- *«If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.»*

  Bruce Schneier

Introduction to IT Security for Data Scientists

Matthias Seitz
matthias.seitz@protonmail.ch

Bern, 31.10.2025

Agenda

01 - Welcome, mutual introduction and expectations

02 - Introduction to IT security

03 - Current Security Threats

04 - Basic Security

05 - How to protect your Assets

06 - Good IT security practices

07 - Roundup and Feedback

01 - Welcome

- About me

- About you

- Expectation for this afternoon

About me

Professional life

- Longtime experience in IT Security
- BSc Computer Science @OST
- Information Security Officer and Product Manager @Switch
- Specialist Cyber Security @Swissgrid

Private

- 37 years old
- Married, 2 kids
- Living in Mettmenstetten, ZH

About you

Some sentences about yourself :-)

What are your and my expectations for this course?

02 - Introduction to IT security

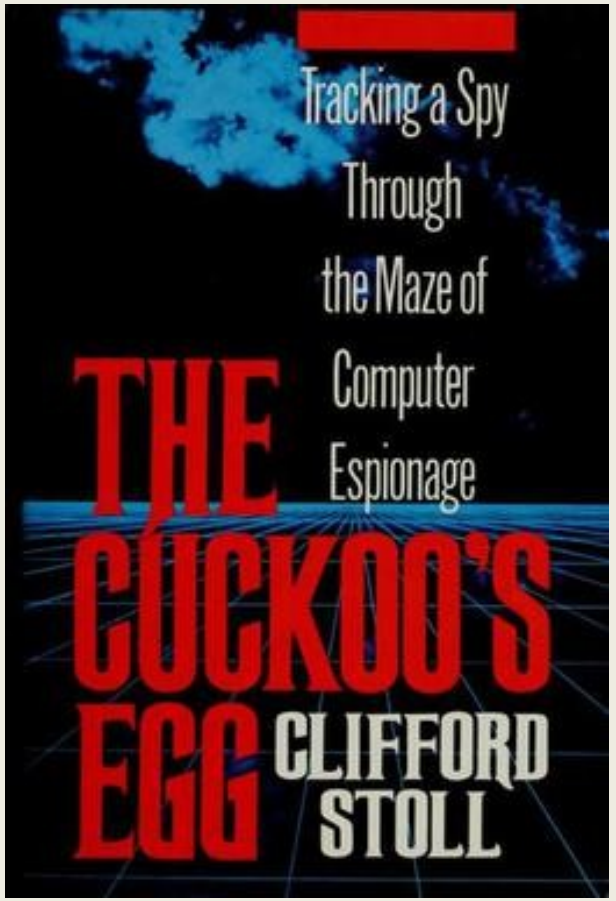
- The early internet

- ENISA Threat Landscape 2025

The early internet - Origin and spirit

- Origins (1960s–1980s): Emerged as ARPANET via US military and universities: A network for **research and knowledge exchange**.
- Openness & Naivety: **Anyone could join without barriers**; naive trust in a small, academic community, no thoughts of abuse.
- **Friendly Collaboration**: Scientists shared ideas, code, and resources freely; collaborative like a "global village", emails and forums fostered dialogue.
- **No Security**: Protocols like TCP/IP without encryption; attacks unlikely in the "trusting" era. The awakening came later (e.g., 1988 Worm).

Book recommondation



https://spyscape.com/article/how-an-astronomer-unraveled-the-worlds-first-cyber-attack

Time travel to 2025

ENISA Threat Landscape 2025

- What is it? **Annual report by the European Union Agency for Cybersecurity (ENISA)** providing an **overview of the EU's cyber threat ecosystem**, focusing on threats, trends, and incidents targeting EU Member States and organizations.
- Purpose: **Delivers actionable insights for policy, awareness, and defense**; analyzes adversary behaviors, vulnerabilities, and geopolitical drivers.
- Period Covered: July 2024 – June 2025, based on ~4,900 curated incidents.
- Main Contents: **Threat overview, key trends (e.g., phishing, AI use), sectorial analysis (e.g., public admin, transport), cybercrime (ransomware), state-aligned activities (espionage), FIMI, hacktivism, TTPs & vulnerabilities, outlook.**
- Key Findings: **Phishing as top vector (60%); DDoS dominant (77%); ransomware persistent; hacktivism ~80% of incidents; AI in >80% phishing**; state-nexus espionage on telecom/logistics; supply chain attacks rising.

ENISA Threat Landscape 2025

https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf

ENISA Threat Landscape 2025

- **Little task**
  - Download the ENISA Threat Landscape 2025
  - https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf
  - Read the first two paragraphs of chapter 3
  - Answer the following questions
    - What are the two most identified initial attack vectors?
    - Are insiders also a possible threat to your company?

03 – Current Security Threats

- Phishing

- Malware

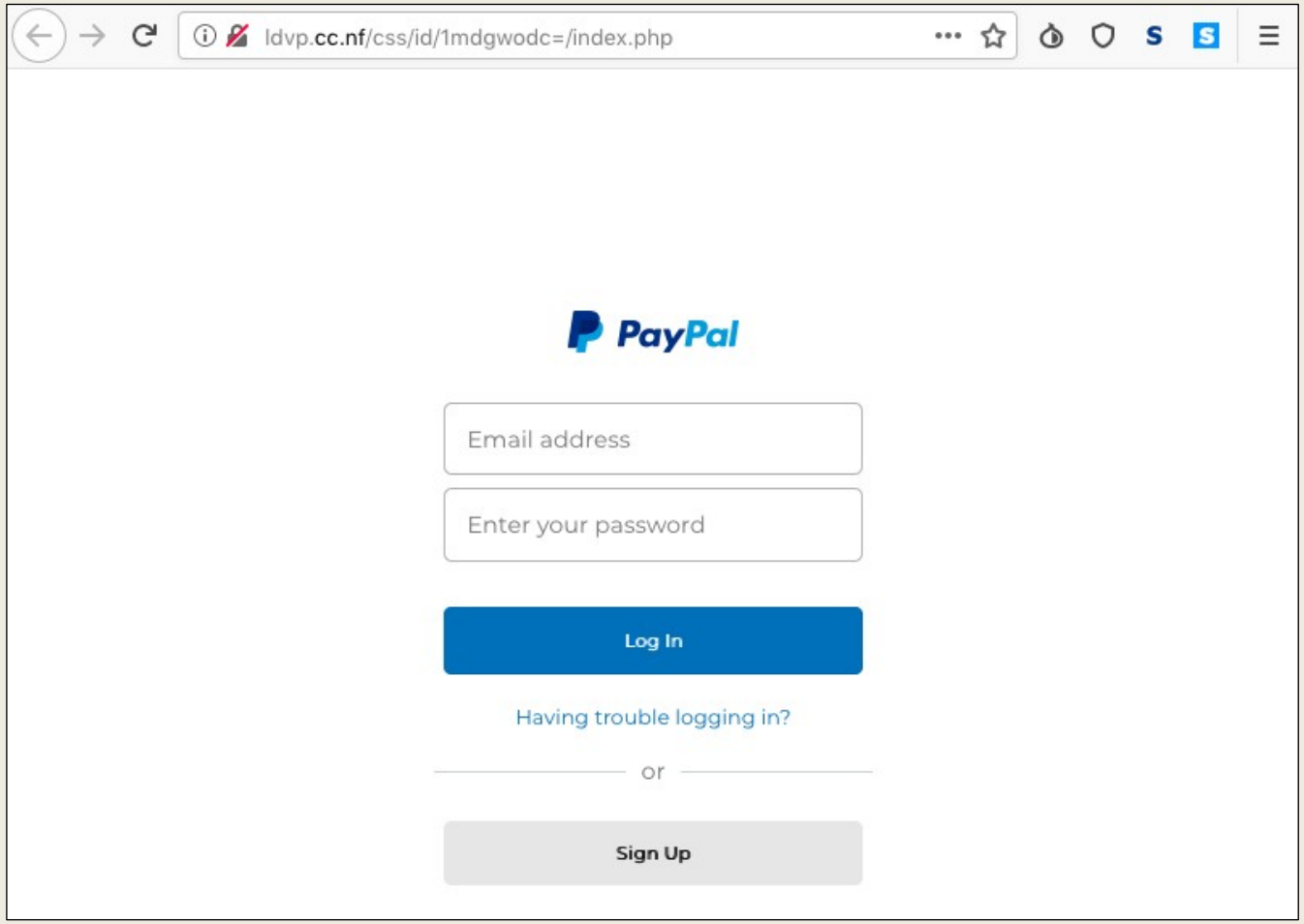
- Ransomware

Phishing

Phishing

- Phishing is a cyber attack where scammers impersonate trustworthy entities (like banks or companies) to trick people into **revealing sensitive information, such as passwords, credit card numbers, or personal data.**
- Common Tactics:
  - Email or Message Lures: Fake emails with urgent requests or links to malicious sites.
  - Deceptive Websites: Cloned pages that look legitimate to capture login credentials.
  - QR Codes (Websites)

Phishing

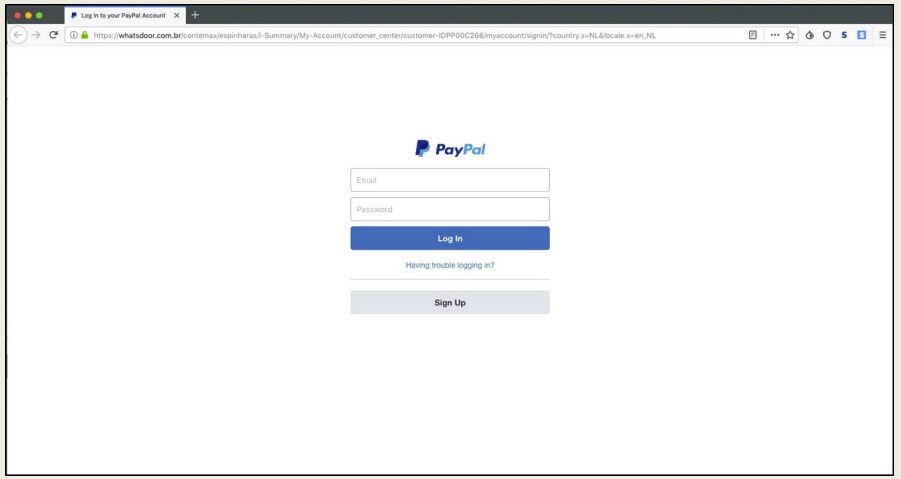

ldvp.cc.nf/css/id/1mdgwodc=/index.php
PayPal
Email address
Enter your password
Log In
Having trouble logging in?
or
Sign Up

Phishing Types

- Generic Phishing
- Spear Phishing
- CEO Fraud / Whale Phishing

Generic Phishing Attack

- Mass sending: Send to hundreds or thousands of victims
- Language / cultural border are typically ignored
- The goal is typically to gain credit card info and/or to steal monetary values



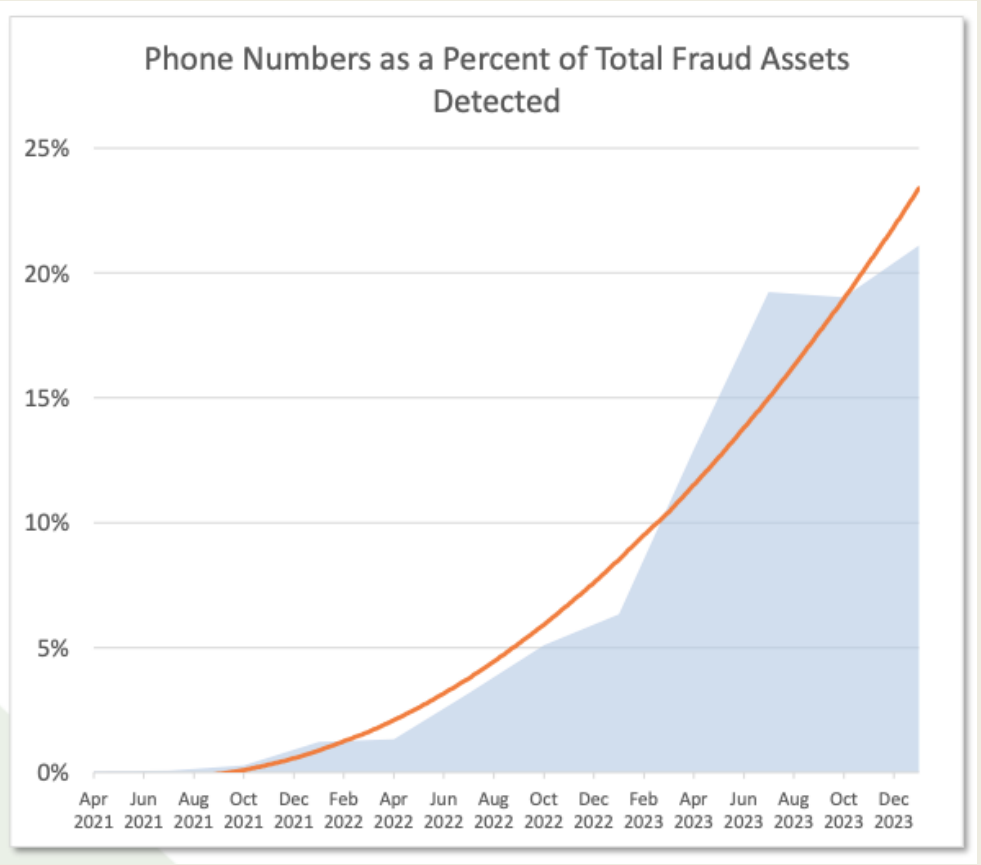
Spear Phishing Attack

- Spear phishing is a targeted attempt to steal credentials from a specific individual
- The individual is typically scouted during targeted research and identified as a possible asset for infiltration
- Spear phishing attempts use malware, keylogger, or email to get the individual to give away the credential
- Typically part of a bigger attack (Lateral movement). Credential stealing for an APT.

