - internet-connected workstation
  - **Vulnerability:**
    - write access on shared drive
  - **Counter measure:**
    - up-to-date anti-virus solution
  - **Asset value at risk**
    - all business data on shared drive

/// What is the risk?

- Strategic risk
  - Trust violated by data breach. Investors turn away.
- Financial risk
  - Unable to attract / service / pay users. Unable to process transactions.
- Operational risk
  - Operational data, software or equipment corrupted.
- Compliance (legal) risk
  - Sensitive data leaked. Data processing laws (GDPR) violated.
- Other risks

Categorization: Jolly, Adam (2003). *Managing Business Risk: A Practical Guide to Protecting Your Business*

/// The culprit: your employee

- Threats
  - **Social engineering**
  - Malware
  - Spyware
  - Trojans, Viruses
  - Keyloggers
  - Exploits
  - Backdoors

Kevin Mitnick

"A company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and encryption and other security technologies, but ***if an attacker can call one trusted person within the company****, and that person complies, and if the attacker gets in, then all that money spent on technology is essentially wasted."*

Source: https://www.quotationof.com/kevin-mitnick.html

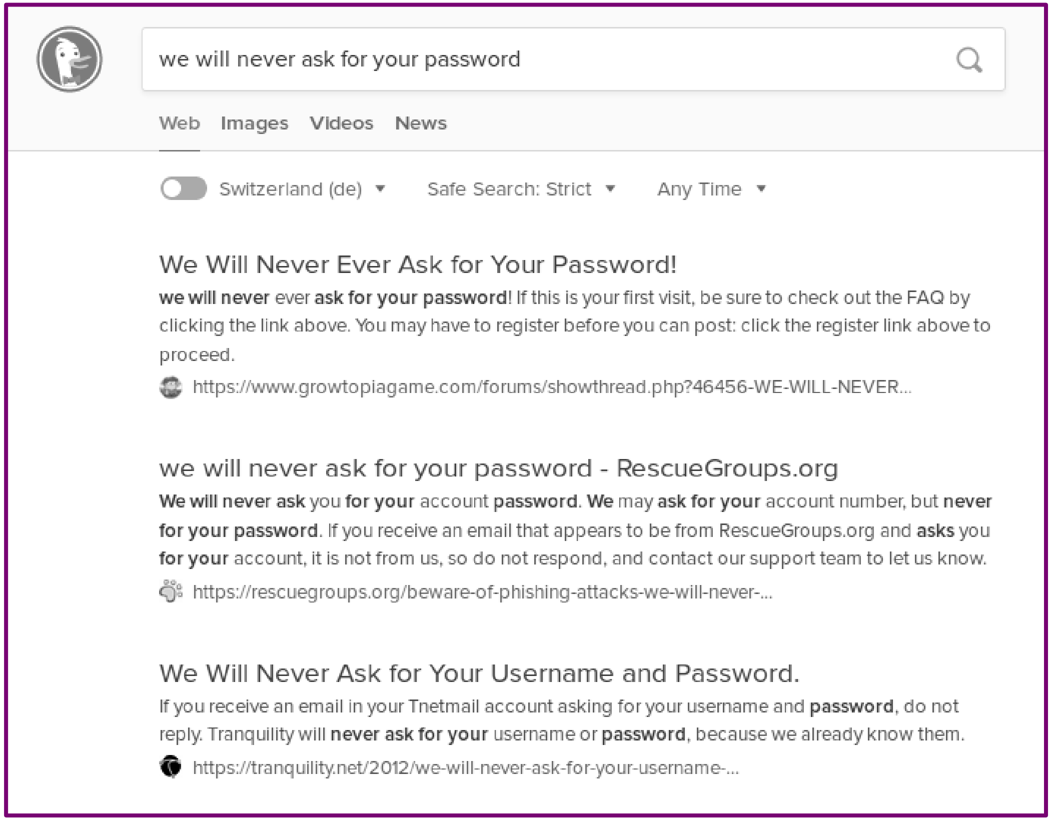
/// The culprit: your employee

- Examples of social engineering
  - Pretexting
  - Phishing
    - Vishing / phone phising
  - Baiting
    - Physical trojan
  - Tailgating

