Switch

Introduction to IT Security for Data Scientists

matthias.seitz@switch.ch
darja-anna.yurovsky@switch.ch

26. Oktober 2023

Agenda

01 - Welcome, mutual introduction and expectations
02 - Introduction to security
03 - Current Security Threats
04 - Basic Security
05 - How to react to a Security Incident
06 - How to protect your Assets
07 - Good IT security practices
08 - Roundup and Feedback

Schedule

09:00 - 10:00	Lecture
10:00 - 10:15	Break
10:15 - 11:15	Lecture
11:15 - 11:30	Break
11:30 - 12:00	Lecture
12:00 - 13:15	Lunch break
13:15 - 14:15	Lecture
14:15 - 14:30	Break
14:30 - 15:30	Lecture
15:30 - 15:45	Break
15:45 - 16:45	Lecture

01 - Welcome, mutual introduction and expections

- About us
- Expectations
- About you
- About Switch
- What is a CERT

About us

Matthias Seitz
- BSc Computer Science
- Information Security Officer and Product Manager @Switch
- Longtime experience in IT security

Darja-Anna Yurovsky
- MA Political Science & MSc Digital Forensics
- IT Security Engineer / Incident Response @Switch
- Longtime experience in IT security & Law Enforcement

What is your and our expectation for this Course?

About you

- Which field are you working in?
- Do you know any security processes in your company (e.g. vulnerability patching, incident response)?
- Do you already have some questions about Security?
- Expectations for this course?

About Switch

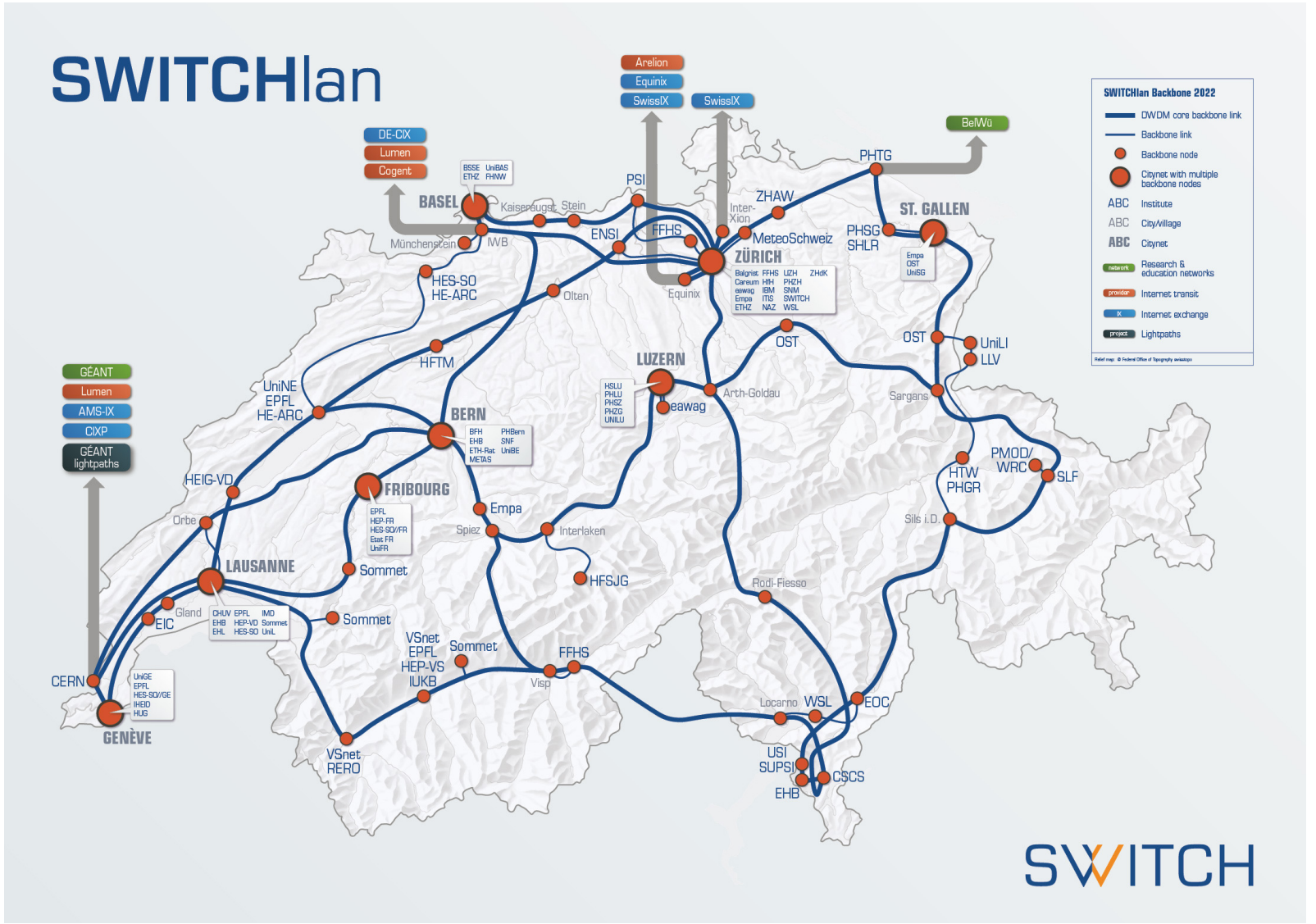
Switch is an integral part of the Swiss academic community.

Based on our core competencies

- Network
- Security
- Identity Management

Switch offers collaboratively developed ICT solutions that empower users in and beyond the academic world to achieve leading edge results in a globally competitive environment.

NREN- National Research and Eductation Network



CERT – Computer Emergency Response Team

Alt. CSIRT (Computer Security Incident Response Team)

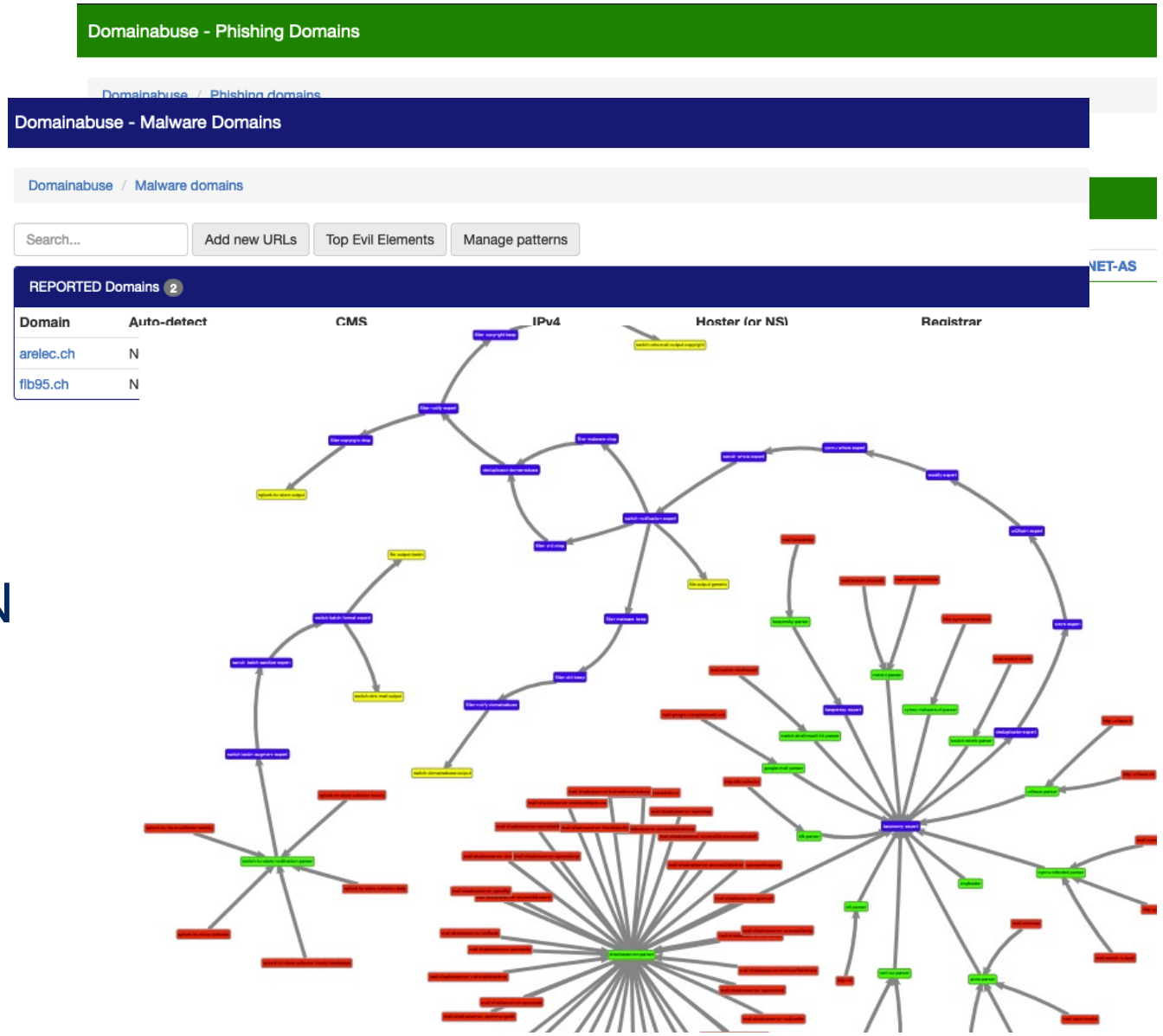
Def. security incident
a security incident is an undesirable event that threatens operational safety and or disrupts operations

Def. incident response
Reactive response to ensure that violations/incident are effectively addressed, contained and restored to normal operation.

The role of data

As part of the Registry
–phishing sites
–fake shops
–infected websites

As part of the CERT and NREN
–malware
–reports of vulnerable services
–resports of open servicse
–DDoS attacks



02 – Introductio to Security

–Security Facts and Figures

Security is about…

Risks & Threats

Economical Size

Processes & Concepts

Risk and security management process

Information Security

Did you know?

https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

ENISA Threat Landscape 2022

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Who are the attackers?

Internal User Error: Users making **mistakes** with configurations which may bring down **critical resources** such as **firewalls**, routers and servers causing wide-spread or departmental company outages.

Opportunistic: These attackers are usually **script kiddies** driven by the desire for **notoriety**

Insider Threat: Insider attackers are typically **disgruntled employees** or ex-employees looking for **revenge** or some type of financial gain.

Hacktivists: These attackers have a **political agenda** and create **high-profile attacks**

Organized Crime: Most often, these cybercriminals engage in **mass attacks** driven by **profits**. Typically looking for social security numbers, health records, credit cards, and banking information.

Government Sponsored: Well funded and often build **sophisticated, targeted attacks**. They are typically motivated by **political, economic, technical, and military agendas**.

Motivation for Threat Actors

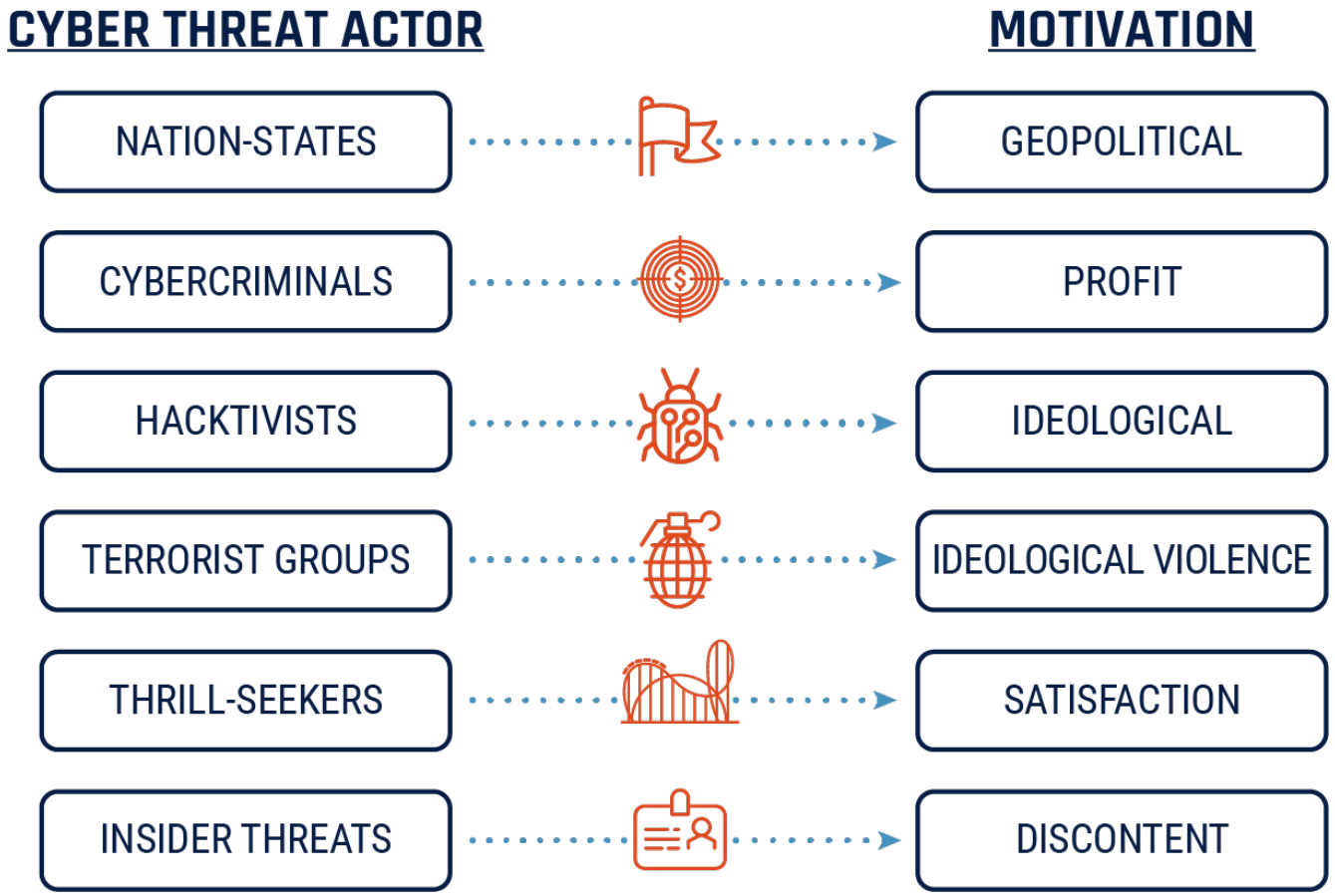


Image Source: https://cyber.gc.ca/sites/default/files/inline-images/motivations-e.png

How Attackers Work (Att&ck Matrix)

Reconnaissance	Resource Development	Initial Access	Execution	Persistence
Privilege Escalation	Defense Evasions	Credential Access	Discovery	Lateral Movement
Collection	Command and Control	Exfiltration	Impact	

source: https://attack.mitre.org/

Discussion

- What could be the motivation from a malicious actors perspective regarding your company?
- How would they affect your business the most?

03 – Current Security Threats

- Phishing
- Social Engineering
- Malware
- Ransomware

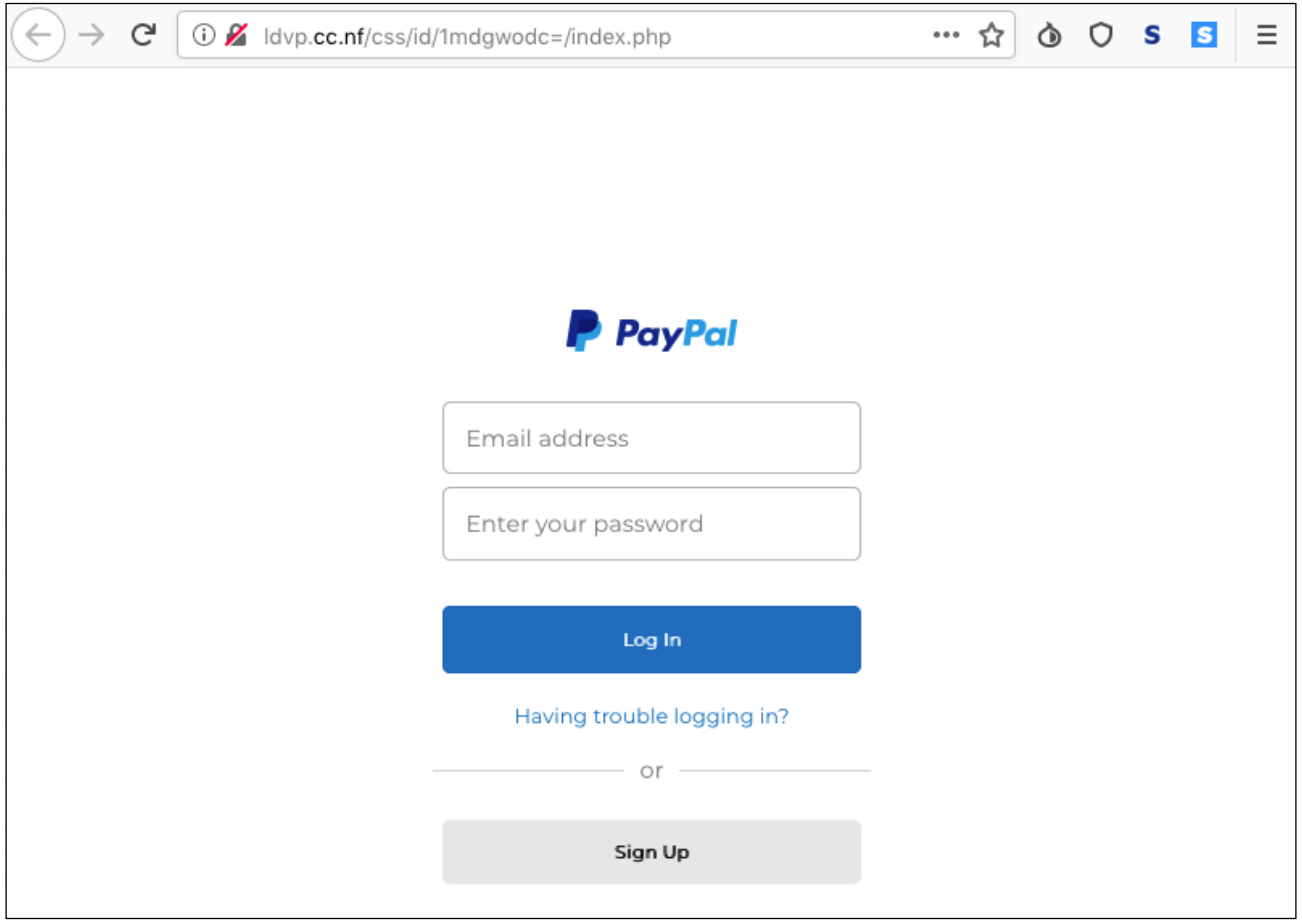
Phishing

Phishing

"Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution **to lure individuals into providing sensitive data** such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can **result in identity theft and financial loss**."

