

# What could possibly go wrong?

## The Human Factor in Cybersecurity

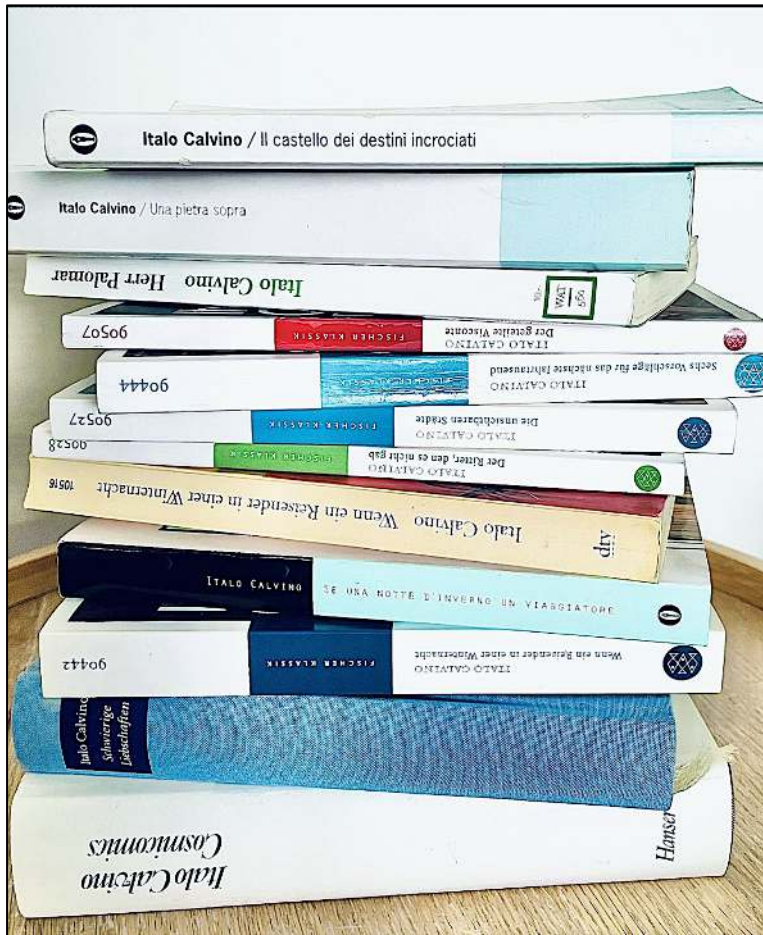
SWITCH

Katja Dörlemann

[katja.doerlemann@switch.ch](mailto:katja.doerlemann@switch.ch)

Online, August 31<sup>st</sup> 2021





*Vulcan's concentration and craftsmanship are needed to record Mercury's adventures and metamorphoses.*

*Mercury's swiftness and mobility are needed to make Vulcan's endless labors become bearers of meaning.*

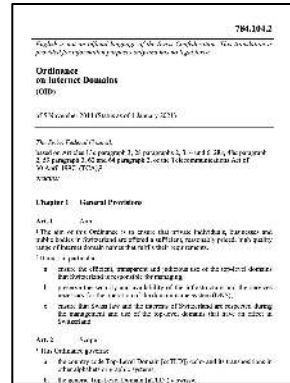
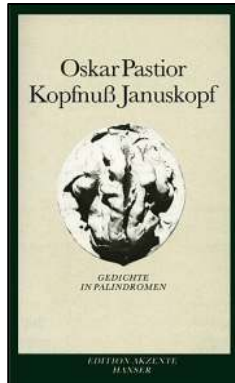
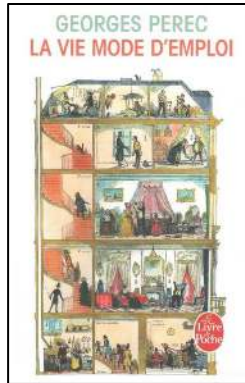
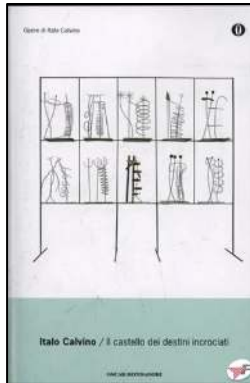
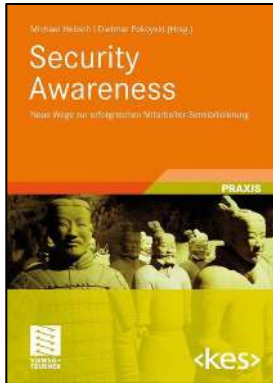
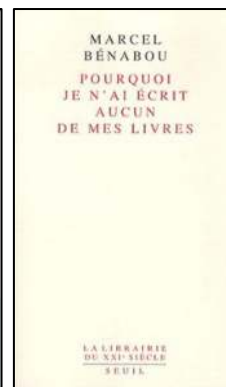
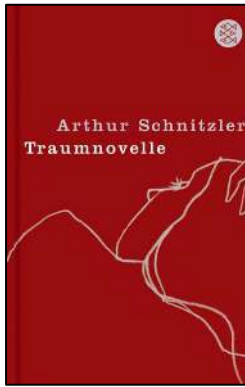
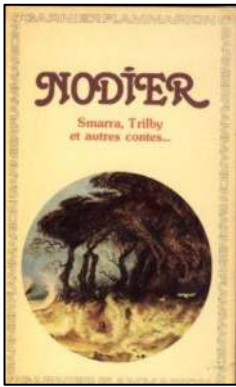
- Italo Calvino, *Genius - Six Memos for the Next Millennium*, 1988



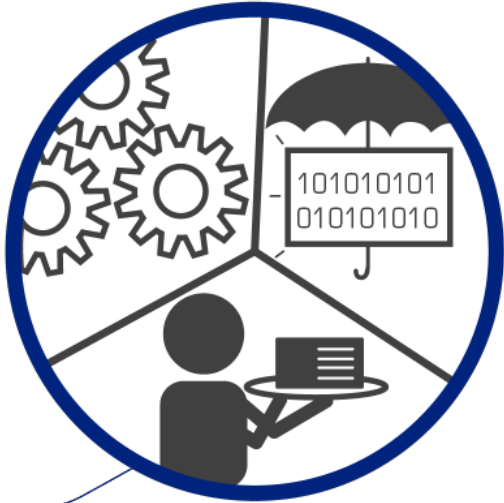
*Vulcan's concentration and craftsmanship are needed to record Mercury's adventures and metamorphoses.*

*Mercury's swiftness and mobility are needed to make Vulcan's endless labors become bearers of meaning.*

- Italo Calvino, *Genius - Six Memos for the Next Millennium*, 1988



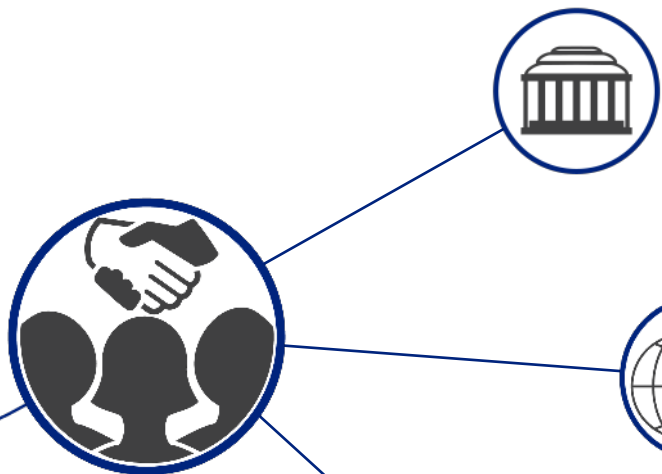
# What we do



**NREN** (National Research and Education Network)

**Registry** for .ch/.li - cc TLDs

# Our customers



## Education, Research & Innovation (ERI) Community

- Swiss universities on tertiary level (academic sector) and their research institutions
- extended ERI community