- Psychological background
  - Psychology of persuasion (2/6)
    - Social proof
    - Authority
  - Decision making
  - Cognitive biases

/// The culprit: your employee

- Social engineering countermeasures
  - Training of employees
  - Standard frameworks
  - Scrutinizing Information
  - Security protocols
  - Event Test
  - Review
  - Waste Management



we will never ask for your password

We Will Never Ever Ask for Your Password!

we will never ever **ask for your password**! If this is your first visit, be sure to check out the FAQ by clicking the link above. You may have to register before you can post: click the register link above to proceed.

https://www.growtopiagame.com/forums/showthread.php?46456-WE-WILL-NEVER...

we will never ask for your password - RescueGroups.org

We will never ask you **for your** account **password**. **We** may **ask for your** account number, but **never for your password**. If you receive an email that appears to be from RescueGroups.org and **asks** you **for your** account, it is not from us, so do not respond, and contact our support team to let us know.

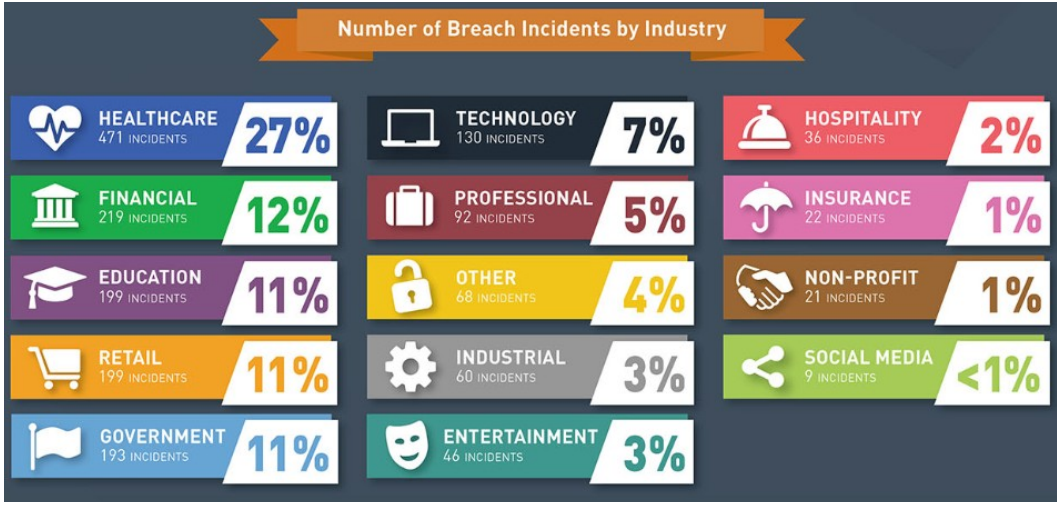
https://rescuegroups.org/beware-of-phishing-attacks-we-will-never-...