Whale Phishing

- Phishing attack that is specifically aimed at wealthy, powerful, or prominent individuals
- As such a user becomes the victim of a phishing attack he can be considered a “big phish,” or, alternately, a "whale"
- Whale phishing involves the same tactics used in spear phishing campaigns
- Also known as CEO Fraud, BEC (Business Email Compromise), FPF (Fake President Fraud) or Bogus Boss Email

Phishing – Not only done via mail



- APWG Phishing Report 1st Quarter 2024

HTTP vs HTTPS

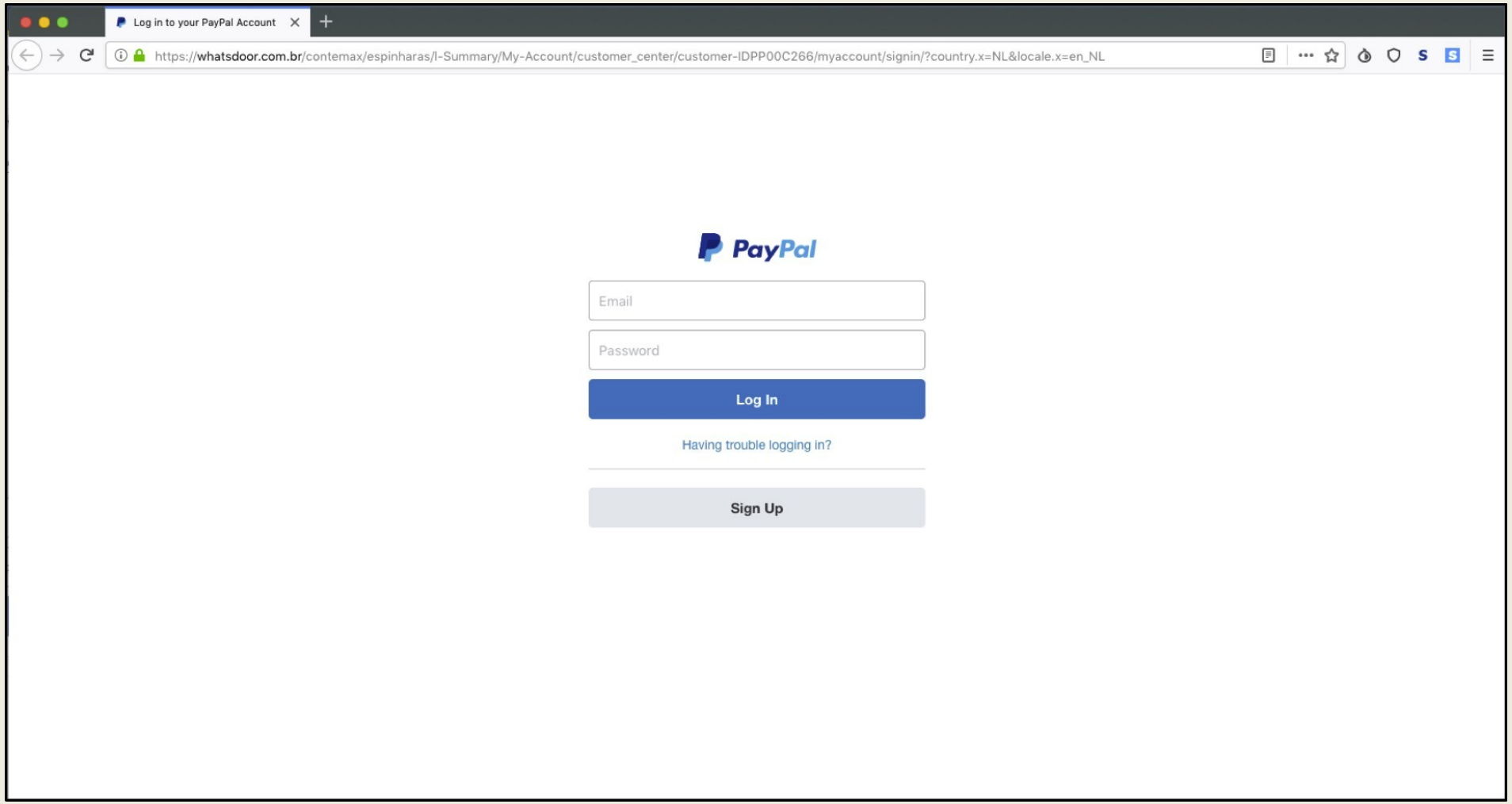
- HTTP stands for Hyper Text Transfer Protocol
- Communication between clients (users) and web servers is done by sending HTTP Requests and receiving HTTP Responses
- HTTP: No Data Encryption Implemented
- Hypertext Transfer Protocol Secure (HTTPS) is an extension of the HTTP protocol. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS)

Does HTTPS help against Phishing?

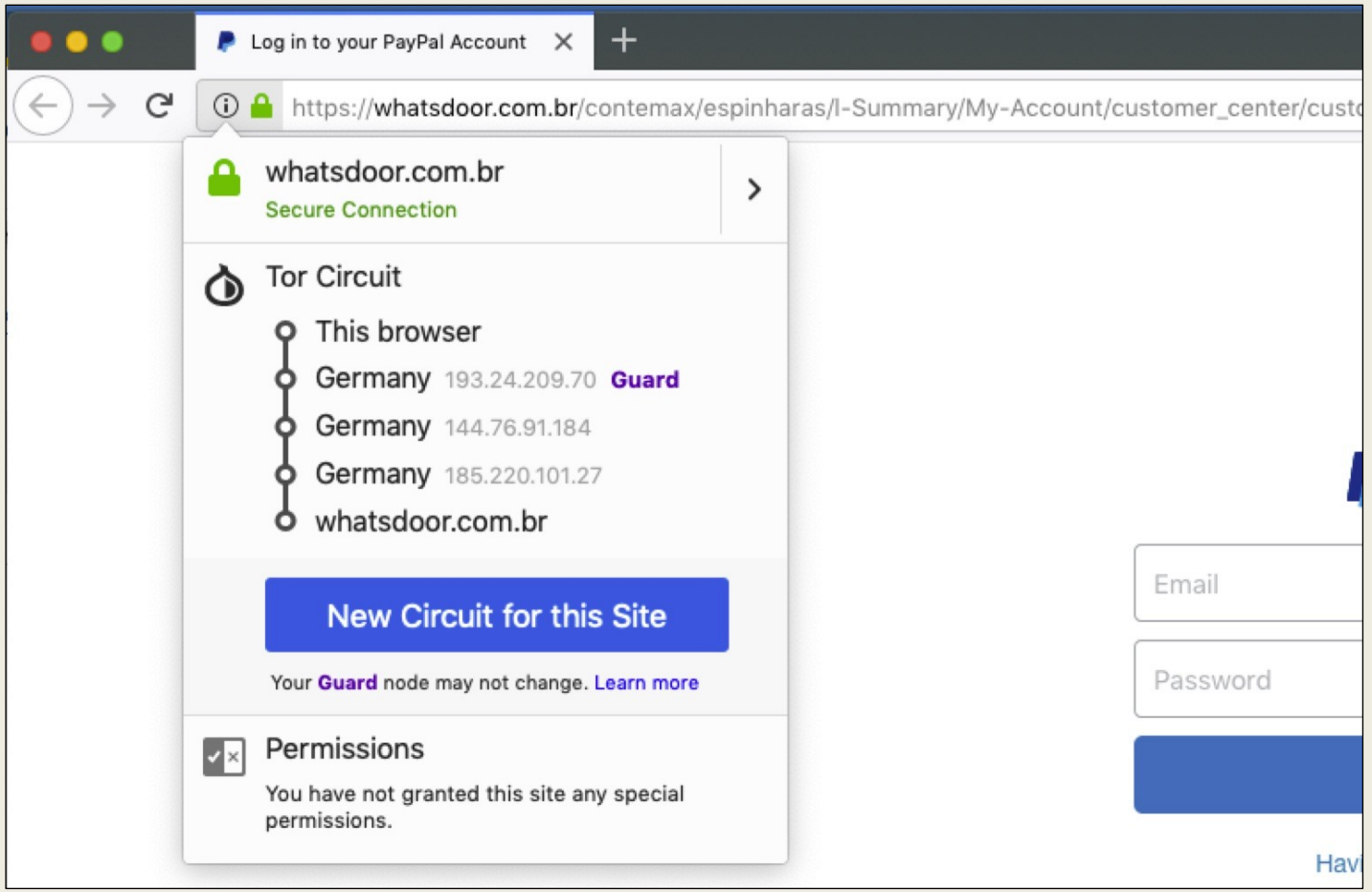
- No. HTTPS and HTTP are just the protocols.
- APWG: "In Q1 2020, a new high of 74 percent of sites used for phishing were protected with SSL"