## Internet Community

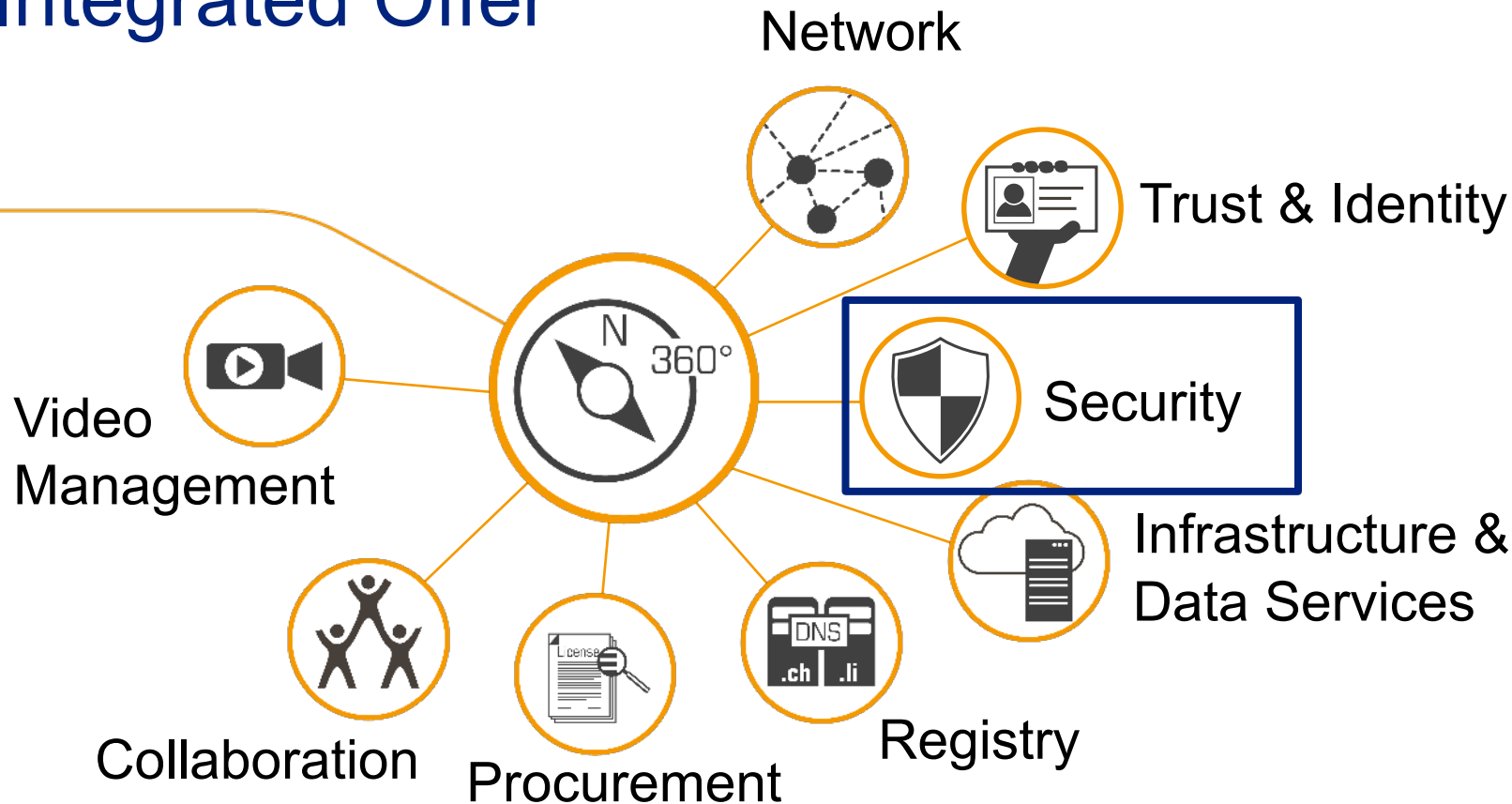
- Internet Service Providers, Hosters, Domain Registrars



## Critical infrastructure organisations (CIO)

- Banking, Industry & Logistics, Energy; Healthcare, Government

# Integrated Offer



# SWITCH-CERT



25 years SWITCH-CERT – information sharing and trusted community

## Customers

- Universities
- Hospitals
- Banks
- Industry & Logistic

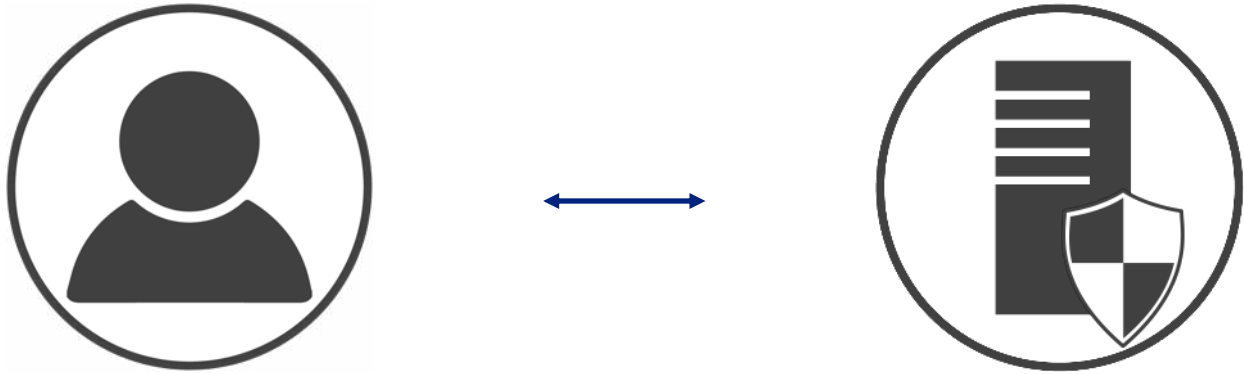
## Services

Cyber Threat Intelligence, Detection, Incident and Response as core competences

## Your benefits

Comprehensive incident support and optimal network security, especially for the Swiss Internet

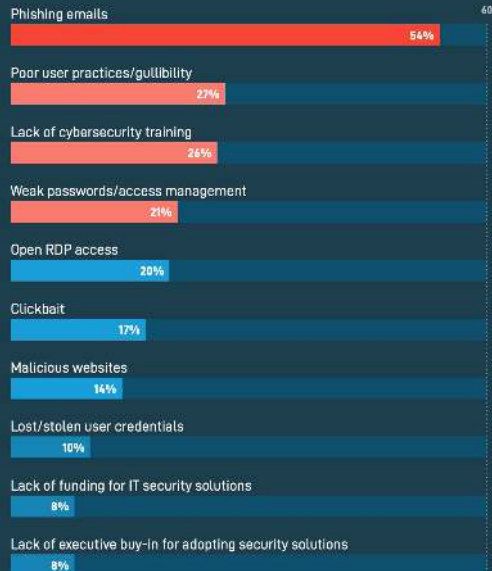




# 11 Biggest cyber security threats in 2021

05/03/2021

## Leading causes of ransomware attacks reported by MSPs:

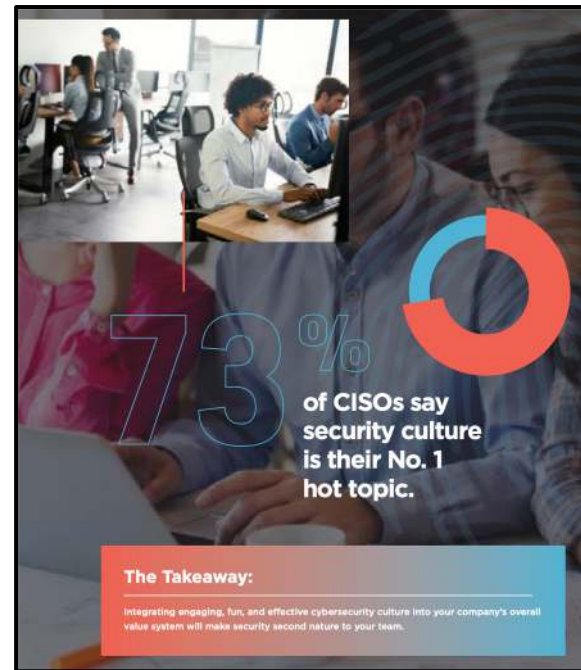


\*Survey respondents were asked to select three answer choices.