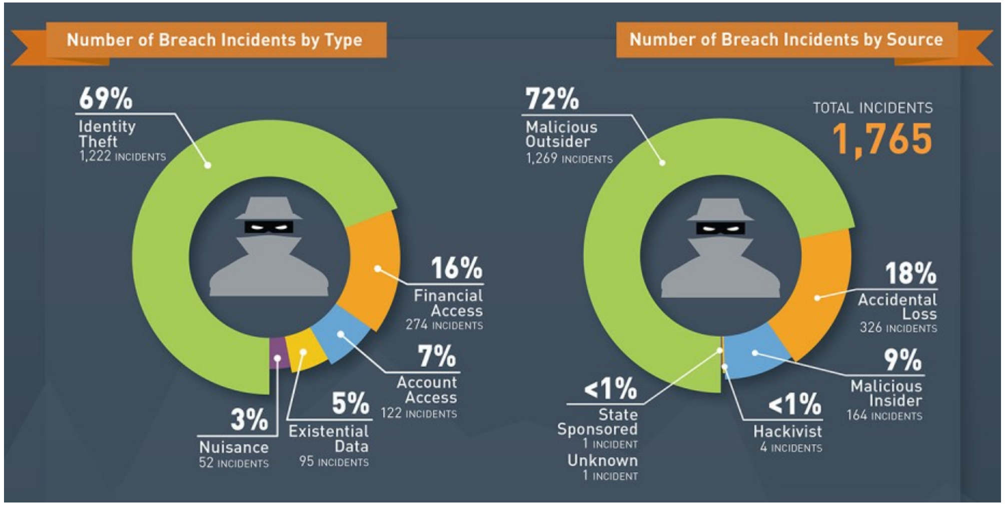
We Will Never Ask for Your Username and Password.

If you receive an email in your Tnetmail account asking for your username and **password**, do not reply. Tranquility will **never ask for your** username or **password**, because we already know them.

https://tranquility.net/2012/we-will-never-ask-for-your-username-...

/// The culprit: your IT security practices





- **Only 4% of breaches** were **“Secure Breaches”** where encryption was used and the stolen data was rendered useless.
- **Only 7% of breaches** were target to actual **technology industry** actors
- **More than 2.5 billion data records** were compromised in 2017

Source: https://www.breachlevelindex.com/

/// The culprit: your IT security practices

- Anatomy of a security breach
  - Gain network access to trusted domain
  - Bypass encryption over the network
  - Attack security holes
  - Acquire / bypass credentials
  - Steal data / keys of at-rest-encrypted data
  - Distribute malware on internal networks

- Prevention: hardening
  - Certificate-based, 2FA-enabled VPN
  - Modern ciphers, valid certificates
  - Security patches, sealed domains
  - Strong password policies, employee education
  - Keys in sealed domains, strong and mandatory encryption
  - Up-to-date network security scanning, workstation protection

/// The culprit: your IT security practices

- Mindset of prevention
  - **How would I** breach the systems?
  - Who/what are the **actors**?
  - What are the credential **assets**?
  - What **can** happen **after** the breach?
  - Can I **detect** an adversary?
  - Can I **identify** the adversary?
  - What is **my loss** by being breached?

- Examples
  - Using a keylogger
  - Employees at finance dept
  - VPN password
  - Download sensitive documents from shared drive
  - Monitoring of unusual behavior
  - Logging access metadata
  - Missing documents, public press, etc

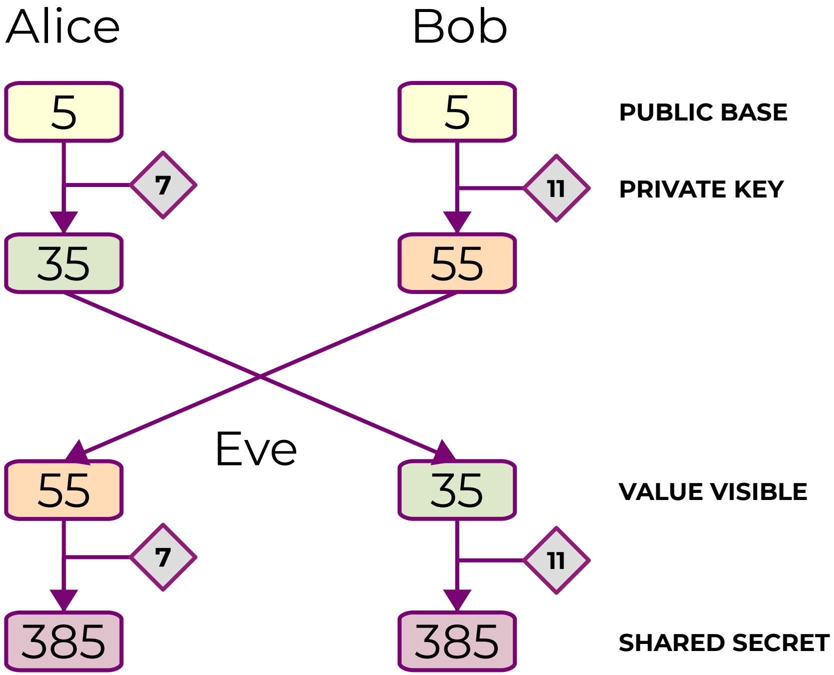
/// The culprit: your IT security practices