http://www.phishing.org/what-is-phishing

Phishing

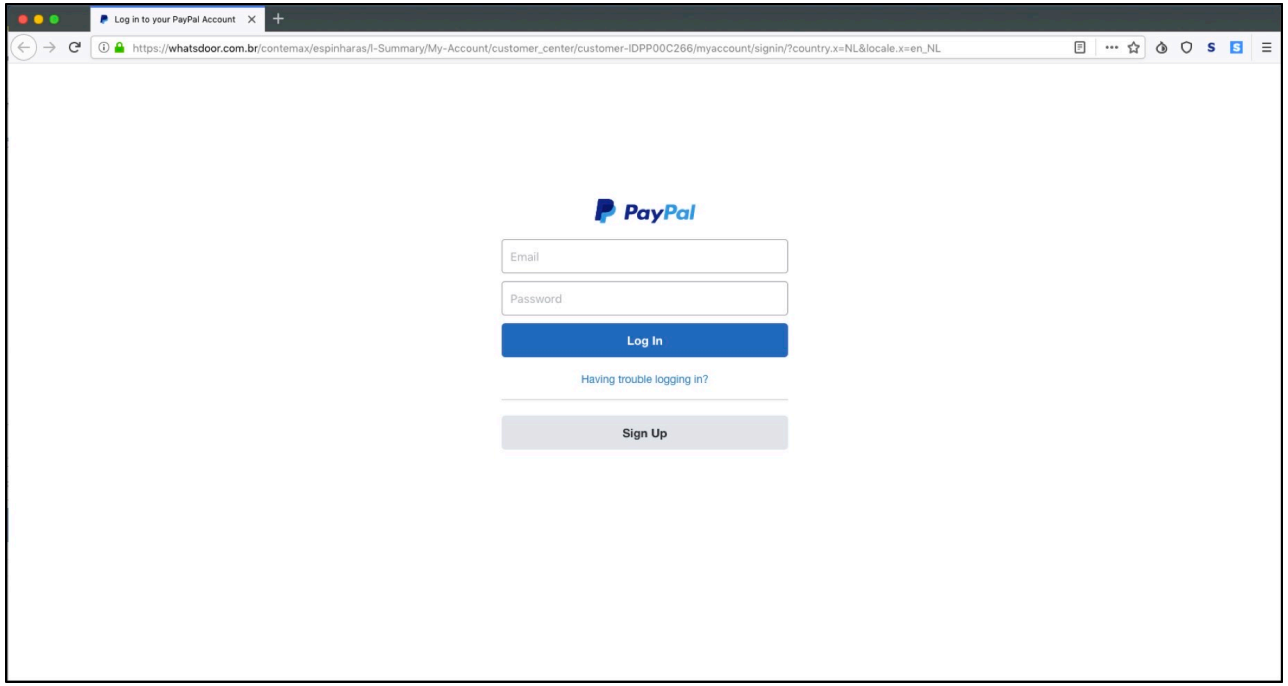

ldvp.cc.nf/css/id/1mdgwodc=/index.php
PayPal
Email address
Enter your password
Log In
Having trouble logging in?
or
Sign Up

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



Switch

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 credentials
- **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

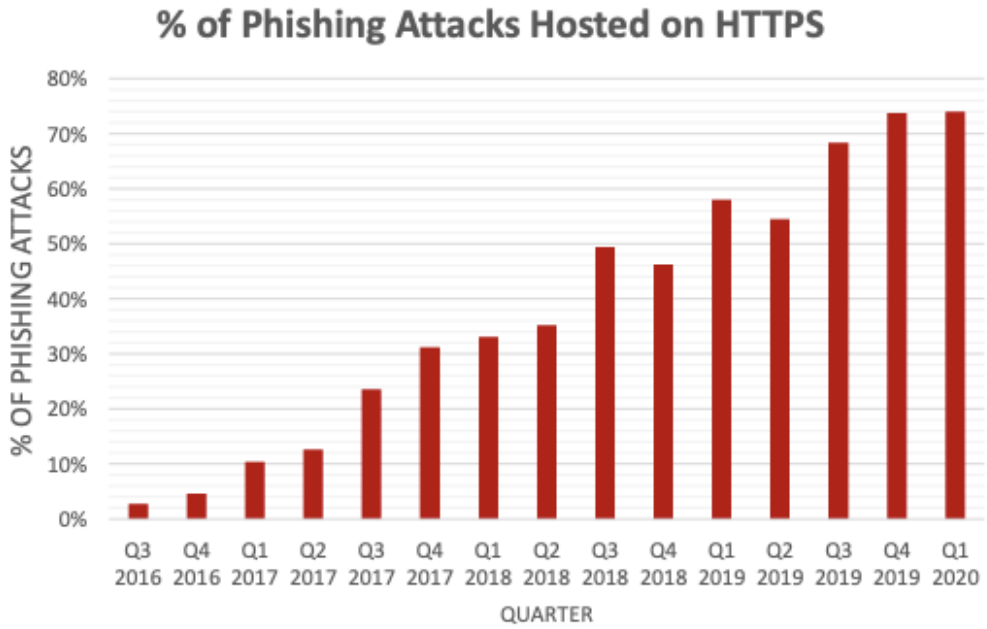
HTTP vs HTTPS

- 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?

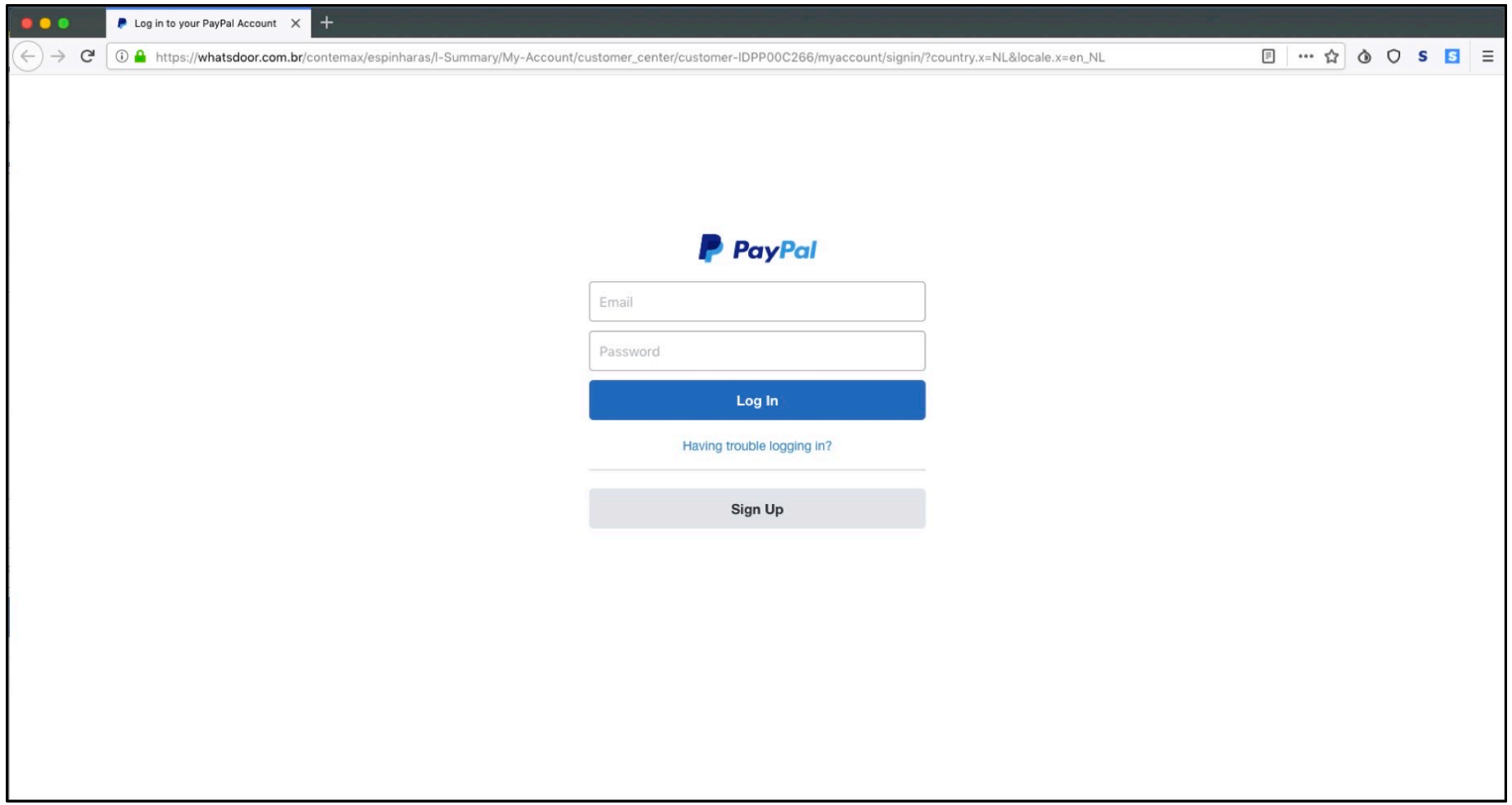
No. HTTPS and HTTP are just the protocols.

APWG: "In Q1 2020, a new high of 74 percent of sites used for phishing were protected with SSL"