Datto Inc, 2020: Dattos Global State of the Channel Ransomware Report.

1. Phishing meets COVID-19
2. Clever ransomware?
3. Polyglot files - Just a .JPG, isn't it?
4. IoT attacks and the growing impact
5. Social engineering and cryptocurrency
6. Malvertising on your Facebook feed
7. Identity theft in COVID-19 times
8. Passwords - Knowledge vs. action
9. Zero-day exploits - The heavy hitter
10. Insider threats - Do you trust your colleague?
11. Deepfakes - Be more data sensitive!

<https://www.gdatasoftware.com/blog/biggest-security-threats-2021>



Livingsecurity 2020: 7 Essential Trends of Human Risk Management For 2021



*I have nothing to hide.*

- All my friends who do not work in Cybersecurity.

Google  
images

cybersecurity



effective cyber security strategy  
information-age.com



Cybersecurity looks to the cloud to ...  
wartails.com



Behavioural aspects of cybersecurity ...  
enisa.europa.eu



EU4Digital: Cybersecurity East | EU4Digital  
nufordigital.eu



Oktober - der Cybersecurity-Magazin ...  
it-daily.net



COVID-19 cyber-attacks: cybersecurity ...  
innovationnewnetwork.com



Cybersecurity Budget Buck ...  
datacenterknowledge.com



cybersecurity Archive - solutions AG  
solutions.ch



Emerging Cybersecurity Trends in 2021 ...  
pandasecurity.com



ABB and IBM partner in cybersecurity ...  
supplychaindigital.com



2020 GCCD Cybersecurity Online Seminar ...  
aicto.org



What is Cybersecurity? - Cisco  
cisco.com



Limits of Cybersecurity ...  
edam.org.tr



Top Cybersecurity Startups from Around the World ...  
gamecdi.com



Cybersecurity | Homeland Security  
dhs.gov



cybersecurity partnership between Togo ...  
esseci.com



Leading Cybersecurity ...  
newroom.cisco.com



Cybersecurity-Überwachung für Schaltanlagen  
indusoft.com



Cybersecurity and Working From Home ...  
whatodays.com



organizations cyber security ...  
bityft.com



Kids Safe Online ...  
vixia.com



Siemens Mobility Global  
mobility.siemens.com



Rail Insider-Technology update ...  
progressivesrailreading.com



PIB | Cyber security  
unpri.org

## Related searches

icon cybersecurity

wallpaper cybersecurity

infographic cybersecurity



Cybersecurity in aviation | EUROCONTROL  
eurocontrol.int



Cyber security spending heading for ...  
information-age.com



How to put cybersecurity at the centre ...  
enisa.europa.eu



Online MBA in Cyber Security - Swiss ...  
asbm.ch



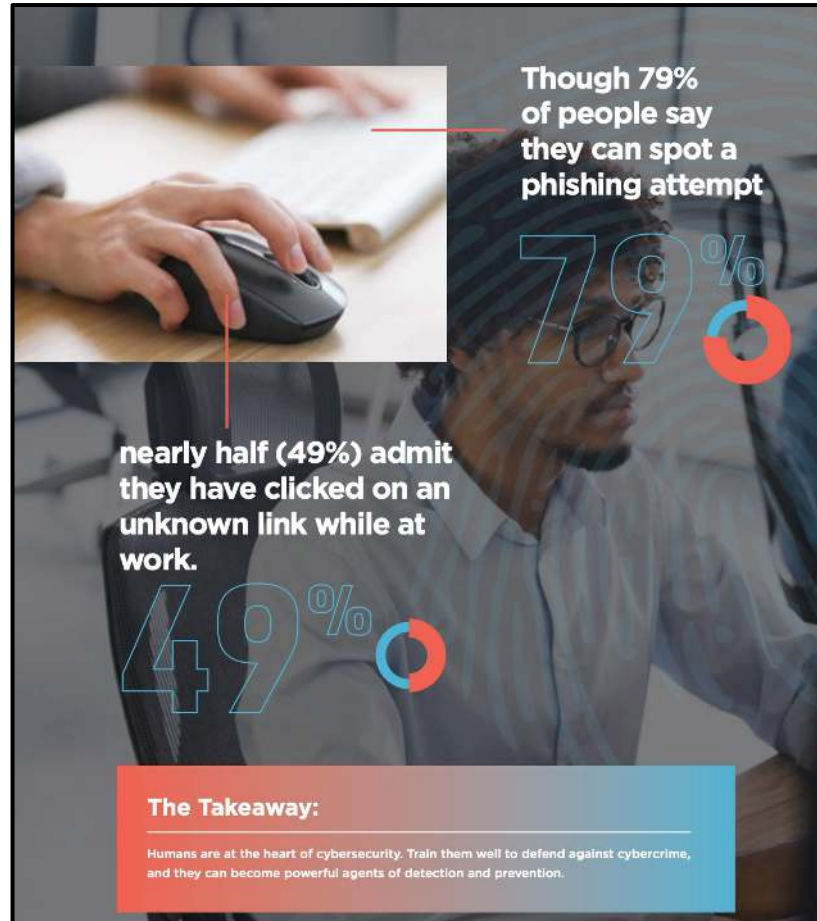
Information Security vs. Cybersecurity ...  
reciprocitylabs.com