- Source: https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf

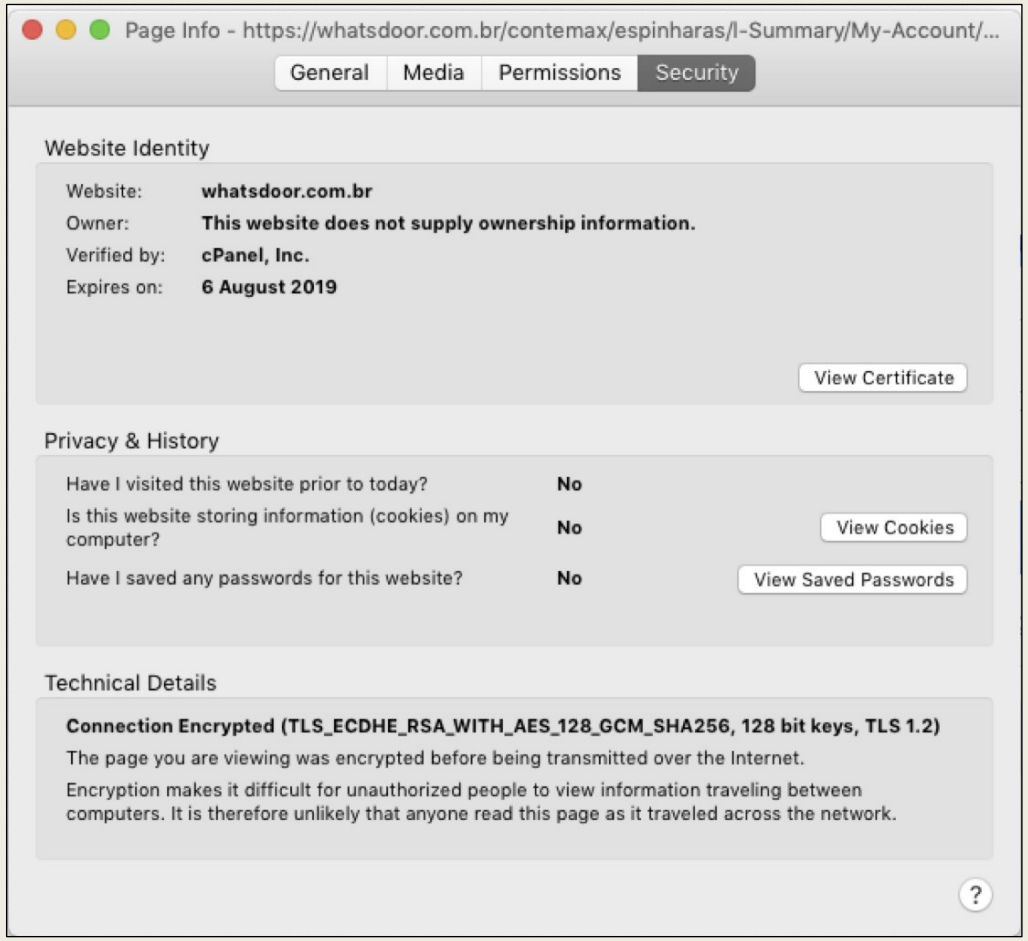
Phishing and HTTPS



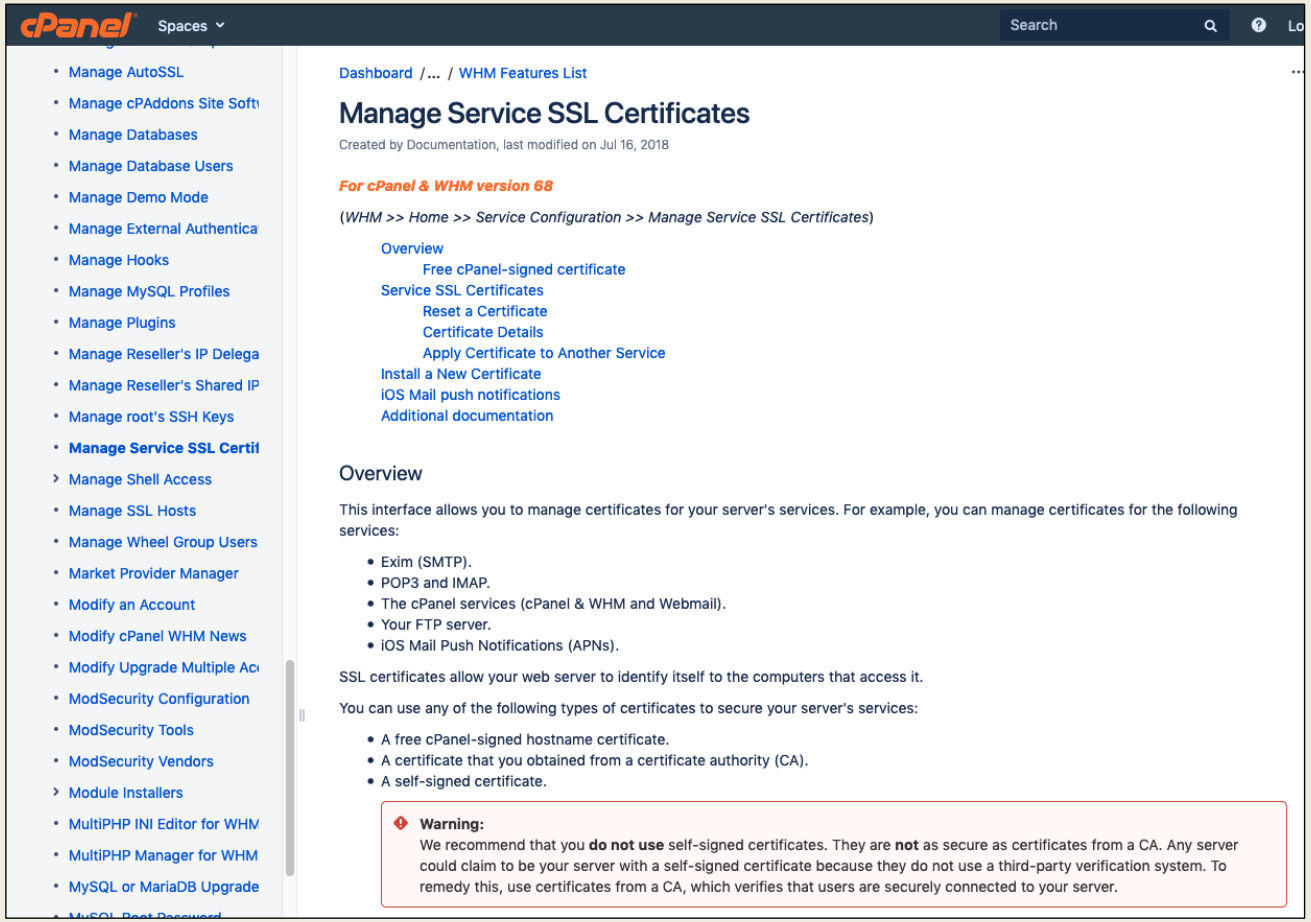
Phishing and HTTPS



Phishing and HTTPS

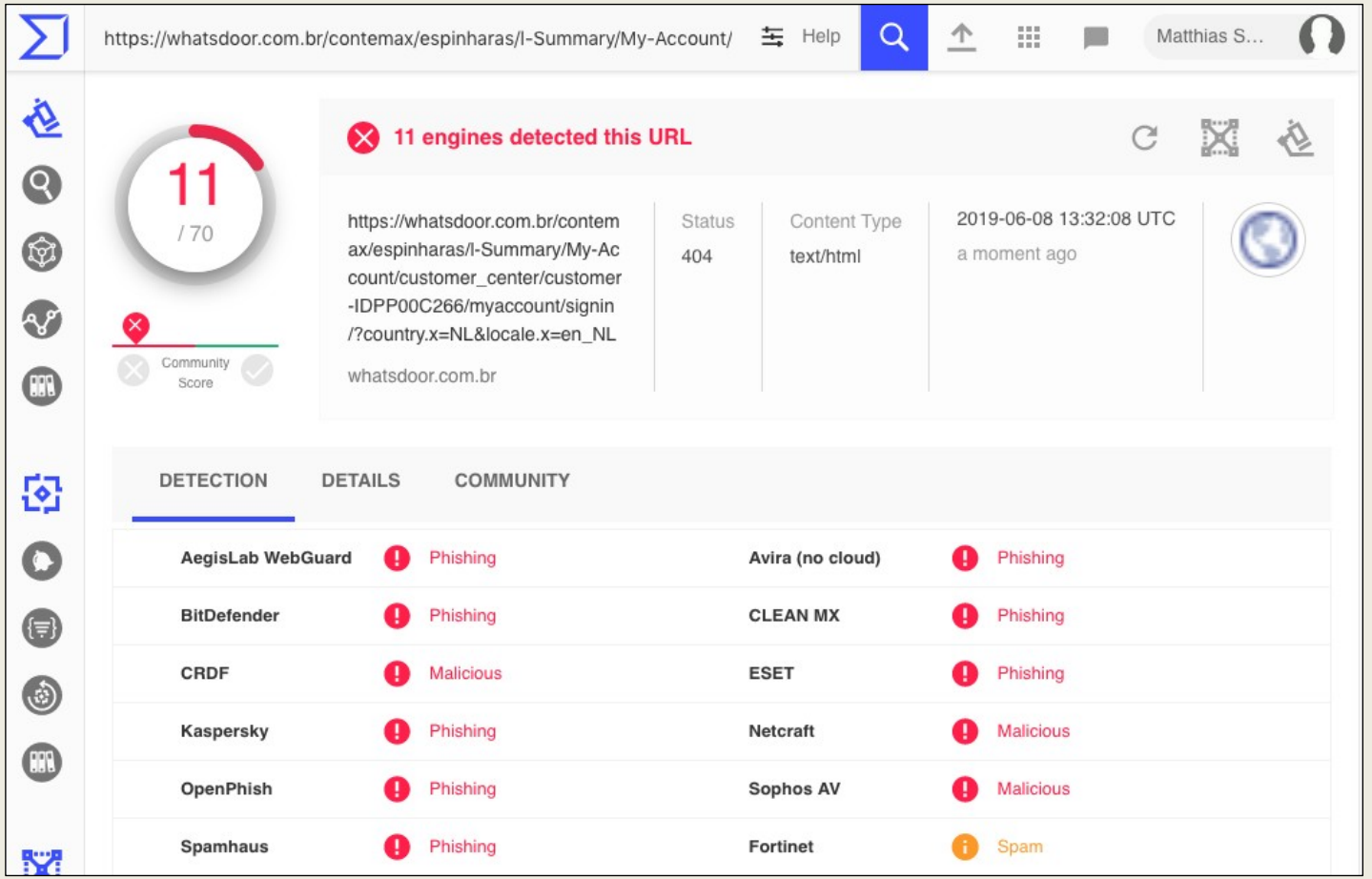


SSL Certificates



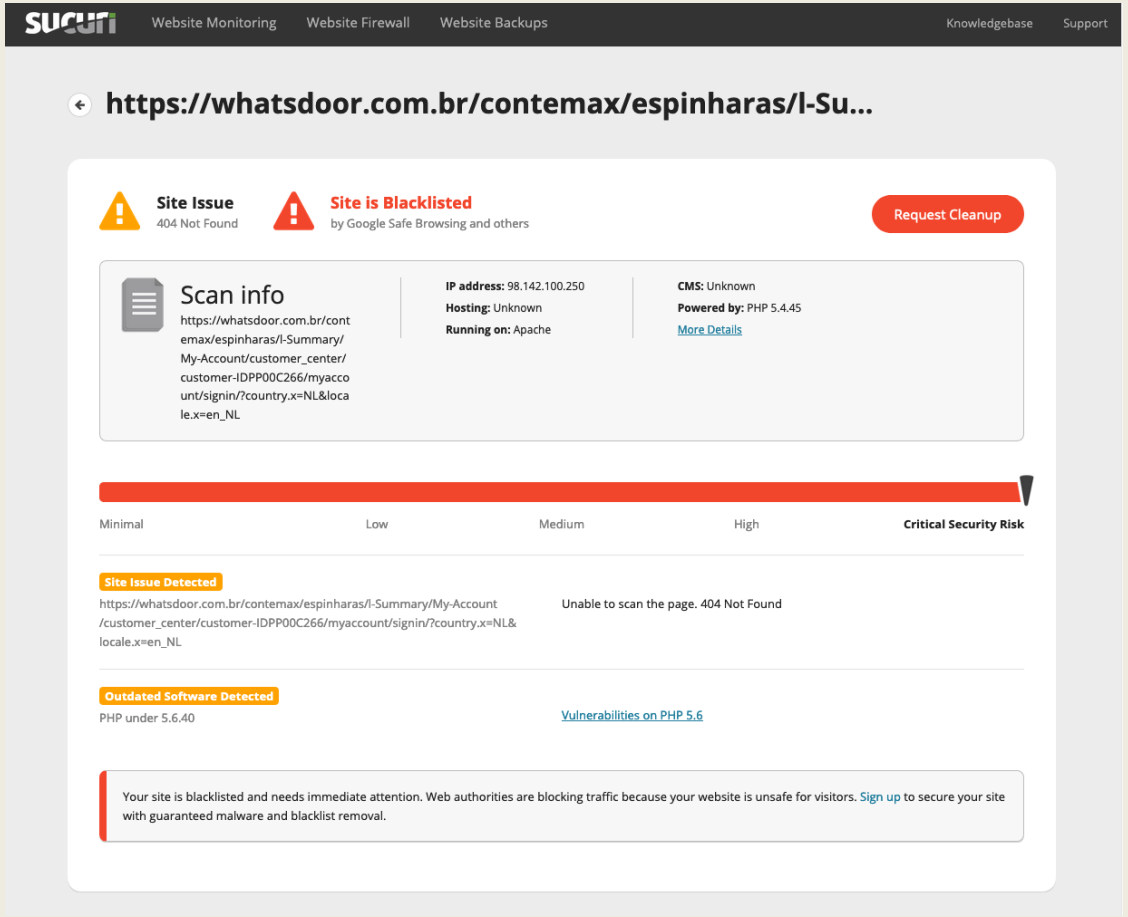
Phishing Checks

https://virustotal.com



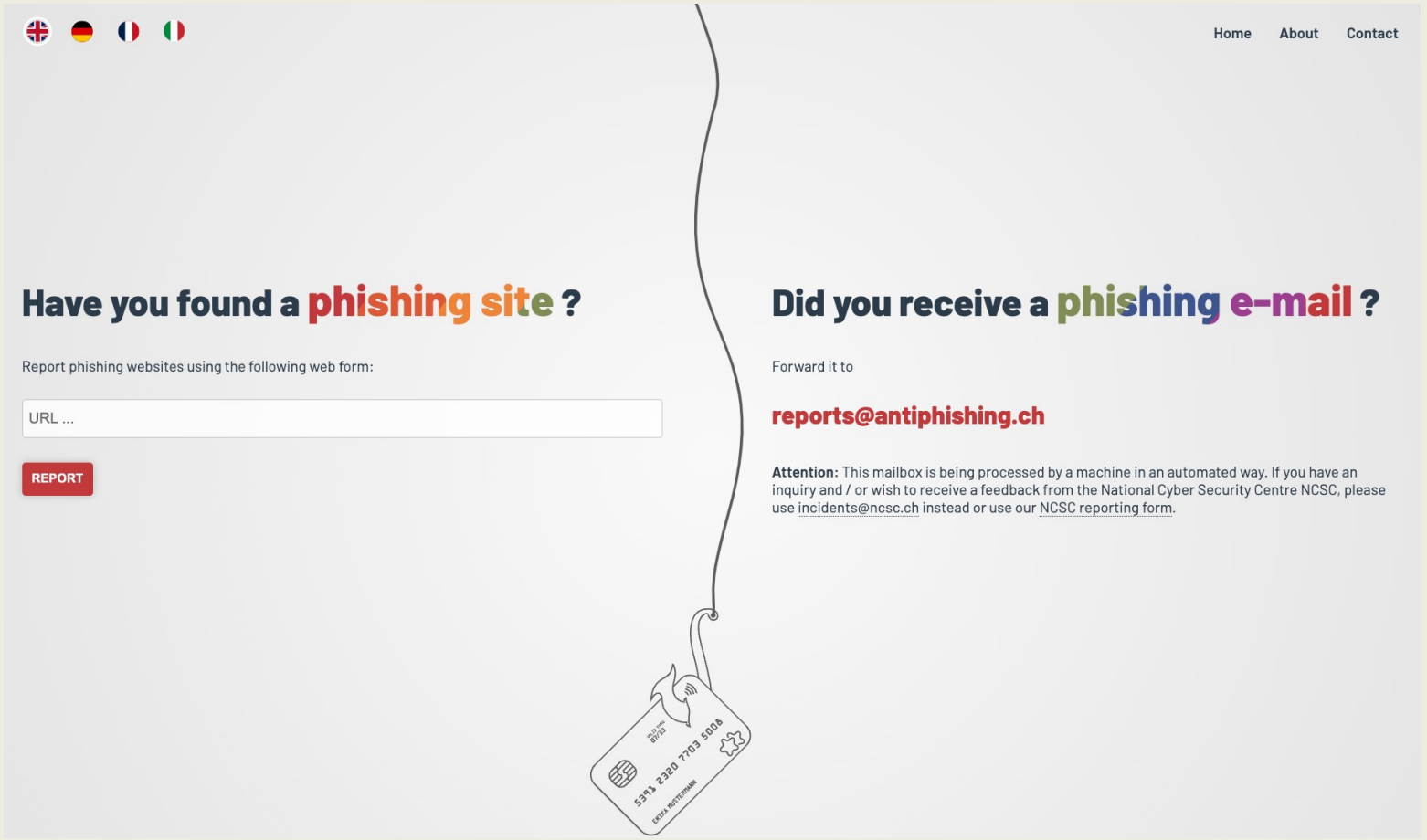
Phishing Checks

https://sitecheck.sucuri.net

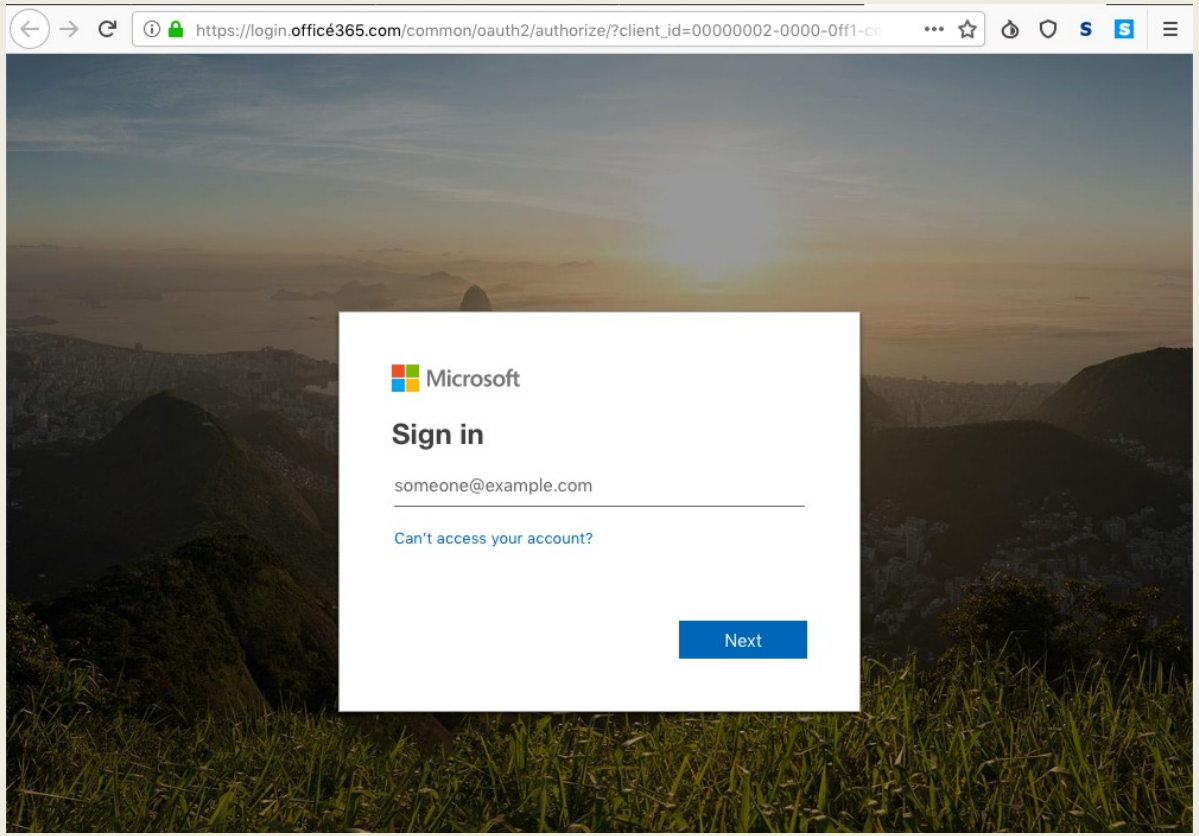


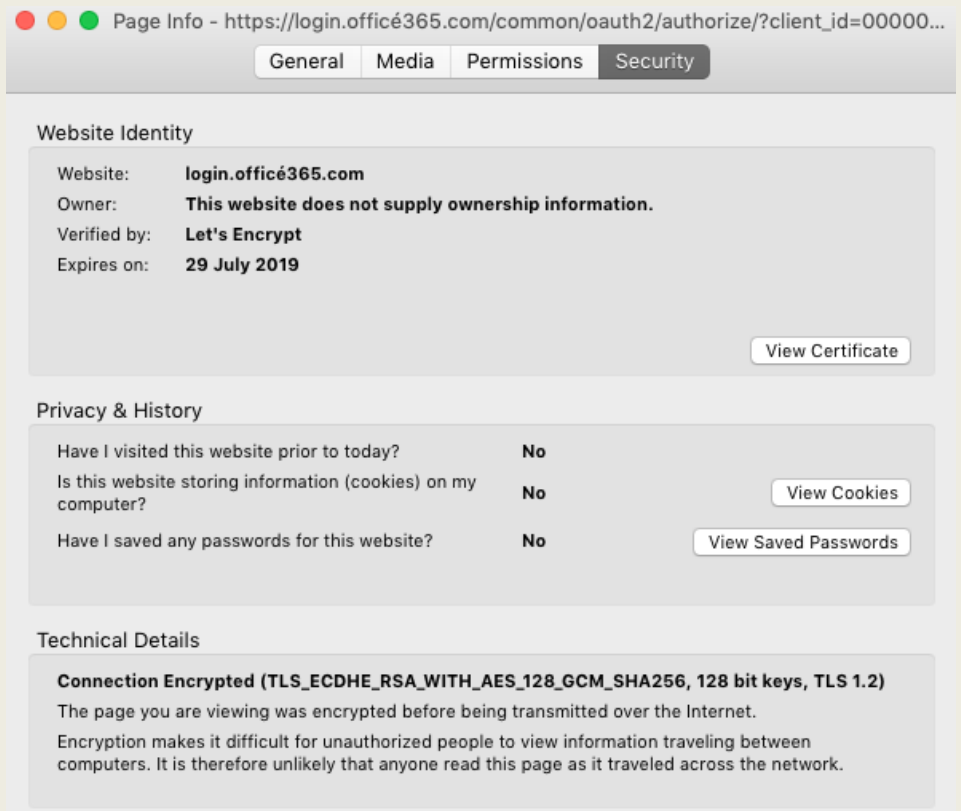
Report Phishing

http://antiphishing.ch/



Advanced Phishing





Advanced Phishing

- https://login.xn--offic365-f1a.com

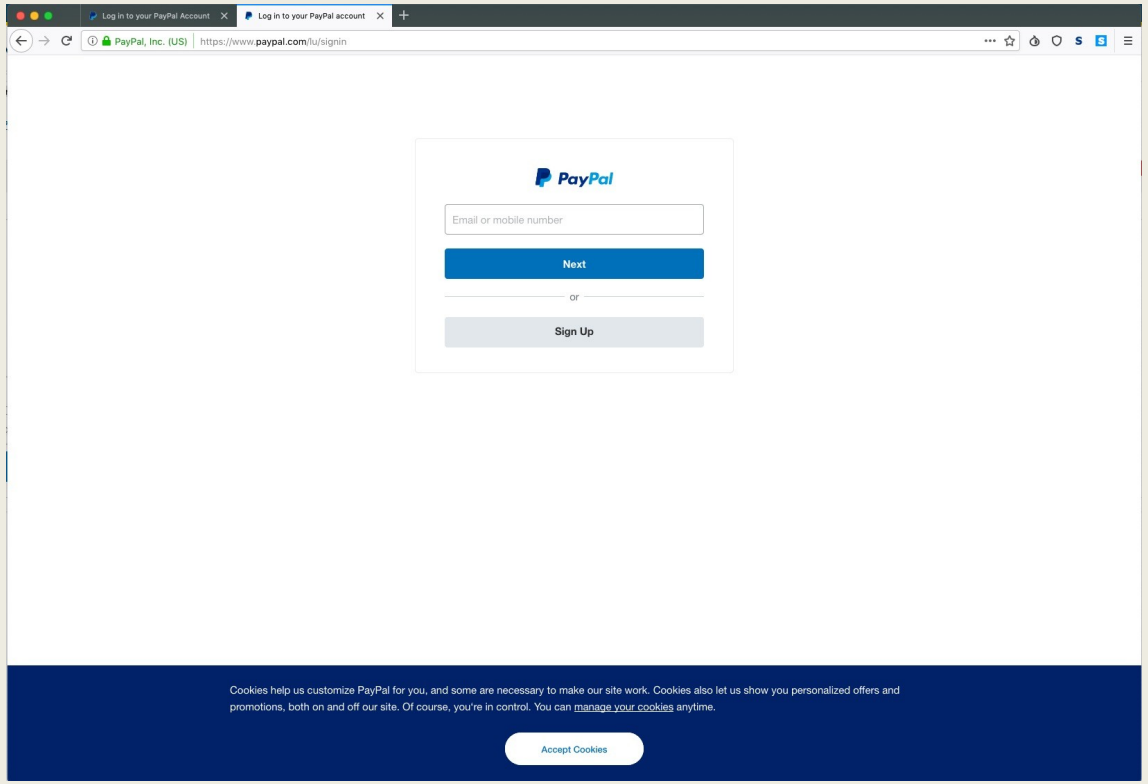