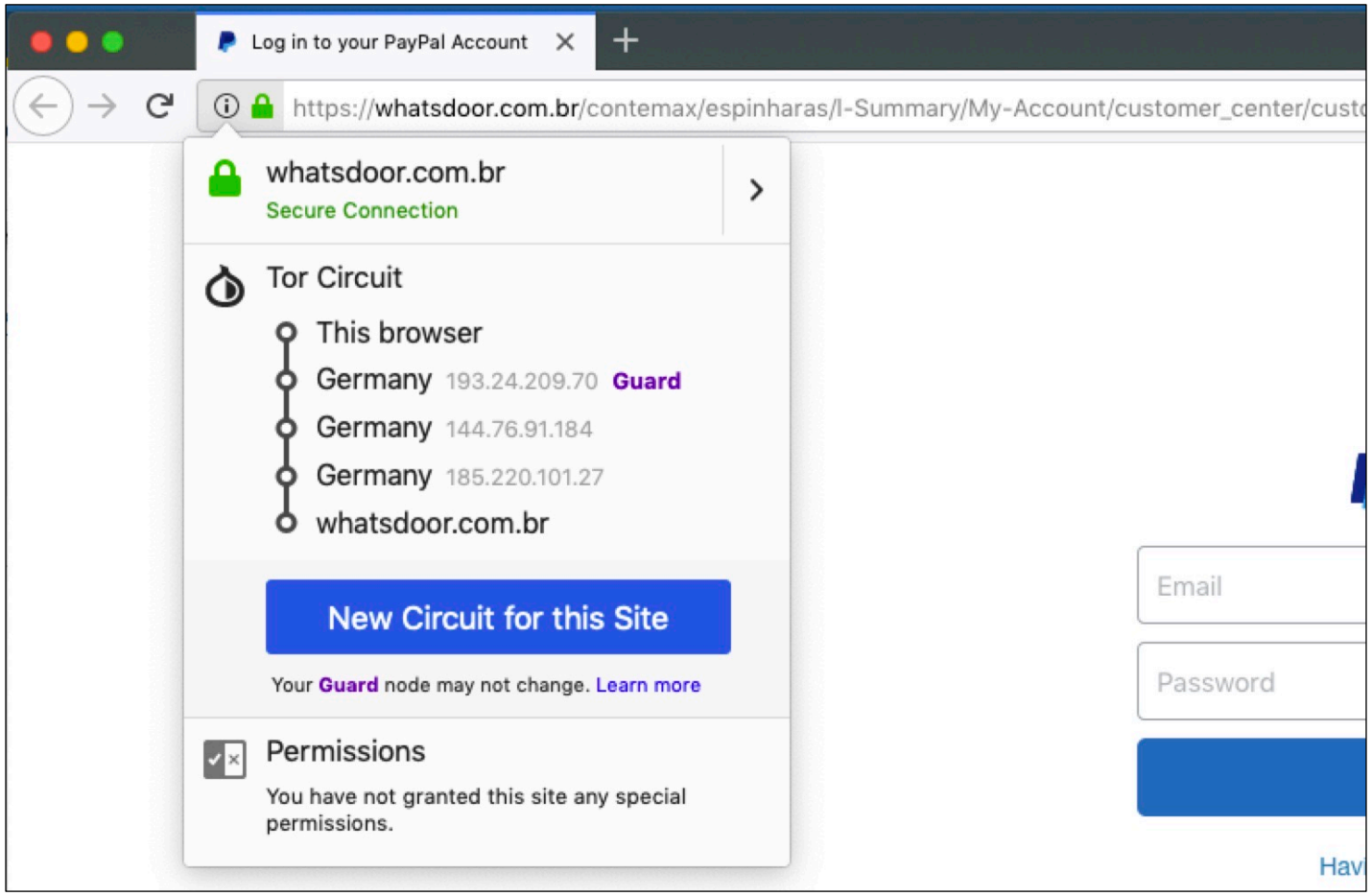


Source:
https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf

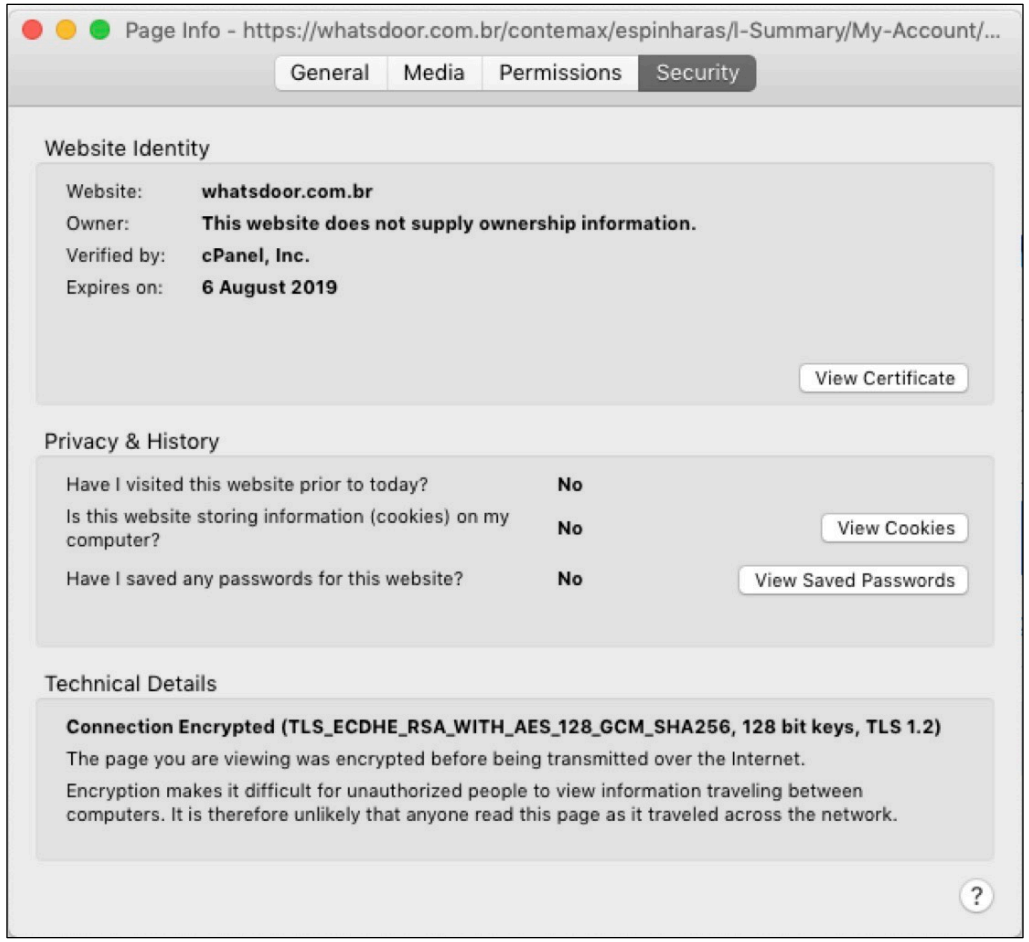
Phishing and HTTPS



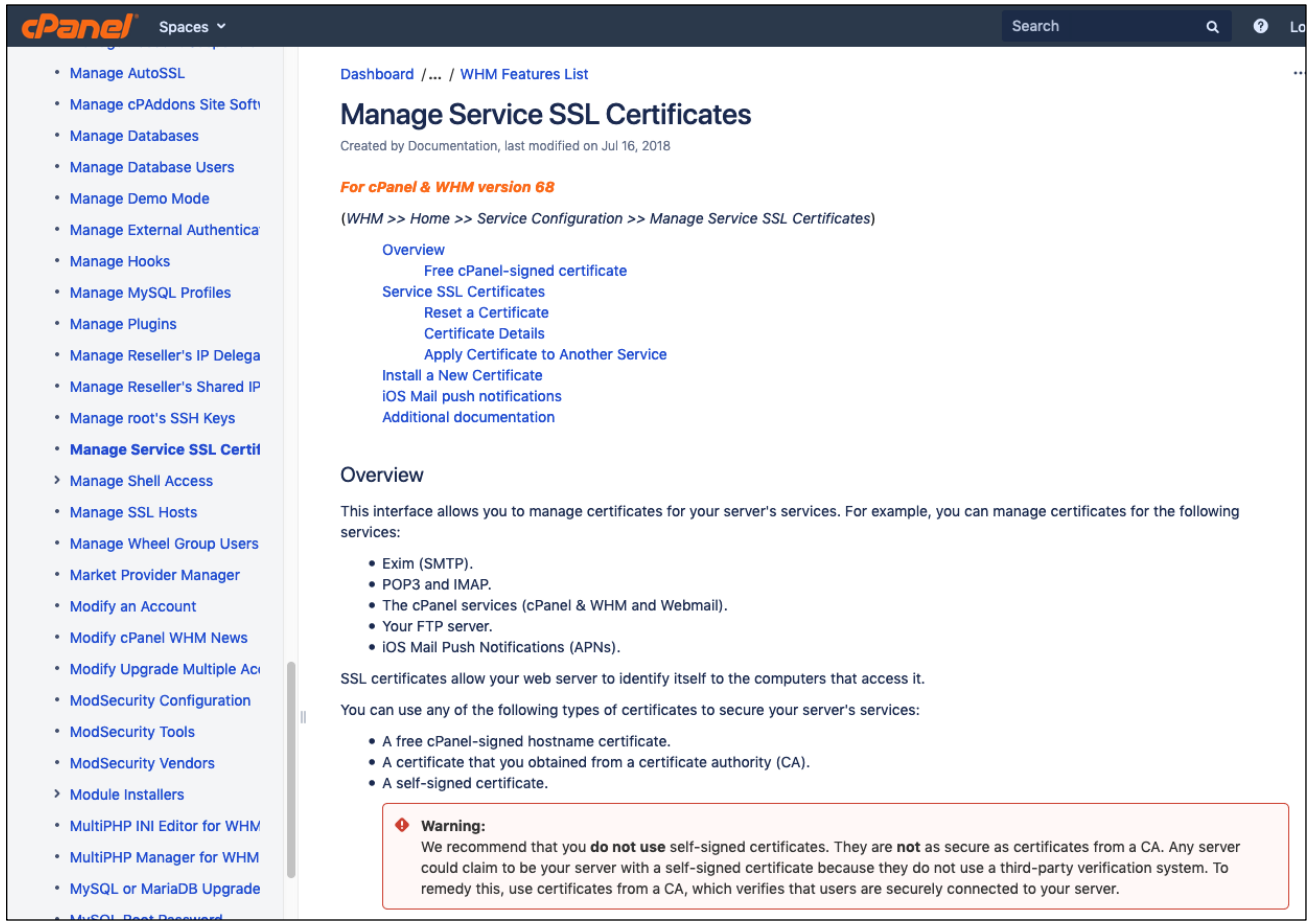
Phishing and HTTPS



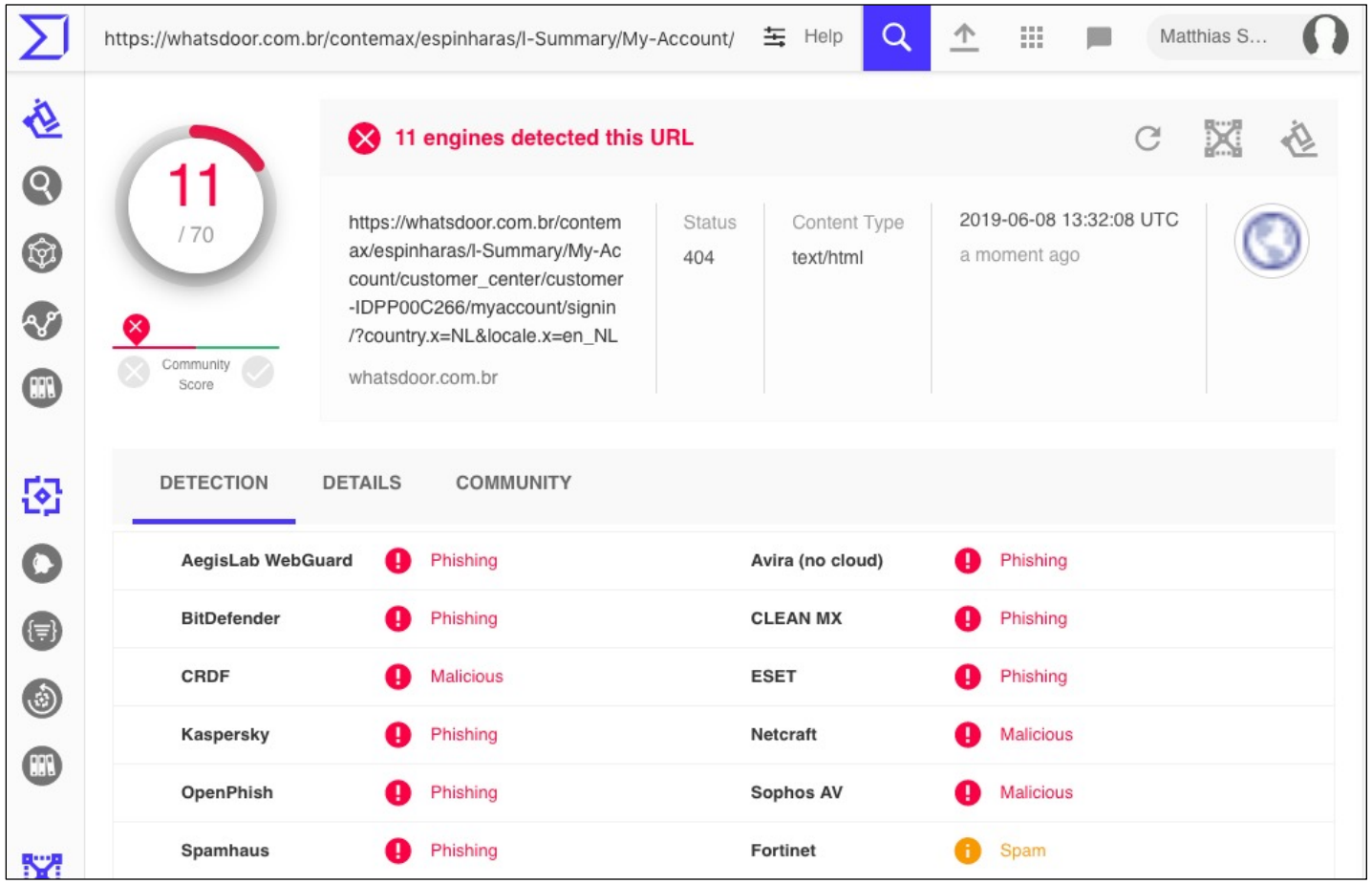
Phishing and HTTPS



Phishing

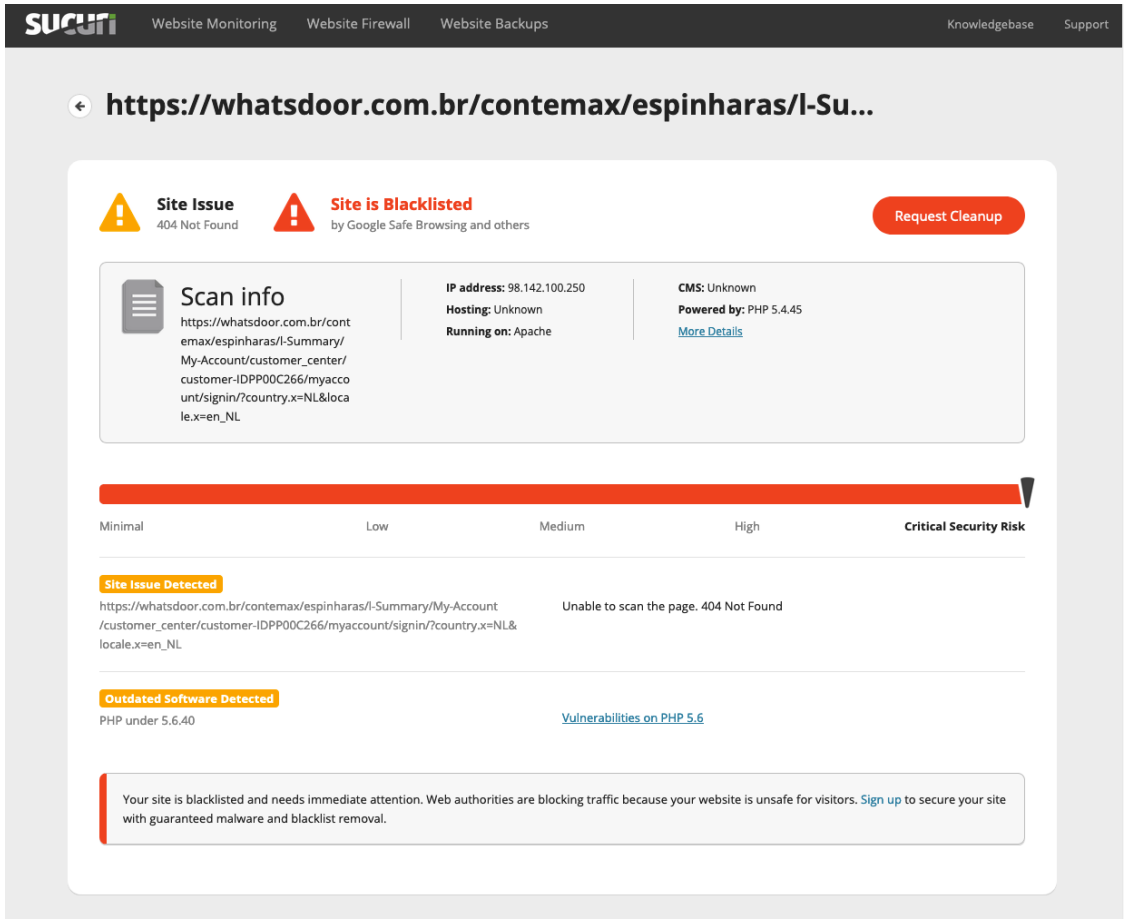

cPanel
Spaces
Search
Manage AutoSSL
Manage cPAddons Site Soft
Manage Databases
Manage Database Users
Manage Demo Mode
Manage External Authentica
Manage Hooks
Manage MySQL Profiles
Manage Plugins
Manage Reseller's IP Delega
Manage Reseller's Shared IP
Manage root's SSH Keys
Manage Service SSL Certif
Manage Shell Access
Manage SSL Hosts
Manage Wheel Group Users
Market Provider Manager
Modify an Account
Modify cPanel WHM News
Modify Upgrade Multiple Ac
ModSecurity Configuration
ModSecurity Tools
ModSecurity Vendors
Module Installers
MultiPHP INI Editor for WHM
MultiPHP Manager for WHM
MySQL or MariaDB Upgrade
Dashboard / ... / WHM Features List
Manage Service SSL Certificates
Created by Documentation, last modified on Jul 16, 2018
For cPanel & WHM version 68
(WHM >> Home >> Service Configuration >> Manage Service SSL Certificates)
Overview
Free cPanel-signed certificate
Service SSL Certificates
Reset a Certificate
Certificate Details
Apply Certificate to Another Service
Install a New Certificate
iOS Mail push notifications
Additional documentation
Overview
This interface allows you to manage certificates for your server's services. For example, you can manage certificates for the following services:
Exim (SMTP).
POP3 and IMAP.
The cPanel services (cPanel & WHM and Webmail).
Your FTP server.
iOS Mail Push Notifications (APNs).
SSL certificates allow your web server to identify itself to the computers that access it.
You can use any of the following types of certificates to secure your server's services:
A free cPanel-signed hostname certificate.
A certificate that you obtained from a certificate authority (CA).
A self-signed certificate.
Warning:
We recommend that you do not use self-signed certificates. They are not as secure as certificates from a CA. Any server could claim to be your server with a self-signed certificate because they do not use a third-party verification system. To remedy this, use certificates from a CA, which verifies that users are securely connected to your server.