- An **https://** primer
  - HyperText Transfer Protocol, Secure
  - Certificate from Certificate Authorities
  - Public-Key Infrastructure

!!! This is a very unscientific and incorrect example !!!

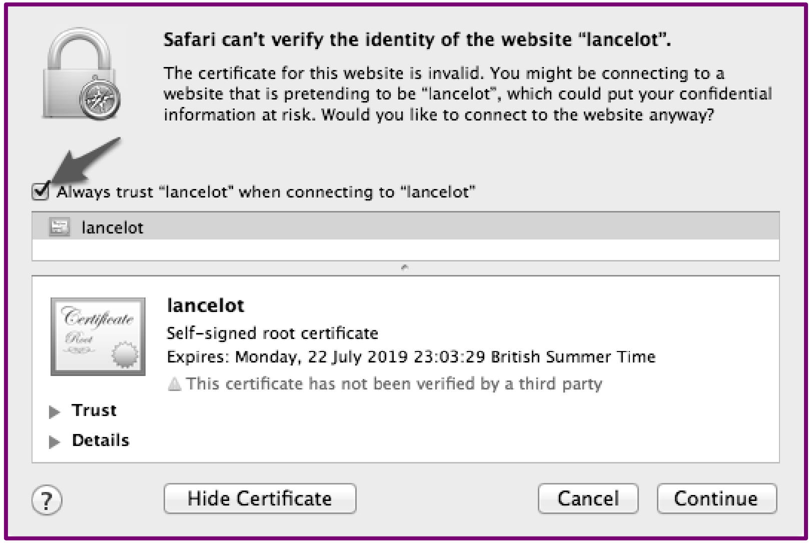
Click to view a 3 minute long
video from Khan Academy
for a scientifically correct explanation

- A **Diffie-Hellman** primer



KORONDI
CLOUD CONSULTING

/// The culprit: your IT security practices



Safari can't verify the identity of the website "lancelot".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "lancelot", which could put your confidential information at risk. Would you like to connect to the website anyway?

☑ Always trust "lancelot" when connecting to "lancelot"