- Punycode is a way to **represent International Domain Names (IDNs) with the limited character set (A-Z, 0-9)** supported by the domain name system.
- For example, "münich" would be encoded as "mnich-kva".
- An IDN takes the punycode encoding, and adds a "xn--" in front of it.
- "münich.com" would become "xn--mnich-kva.com".
- Punycode rendering depends on the browser. Firefox will display it as a look-alike domain

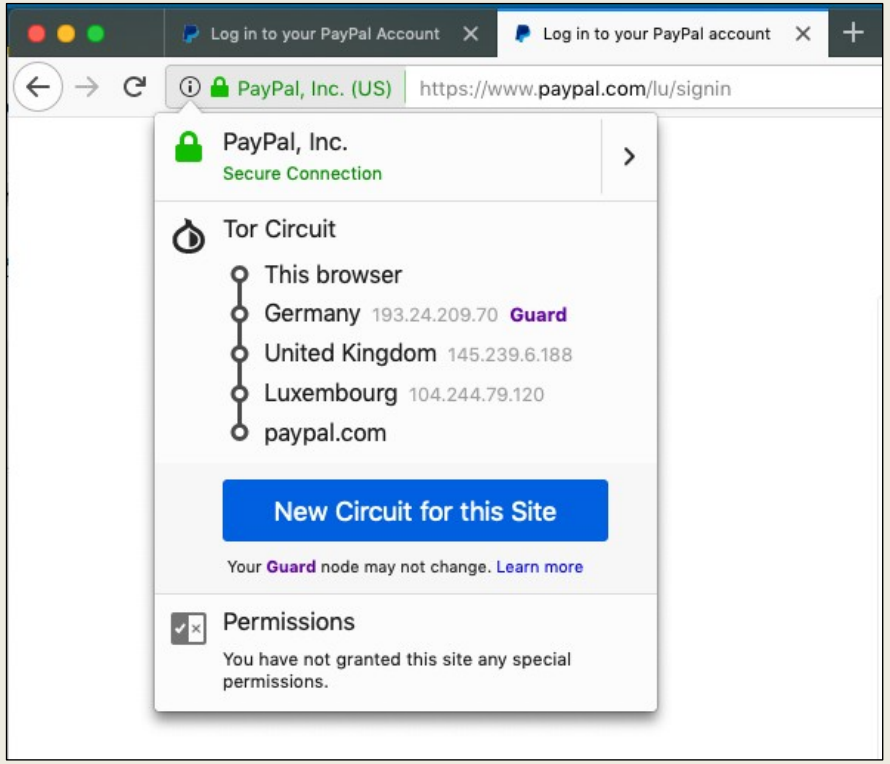
Phishing Task

- Check the behavior of a **secure and legitimate domain**, e.g. google.ch via
  - https://virustotal.com and https://sitecheck.sucuri.net

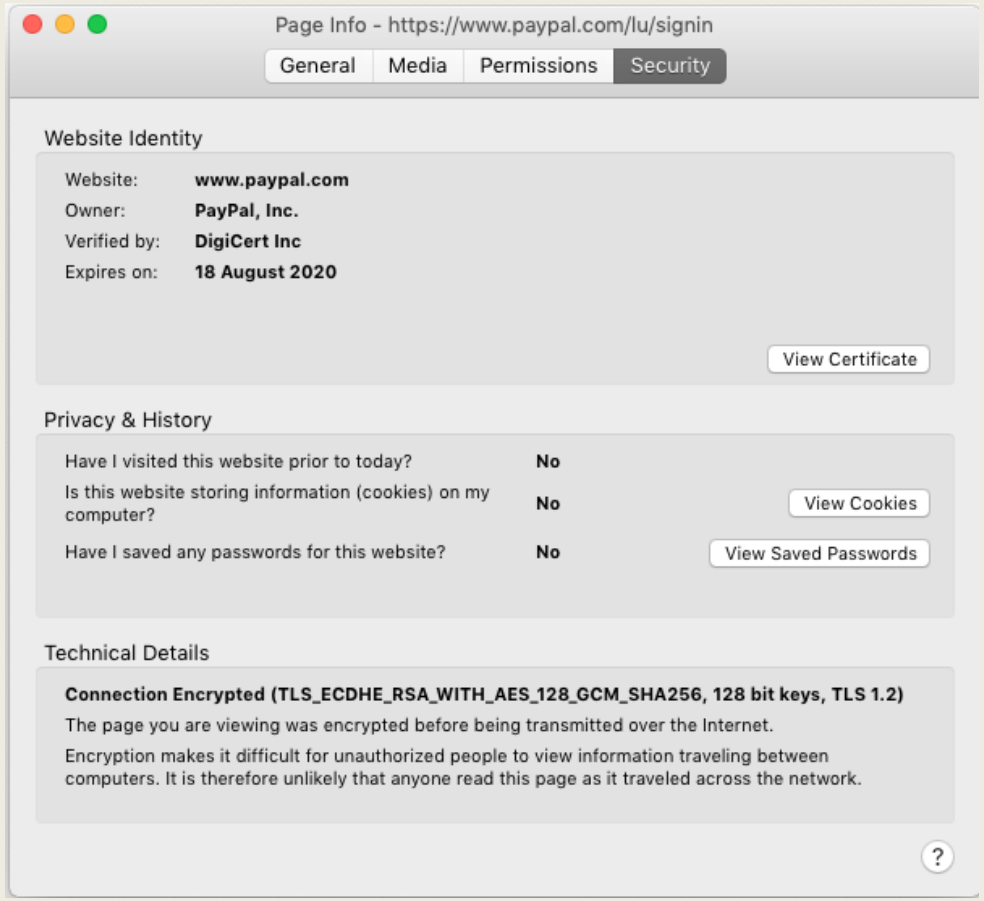
- Check the behavior of a **phishing domain** via
  - https://virustotal.com and https://sitecheck.sucuri.net