Phishing Checks



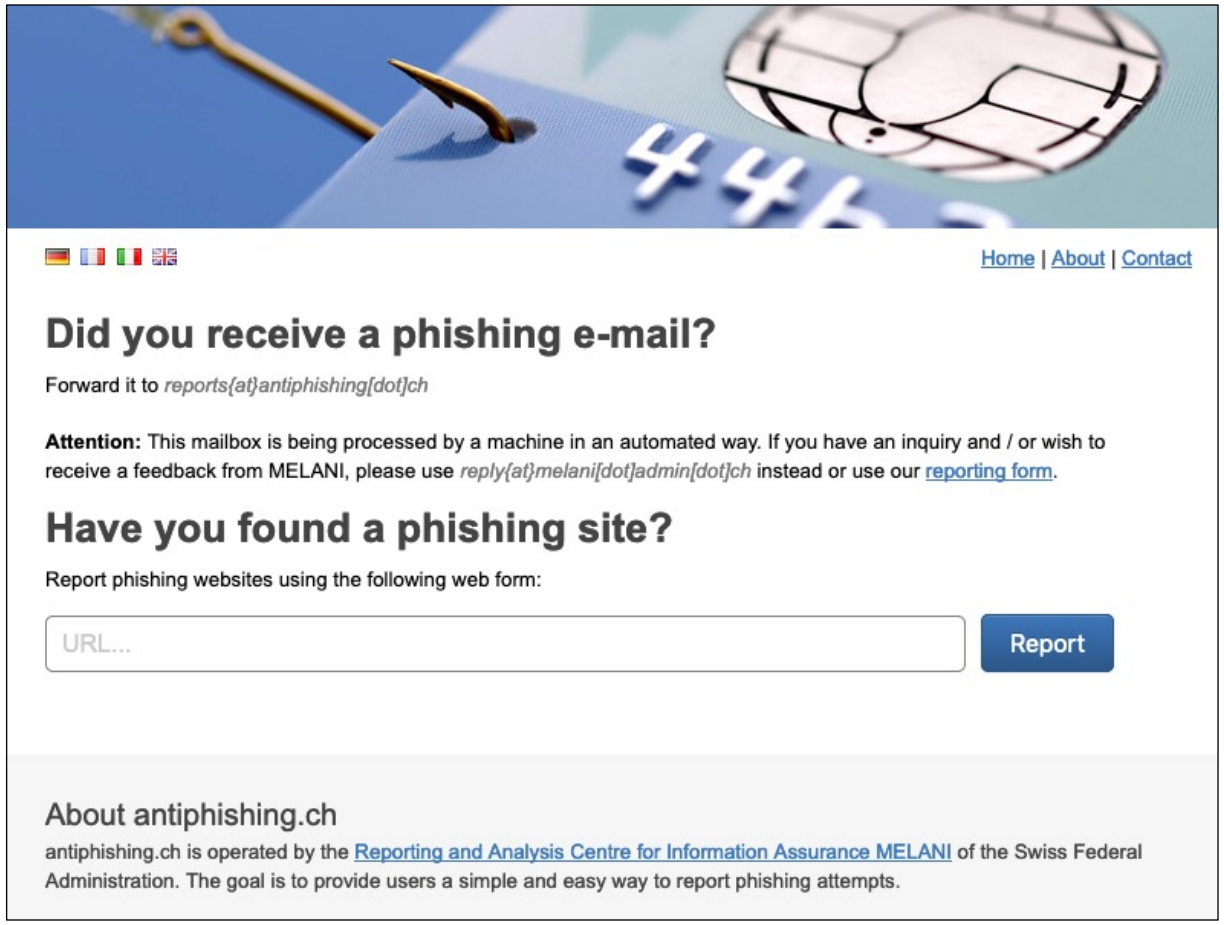
https://www.virustotal.com

Phishing Checks



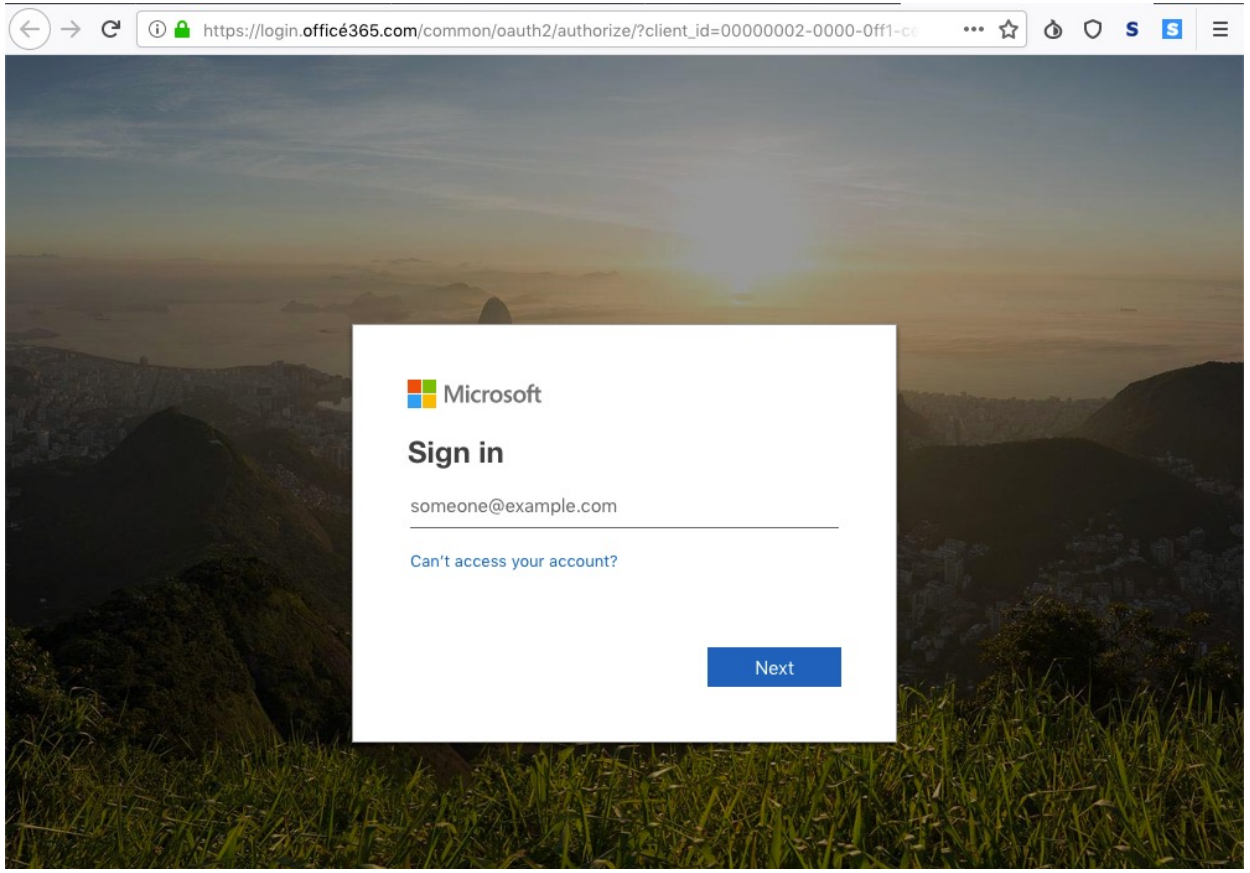
https://sitecheck.sucuri.net/

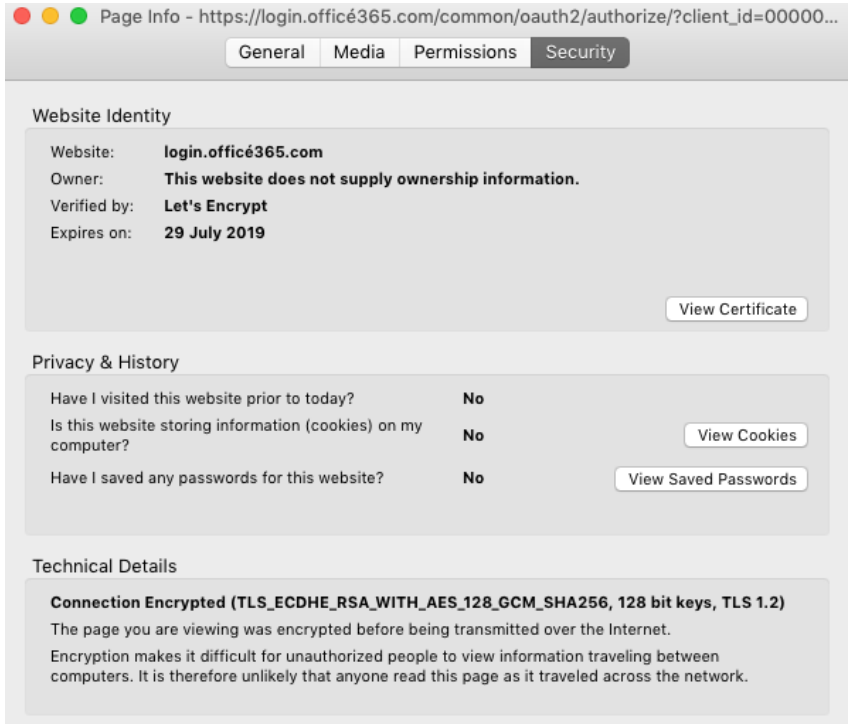
Report Phishing



https://www.antiphishing.ch

Advanced Phishing





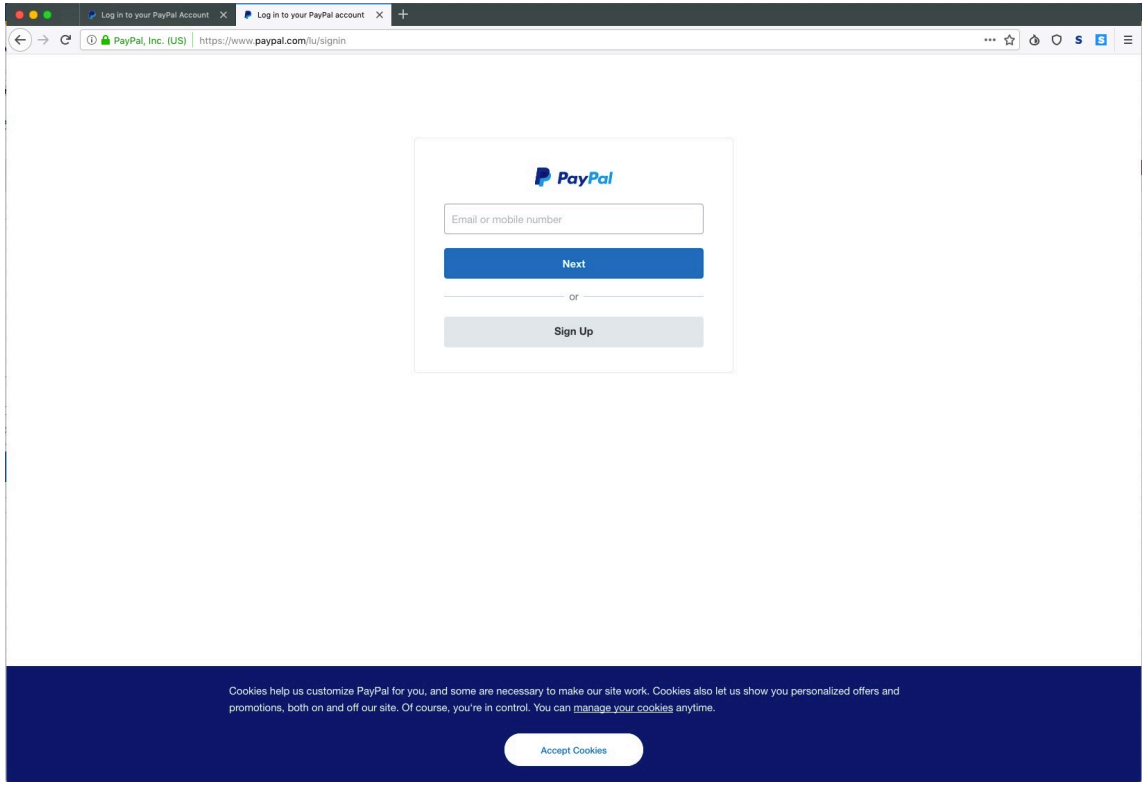
Advanced Phishing

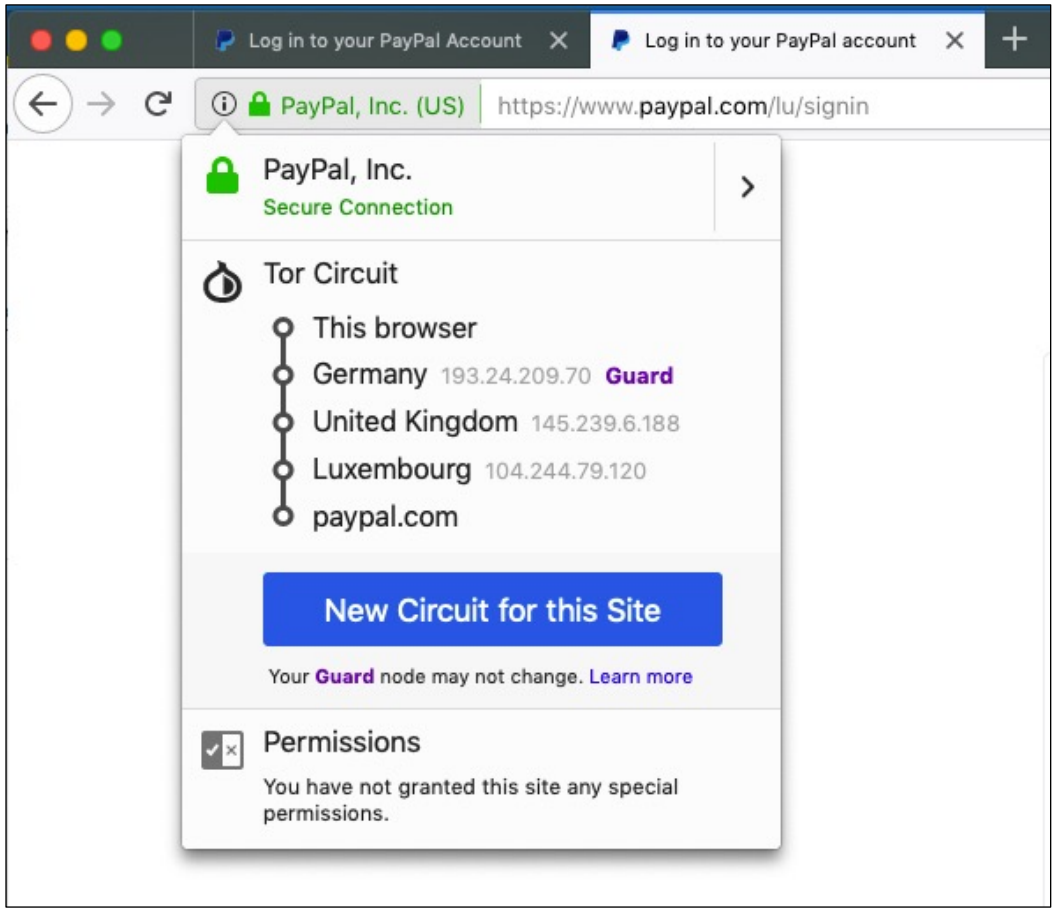
https://login.xn--offic365-f1a.com

Punycode

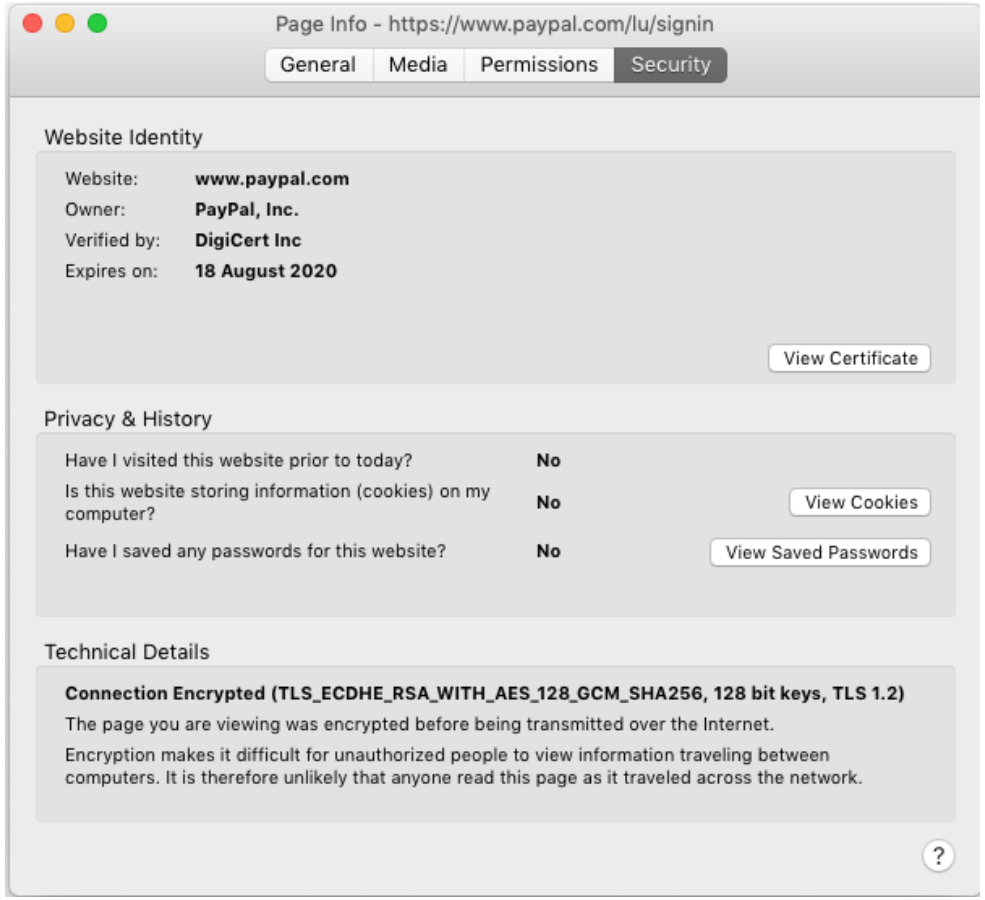
- Is a way to **represent International Domain Names (IDNs) with the limited character set (A-Z, 0-9)** supported by the domain name system.
- For example, "münich" would be encoded as "mnich-kva".
- An IDN takes the punycode encoding, and adds a "xn--" in front of it.
- "münich.com" would become "xn--mnich-kva.com".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