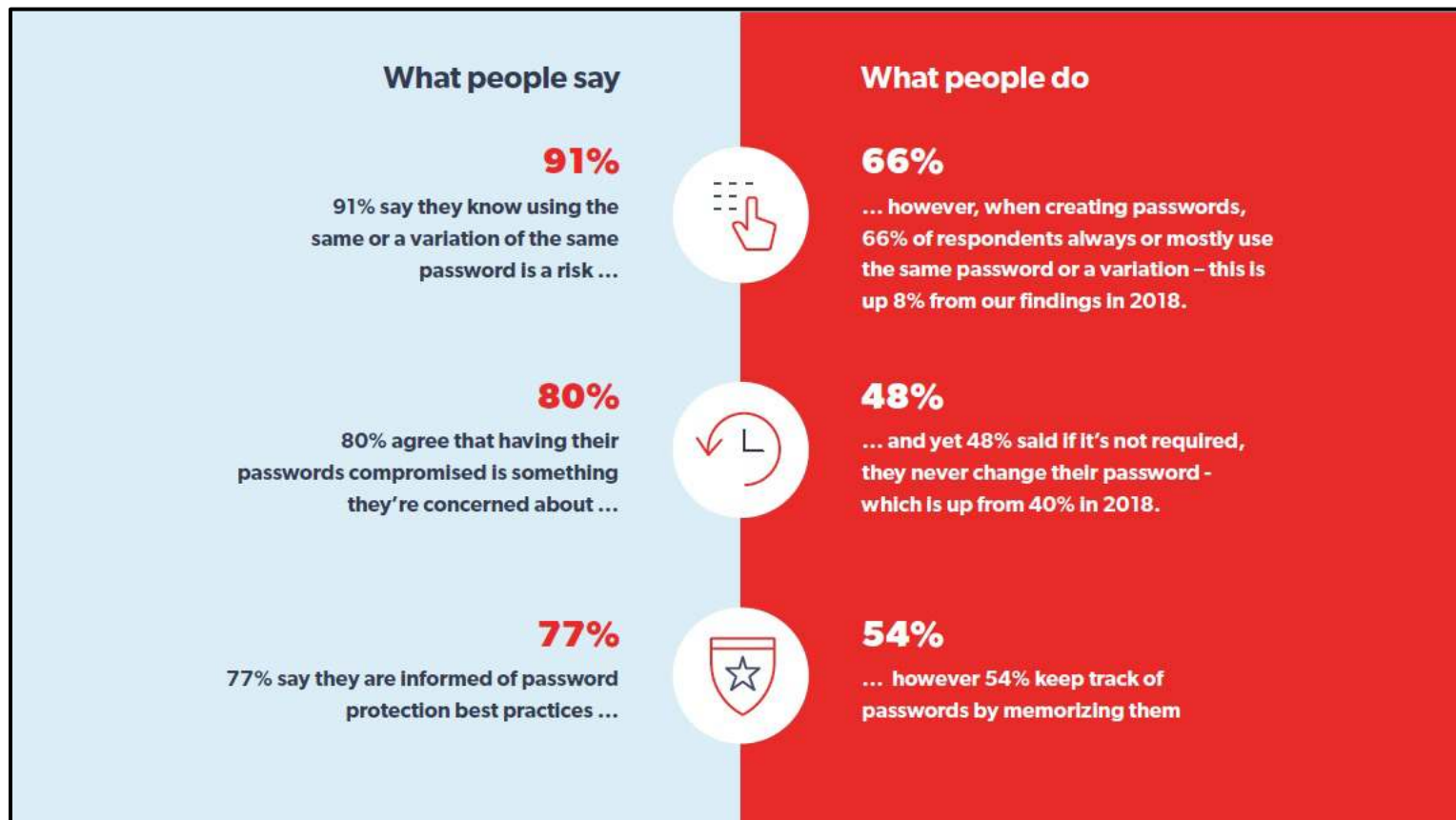
Connectivity & Cybersecurity  
isa.org



Your Single Source for Cybersecurity ...  
softwareone.com



Livingsecurity 2020: 7 Essential Trends of Human Risk Management For 2021



LastPass 2020: Psychology of Passwords: The online Behavior that's putting you at risk

We don't know what we don't know.



We don't care.





*AHHHHHHHHHHHHH!*

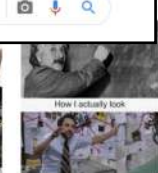
- All my friends who work in Cybersecurity.



Google

Bilder

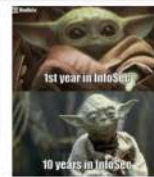
cybersecurity meme

The Cyber Security Hub.com ...  
facebook.comInformation Security meme | Informati...  
pinterest.comTop 10 Cybersecurity ...  
balbix.comThe Cyber Security Hub.com ...  
facebook.comTop 10 Cybersecurity Me...  
balbix.comSeekingFire Consulting  
seekingfire.comFriday meme #meme #...  
twitter.comThe Best and Funniest Security Memes ...  
cybersecurity.att.comTop 10 Cybersecurity M...  
balbix.comLA Creative Tech on Twitter: "It be ...  
twitter.comThe Cyber Security Hub.com ...  
facebook.comCybersecurity Memes ...  
wattpad.comAdvanced Cybersecurity Package ...  
the20.comWhat is cybersecurity? ...  
archerint.comCyber Security: meme  
reddit.comCyber Security | Meme...  
pinterest.comNew Cyber Security Meme Memes...  
me.meCyber Security Awareness Month ...  
medium.comCyber Security Memes For All...  
memes.comCyber Security Memes For All You ...  
memes.comTGF #CyberSecurity #SQL Thank...  
twitter.com4 Tricks to Make a Cybersecurity ...  
digitalshadows.comBest 30+ Cybersecurity fun on 9GAG  
9gag.comto Cybersecurity for Bu...  
amazon.comEvery threat is an opportunity....  
9gag.com

Google

Bilder

cybersecurity meme

The Cyber Security Hub.com ...  
facebook.comInformation Security meme | Informati...  
pinterest.comTop 10 Cybersecurity ...  
balbix.comThe Cyber Security Hub.com ...  
facebook.comTop 10 Cybersecurity Me...  
balbix.comSeekingfire Consulting  
seekingfire.comFriday meme #meme #...  
twitter.comThe Best and Funniest Security Memes ...  
cybersecurity.att.comTop 10 Cybersecurity M...  
balbix.comLA Creative Tech on Twitter: "It be ...  
twitter.comThe Cyber Security Hub.com ...  
facebook.comCybersecurity Memes ...  
wattpad.comAdvanced Cybersecurity Package ...  
the20.comWhat is cybersecurity? ...  
archerint.comCyber Security: meme ...  
reddit.comCyber Security | Meme...  
pinterest.comNew Cyber Security Meme Memes...  
me.meCyber Security Awareness Month ...  
medium.comCyber Security Memes For All...  
memes.comCyber Security Memes For All You ...  
memes.comTGIF #CyberSecurity #SQL Thank...  
twitter.com4 Tricks to Make a Cybersecurity ...  
digitalshadows.comBest 30+ Cybersecurity fun on 9GAG  
9gag.comto Cybersecurity for Bu...  
amazon.comEvery threat is an opportunity....  
9gag.com

USER WITH LOCAL ADMIN RIGHTS APPEARS FROM ATTACHMENT



The cybersecurity program you're forced to run on your current budget



HOW DOES ONE "ACCIDENTALLY"



THAT MAKES ME EVEN GRUMPIER.