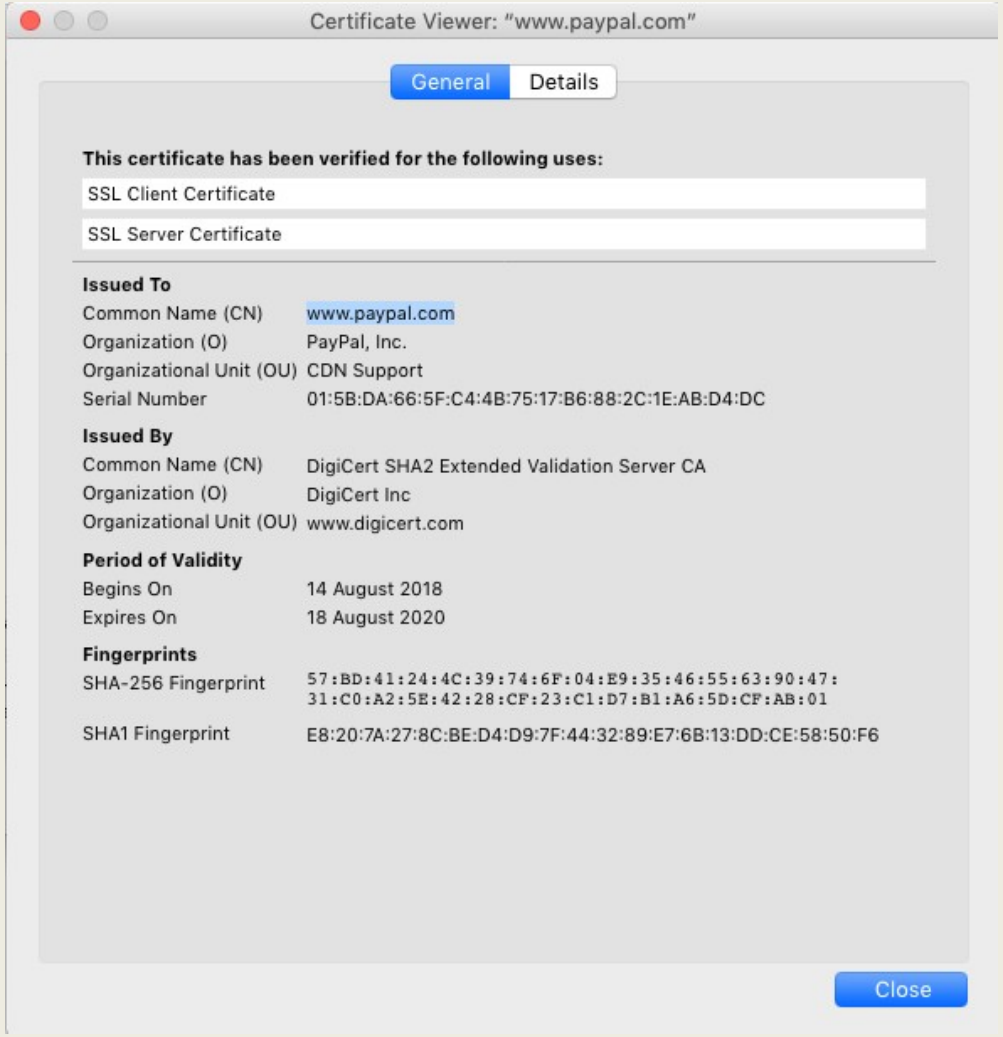
TLS Certificates



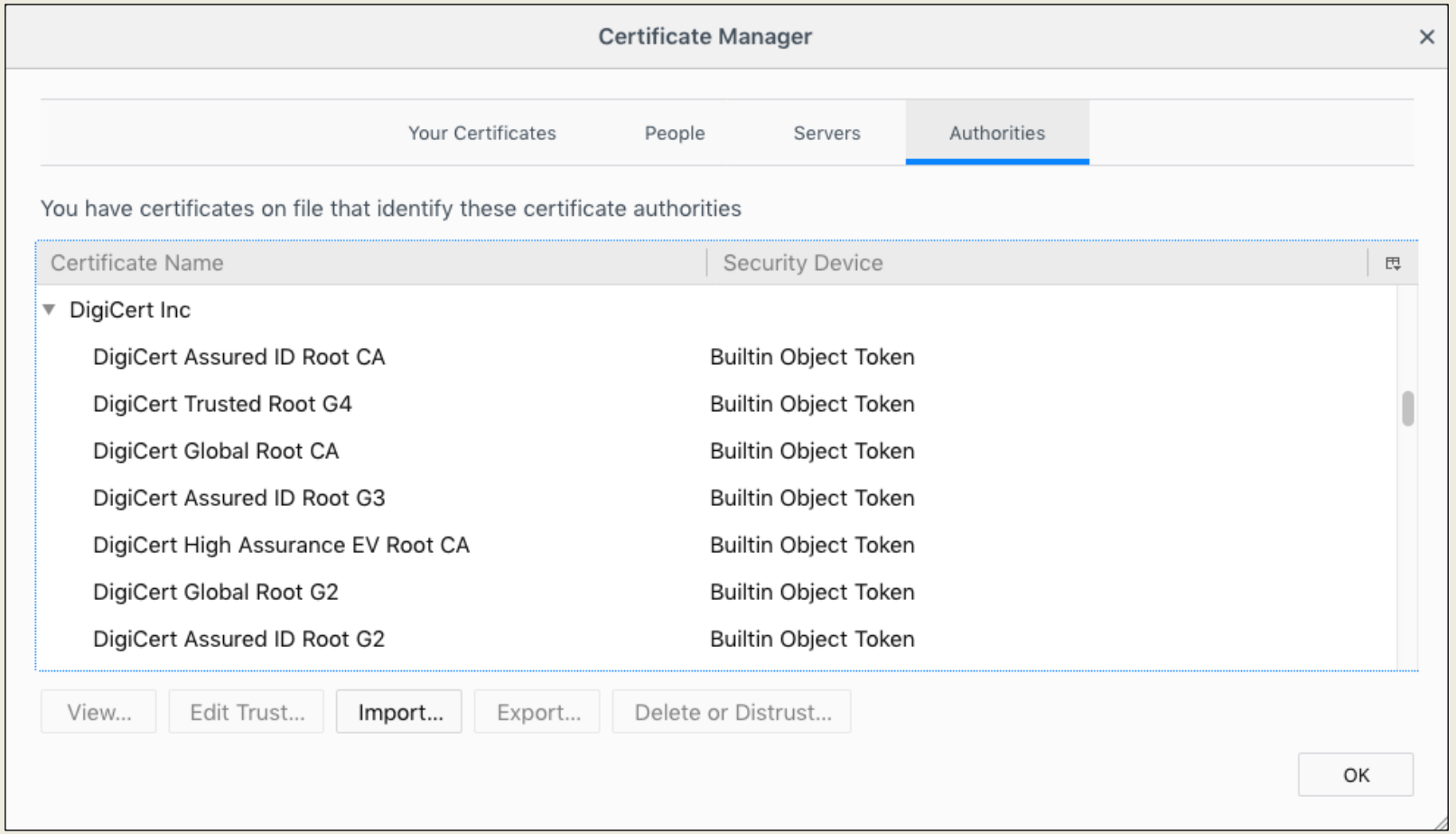


TLS Certificates

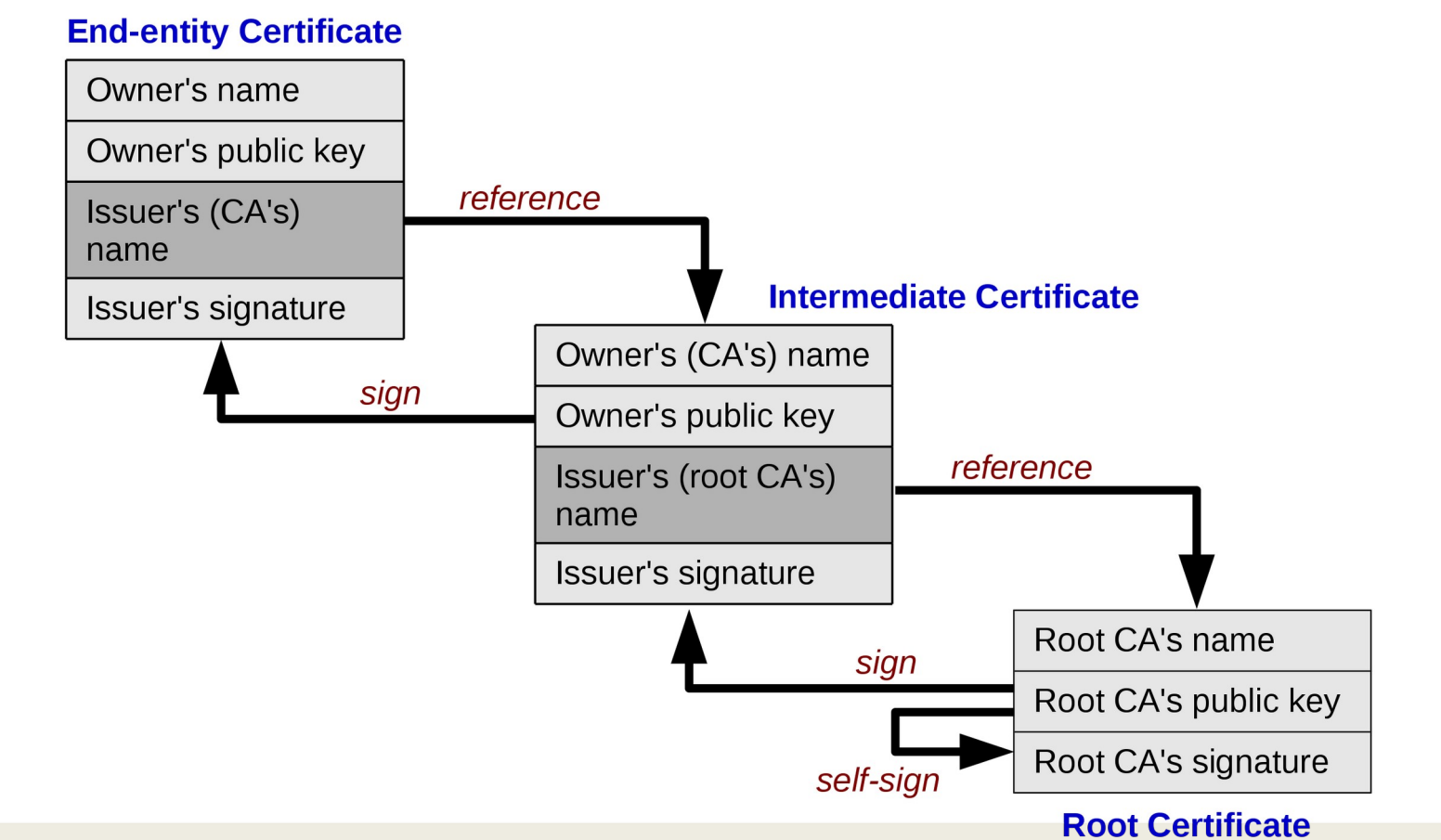




TLS Certificates



TLS Certificates



TLS Certificates

- Deprecation of SSL: SSL is insecure and no longer recommended; **always use TLS 1.2 or higher (preferably 1.3) for new implementations**.
- Common Misnomer: Note that "SSL" is often used **colloquially to mean TLS**, especially in marketing (e.g., "SSL certificates" are really TLS certificates).
- Versions and Security: **TLS versions, e.g., TLS 1.0 and 1.1 are also deprecated (as of 2021), leaving 1.2 and 1.3 as secure options**. Vulnerabilities like those in SSL 3.0 that led to its phase-out.
- Practical Implications: **Servers should disable SSL/TLS weak versions via configuration (e.g., in Apache or Nginx)**, and users should check for HTTPS with strong TLS in browsers (look for the padlock icon and verify via tools like SSL Labs).
- Future Outlook: **TLS 1.3 (2018) is the gold standard now**, with ongoing work on post-quantum cryptography for future threats.

Malware

- Malware, short for **malicious software**, refers to any program or code intentionally designed to damage, disrupt, or gain unauthorised access to computer systems, networks, or data. It is created by cybercriminals to infect devices, steal information, or cause harm.
- Key Characteristics:
  - Intentionally harmful
  - Can spread via email attachments, infected websites, software downloads, or ..
  - Affects computers, smartphones, servers, and other devices
- Examples of Malware:
  - Viruses: Attach to legitimate files and spread when the file is executed, e.g., the ILOVEYOU virus via email in 2000.
  - Ransomware: Encrypts files and demands payment for decryption, e.g., WannaCry which affected hundreds of thousands of computers in 2017.

Malware

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#/media/File:Wana_Decrypt0r_screenshot.png

History of Malware

- The concept of malware dates back to the early days of computing, evolving from experimental programs to sophisticated cyber threats. Below are some milestones
- 1971: Creeper Virus – The first experimental self-replicating program, created by Bob Thomas, which displayed the message "I'm the creeper, catch me if you can!" on ARPANET computers.
- 1982: Elk Cloner – The first virus to spread in the wild, targeting Apple II computers via floppy disks, written by a teenager as a prank.
- ...
- 2010: Stuxnet – A highly advanced worm targeting industrial control systems, believed to be developed by nation-states to sabotage Iran's nuclear program.
- 2010s–Present: Rise of ransomware (e.g., CryptoLocker in 2013) and fileless malware, with threats becoming more targeted and monetised through cryptocurrencies.
- **Malware has shifted from pranks and experiments in the 1970s–1980s to profit-driven and state-sponsored attacks in modern times.**

History of Malware

https://en.wikipedia.org/wiki/Stuxnet#/media/File:Natanz_nuclear.jpg

Types and Subgroups of Malware

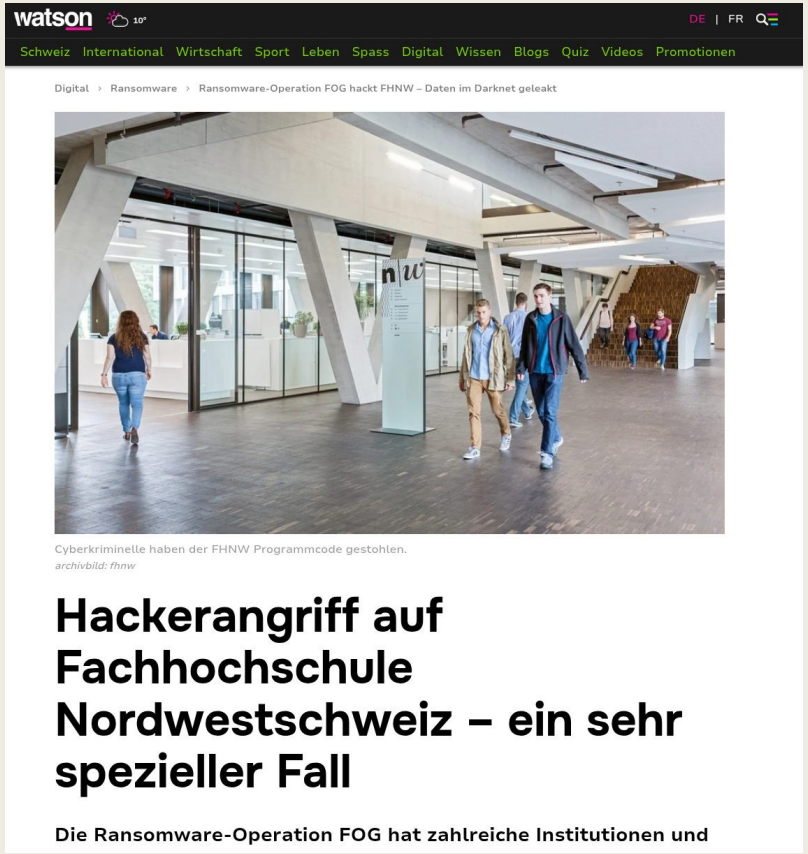
- Malware can be categorised into various types based on behaviour, method of infection, and purpose. Many types have subgroups or hybrids. Below are common types with examples:
- **Viruses**: Self-replicating code that attaches to files. Subgroups: Macro viruses (e.g., in Microsoft Office documents), boot sector viruses.
- **Worms**: Spread independently across networks. Example: Conficker worm, which exploited Windows vulnerabilities.
- **Trojans**: Masquerade as benign software. Subgroups: Remote Access Trojans (RATs) for backdoor access, banking Trojans for stealing financial data.
- **Ransomware**: Encrypts data and demands ransom. Subgroups: Crypto-ransomware (encrypts files), locker ransomware (locks device access). Examples: Locky, Ryuk.

Types and Subgroups of Malware

- **Spyware**: Secretly monitors user activity. Subgroups: Keyloggers (record keystrokes), screen scrapers. Example: Pegasus spyware used for surveillance.
- **Adware**: Displays unwanted ads. Often bundled with free software; can include tracking components.
- **Rootkits**: Hide malware presence by altering system functions. Subgroups: Kernel-mode rootkits (deep system access), user-mode rootkits.
- **Fileless Malware**: Operates in memory without files on disk, making detection harder. Often uses legitimate tools like PowerShell.
- **Botnets**: Networks of infected devices controlled remotely. Used for DDoS attacks or spam. Example: Mirai botnet targeting IoT devices.

- Other types include keyloggers, wiper malware (destroys data), and crypto-jackers (mines cryptocurrency).

Ransomware attacks against Universities



watson 10° DE | FR

Schweiz International Wirtschaft Sport Leben Spass Digital Wissen Blogs Quiz Videos Promotionen

Digital › Ransomware › Ransomware-Operation FOG hackt FHNW – Daten im Darknet geleakt

Cyberkriminelle haben der FHNW Programmcode gestohlen.
archivbild: fhnw

Hackerangriff auf Fachhochschule Nordwestschweiz – ein sehr spezieller Fall

Die Ransomware-Operation FOG hat zahlreiche Institutionen und

- https://www.watson.ch/digital/ransomware/408205938-ransomware-operation-fog-hackt-fhnw-daten-im-darknet-geleakt

Ransomware attacks against Universities

Schon wieder Cyberangriff auf Hochschule in Neuenburg

Von Keystone-sda/paz, 4. Juli 2022 um 17:38

SECURITY CYBERANGRIFF FACHHOCHSCHULE NEUENBURG HOCHSCHULE RANSOMWARE SCHWEIZ

Nach der Universität hat es diesmal die Fachhochschule Neuenburg getroffen. Alle Server wurden heruntergefahren.

Nach der Universität Neuenburg im Februar ist nun auch die Fachhochschule Haute Ecole Arc in Neuenburg Opfer eines Hackerangriffs geworden. Die Hochschule teilte mit, dass sie in Kürze den Zugriff auf alle ihre Server abschalten und ihre E-Mails blockieren werde.