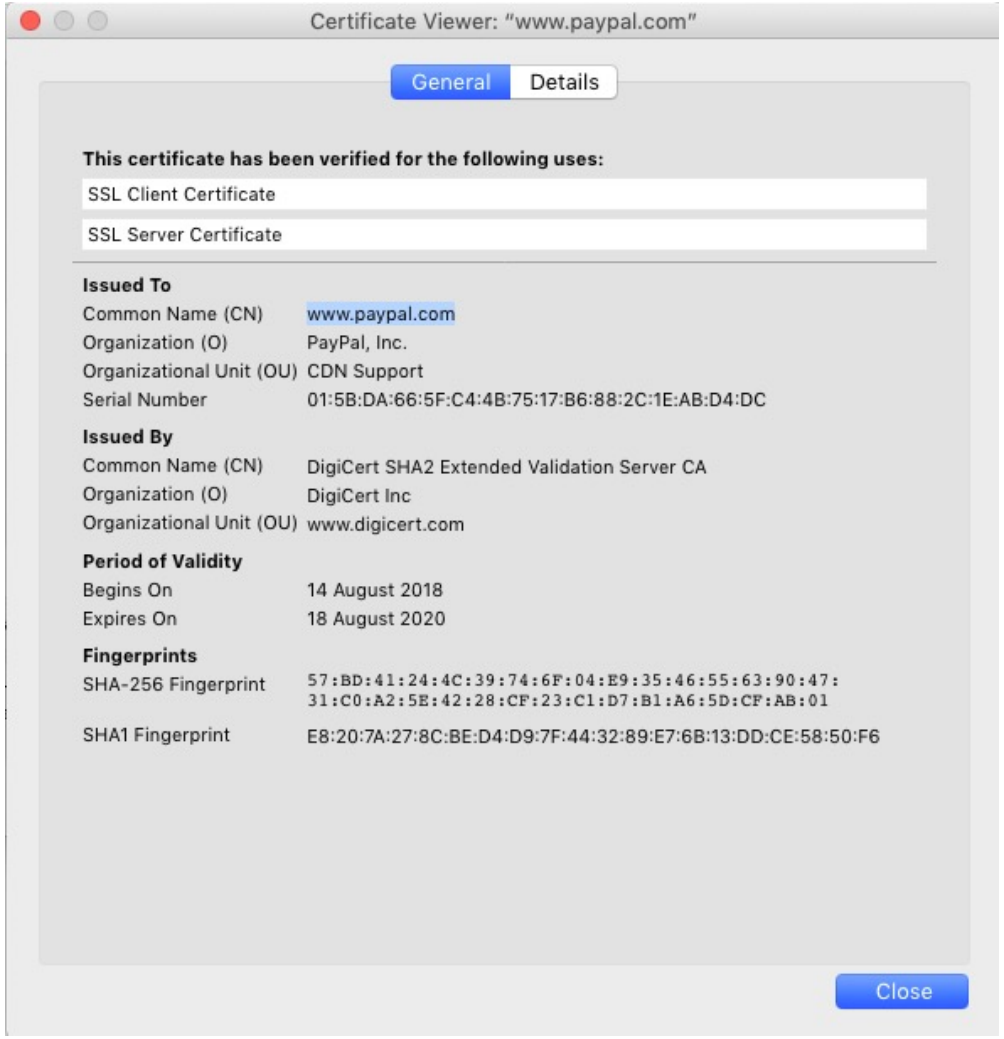
SSL / TLS Certificates



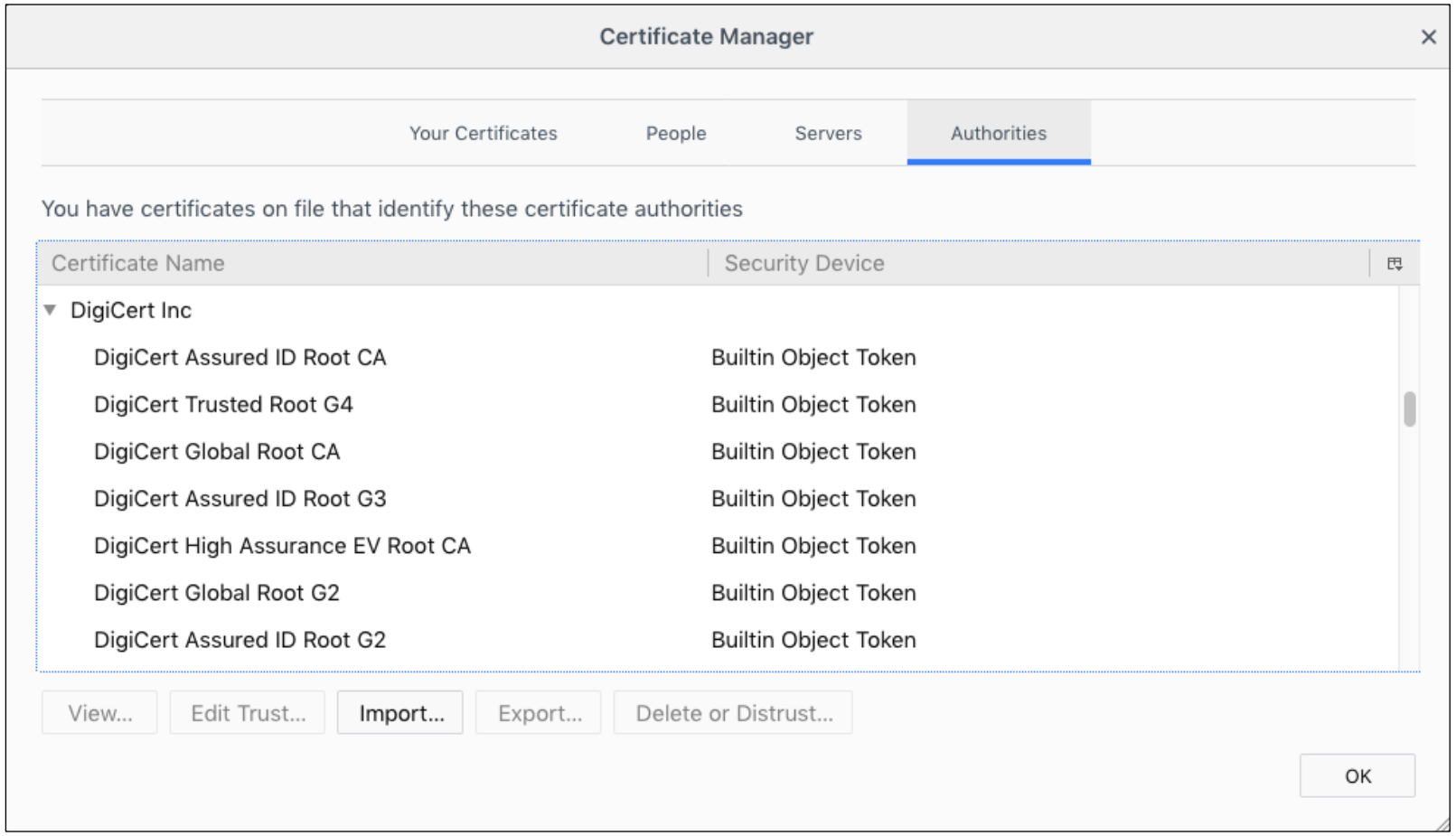


SSL / TLS Certificates

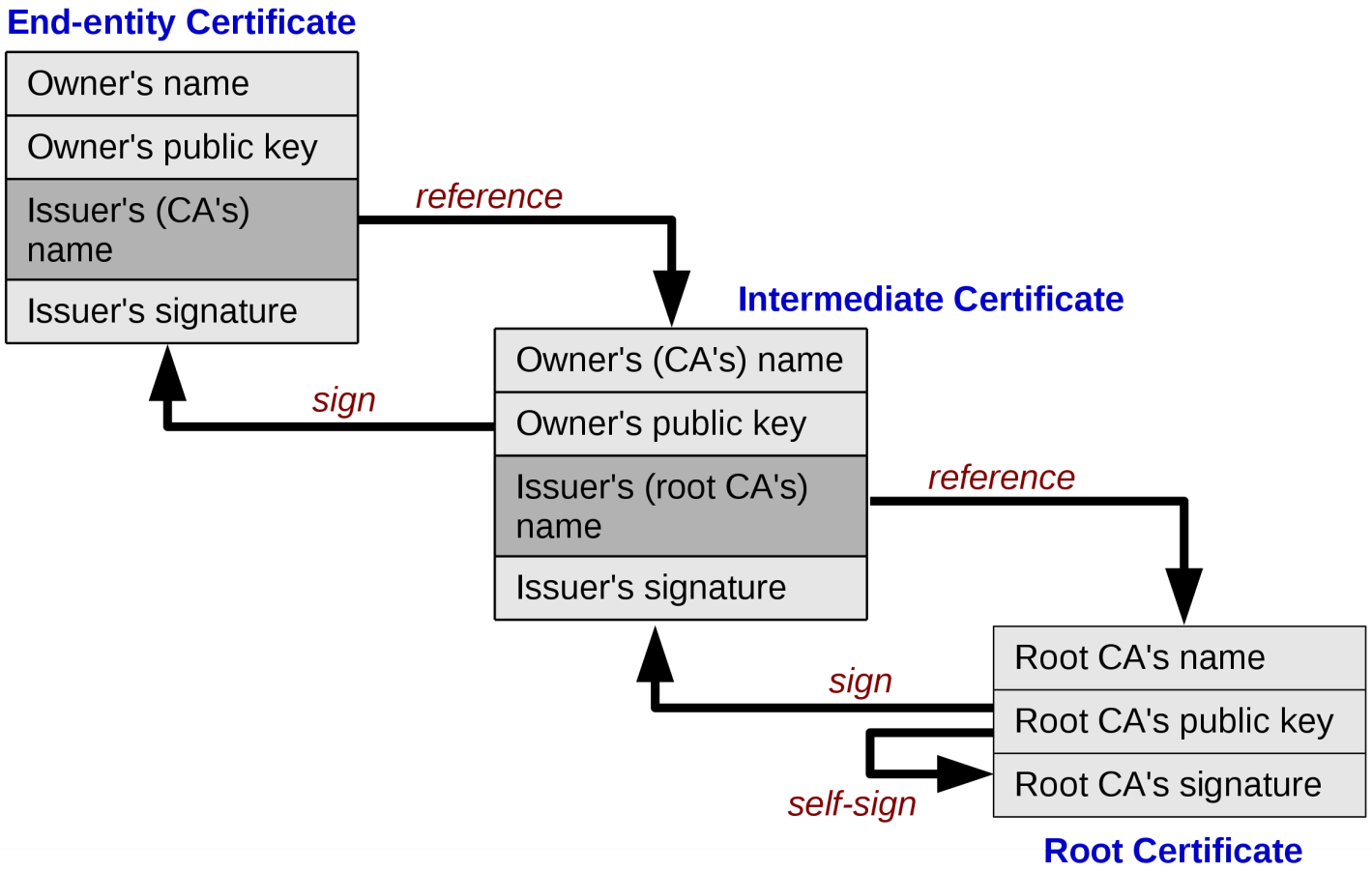




Certificates

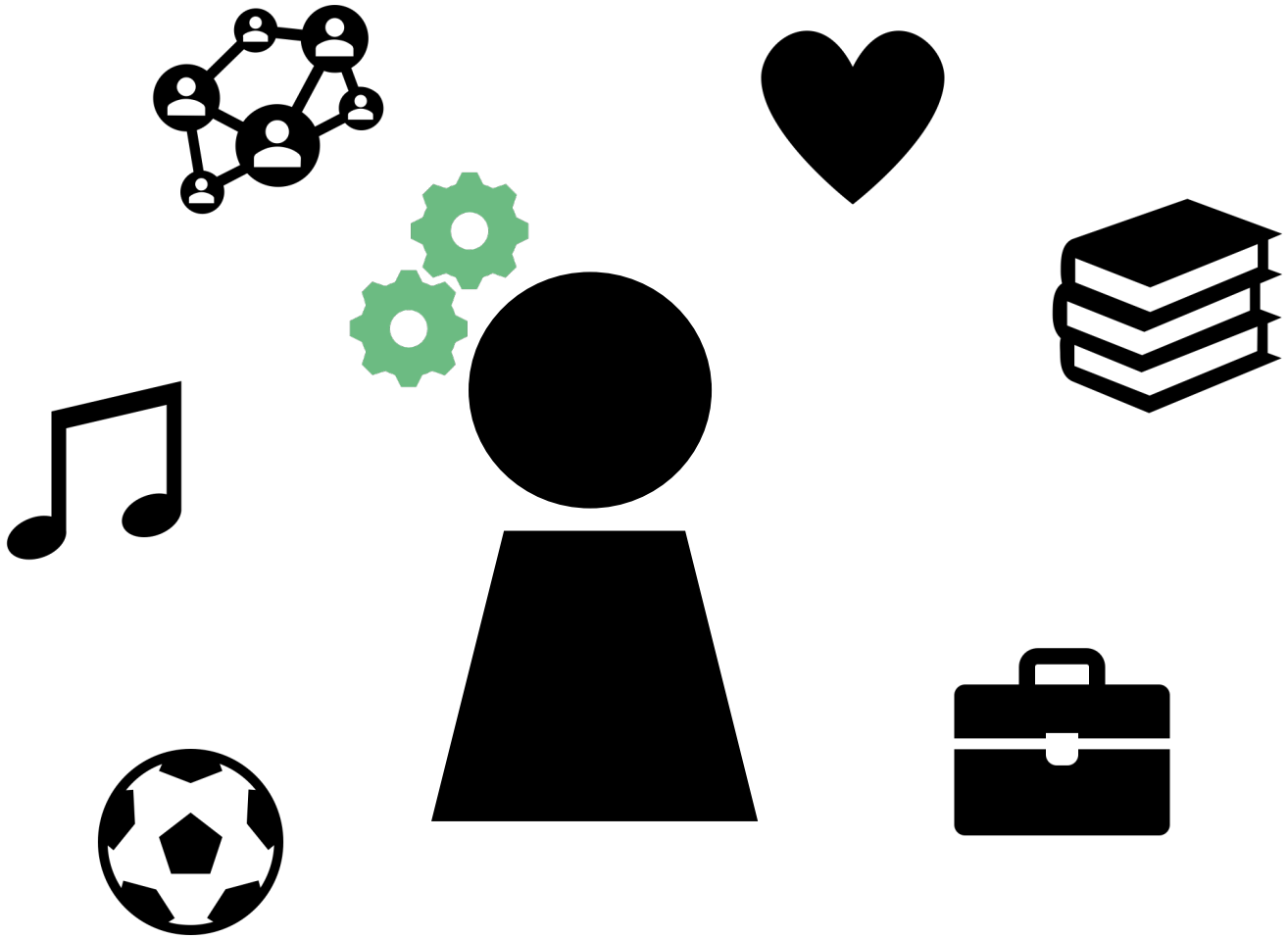


Chain of Trust and Root CA’s



Social Engineering?

Hacking people – how?



Social Engineering Tools

- Information Gathering
- Tailgaiting
- Dumpster Diving
- Wing (wo)man
- Eavesdropping
- Investigation on site
- Network check
- Shoulder Surfing
- Manipulation (pressure, fear, charme, temptation)

3 tips to fight tricksters

Take your time

Reality Check

Check back

Malware

Malicious Software

designed to damage or disrupt information systems and data

AND / OR

gain unauthorized access to a network

Classification Malware

Stealers	Replicators	Autonomous	Remote
Sniffer Password Grabbers Keyloggers	Virus Worm	Rootkit Logical bomb	Ransomware Scareware Backdoor Bots

Cyber Kill Chain

source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Malware Trends

source: https://any.run/malware-trends/

RedLine Stealer

- Underground forums sale (100/150$)
- Harvests information from browser (credentials, auto-complete, credit card info, fingerprint, cryptocurrency)

Emotet

- Historically banking malware
- Organized in botnet -> C2
- Back door & infection with payloads
- Today: infrastructure as a service (IaaS) for
- Delivering of malware to infected systems
- Taken down by authorities in January 2021 -> back in November 2021

Wanna Cry

- Encrypts data (ransomware) -> cryptoworm
- Target Microsoft Windows systems
- Exploit EternalBlue by NSA
- 2017 unprecedented scale of attack
- Hospitals and health services
- Kill Switch

Malware

Demo https://hybrid-analysis.com

https://helgrind.Switch.ch/joesandbox/index.php/analysis/665042

Ransomware

Definition

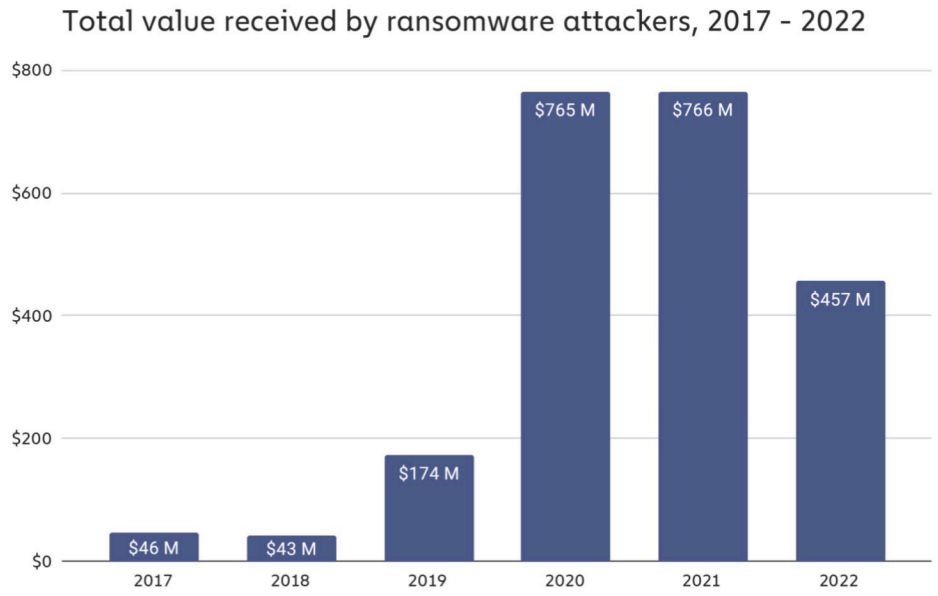
Ransom

Malware

Malware that infects a system and then locks out the user until he pays a sum of money to unlock his data.

Ransomware in 2023

- most serious threat for organizations
- highly scalable, low barrier, endless vectors
- mature software and infrastructure offered as a service with easy UI
- Homepage of perpetrators with SLA and leaked data
- RaaS: Ransomware as a Service
- Comfort of crime from the couch



https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay

The Development of Ransomware

Proto-ransomware: encrypted files, but pretend to be something else like licence or corruption, fix files for a **fee**

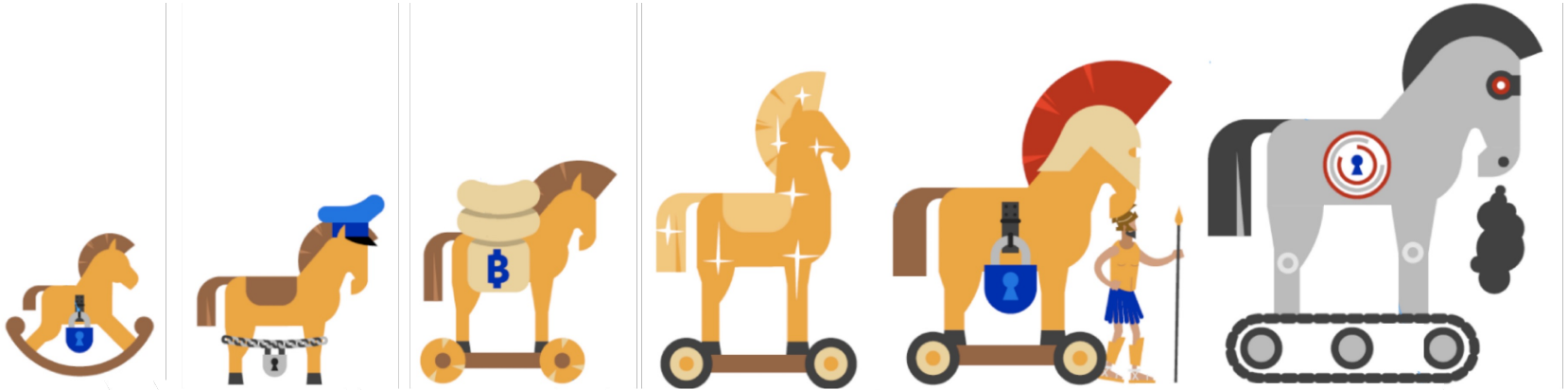
Police themed: Locked screens, pretending to be somebody and victims pay a "**fine**" to use device again

Bitcoin Boom: Use of crypto currency for all transactions

Gold rush: large and untargeted campaigns (i.e. Wanna Cry)

Big-game hunting: targeting big organizations for large payout

Ransomware 2.0: encryption and threat to leak stolen data, double extortion



Ransomware Types

Locker Ransomware

-Locks access to operating system, applications, network
-Software for unblocking access
-Data not changed
-recovery is easier

Crypto Ransomware

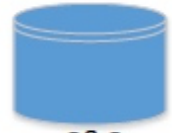
- Encryption of data using a cryptographic method
- Password or software for decryption
- Only vulnerabilities in applied cryptography allow decryption
- All devices affected that have network access and data

How it works (Crypto)

victim

victim-pc

C&C server



C&C database

11. payment is made

1. attack vector for access
2. malware is executed
3. Domain of the C&C server is determined via Domain Generation Algorithm
4. programme code is reloaded
5. Individual ID is generated and transmitted
8. Data is provided with a lock (encrypted with the
encrypted with the public key) and C&C server notified on success
10. Warning message with payment instructions is displayed
13. The lock can be opened with the key (data is decrypted)

6. Cryptographic key pair is generated. Public key is transmitted to the victim PC
9. Bitcoin payment address is generated and transmitted to the warning message with victim PC

12. Checks whether payment has been received and, if successful, transmits the key to the private ID

7. Private key (for decryption) and ID are secured

Business model

- Very worthwhile
- High level of victim suffering
- Recovery costs are higher than ransom Targeted OSINT of victims
- Anonymity of BTC
- Double extortion (stolen data and encryption)
- Costly incident for companies

1.1. Company revenue search

Find company website

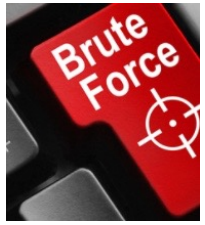
Google: website+revenue (mycorporation.com+revenue)

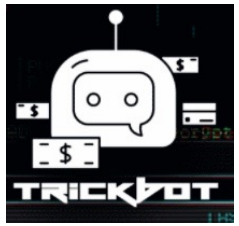
("mycorporation.com" "revenue")

Check more than one website if possible

Business model – RaaS (Ransomware as a Service)

Access





Dropper / Recon

Ransomware

Money Laundering

Key Points Ransomware

- Generally perceived as one of the biggest IT risks
- widespread and aimed attacks
- ransom often depends on annual revenue
- ransomware-as-a-service: different operators
- variety of initial access vectors and TTPs
- Ransomware attacks are also data breaches (double extortion)
- Ransomware attacks can also affect OT/IoT
- OS independent Ransomware
- Virtual machine based rootkits (VMBRs) and hypervisor exploits for cloud providers
- supply chain attacks

Clop Ransomware at Maastricht University

Time (2019)	Movement
Oct	First Breach by Phising
Nov	Lateral Movement (System with failed Patches)
23. Dec	Ransomware attacks and Displays Message
24. Dec	Contact Fox-IT for
26. Dec	Police has been notified
30. Dec	University decides to pay 217'000 $ in Bitcoins

sources:
https://www.rijksoverheid.nl/documenten/rapporten/2020/02/05/reactie-universiteit-maastricht-op-rapport-fox-it
https://portswigger.net/daily-swig/ransomware-attack-maastricht-university-pays-out-220-000-to-cybercrooks

PS: Some Members of the Group behind CLOPS have just been been arrested https://www.youtube.com/watch?v=PqGaZgepNTE

Clop Ransomware at Maastricht University

NEWS

Dutch university wins big after Bitcoin ransom returned

Maastricht University has doubled its money thanks to a ransomware attack three years ago. The university plans to help struggling students with its new funds.

Key Points: Current Security Topics

- There are different types of phishing
- Report phishing if you can
- Ransomware is a big Threat
- Malware as a Service

04 – Basic Security

–Vulnerabilities and CVE
–Patching and workarounds
–Security Standards

Vulnerabilities

“A security flaw, glitch, or weakness found in software code that could be exploited by an attacker (threat source).”
(from NIST)

Software is and will most likely never be without flaws

=> Everyone will be affected more or less by vulnerabilities

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.