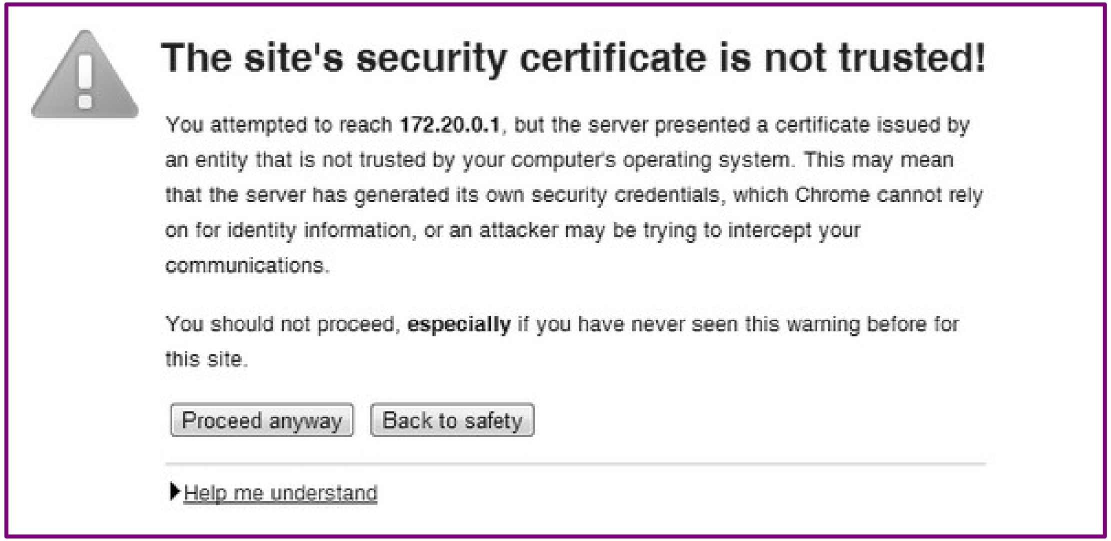
lancelot

lancelot

Self-signed root certificate

Expires: Monday, 22 July 2019 23:03:29 British Summer Time

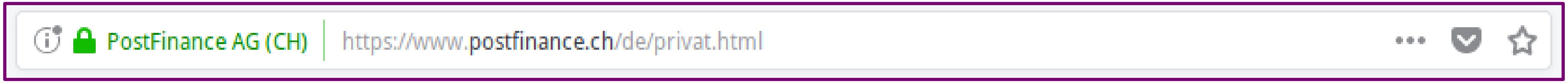
⚠ This certificate has not been verified by a third party



The site's security certificate is not trusted!

You attempted to reach **172.20.0.1**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.



PostFinance AG (CH) | https://www.postfinance.ch/de/privat.html

Padlock icon: https://support.mozilla.com/en-US/kb/how-do-i-tell-if-my-connection-is-secure

/// The culprit: your IT security practices

- The Man-In-The-Middle attack with HTTPS
  - **The browser verifies** the website’s certification against a known list of issuers
  - If the website certificate is **self signed**, a warning is shown
  - If the user **bypasses** the warning message, a third party is able to relay messages between the user and the website
  - Relayed messages are decrypted, read, then **re-encrypted** with a different key
  - **User won’t notice** anymore, since the warning messages are muted.

/// The culprit: your IT security practices

- Whose fault is this?
  - The user of my website was notified by the browser, she should not bypass the security warning
  - The owner of the website used a self-signed certificate, he should have paid for a signed one.
- Theoretically / legislatively: **the visitor of the website**
  - She is responsible to take all the security measures
- In practice:
  - It’s **YOUR** fault. Try explaining to the public otherwise.

/// Information Security Culture

- **Pre-Evaluation**

  identify the awareness, analyse current security policy

- **Strategic Planning**

  set clear targets (e.g. clustering people)

- **Operative Planning**

  create a good security culture; training programs

- **Implementation**

  commitment of all organizational members

- **Post-evaluation**

  build on continuous improvement

Source: Schlienger, Thomas; Teufel, Stephanie (2003). "Information security culture-from analysis to change"

/// Information Security Culture

- Use HTTPS everywhere
  - Let's Encrypt
- Introduce password / key manager
  - ';--have i been pwned?
  - bitwarden
- Make 2-factor-authentication mandatory
  - AndOTP
- Make mobile device administration mandatory
- Implement firewalling
- Use Virtual Private Network
  - OpenVPN
- Use full-disk encryption
  - LUKS, BitLocker, FileVault
- Use data protection solutions
  - Acronis
    (True Image, Backup, Files Advanced)
- Educate. Train. Inform.

/// Example of stealing a password

demo time!

/// Sources to consult

- https://en.wikipedia.org/wiki/Information_security (and subpages)
- https://threatpost.com/
- https://www.cvedetails.com/
- https://www.iif.com/
- https://www.owasp.org/
- https://haveibeenpwned.com/
- Forums:
    - https://news.ycombinator.com/ (generic; important security news published regularly)
    - https://www.reddit.com/r/security/
    - https://www.reddit.com/r/netsec/

Thank you!

Questions?