- https://www.inside-it.ch/schon-wieder-cyberangriff-auf-hochschule-in-neuenburg-20220704

What is Ransomware? A Short History

- **Definition**
  Ransomware is a type of malware that encrypts a victim's files or locks their device, demanding payment (usually in cryptocurrency) for decryption or access. It holds data hostage, threatening permanent loss or exposure if unpaid.
- **Key Historical Milestones**:
- 1989: First known ransomware, the AIDS Trojan (PC Cyborg), distributed via floppy disks, demanding $189 for decryption.
- 2005-2010: Early forms emerge, like GPCode, using weak encryption and targeting individuals.
- 2013: CryptoLocker popularizes strong encryption and Bitcoin payments, marking the modern era.
- 2017: WannaCry global outbreak affects 200,000+ systems in 150 countries, exploiting Windows vulnerabilities.
- Evolution: From simple locker malware to sophisticated crypto-ransomware, driven by anonymous payments and exploit kits.

Double Extortion Attacks and Key Ransomware Facts

- Double Extortion is an advanced ransomware tactic where attackers **not only encrypt data but also steal (exfiltrate) it**, threatening to leak or sell it publicly if ransom isn't paid. This doubles pressure on victims, bypassing backups as a recovery option.
- Emerged around **2019-2020** as an **evolution from traditional encryption-only attacks**. Pioneered by the Maze group, it built on earlier ransomware by adding data theft to increase leverage and payouts. **By 2025, it's the dominant strategy**, with multi-extortion (e.g., adding DDoS or harassment) on the rise.
- Ransomware as a Service (RaaS): Criminal groups rent out ransomware tools to affiliates, lowering barriers for attacks.
- Impacts: Targets critical sectors like healthcare and infrastructure; e.g., delays surgeries or disrupts services. Average ransom demands exceed $1 million, but paying doesn't guarantee data recovery.
- Trends: Over 60% of attacks now involve data exfiltration; attackers use dark web sites to "name and shame" non-payers.
- Prevention Tip: Regular backups, multi-factor authentication, and employee training are essential defenses.

Howto handle suspicious files

- What Are Suspicious Files?
- Files that may contain malware, such as **attachments in unusual or unsolicited emails** (e.g., from unknown senders or with odd subject lines).
- **Downloads from untrusted websites**, including pirated software or "cracks" for applications.
- Files with **unusual or double extensions** (e.g., invoice.pdf.exe or photo.jpg.scr).
- **Unexpected downloads prompted by pop-ups or ads on websites**.
- **Files** received via social media, messaging apps, or file-sharing services **from unfamiliar contacts**.
- **Documents with enabled macros** (e.g., .docm or .xlsm) from unknown sources.
- Torrents or files from peer-to-peer networks that promise free premium content.

Howto handle suspicious files

- Key Steps to Follow
- **Do not open or execute**: Avoid running any suspicious files immediately. This includes executable files (.exe), scripts, or unknown attachments.
- **Scan with antivirus software**: Use a reputable antivirus tool to check the file before opening. (e.g. https://virustotal.com)
- **Delete if in doubt**: If the file seems risky and is not essential, delete it permanently.
- **Report if necessary**: Inform your IT team or email provider if it's from a work or suspicious source.
- **Cracks** for paid applications could also contain malware...
- **Always prioritise safety: When in doubt, throw it out!**

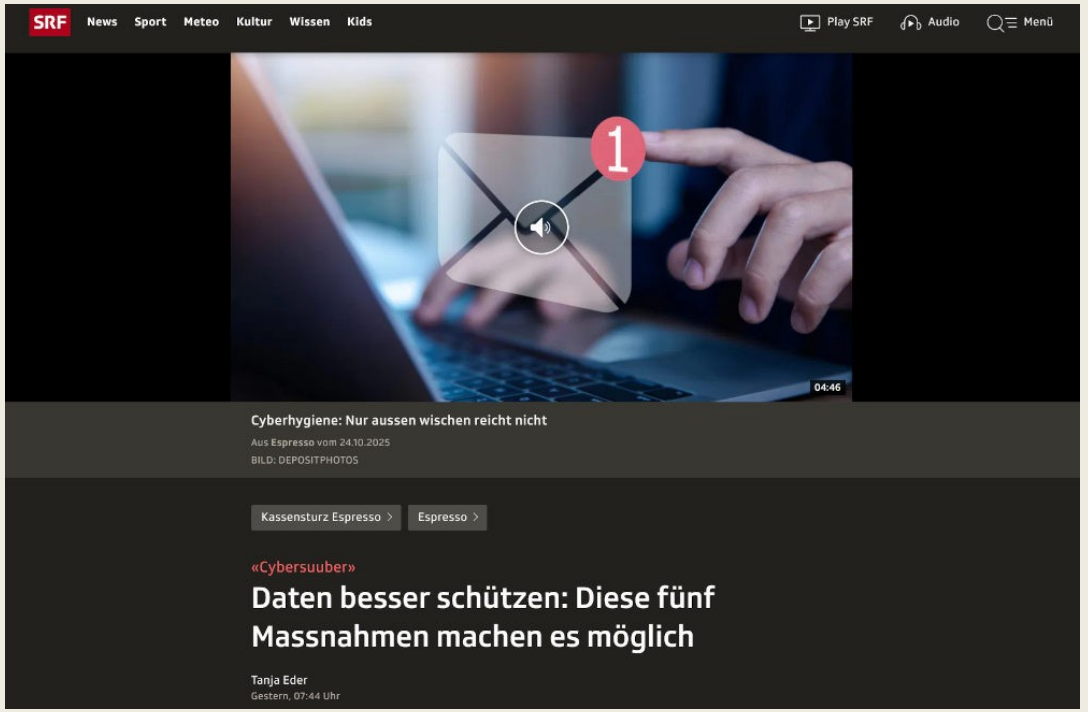
04 – Basic Security

- Vulnerabilities and CVE

- Patching and Workarounds

- Security Standards

Introduction



SRF, srf.ch, 25.10.2025

https://www.srf.ch/sendungen/kassensturz-espresso/espresso/cybersuuber-daten-besser-schuetzen-diese-fuenf-massnahmen-machen-es-moeglich

Vulnerabilities

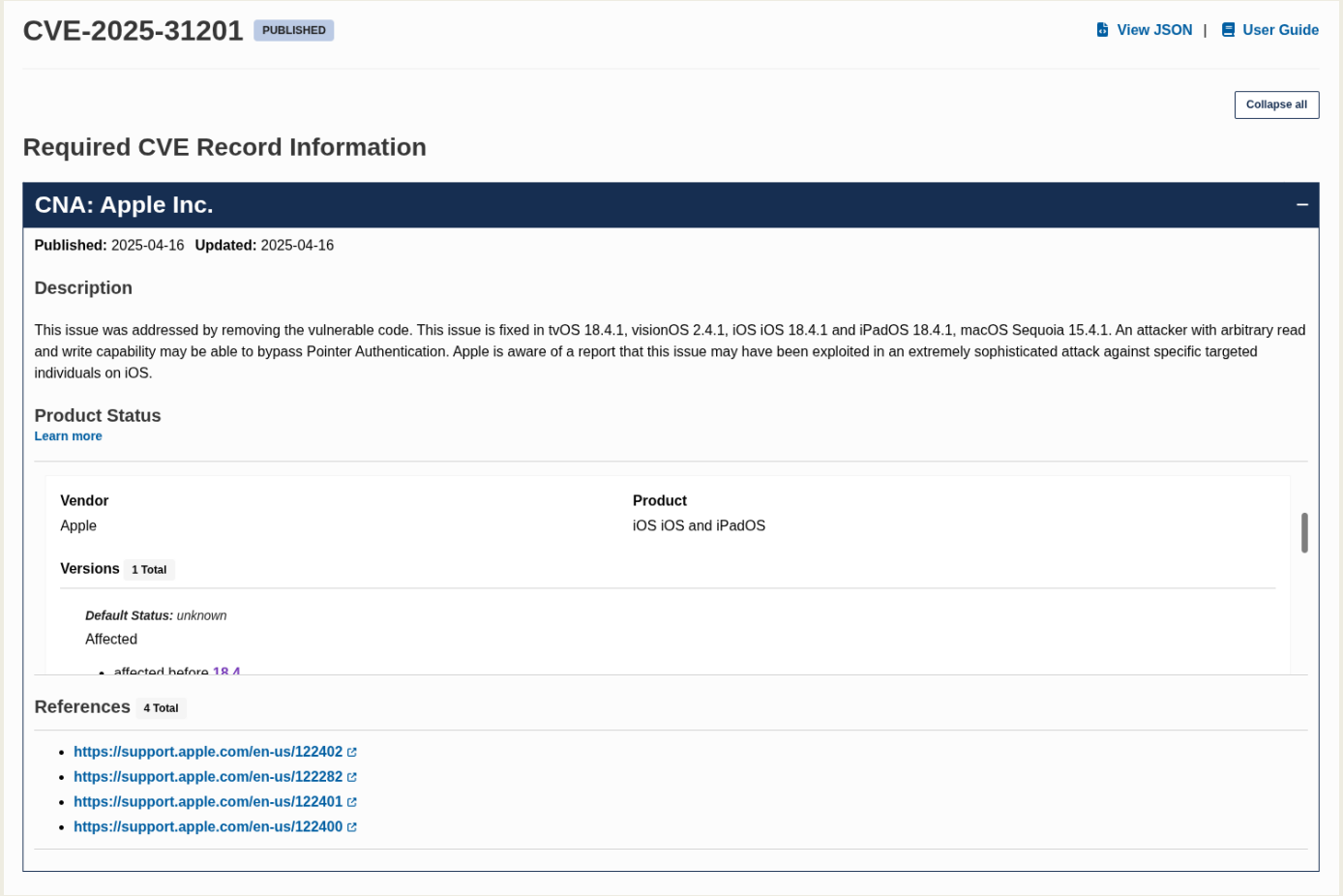
- «***A security flaw, glitch, or weakness found in software code that could be exploited by an attacker (threat source).***»
  Source: https://csrc.nist.gov/glossary/term/vulnerability

- Why are Vulnerabilities Inevitable?
  - Complexity of modern software leads to errors
  - Human factors: Programming mistakes, time pressure, inadequate testing
  - New threats evolve constantly

- **Measures:**
  - Regular updates and patches
  - Security audits (e.g., penetration tests)
  - Development of secure coding practices

- **Conclusion**: Vulnerabilities are an unavoidable part of software, but risks can be minimized through proactive measures.

Vulnerabilities



https://www.cve.org/CVERecord?id=CVE-2025-31201

Common Vulnerabilities and Exposure (CVE)

- CVE is a **dictionary** of common names for **publicly known cybersecurity vulnerabilities**. CVE's common identifiers, called CVE Identifiers, make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools.

- Files **CVE** is:
  - **One name for one vulnerability** or exposure. Also
  - One **standardized description** for each vulnerability or exposure
  - A **dictionary** rather than a database
  - The way for disparate databases and tools to **"speak" the same language**
  - The way to **interoperability and better security coverage**
  - A **basis for evaluation** among tools and databases. Free for public download and use
  - **Industry-endorsed via the CVE Numbering Authorities (CNAs)**, CVE Editorial Board, and CVE-Compatible Products

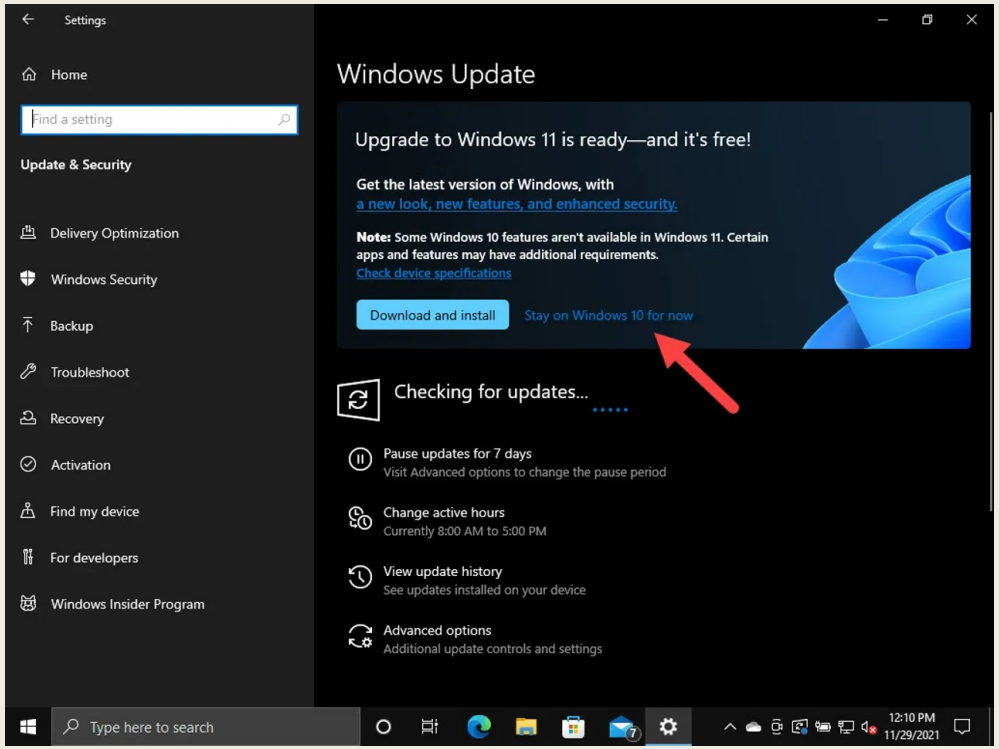
- Dictionary available at https://www.cve.org/

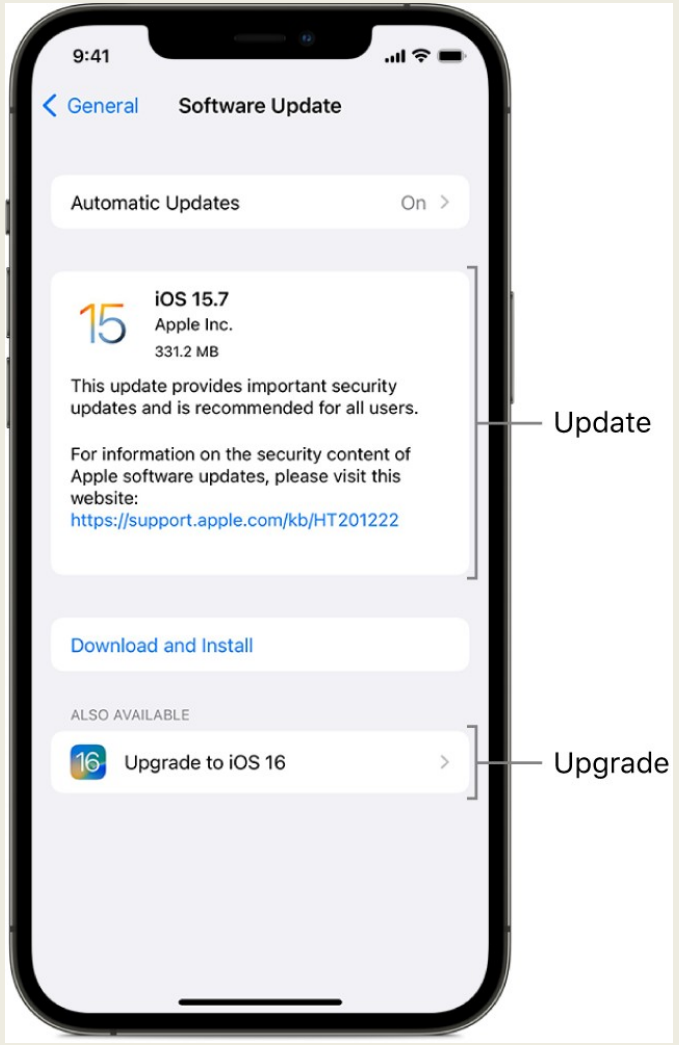
  Source: https://cve.mitre.org/docs/cve-intro-handout.pdf

CVE Task

- Visit the CVE dictionary website
- How many CVE records (aka vulnerabilites) are listed in total in the CVE directory?
- Search for all publicly known vulnerabilities for the software **SugarCRM**.
  - How many records do you find?
  - From which year is the first CVE entry?