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

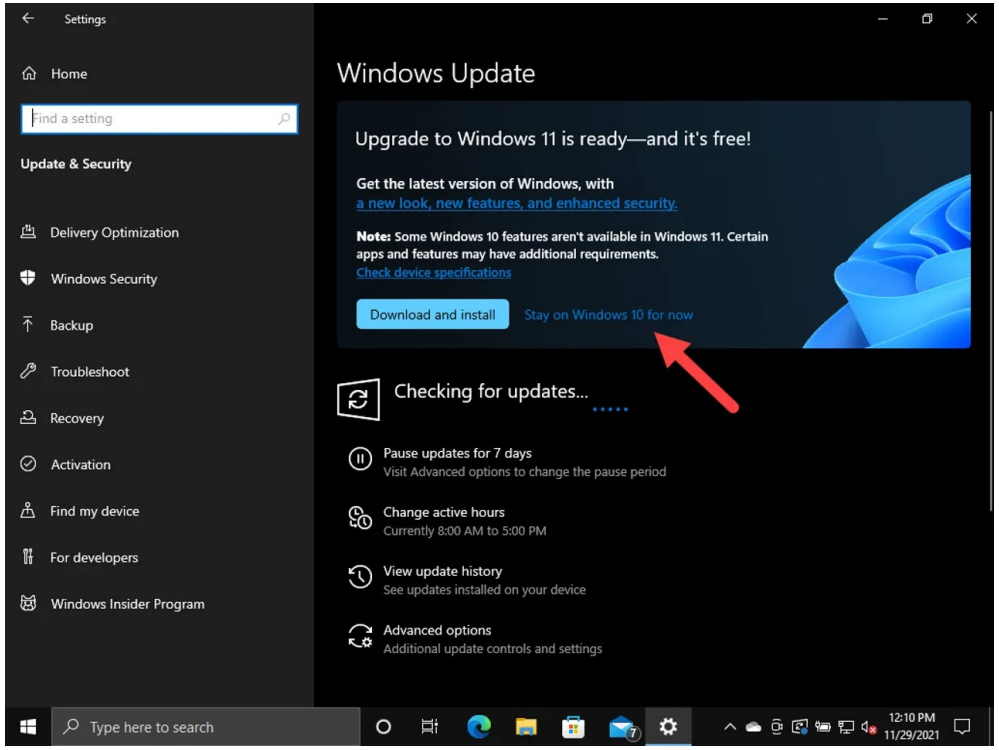
CVE - Tasks

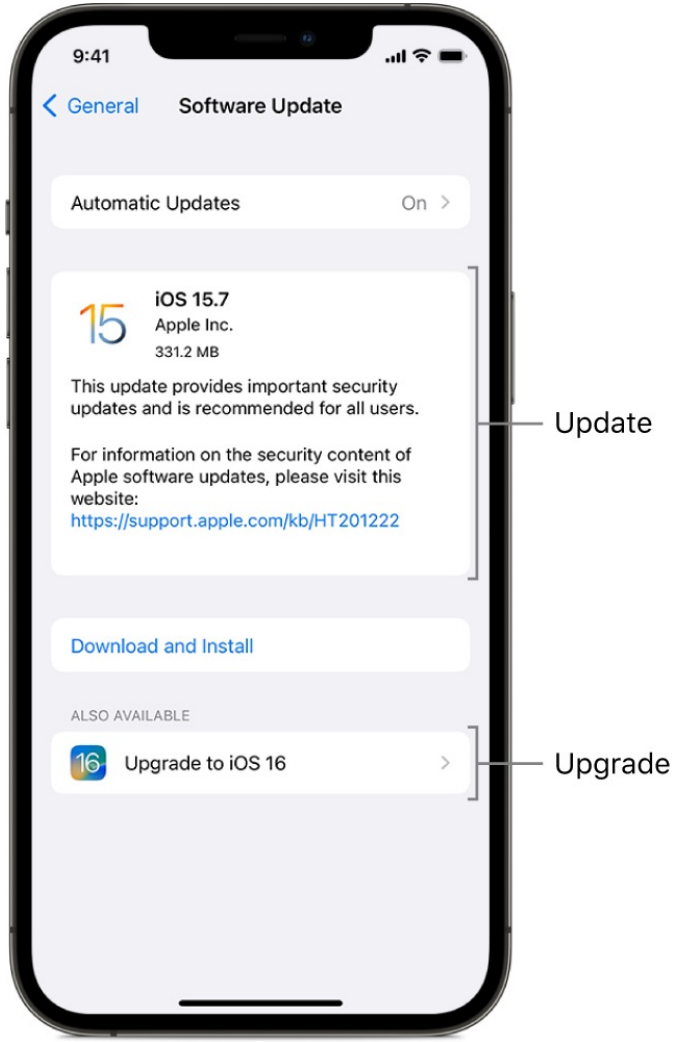
- Visit the CVE dictionary website
- How many CVE records (aka vulnerabilites) are listed in total in the CVE directory?
- Search for all publicly known vulnerabilities for the software SugarCRM.
  - How many records do you find?
  - From which year is the first CVE entry?

Patching and Workarounds

- 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.
- Subscribe to your software vendors Security advisories

Software Update (aka patching) Examples





Patching and Workarounds: Task

- Search for the Debian security mailing advisories (debian-security-announce)
- Locate the Subscribe / Unsubscribe form
- Which date has the latest posting on the debian-security-announce mailing list?

Security Standards

- ICT minimum standard from the BWL
- 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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Created by the «Bundesamt für wirtschaftliche Landesversorgung»

«Each individual business and organisation has a fundamental responsibility to protect itself. However, wherever the functioning of critical infrastructures is affected, the state also has a responsibility, based on its remit as laid down in the Federal Constitution, and on the National Economic Supply Act. This Minimum ICT Standard is an expression of the responsibility of the state to protect its citizens, its economy, and its institutions and public administration.

It is **recommended that operators of critical infrastructures implement this Minimum ICT Standard. This document nonetheless provides any interested business or organisation with a decision-making guide and specific instructions for improving its own ICT resilience.**»

https://www.bwl.admin.ch/bwl/en/home/themen/ikt/ikt_minimalstandard.html

ICT Minimum Standard

3 Sections
– Introductions
– Implementations
– Assessment

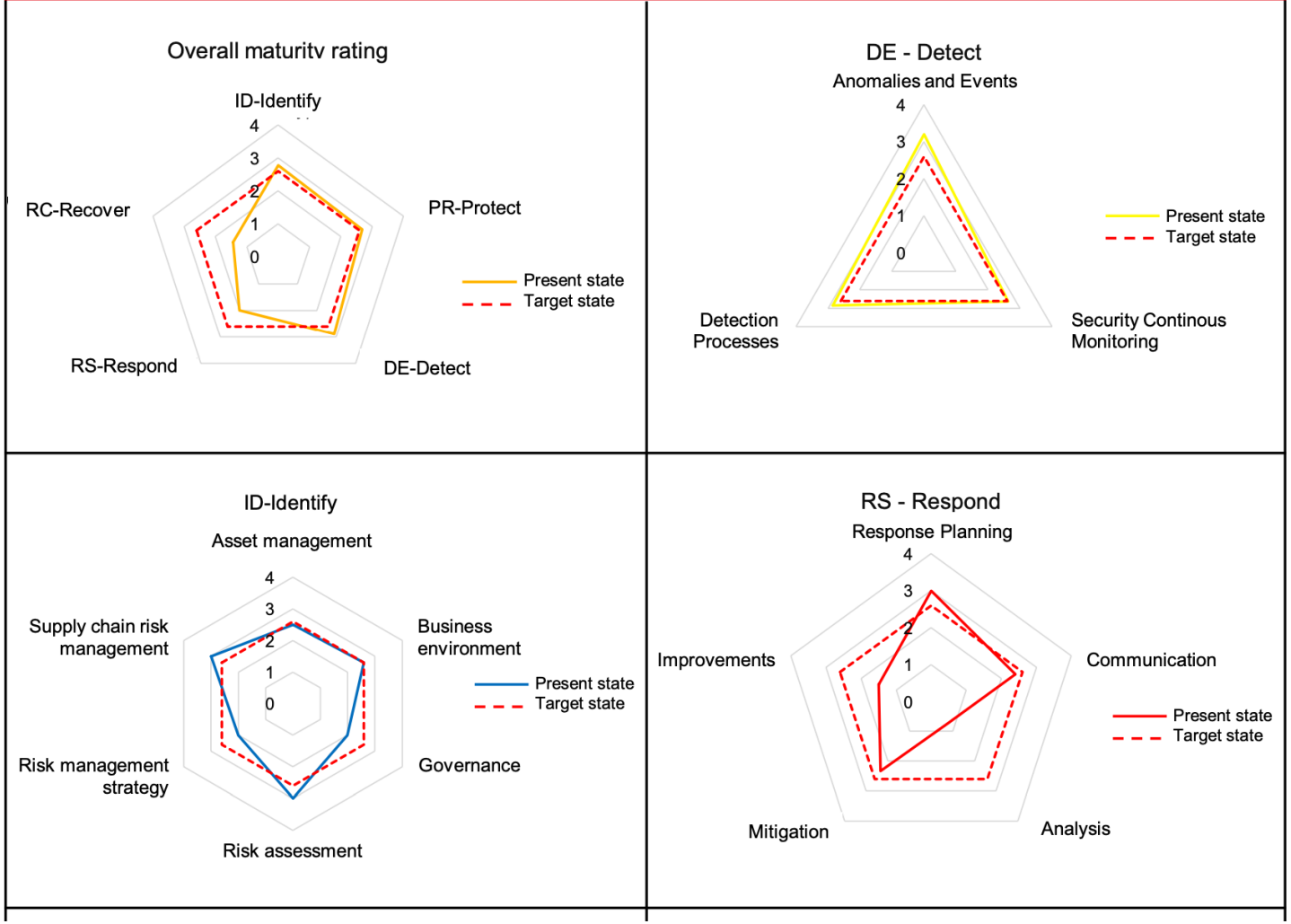
Assessment

Assessment: Define the «Target state» and compare it with the «Current state» of the ICT landscape

2023_IKT-Minimalstandard-Assessment.Tool
https://www.bwl.admin.ch/dam/bwl/en/dokumente/themen/ikt/excelblatt_minimalstandard.xlsx.download.xlsx/2023_IKT-Minimalstandard-Assessment.Tool-1.1-2023_Revision%205_E_D_F_I.xlsx

Assessment

Example of how an assessment is evaluated.



From «Minimum standard for improving ICT resilience»

Standards – 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?

Standards – 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?

Key Points: Basic Security

- Publicly known Security vulnerabilities are collected in CVE dictionaries
- Regularly patch your systems
- Don’t reinvent the weel => Use existing standards as templates and orient yourself to these standards
- The ICT minimum standard is popular is Switzerland

05 – How to react to a Security Incident

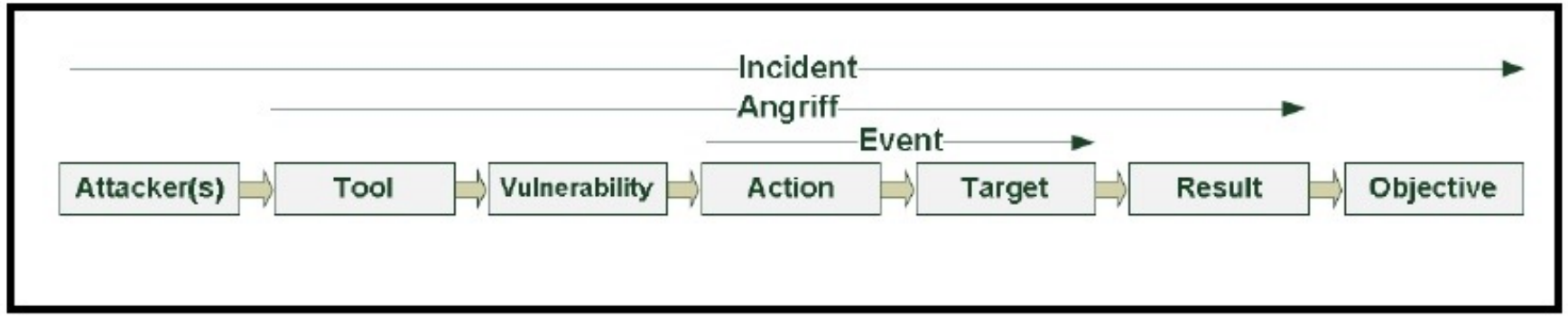
Defintion Security Incident

Ein Ereignis, das tatsächlich oder potenziell die Vertraulichkeit, Integrität oder Verfügbarkeit eines Informationssystems oder der Informationen, die das System verarbeitet, speichert oder überträgt, gefährdet.

Gruppe	Auswirkungen	Beispiele
Major	sehr hoch	DDoS, Ransomware
Moderate	hoch	Trojaner Verteilung, unautorisierte Veränderungen im System
Minor	normal	Spam, Copyright

CERT – Computer Emergency Response Team

Common incident taxonomie



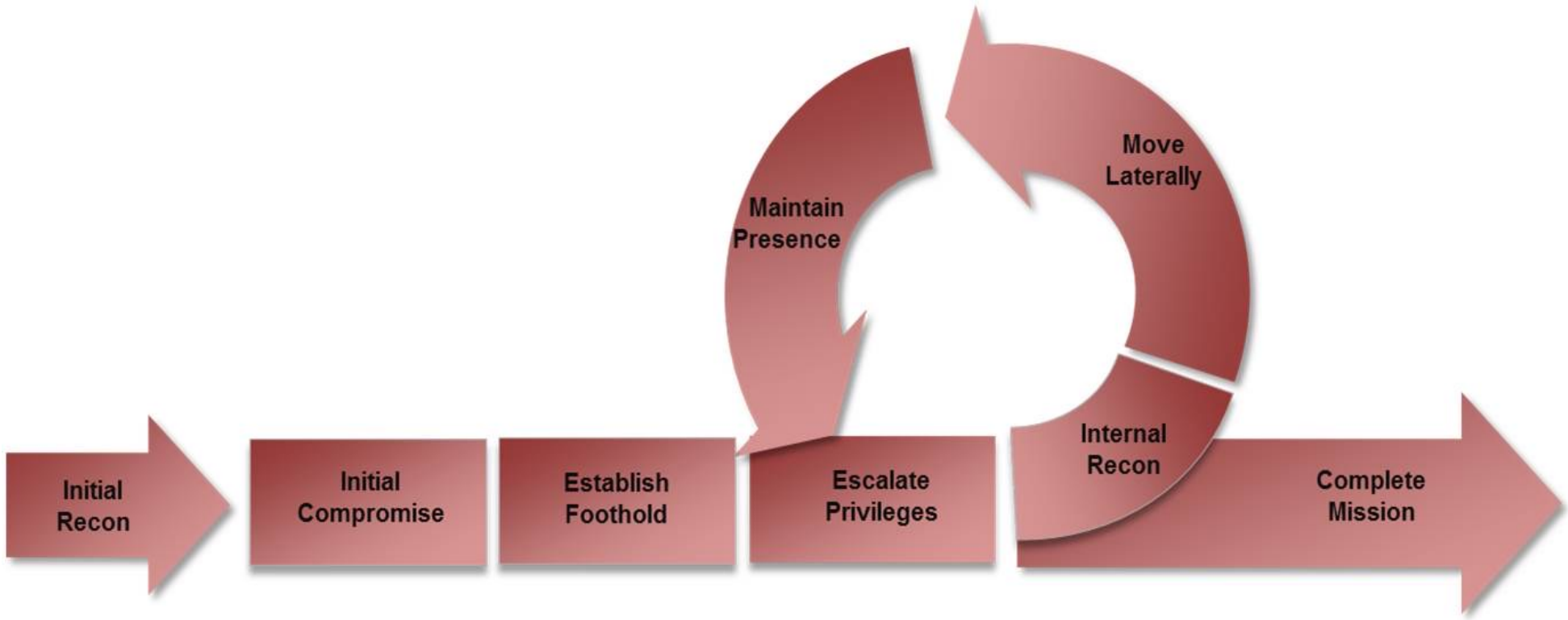
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Classification of information (e.g. TLP)

elastic

MISP
Threat Sharing
https://github.com/MISP/misp-taxonomies/

Cyber attack lifecycle



Phase 1
Initial Access

Phase 2
Lateral Movement & Privilege Escalation
Goal: Domain Admin

Phase 3
Exfiltration of data
Encryption of data
Demand ransom

The 3 Stages

Prevent
- General Rules
- Protection Requirements Analysis
- Defense in Depth

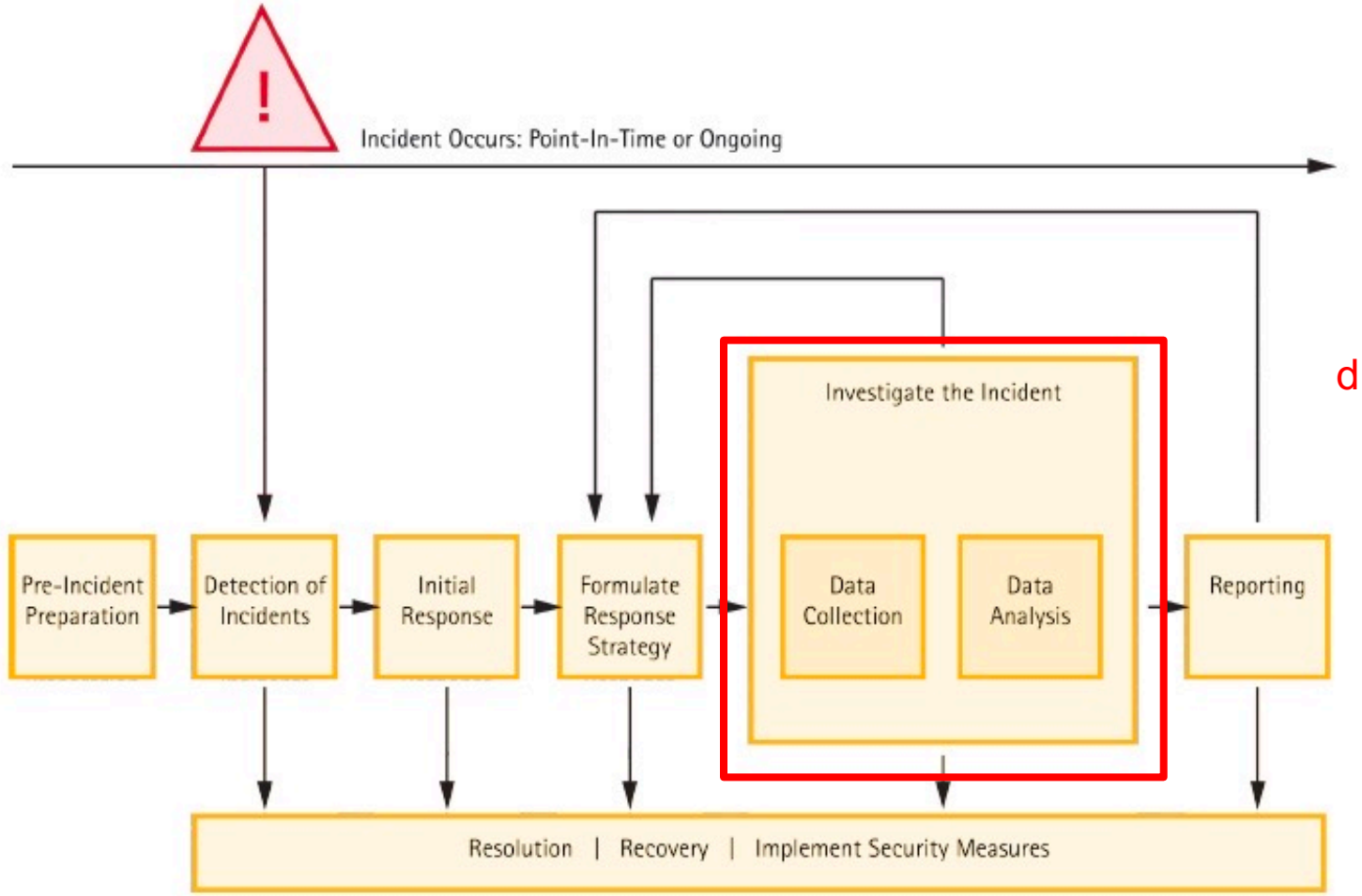
Detect
- Security Monitoring
- Network Monitoring
- Threat Hunting