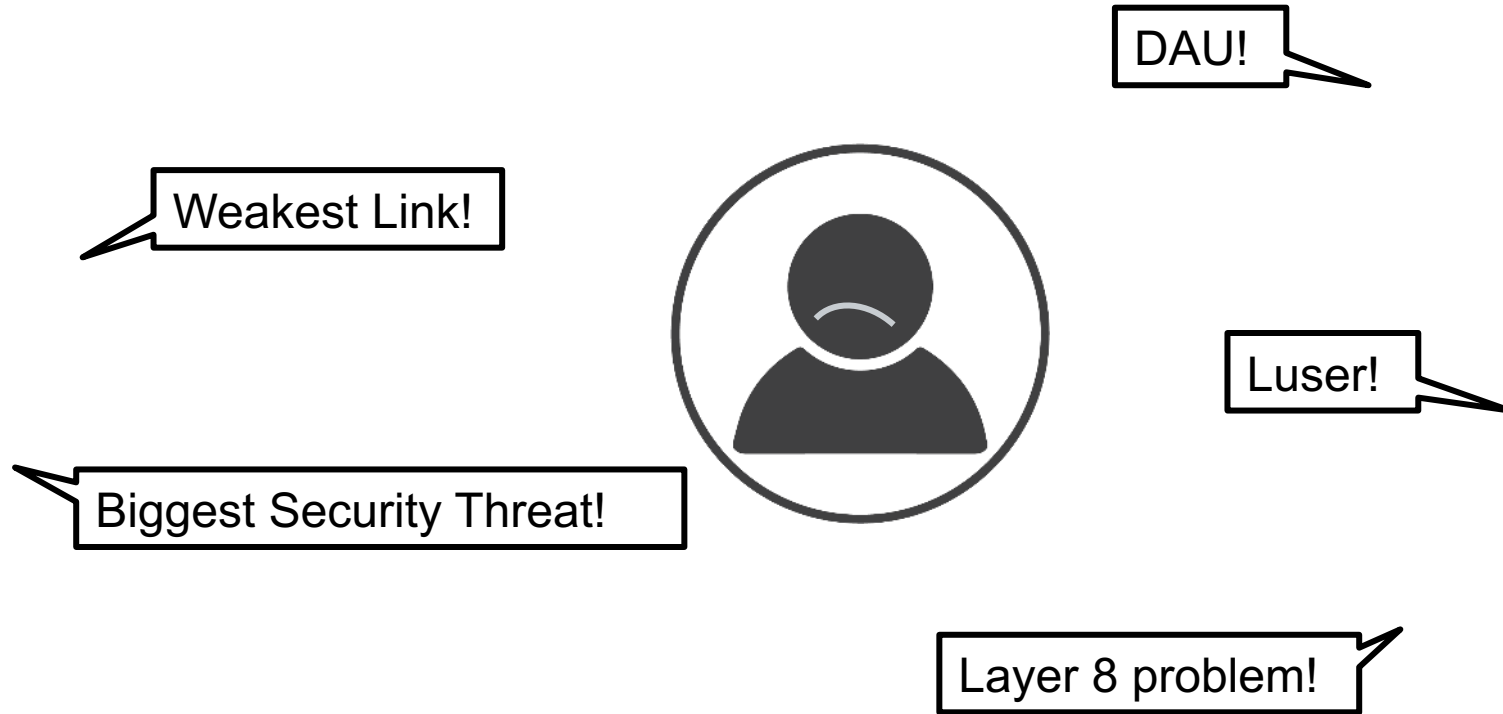
THAT MAKES ME EVEN GRUMPIER.



THAT MAKES ME EVEN GRUMPIER.



# Shaming the human factor



# SECURITY AWARENESS



# Security Awareness ...

## **ISO 27000:2016:**

...“is [one of the] fundamental principles [that] contribute to the successful implementation of an ISMS”.

## **OECD Guidelines for the Security of Information Systems and Networks:**

...“is the first line of defence for the security of information systems and networks.”

## **NIST SP800-50:**

...“program explains proper rules of behavior for the use of agency IT systems and information. [...] it starts with awareness, builds to training, and evolves into education.”

## **wikipedia:**

...“is the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization.”

# Security Awareness ...

## ISO 27000:2016:

...“is [one of the] **fundamental** principles [that] contribute to the successful implementation of an ISMS”.

## NIST SP800-50:

...“program explains proper rules of behavior for the use of agency IT systems and information. [...] it starts with **awareness**, builds to **training**, and evolves into **education**.”

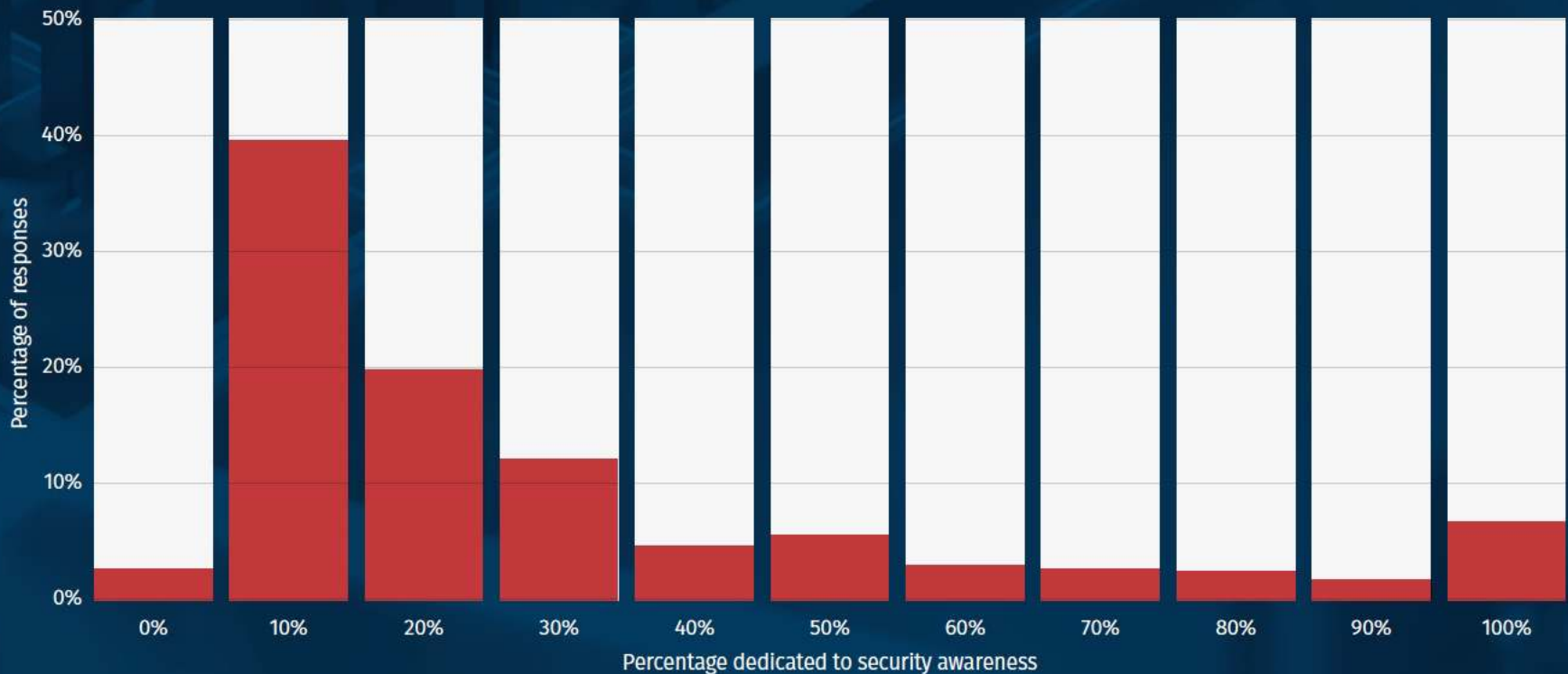
## OECD Guidelines for the Security of Information Systems and Networks:

...“is the **first line of defence** for the security of information systems and networks.”

## wikipedia:

...“is the **knowledge and attitude** members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization.”

## Percentage of Time Spent on Security Awareness



SANS: 2021 Security Awareness Report. Managing Human Cyber Risk

# Security Awareness ...

## ISO 27000:2016:

...“is [one of the] **fundamental** principles [that] contribute to the successful implementation of an ISMS”.

## NIST SP800-50:

...“program explains proper rules of behavior for the use of agency IT systems and information. [...] it starts with **awareness**, builds to **training**, and evolves into **education**.”

## OECD Guidelines for the Security of Information Systems and Networks:

...“is the **first line of defence** for the security of information systems and networks.”

## wikipedia:

...“is the **knowledge and attitude** members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization.”