Patching and Workarounds





Patching and Workarounds

- A **patch is an additional piece of software** that can be installed to **fix** the affected software and close the vulnerability.
- The devlopment of a patch **can take time: Hours to weeks**
- If there is no patch available, in some cases the software vendor will describe a **«workaround» to disable the vulnerable part of the software**.
- **Patch Tuesday**: 2nd Tuesday of the month. Time when many big software vendors regularly release software patches for their software products.
- Important: Subscribe to your software vendors Security advisories. Then you will be informed about vulnerabilities.

Patching and Workarounds Task

- Visit the **Debian security mailing advisories** (debian-security-announce):
- https://lists.debian.org/debian-security-announce/
- Locate the **Subscribe / Unsubscribe form**
- Which **date** has the latest posting on the debian-security-announce mailing list?

Security Standards

- Standards provide a proven framework for safeguarding sensitive data and systems against evolving threats, ensuring consistency and reliability across organisations.
- By adhering to these standards, businesses can minimise vulnerabilities, reduce the risk of costly breaches, and enhance their overall resilience to cyberattacks.
- Compliance with established standards also helps meet regulatory requirements, avoiding legal penalties and reputational damage.
- Ultimately, following security standards fosters trust among stakeholders and promotes a culture of proactive risk management.

Security Standards

- Some Standards
  - ICT minimum standard from the BACS / NCSC
  - NIST cybersecurity framework (National Institute of Standards and Technology)
  - BSI (Federal Office for Information Security)
  - ISO/IEC 27001 (International Organization for Standardization)
  - CIS (Center for Information Security)

ICT minimum standard

- Created by the BACS (Bundesamt für Cybersicherheit)
- «Individual businesses and organisations have a fundamental responsibility to protect themselves. However, **wherever the functioning of critical infrastructures is affected, the state has a responsibility to protect them (National Economic Supply Act)**. The ICT minimum standard is an expression of the state's responsibility to protect citizens, the economy, institutions and public administration.»
- «**All operators of critical infrastructures are advised to implement the respective ICT minimum standards**. Minimum standards in the electricity sector have been mandatory since 1 July 2024 and are expected to become binding for gas providers from 1 July 2025. **However, the standards also offer guidance to all other companies and organisations on how to improve their own ICT resilience.**
- https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/ikt-minimalstandards.html

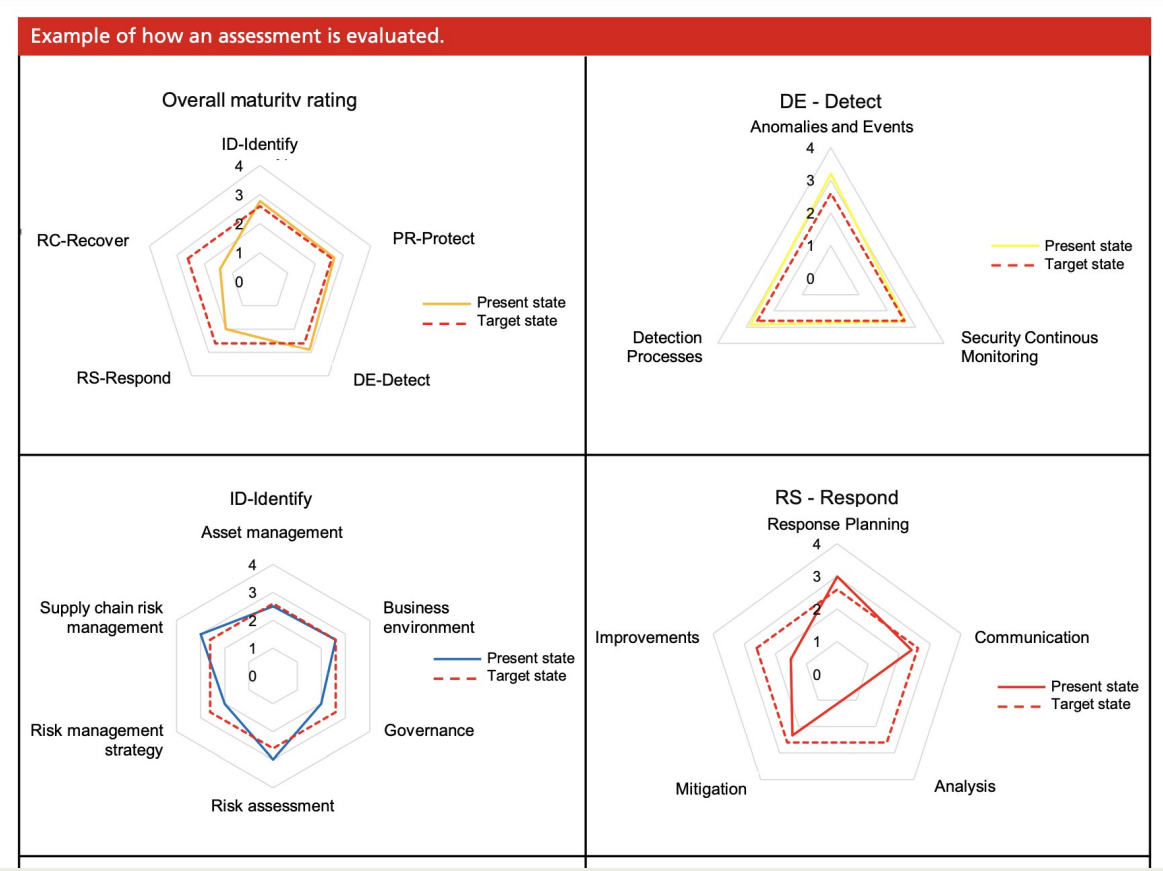
ICT minimum standard

- 3 Sections
  - **Introductions**
  - **Implementations**
  - **Assessment**

ICT minimum standard: Assesment tool

- Assessment: Define the «Target state» and compare it with the «Current state» of the ICT landscape
- Assesment tool:
- https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/infos-unternehmen/ikt-minimalstandards/IKT-Minimalstandard-Assessment-Tool-1-1-2023_Revision_5_E_D_F_I.xlsx.download.xlsx/IKT-Minimalstandard-Assessment-Tool-1-1-2023_Revision_5_E_D_F_I.xlsx

ICT minimum standard: Assesment tool



- https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/ikt-minimalstandards.html

ICT minimum standard: Task 1

- Download the current (2023) version of the ICT minimum standard
- In «Section 1 – Introduction» Read the subchapter «Vendor management» in the chapter «Elements of a defence-in-depth strategy»
- What procedure can help to minimise the risk regarding vendors?

ICT minimum standard: Task 2

- In «Section 2 – Implementation» Read the subchapter «Asset management» in the chapter «Identify»
- What are the 6 tasks regarding asset management if you want to fullfil the ICT minimum standard?

Basic Security: Take Aways

- Publicly known Security vulnerabilities are collected in CVE dictionaries
- Inform yourself about your vulnerabilities
- Regularly patch your systems
- Be ready for «Emergency» patches
- Don’t reinvent the wheel => Use existing standards as templates and orient yourself to these standards
- Use standards
- The ICT minimum standard is popular is Switzerland and a good starting point

05 – How to protect your assets?

- Introduction
- CIA Triad
- Methods to ensure
  - Confidentiality
  - Availability
  - Integrity
- Secure Authentication

What is Information Security (InfoSec)?

- Definition: The practice of **protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destructio**n.
- Core Principles (**CIA Triad**):
  - **Confidentiality**: Ensuring only authorizsd individuals can access sensitive data (e.g., encryption, access controls).
  - **Integrity**: Preventing improper alteration or destruction of information (e.g., checksums, digital signatures).
  - **Availability**: Guaranteeing reliable and timely access to data and systems (e.g., backups, redundancy).
- Scope: **Broad**, covers digital data, physical documents, human elements, and organisational policies.
- Why It Matters: Protects against risks like **data breaches, espionage, or natural disasters in any form of information handling**.

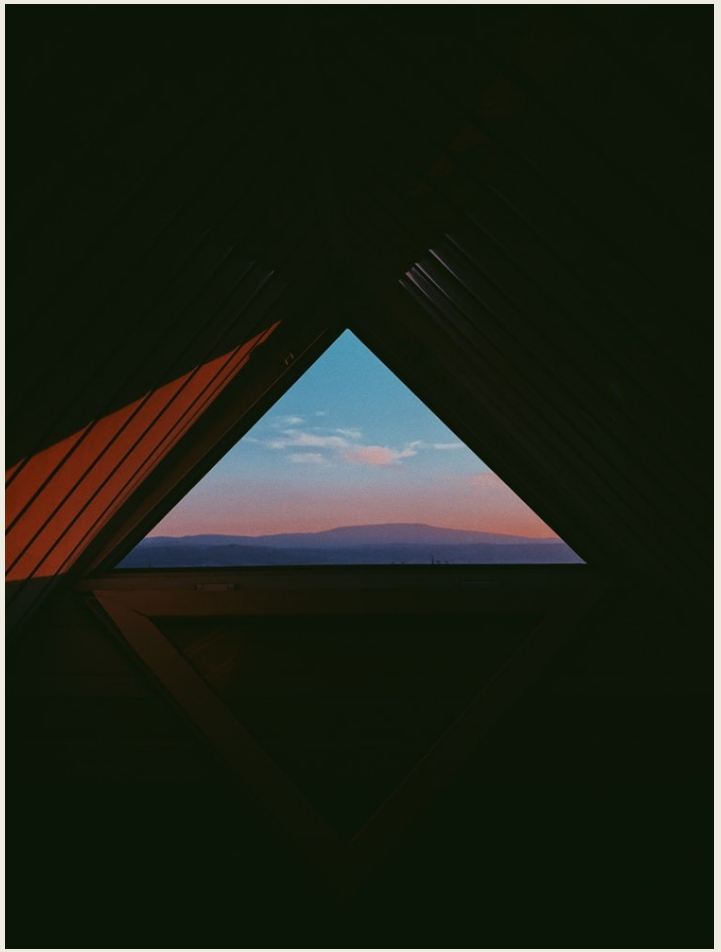
What is IT Security? (And How It Differs from InfoSec)

- Definition: A **subset of information security** focused on safeguarding information technology **systems**, including hardware, software, networks, and data stored digitally.
- Core Focus Areas:
  - Protecting against cyber threats like hacking, malware, phishing, and DDoS attacks.
  - Tools and Practices: Firewalls, antivirus software, intrusion detection systems, and secure coding.
  - Emphasis on digital infrastructure: Servers, cloud services, endpoints, and online communications.
- Differences from Information Security:
  - Scope: IT Security is narrower, dealing primarily with technology and cyber risks; InfoSec is holistic, including non-digital aspects like physical security (e.g., locked file cabinets) and human factors (e.g., employee training).
  - Overlap: IT Security supports InfoSec's goals but doesn't cover everything (e.g., InfoSec includes legal compliance and risk management beyond IT).
  - Example: A data leak via a hacked server is IT Security; losing a paper document is InfoSec but not purely IT.

The CIA triad

- The “CIA triad.” CIA stands for:
- **Confidentiality** through preventing access by unauthorized users
- **Integrity** from validating that your data is trustworthy and accurate.
- **Availability** by ensuring data is available when needed

- https://www.ibm.com/blogs/cloud-computing/2018/01/16/drive-compliance-cloud/



CIA triad example

CIA triad example

- **Scenario Description**: Imagine a patient in a general hospital (e.g., a city hospital) needs specialised treatment only available at a specialty hospital (e.g., an oncology center). The patient must be physically transferred, and all relevant data, such as medical history, lab results, X-rays, and treatment plans, **must be securely sent from the general to the specialty hospital**. This typically occurs via digital systems like secure networks or encrypted file transfers. The goal is seamless, secure transmission to continue treatment **without delays or risks**.
- **Key Context**: This process relies on the **CIA Triad (Confidentiality, Integrity, Availability**), the core principles of information security, to protect patient data and ensure optimal care.

Applying the CIA triad

- **Confidentiality**: Transmitted information must only be viewable by authorised personnel, such as doctors and medical staff in the involved hospitals. Unauthorised parties (e.g., hackers or external vendors) are blocked. Practices: **Data encryption during transfer** (e.g., HTTPS or VPN), **strict access controls** (e.g., two-factor authentication). **Breach risk: Privacy violation via data theft**.
- **Integrity**: Data must be transferred **completely and without alteration**, from technical errors or attacks. Practices: Digital signatures or hash checks for authenticity verification; recipient-side validation. **Risk: Altered lab values could lead to wrong treatments, endangering the patient's life**.
- **Availability**: Systems accessed by doctors and staff must be **available 24/7 without downtime**. Practices: **Redundant servers, backups, and contingency plans against failures** (e.g., power outages or DDoS attacks). **Risk: Delayed data access could prevent urgent procedures, potentially life-threatening**.
- Summary: This example illustrates how the CIA Triad ensures patient data is secure and usable, aligning with standards like HIPAA (US) or GDPR (EU) for effective healthcare.