Respond
- Emergency Response Plan
- Ransomware Playbook

The real costs of an attack

- paying the ransom is only the beginning
- downtime
- reputational damage
- establish new security measures in the organization
- prevention is much cheaper as recovery
- ransomware is always the last step (RaaS)
- the question is not if but when

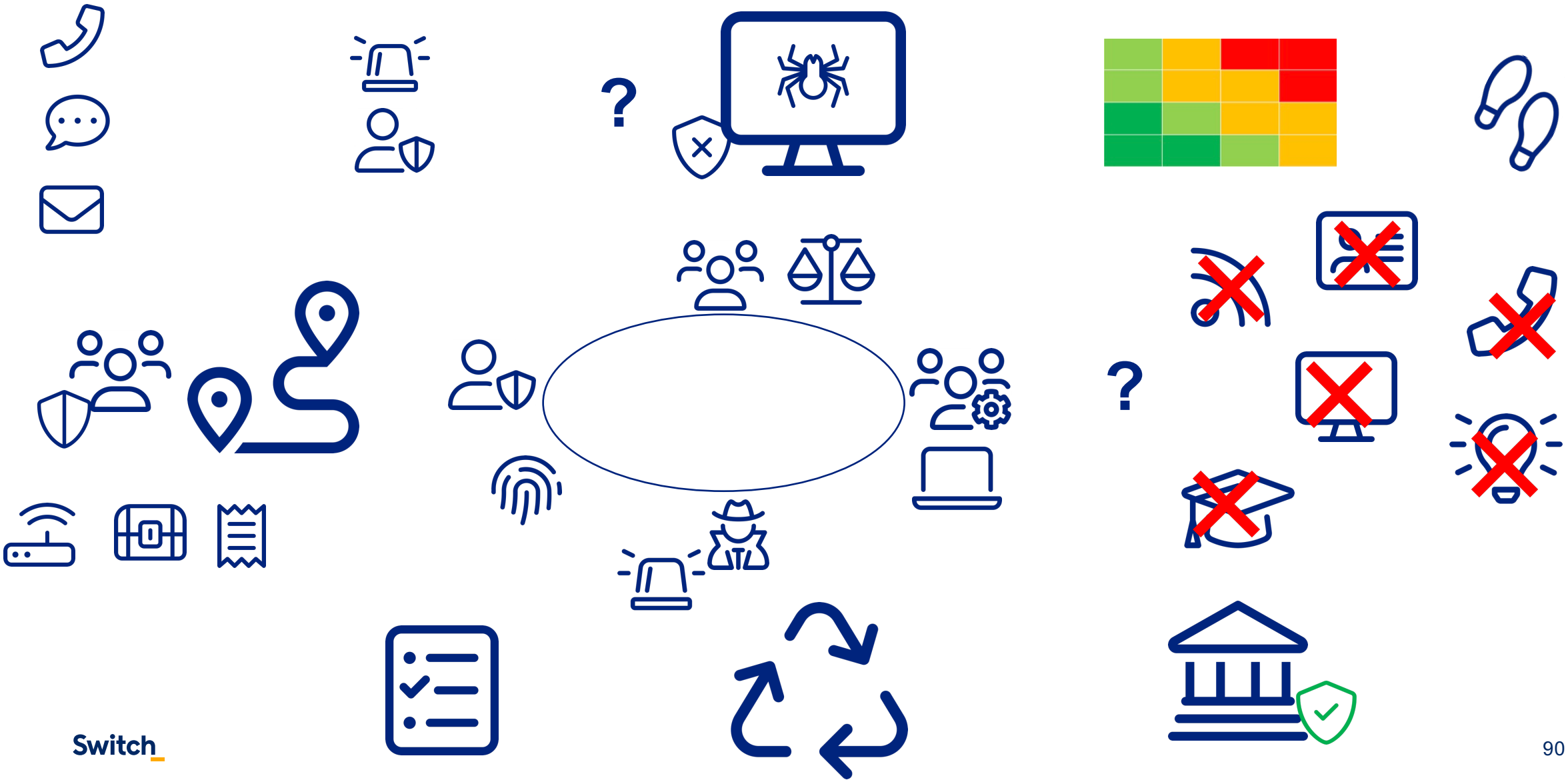
Incident Response Process



digital forensic

Example Incident Response at Switch-CERT

Example Incident Response



How to react to a Security Incident

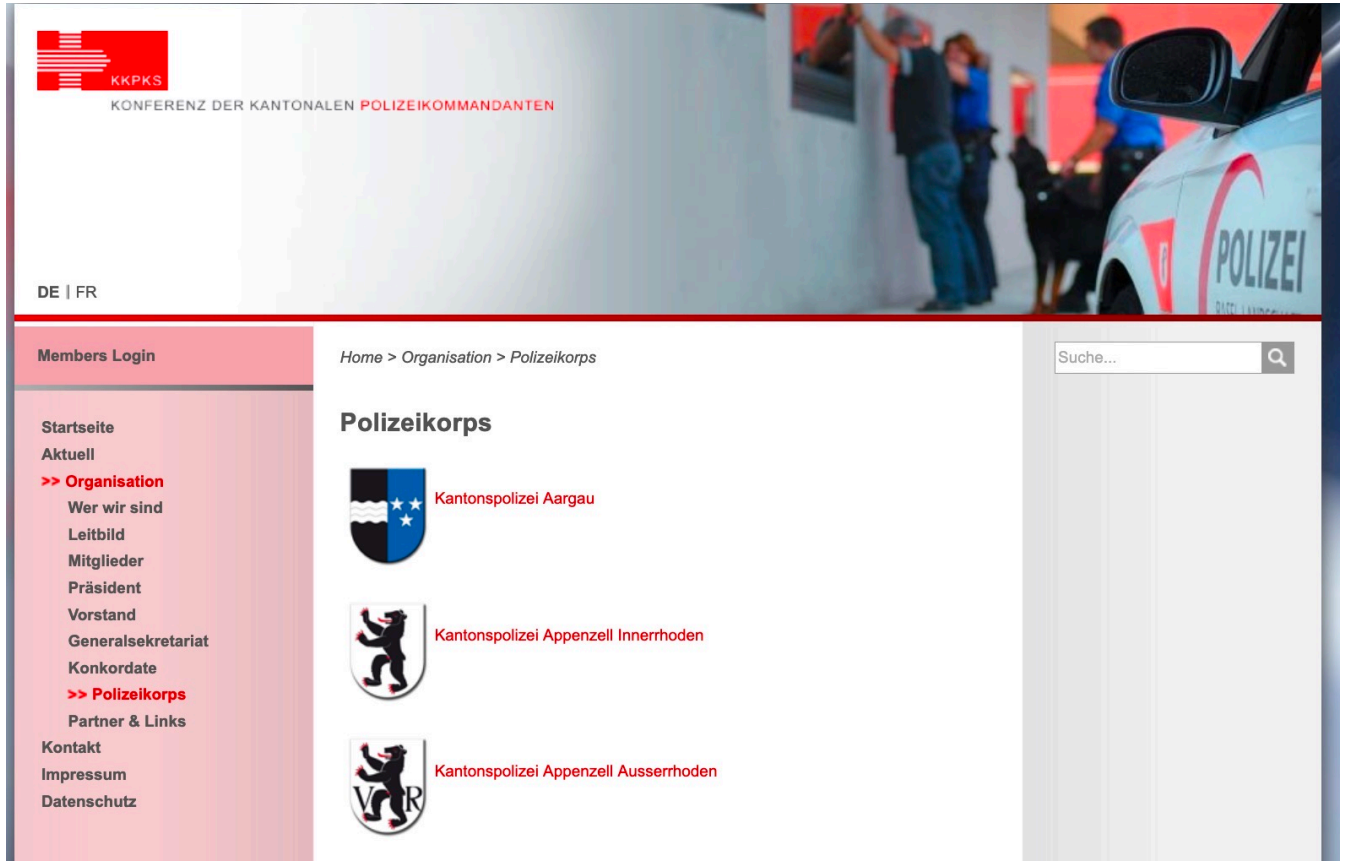
Contact the right person within your organisation
- CISO
- Security Officer, SOC, CERT
- IT department
- CEO, Marketing / Communication

Get external support if necessary
- Incident Response Specialists, Forensic Experts, CERT/CSIRT

Report the Security Incident
- NREN organisations: Switch-CERT (https://www.Switch.ch/security/contact/)
- NCSC(https://www.govcert.admin.ch/report/)

Press charges (against unknown)
- https://www.kkpks.ch/de/organisation/polizeikorps

How to React to a Security Incident



https://www.kkpks.ch/de/organisation/polizeikorps

06 – How to Protect your Assets

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

Information Security

The term “information security” means **protecting information and information systems** from **unauthorized access, use, disclosure, disruption, modification, or destruction** in order to provide
(A) **integrity**, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
(B) **confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
(C) **availability**, which means ensuring timely and reliable access to and use of information.

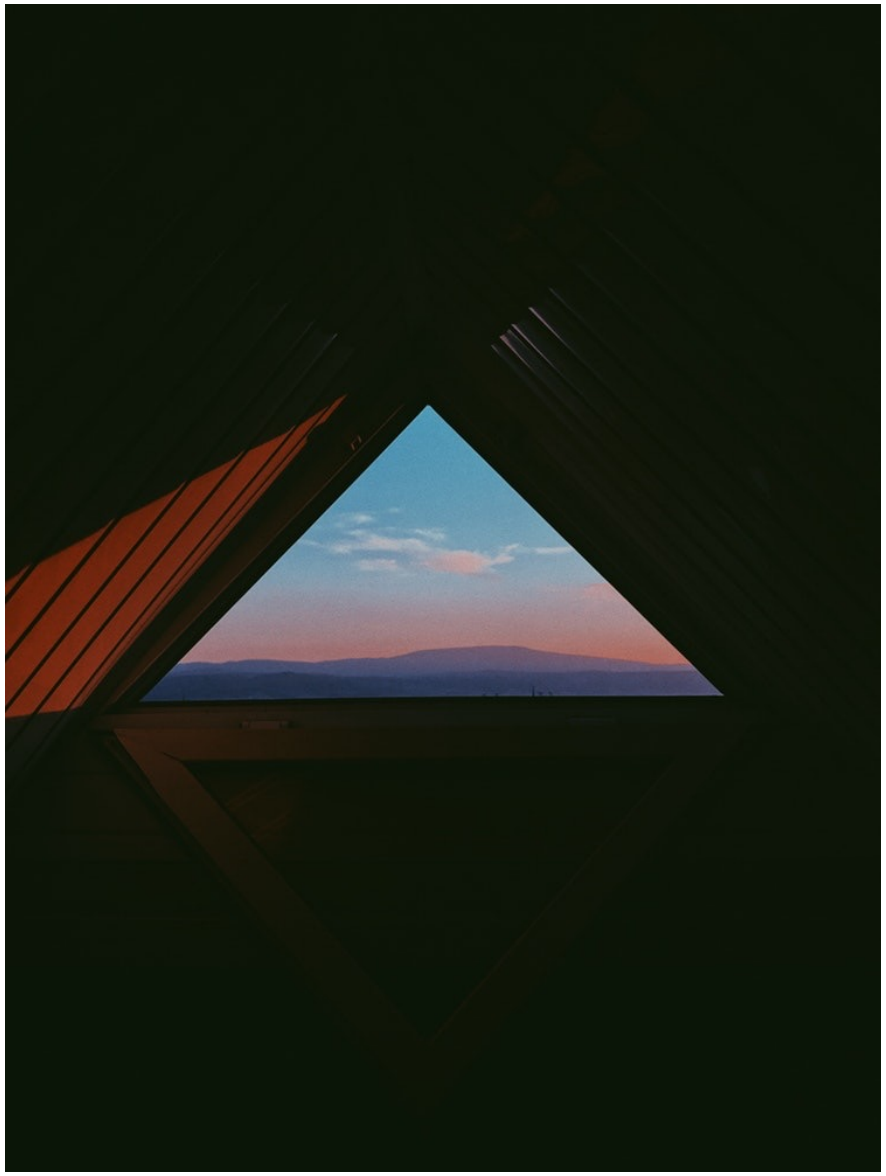
https://www.law.cornell.edu/uscode/text/44/3542

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

The CIA triad

Situation: General hospital and a specialised hospital. A patient has to be transferred to the specialised hospital. All available information from the patient should be transferred from the general hospital to the specialised hospital.

From the CIA point of view:

- **Confidential**: No one except the authorised persons (doctors, medical staff) is able to view the transmitted information.
- **Integrity**: The information is fully transferred and no data has been altered.
- **Availability**: The systems that the doctors / staff will access will be available at all times.

Methods to ensure Confidentiality

- Data encryption and authentication
- Encryption of the data in transit
- Using User IDs, passwords and other methods to access the encrypted data
- Extra measures (extreme form): Air gapped computers, disconnected storage devices hard copy only

Methods used to ensure Integrity

- Maintaining the **consistency**, **accuracy**, and **trustworthiness** of data over its entire life cycle
- Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorised people
  - File permissions and user access controls
  - Version Control Systems (VCS)
- Detect changes
  - Cryptographic checksums

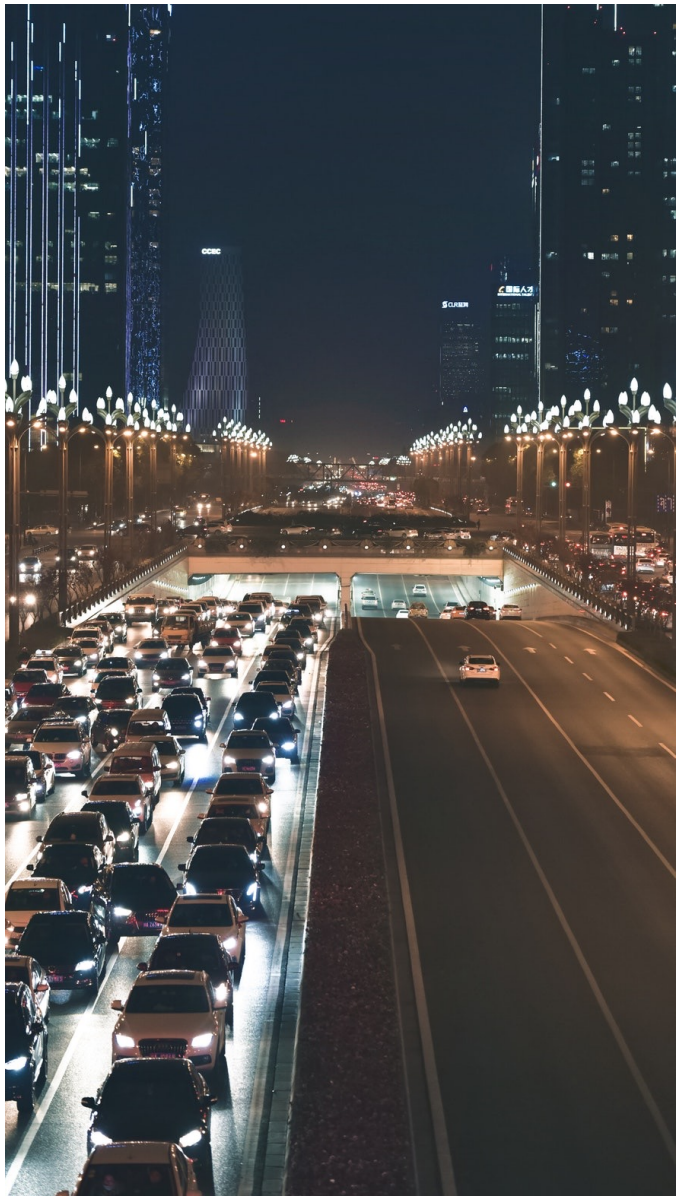
Methods used to ensure Integrity

- **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 all" | 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): The process of determining whether someone or something is who or what it declares itself to be.