**EDUCATION**

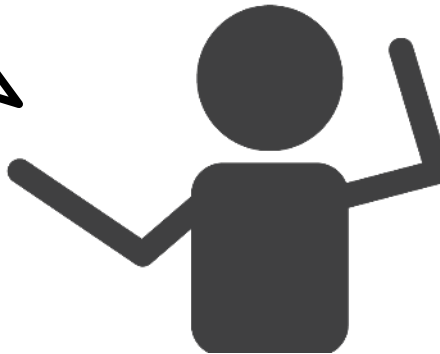
Learning new skills  
and the theory  
behind them

**AWARENESS**

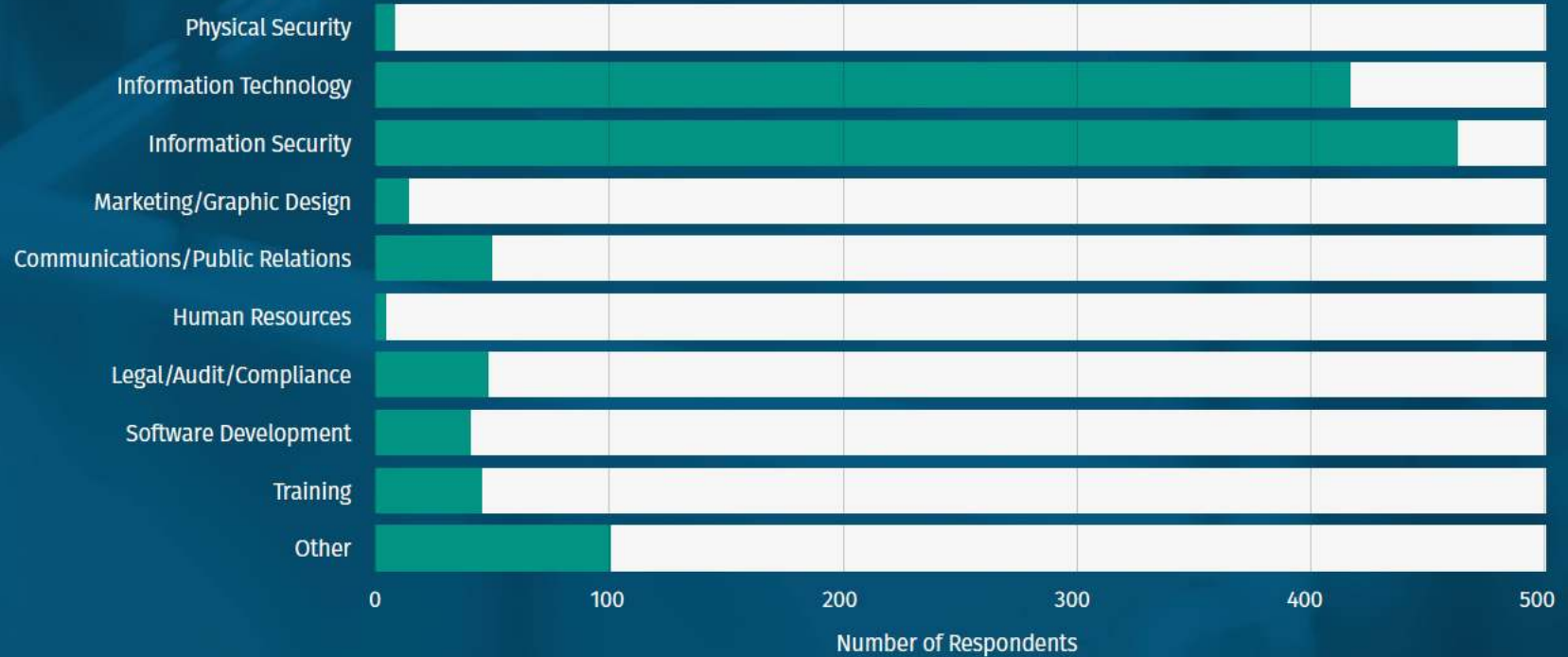
Raising awareness of and  
interest in a special topic

**TRAINING**

Learning and training  
(new) skills



## Backgrounds of Security Awareness Professionals



ETH zürich

EPFL

## Master in Cyber Security

Joint program EPFL-ETHZ

## CORE COURSES

252-0463-00L	Security Engineering	autumn	7
252-1414-00L	System Security	autumn	7
263-4640-00L	Network Security	autumn	8
263-4660-00L	Applied Cryptography	spring	8

## CORE ELECTIVES

252-0811-00L	Applied Security Laboratory	autumn	8
252-1411-00L	Security of Wireless Networks	autumn	6
227-0575-00L	Advanced Topics in Communication Networks	autumn	6
227-0579-00L	Hardware Security	autumn	6
252-0408-00L	Cryptographic Protocols	spring	6
263-2925-00L	Program Analysis for System Security + Reliability	spring	6
263-4600-00L	Formal Methods for Information Security	spring	5
263-4656-00L	Digital Signatures	spring	4

## SEMINAR

at least 2

252-4601-00L	Current Topics in Information Security	autumn	2
263-4651-00L	Current Topics in Cryptography	spring	2

## SEMESTER PROJECT

12

260-0100-00L	Semester Project		12
--------------	------------------	--	----

## INTER FOCUS COURSES

16

263-0006-00L	Advanced Systems Lab	spring	8
263-0007-00L	Algorithms Lab	autumn	8
263-0008-00L	Computational Intelligence Lab	spring	8
263-0009-00L	Information Security Lab	autumn	8

Lucerne University of  
Applied Sciences and ArtsHOCHSCHULE  
LUZERN

**Bachelor in Information and Cyber Security** A field of activity with great potential

## Kernmodule

- Algorithmen & Datenstrukturen
- Betriebssysteme & Sicherheit
- Computer & Network Architecture
- Datenbanksysteme
- Datenschutz
- Diskrete Mathematik
- Ethik
- Information Security Fundamentals
- Information Security Lab
- Management of Information Security
- Objektorientierte Programmierung
- Security Requirement Engineering
- Web-Technologien



# CAS Angewandte IT-Sicherheit

Modul "Security Architecture and Management"

Modul "Cryptography and Network Security"

Modul "Software and Systems Security"



## CAS Cyber Security Expert

Consists of the following modules

- ISO/IEC 27001 Foundation
- ISO/IEC 27001 Foundation in ISMS Exam
- Cyber Security – Implement Network and System Security («P3S»)
- Cyber Security Tester – Hands-on Foundation («HAK»)
- Cyber Security Tester – Hands-on Professional («HAK2»)
- Cyber Security Tester – Hands-on Advanced («HAK3»)
- OSSTMM Professional Security Tester Fast Track («BPST»)
- Secure Web Development («SWO»)
- Exam Preparation



## MASTER IT-SICHERHEIT / NETZE UND SYSTEME PO 13

### Pflicht Module

Name

Betriebssystemssicherheit

Diskrete Mathematik

Einführung in die Kryptographie 1

Netzicherheit 1

Rechnerarchitektur

Einführung in die Kryptographie 2

Einführung in die theoretische Informatik

Netzicherheit 2

Kryptographie

Summe

### Cybersecurity Team Roles

Real-world team role allocation in cybersecurity aligns closely with what current professionals describe as ideal.

■ Current Average Percentage of Cybersecurity Team Roles  
■ Ideal Average Percentage of Cybersecurity Team Roles



### Top Cybersecurity Skills Needed

Cybersecurity professionals plan to develop their skills across multiple areas over the next two years, with 40% specifically naming cloud computing security as an area of focus.



We don't have the expertise.



We don't have the time.

Cybersecurity needs...

...more **interdisciplinarity**.