Methods to ensure Confidentiality

- **Encryption Techniques**: Use strong encryption algorithms (e.g., AES-256) for data at rest (stored data) and in transit (data being transferred). This scrambles information, making it unreadable without the proper decryption key.
- **Authentication and Access Controls**: Implement user IDs, passwords, multi-factor authentication (MFA), and role-based access control (RBAC) to verify identities and restrict access to authorized personnel only. Follow the principle of least privilege, grant users only the access they need.
- **Secure Transmission Protocols**: Employ protocols like HTTPS, VPNs, or TLS to protect data during transfer, preventing interception by unauthorised parties (e.g., man-in-the-middle attacks).
- **Extreme Measures for High-Sensitivity Data**: For critical scenarios, use air-gapped computers (isolated from networks), disconnected storage devices (e.g., offline USB drives), or hard-copy-only formats (e.g., printed documents in secure vaults) to eliminate digital exposure risks.

Methods to ensure Integrity

- Core Concept: Maintaining the **consistency**, **accuracy**, and **trustworthiness** of data **over its entire life cycle, from creation to deletion**. This prevents degradation from errors or interference.
- Protection Against Unauthorised Changes: Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorised people, using defenses against internal/external threats.
  - **File Permissions and User Access Controls**: Set granular permissions (e.g., read/write) and ACLs/MAC to limit edits, reducing risks from users or breaches.
  - **Version Control Systems (VCS):** Use tools like Git or SVN to track revisions, log changes, and enable recovery from alterations.
- Detect Changes: Implement tools to identify alterations, enabling quick response and authenticity verification.
  - **Cryptographic Checksums**: Apply hashes like SHA-512; mismatches detect tampering in transfers or storage.

Methods to ensure Integrity

- HMAC: Hash-based message authentication code
  - Is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key
  - ~~MD5~~, SHA-256, SHA-3, ...

```
macbook:~ seitz$ echo -n "Hi all" | shasum -a 256
e6cf54f1c0d4ec54e879ae23f41f87c7361550d7b385d20bd2ba4e9c6064a71a  -

macbook :~ seitz$ echo -n "Hi al1" | shasum -a 256
005a9b72487248c324348c754b7b7a695dd6b98aa0058ff6363f365763d11e8d  -
```

Methods used to ensure Availability

- Redundant hardware
- Fully maintained hardware and software
- Keep up to date with all necessary system upgrades and updates
- Ensure to have enough bandwidth to and from the systems
- Remove bottlenecks
- Hot failover
- RAID
- Planed (Disaster recovery plan - DRP) and trained disaster recovery.
- Backups
  - Geographically-isolated location
  - Fireproof, waterproof safe
- Measures against DDoS

Authentication and Authorisation

- **Authentication (Who You Are)**: Verifies identity to confirm if someone or something is who they claim to be.
  - Question: "Are you really Person X?"
  - Methods: Login forms (username/password), HTTP Basic/Digest authentication, X.509 certificates, biometrics (e.g., fingerprints), multi-factor authentication (MFA like OTPs).
- **Authorisation (What You Can Do)**: Determines permissions to access resources after authentication.
  - Question: "What actions are you allowed?"
  - Methods: Access control lists (ACLs), role-based access control (RBAC), URL restrictions, secure object/method protections (e.g., API endpoints).
- Note: **Authentication must precede authorisation**; together, they enforce secure access in systems like web apps or networks.

Authentication and Authorisation

Factors for Authentication

- Something you **know**
  - Operating system password
  - Credit Card PIN
  - Safe pin
  - Smartphone unlock combination
  - Secret handshakes

Factors for Authentication

- Something you **have**
  - Physical objects
  - Keys
  - Smartphones
  - Smart Cards
  - USB drives
  - Token devices

Factors for Authentication

- Something you **are**
  - Fingerprint
  - Palm
  - Iris
  - Retina
  - Blood
  - DNA

Factors for Authentication

- (**Somewhere** you are)
  - Related to your location
  - IP address

Factors for Authentication

- (Something you **do**)
  - Gestures
  - Related to something you know

Multifactor Authentication (MFA)

- **Combining two or three factors** from the previous categories
- More secure because an attacker needs multiple skills to breach an account
- Attacker needs to perform multiple successful attacks simultaneously
- Famous example: 2FA
- **If available: You should use 2FA**

MFA examples

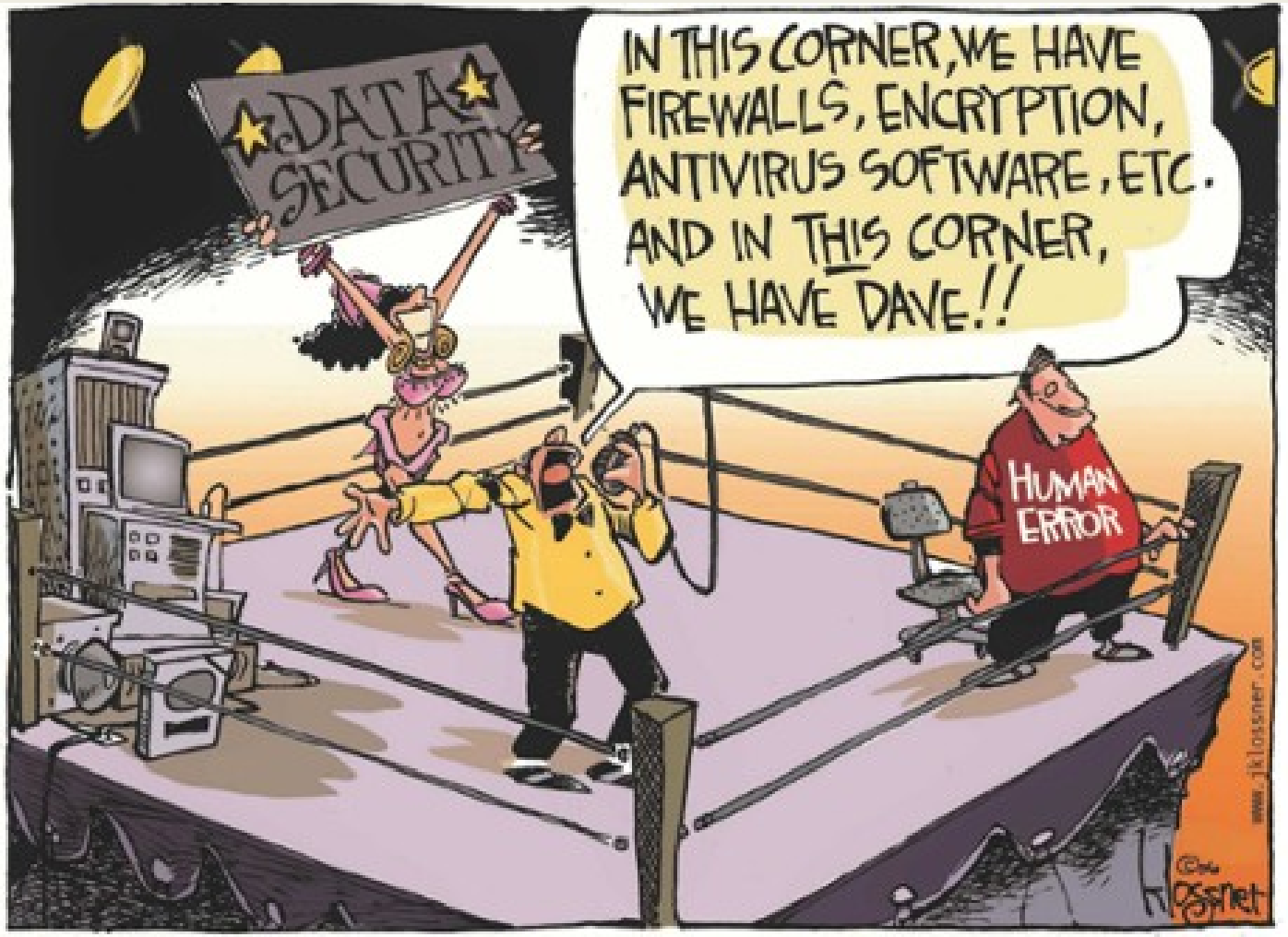
«How to protect your assets» Take Aways

- Know the CIA Triad and their components
- Use different factors and more then one to protect you assets
- Authentication (Who you are) and Authorisation (What you can do)
- Know the methods to ensure confidentiality, integrity and availability

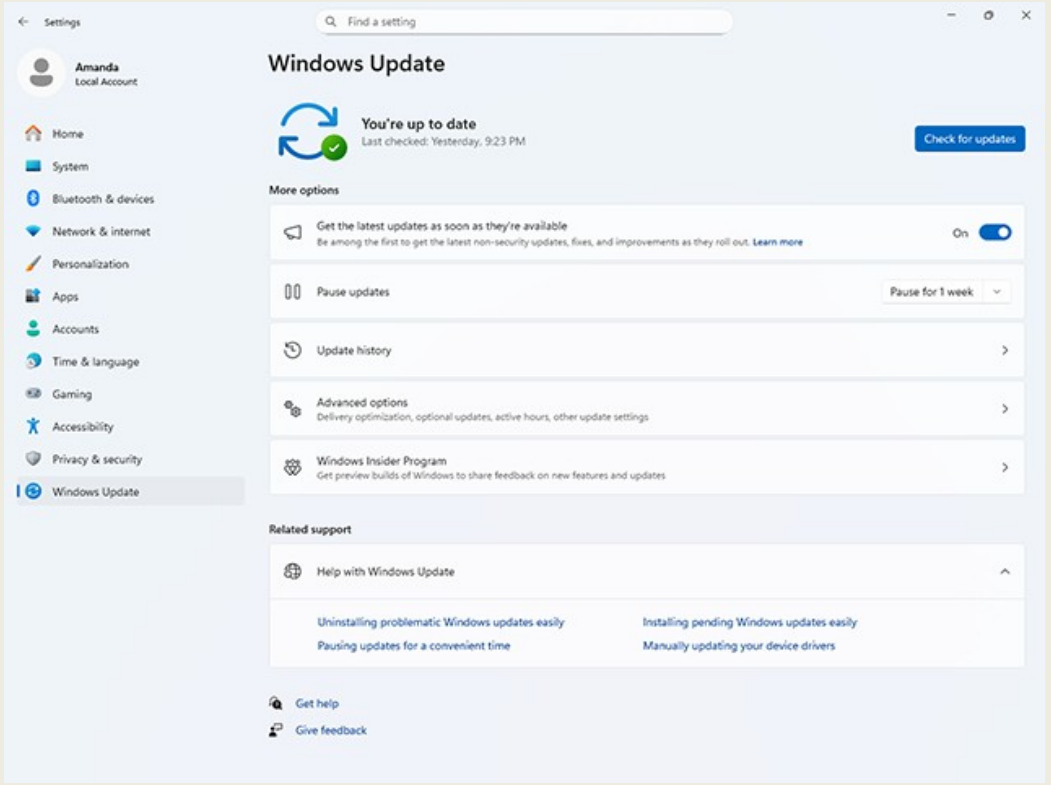
06 – Good IT Security Practices

- Patch your systems
- Use a Password Manager

The Human Factor

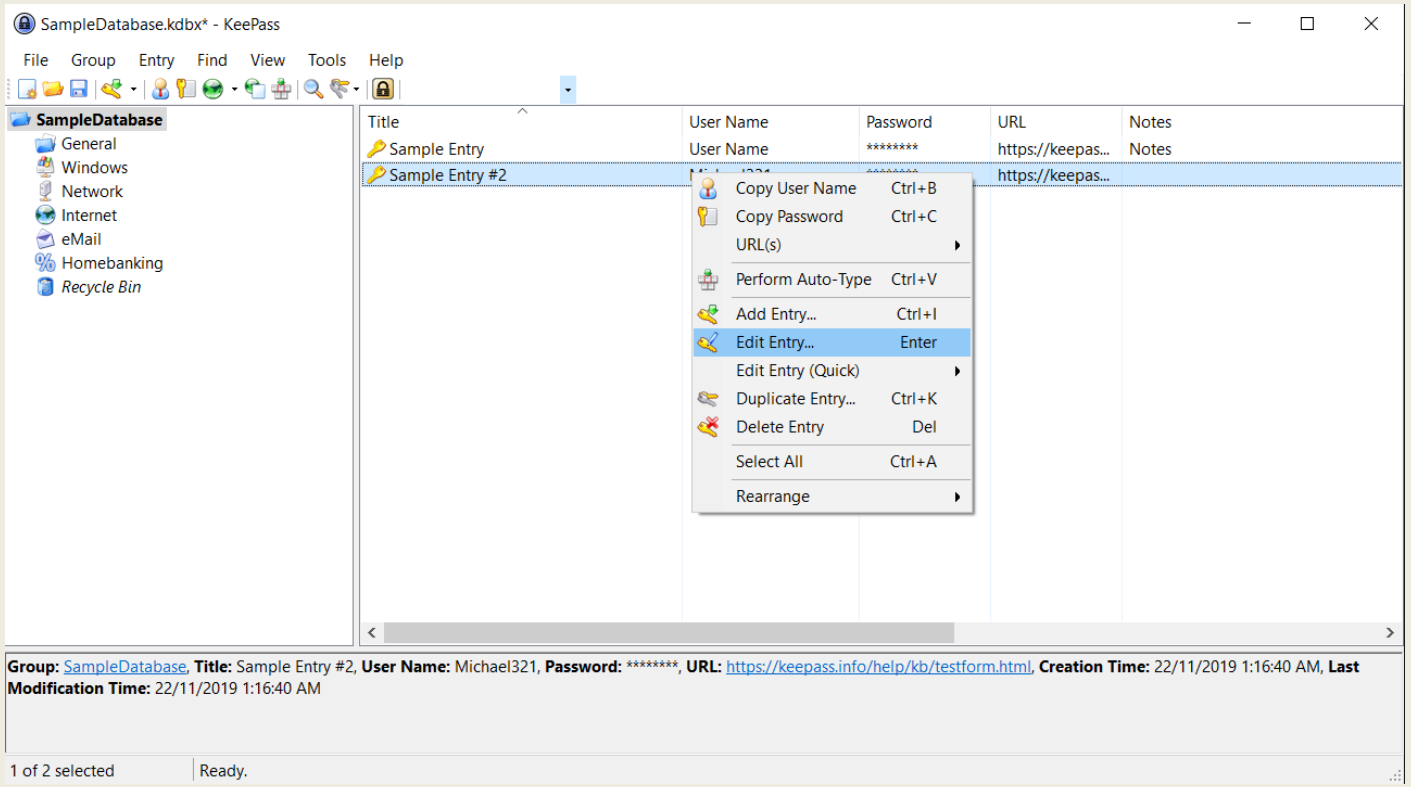


Patch your systems



- https://en.wikipedia.org/wiki/Windows_Update#/media/File:Windows_Update_screenshot.png

Use a Password Manager



- https://en.wikipedia.org/wiki/KeePass#/media/File:KeePass_Main.png

07 – Roundup and Feedback

Please fill out the Feedback form from the University of Bern