- "Are you really person X?"
- Technical methods: Login Form, HTTP authentication, HTTP digest, X.509 certificate, …

Authorisation (What you can do): Decides if you have permission to access a resource

- Methods: Access controls for URLs, Secure objects and methods, Access control lists (ACLs)

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

Multi factor authentication - Examples

Paper: “Evaluating Login Challenges as a Defense Against Account Takeover”

“In this paper, we study the efficacy of **login challenges** at **preventing account takeover** …. These secondary authentication … trigger in response to a suspicious login or account recovery attempt. Using Google as a case study … preventing over 350,000 real-world hijacking attempts stemming from automated bots, phishers, and targeted attackers. We show that knowledge-based challenges prevent as few as 10% of hijacking attempts rooted in phishing and 73% of automated hijacking attempts. **Device-based challenges provide the best protection, blocking over 94% of hijacking attempts rooted in phishing and 100% of automated hijacking attempts**.”

https://ai.google/research/pubs/pub48119

Google’s automatic, proactive hijacking protection

“if we **detect** a **suspicious sign-in attempt** (say, from a new location or device), we’ll ask for **additional proof** that it’s really you. This proof might be confirming you have access to a trusted phone or answering a question where only you know the correct response.“

“If you’ve signed into your phone or set up a recovery phone number, we can provide a similar level of protection to 2-Step Verification via device-based challenges. We found that an **SMS code sent to a recovery phone number helped block 100% of automated bots, 96% of bulk phishing attacks, and 76% of targeted attacks**. **On-device prompts, a more secure replacement for SMS, helped prevent 100% of automated bots, 99% of bulk phishing attacks and 90% of targeted attacks.**“

https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

Google’s automatic, proactive hijacking protection

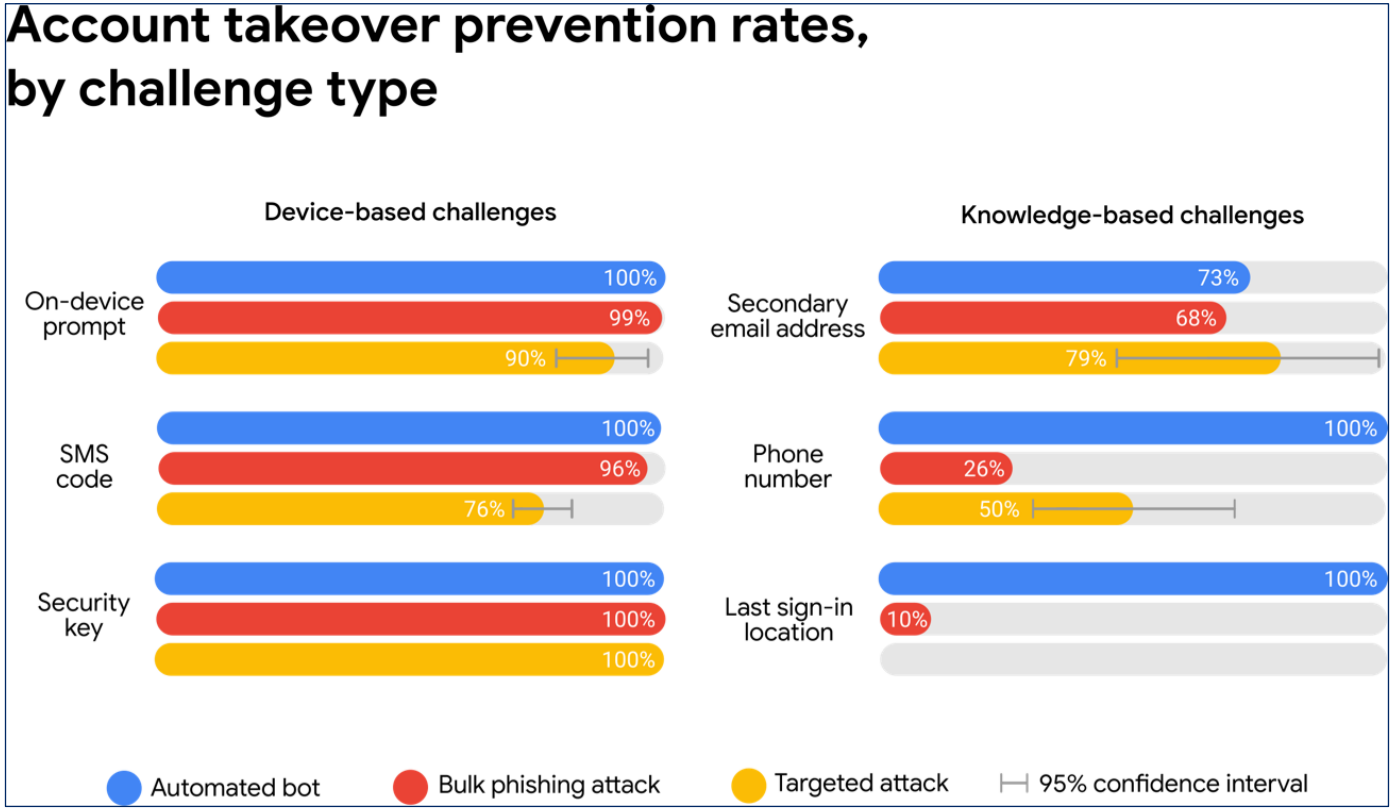


Image Source: https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

Key Points: How to protect your assets

The CIA Triad

Use different factors and more then one to protect you assets

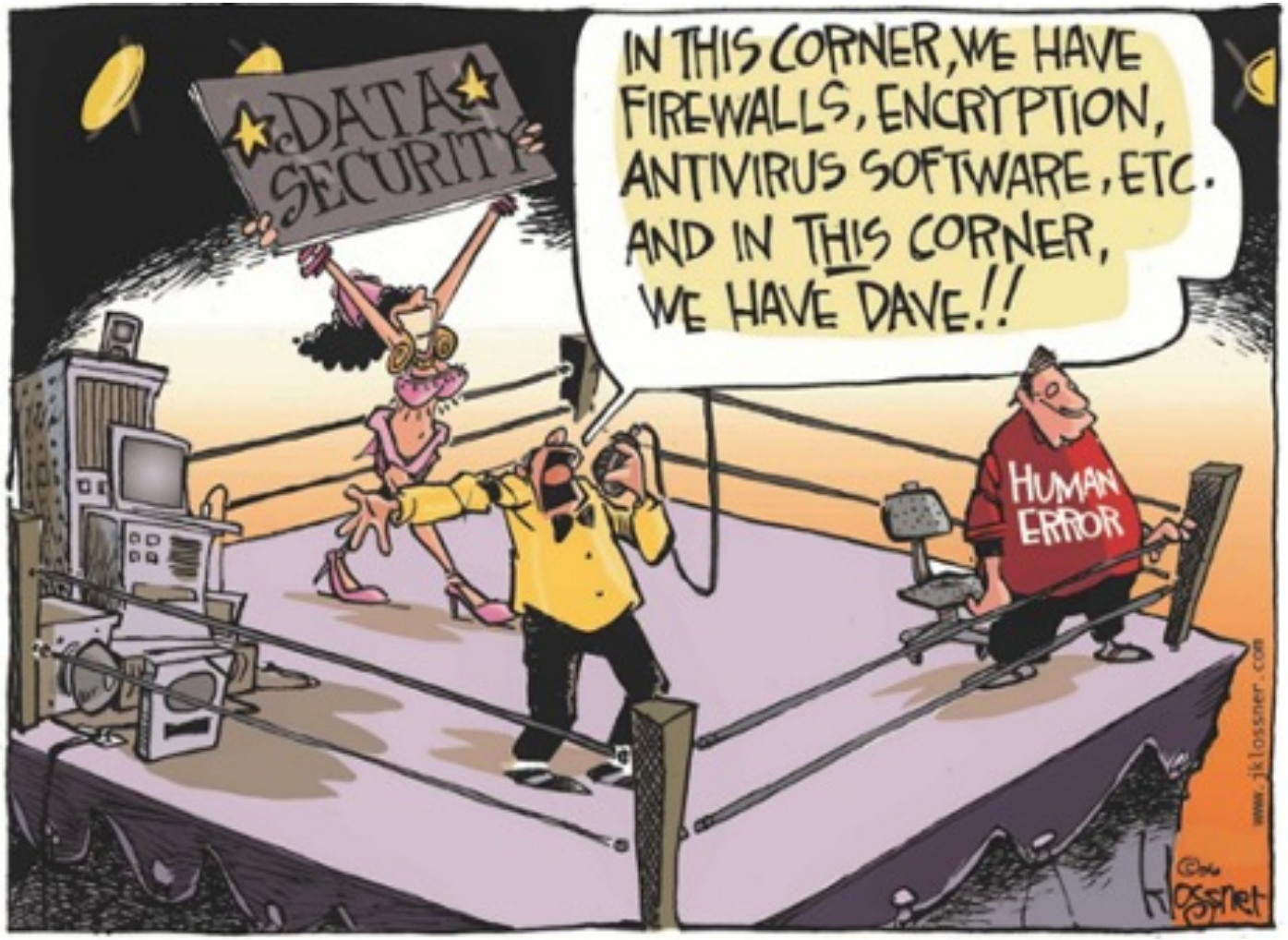
Authentication (Who you are) and Authorisation (What you can do)

07 – Good IT Security Practices

–Awareness
–Passwords

Our Message to you:
You are **the most important link** in the Chain of Security!

The Human Factor



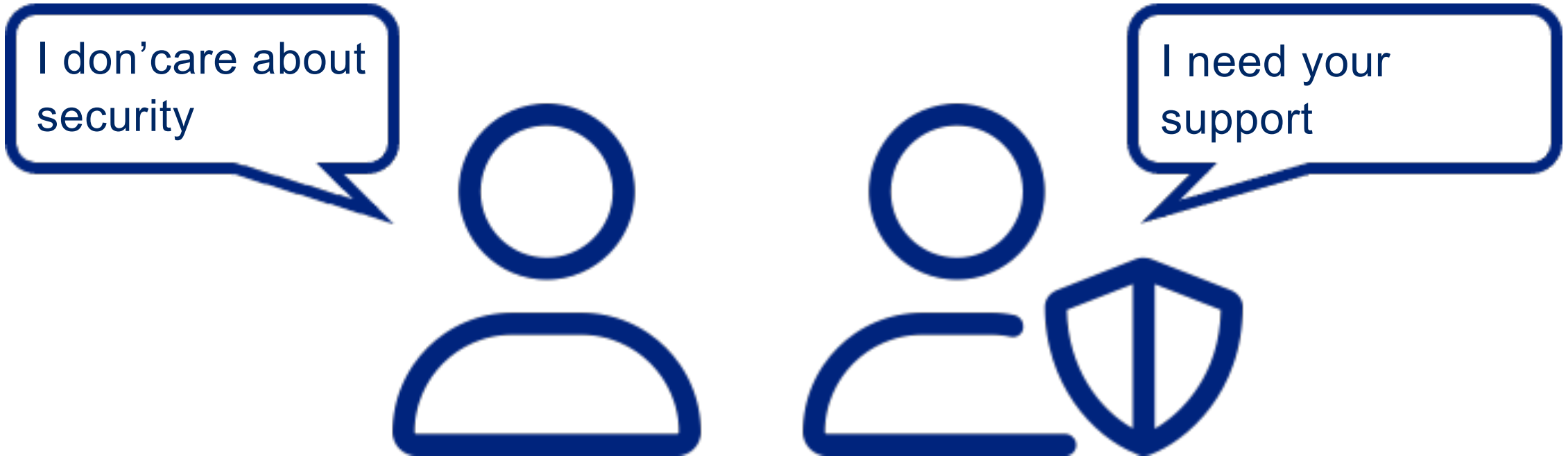
Awareness

Training/Education
Teaching and practising (new) skills and the theory behind them

Awareness
Raise awareness and interest in a particular topic

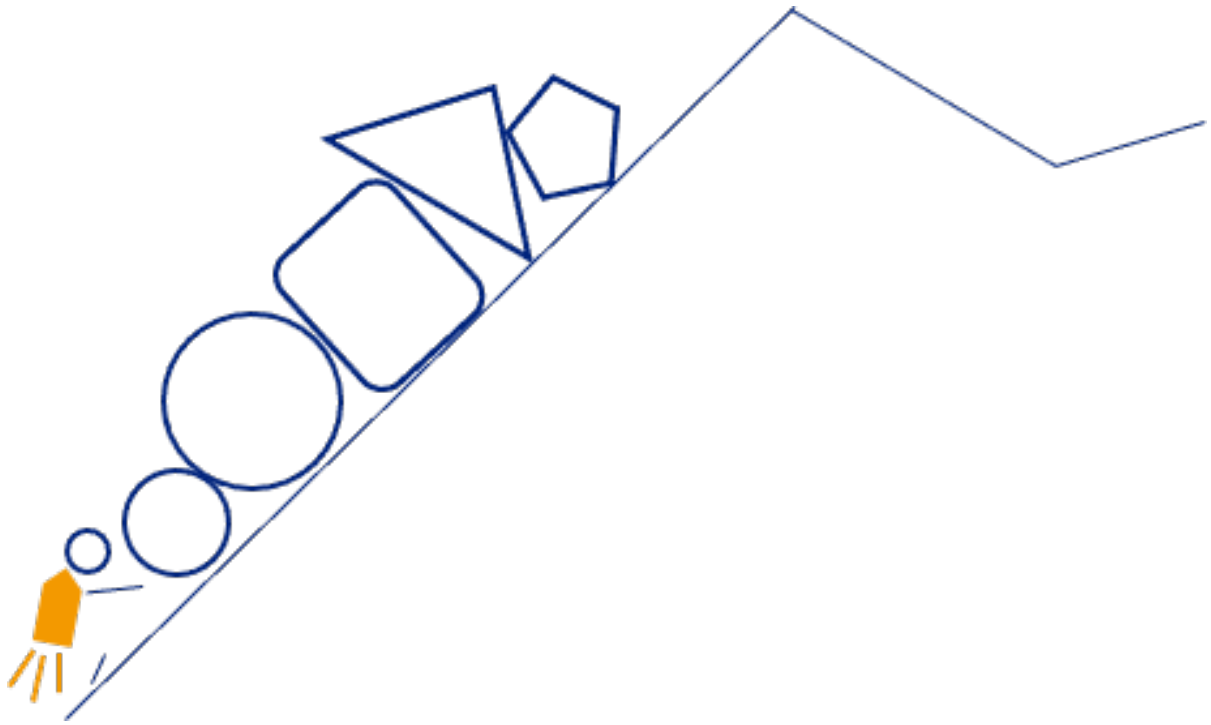
Processes/Tools
Enable and support safe action

Mutual Understanding



Best Practice with Password (NIST Standard)

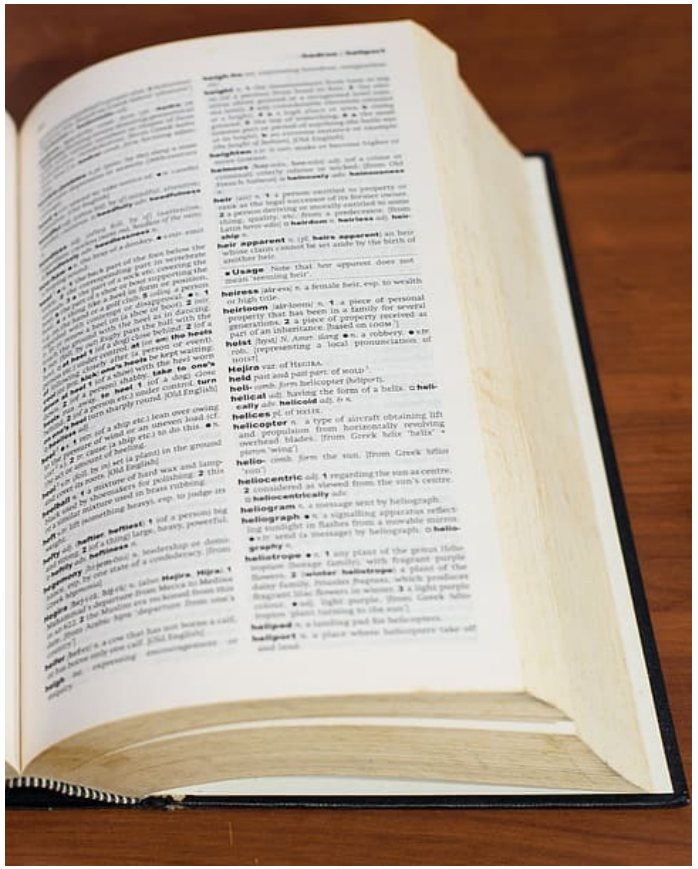
- Use longer, complex passwords
- expiration of passwords
- Unique passwords
- Check compromised passwords
- MFA
- Use a Password Manager!



How attacker find bad passwords

- Passwords are Stored as hashes

- Brute Force
- Dictionary Attack
- Rainbow Tables (precalculated Hashes)
- Rule Based Dictionary | Brute Force



source:
https://securityboulevard.com/2020/05/a-brief-summary-of-nist-password-guidelines/
https://pages.nist.gov/800-63-3/sp800-63b.html

Password Leaks and Checks

Latest Password Leak June 2021 (RockYou2021)
Have i been pwned?

https://haveibeenpwned.com/

Hashcat Hands-on

Responsibility/Criminal Liability/Prosecution

Hacking Article 143bis StGB

- **Unauthorised access to a data processing system**
- **Art. 143bis** [184]

[1] Any person who obtains unauthorised access by means of data transmission equipment to a data processing system that has been specially secured to prevent his access shall be liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty.

[2] Any person who markets or makes accessible passwords, programs or other data that he knows or must assume are intended to be used to commit an offence under paragraph 1 shall be liable to a custodial sentence not exceeding three years or to a monetary penalty.

Responsibility/Criminal Liability/Prosecution

- Damage to data
- Art. 144bis

1. Any person who without authority alters, deletes or renders unusable data that is stored or transmitted electronically or in some other similar way shall be liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty.

If the offender has caused major damage, a custodial sentence of from one to five years may be imposed. The offence is prosecuted ex officio.

2. Any person who manufactures, imports, markets, advertises, offers or otherwise makes accessible programs that he knows or must assume will be used for the purposes described in paragraph 1 above, or provides instructions on the manufacture of such programs shall be liable to a custodial sentence not exceeding three years or to a monetary penalty.

If the offender acts for commercial gain, a custodial sentence of from one to five years may be imposed.

Key Points: Good IT Security Practices

Security is not only a technical problem

You can help your company to be safe

Use a Password-Manager

be aware of your criminal liability

08 – Roundup and Feedback

Please fill out the Feedback form from the University of Bern

Switch_