# Let's imagine...





*If you want people to do something, make it easy.*

– Richard Thaler, Professor of Behavioral Science and Economics at the University of Chicago Booth School of Business

# What's the message?



**allow vs. forbid**



# How to protect our data?

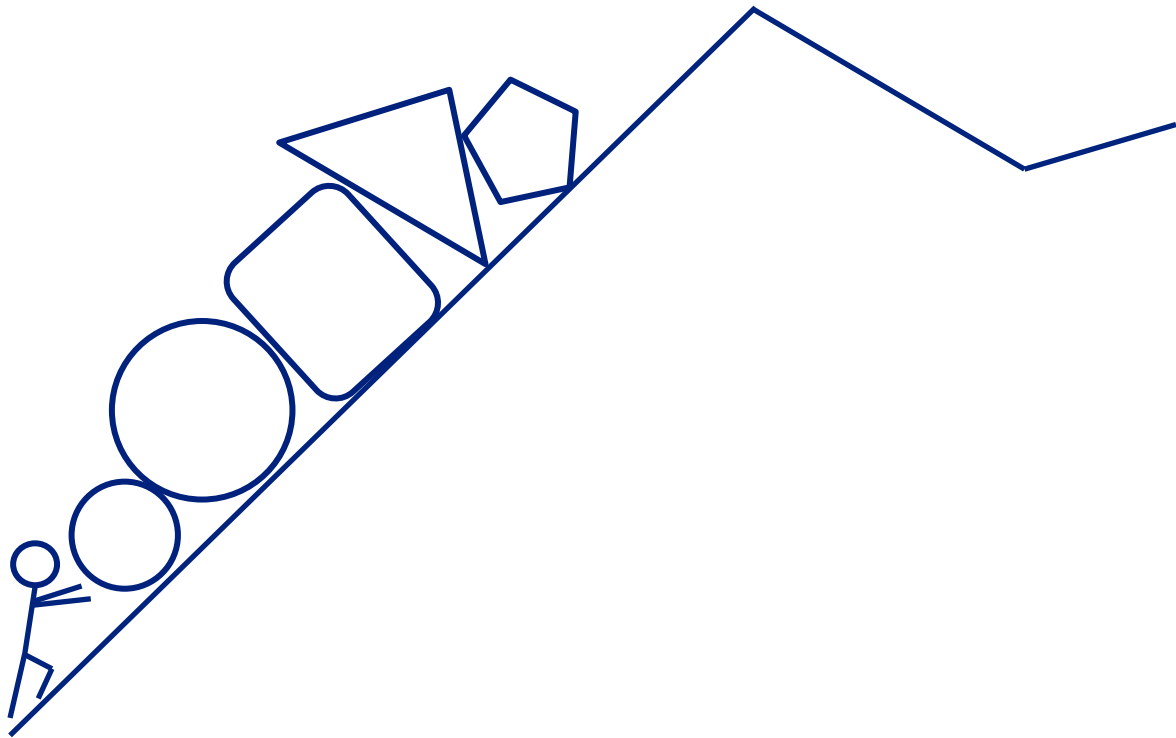
Passwords

Complex passwords

Regular password change

Unique passwords

MFA



# How to protect our data?

Passwords

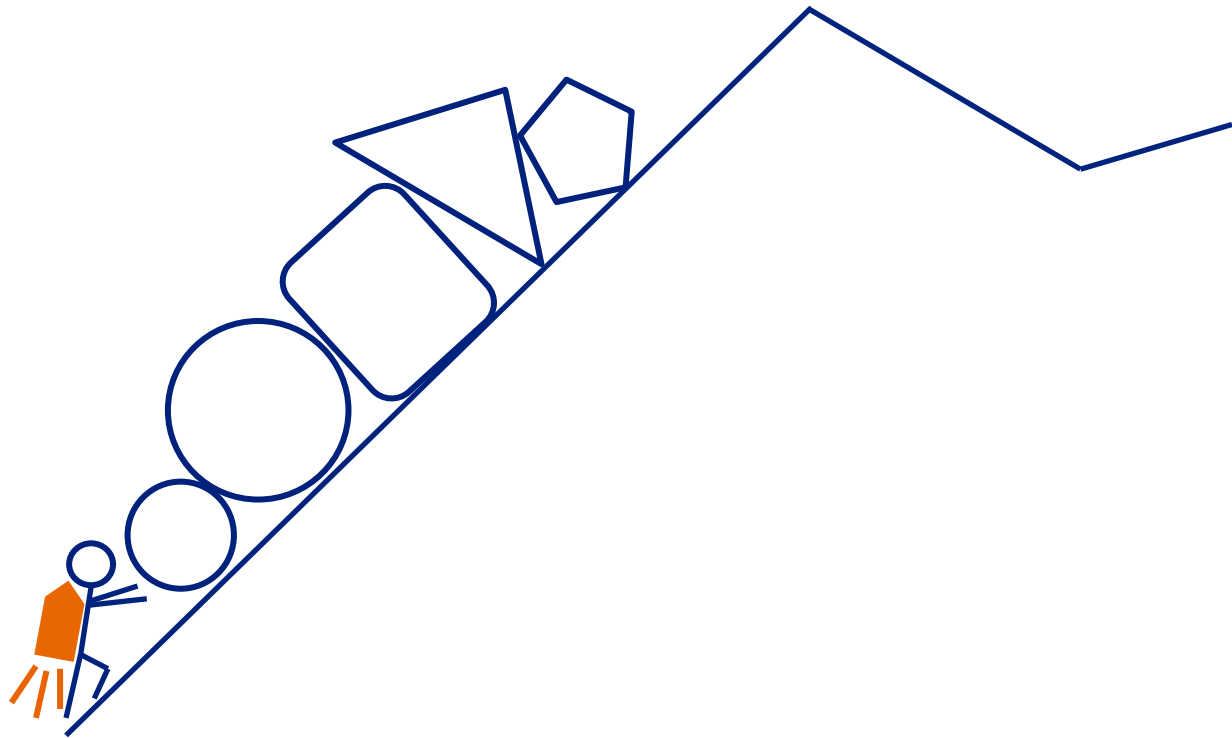
Complex passwords

Regular password change

Unique passwords

MFA

Password manager/vault



# Is it 2FA? MFA?

	English	German	French	Italian
<b>Facebook</b>	Two-factor authentication	Zweistufige Authentifizierung	Authentification à deux facteurs	Autenticazione a due fattori
<b>Twitter</b>	Two-factor authentication	Zwei-Faktor-Authentifizierung	Authentification à deux facteurs	Autenticazione a due fattori
<b>LinkedIn</b>	Two-step verification	Zweistufige Authentifizierung	Vérification en deux étapes	Verifica in due passaggi
<b>Instagram</b>	Two-Factor Authentication	Zweistufige Authentifizierung	Authentification à deux facteurs	Autenticazione a due fattori
<b>Google</b>	2-Step Verification	Bestätigung in zwei Schritten	Validation en deux étapes	Verifica in due passaggi
<b>Wordpress</b>	Wordfence Login Security (2FA)	Wordfence Login Security (2FA)	Wordfence Login Security (2FA)	Wordfence Login Security (2FA)
<b>eduID</b>	Two-Step Login	Two-Step Login	Authentification en deux étapes	Login in due passaggi
<b>NCSC</b>	two-factor authentication	Zwei-Faktor Authentifizierung	Authentification forte (à deux facteurs)	Autenticazione a due fattori

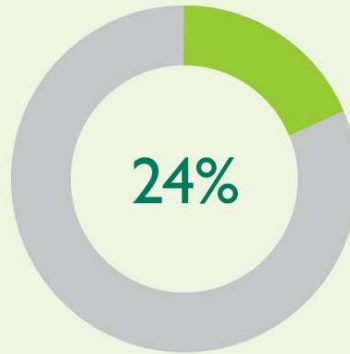
# Where are the security settings?

<b>LinkedIn</b>	Settings & Privacy   Sign in & Security   Account Access   Two-step verification
<b>Facebook</b>	Settings and Privacy   Settings   Security and login   Two-factor authentication
<b>Instagram</b>	Settings   Privacy and Security   Two-Factor Authentication
<b>Twitter</b>	More   Security and Account access   Security   Two-factor authentication

## Women at Work in Cybersecurity

With a more accurate approach to surveying the cybersecurity workforce, (ISC)<sup>2</sup> found that nearly one quarter of respondents to our workforce study were female.

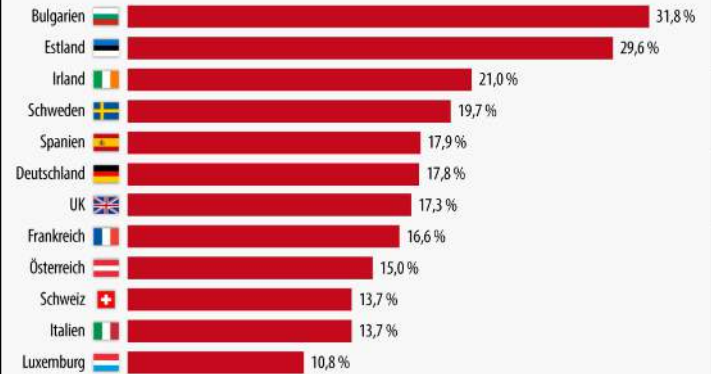
■ Women ■ Men



<https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx>

## IKT-Fachleute sind europaweit meist Männer

Frauenanteil an den beschäftigten IKT-Fachleuten pro Land 2014



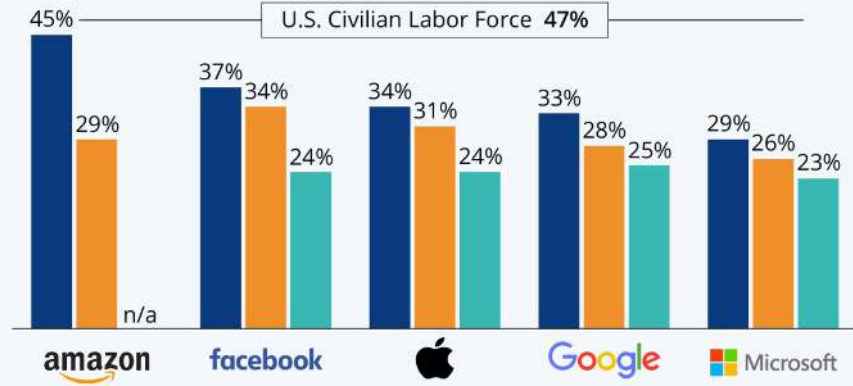
Quelle: Eurostat

Frankfurter Allgemeine statista

## Women's Representation in Big Tech

Percentage of female employees in the workforce of major tech companies\*

■ Total Workforce ■ Leadership Jobs ■ Tech Jobs



\* latest available data as of June 2021

Source: Company reports



statista



Employing more women is not enough,  
but it is a good start.



Cybersecurity needs...

...more **interdisciplinarity**.

...more **diversity**.



*Cybersecurity is not about fixing the IT infrastructure –  
but about interactions between technology and social actors.*

– Dr. Myriam Dunn Cavelty, Senior Lecturer for Security Studies (ETHZ)

## Human-Centred Security: Addressing psychological vulnerabilities

RESEARCH-ARTICLE

### Passwords and the evolution of imperfect authentication

**Authors:** Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano

[Authors Info & Affiliations](#)

**Publication:** Communications of the ACM • June 2015 • <https://doi.org/10.1145/2699390>



"Information security should put humans at the centre. If they truly are security's 'weak point' then start by understanding their vulnerabilities and managing them"

## Human-Centred Security: Positively influencing security behaviour

### About this webinar

Human error and negligence still contribute to a significant number of security incidents, yet current approaches to mitigating this risk are failing to have the desired impact. Many organisations have not always prioritised the effective management of this risk and have historically relied upon security awareness to influence security behaviour. Yet this only resolves a small part of the problem and neglects other factors. A robust human-centred security programme is required.

## IFIP International Symposium on Human Aspects of Information Security & Assurance (HAISA 2021)

Virtual (Online), 7<sup>th</sup> - 9<sup>th</sup> July 2021



## Why human-centred cyber security is the future



Nov 27, 2017 · 4 min read



Journal of Information Security and Applications

Volume 34, Part 1, June 2017, Pages 76-81



### Contemplating human-centred security & privacy research: Suggesting future directions

Karen Renaud <sup>a</sup>, Stephen Flowerday <sup>b</sup>



Seventeenth Symposium on Usable Privacy and Security

[https://www.researchgate.net/publication/318284979\\_Contemplating\\_human-centred\\_security\\_privacy\\_research\\_Suggesting\\_future\\_directions](https://www.researchgate.net/publication/318284979_Contemplating_human-centred_security_privacy_research_Suggesting_future_directions)  
<https://www.securityforum.org/research/human-centred-security/>  
<https://www.brighttalk.com/webcast/9923456327/human-centred-security-positively-influencing-security-behaviour>  
<https://gosperscript.com/blog/why-human-centred-cyber-security-is-the-future/>  
<https://dl.acm.org/doi/10.1145/2699390>  
<https://www.usenix.org/conference/soups2021>  
<https://www.haisa.org>

## MOBILE SECURITY



TEACHING

RUB

RUB » EI » MOBSEC » Teaching » Courses » Usable Security and Privacy

## INTRODUCTION TO USABLE SECURITY AND PRIVACY (BACHELOR)

Die Studierenden verstehen die grundsätzliche Problematik und Wichtigkeit der Benutzbarkeit von technischen Systemen durch Menschen, insbesondere im Umgang mit IT Sicherheitstechnik. Darüber hinaus erlangen sie ein grundlegendes Verständnis von Methoden und zentralen Erkenntnissen der Usable Security und Privacy Forschung, sowie grundlegende Handreichungen für die Praxis. Die Vorlesung behandelt insbesondere folgende Themen:

- Einführung
  - Überblick
  - Entstehung des Forschungsgebietes
  - Grundlagen menschlichen Verhaltens in der IT Sicherheit
- Methodische Grundlagen
  - Einführung Quantitative Methoden (z. B. Usability-Experimente)
  - Einführung Qualitative Methoden (z. B. Interviews/Umfragen)
  - Statistische Methoden (deskriptive Statistik, statistische Tests)
- Zentrale Anwendungen
  - Benutzbare Authentifizierung
  - Warndialoge/Phishing
  - Verschlüsselungstechniken von Dateien und Kommunikation
  - Security Awareness
  - Developers
  - Operators

Lecture: [Introduction to Usable Security and Privacy](#)

## USABLE SECURITY AND PRIVACY (MASTER)

Diese Veranstaltung vermittelt Kenntnisse der Usable Security und Privacy. Die Studierenden verstehen, warum die Usability technischer Systeme entscheidenden Einfluss auf deren Sicherheit haben kann. Darüber hinaus sollen Sie in die Lage versetzt werden, einfache Studien zur Usability selbst durchzuführen. Die Vorlesung behandelt insbesondere folgende Themen:

- Überblick
  - Benutzbare Authentifizierung
  - Nutzer und Phishing
  - Vertrauen/Trust, PKI, PGP
  - Privatheit und Tor
  - Privacy policies
  - Design und Auswertung von Benutzerstudien

Lecture: [Usable Security and Privacy](#)



# WE SHAPE TECH

We Shape Tech is a global platform for greater diversity and inclusion in technology and innovation



## Girls in Tech™ Switzerland




*We inspire women to fall in love  
with programming.*

Django Girls organize free Python and Django workshops, create open sourced online tutorials and curate amazing first experiences with technology.





<https://swit.ch/security-awareness-day>



<https://www.securityawarenessinsider.ch>



# SWITCH

Working for a better digital world

