Cybersecurity Education

Computation World 2020

Andreas Aßmuth

Technical University of Applied Sciences
OTH Amberg-Weiden

2020-10-26

About me

Professor of Computer Networks and Mathematics

Dean of Studies (Department of Electrical Engineering, Media and Computer Science)

CIO of OTH Amberg-Weiden

Teaching:

- Mathematics
- Computer Networks
- Cryptography
- Coding Theory
- Information Security

IARIA Fellow

Current Research Projects

AutoDrive

Horizon 2020, ECSEL Joint Undertaking
Grant Agreement n° 737469
`https://autodrive-project.eu/`

Airborne **DA**ta **C**ollection **O**n **R**esilient **S**ystem **A**rchitectures (ADACORSA)

Horizon 2020, ECSEL Joint Undertaking
Grant Agreement n° 876019
`https://adacorsa.eu/`

Intelligent **Sec**urity for Electric Actuators and Converters in Critical Infrastructures (iSEC)

Bavarian Ministry of Economic Affairs, Regional Development and Energy, Grant Agreement n° IuK621

Outline

1 Introduction

2 Cybersecurity and the COVID-19 Pandemic

3 Cybersecurity Education

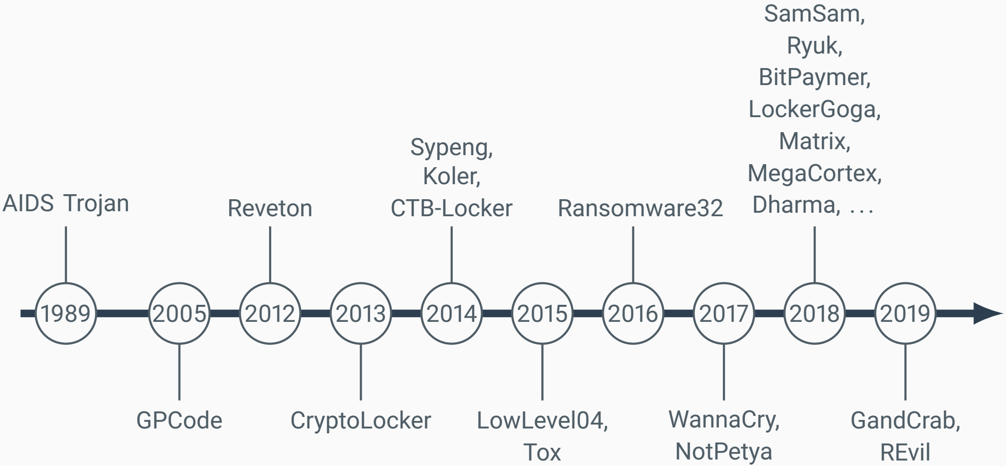
4 Conclusion and Outlook

Allianz Risk Barometer 2020 Top 10 Threats

2019: 37 %	39 %	(2)	▲	1	**Cyber incidents**
2019: 37 %	37 %	(1)	▼	2	Business interruption
2019: 27 %	27 %	(4)	▲	3	Changes in legislation and regulation
2019: 28 %	21 %	(3)	▼	4	Natural catastrophes
2019: 23 %	21 %	(5)	●	5	Market developments
2019: 19 %	20 %	(6)	●	6	Fire, explosion
2019: 13 %	17 %	(8)	▲	7	Climate change
2019: 13 %	15 %	(9)	▲	8	Loss of reputation or brand value
2019: 19 %	13 %	(7)	▼	9	New technologies
2019: 8 %	11 %	(13)	▲	10	Macroeconomic developments

Source: Allianz Global Corporate & Specialty, 2020-01-14.
https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020-de.html

Business as Usual I Ransomware

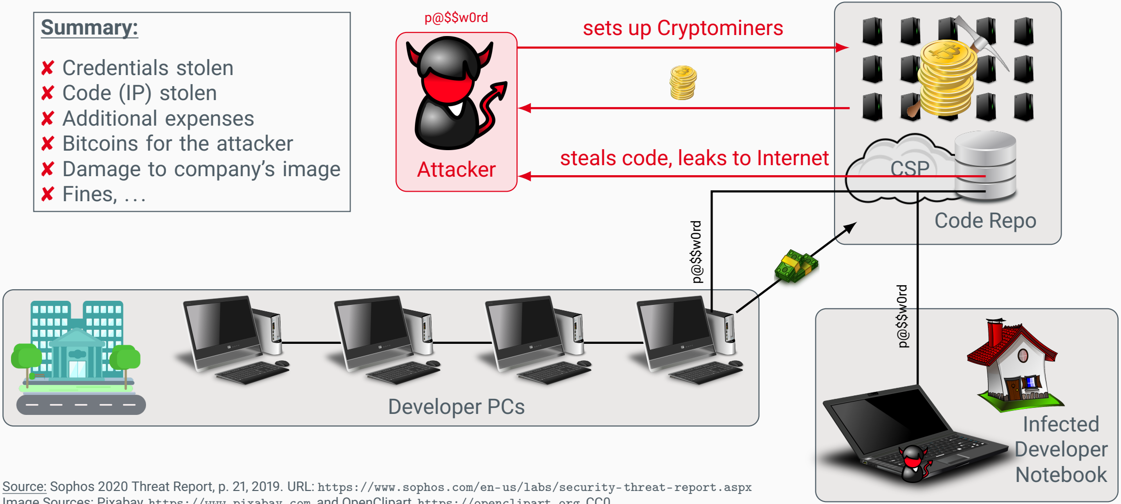


Source: Sophos 2020 Threat Report, p. 6, 2019. URL: `https://www.sophos.com/en-us/labs/security-threat-report.aspx`

Business as Usual II Cloud Security Breach Scenario

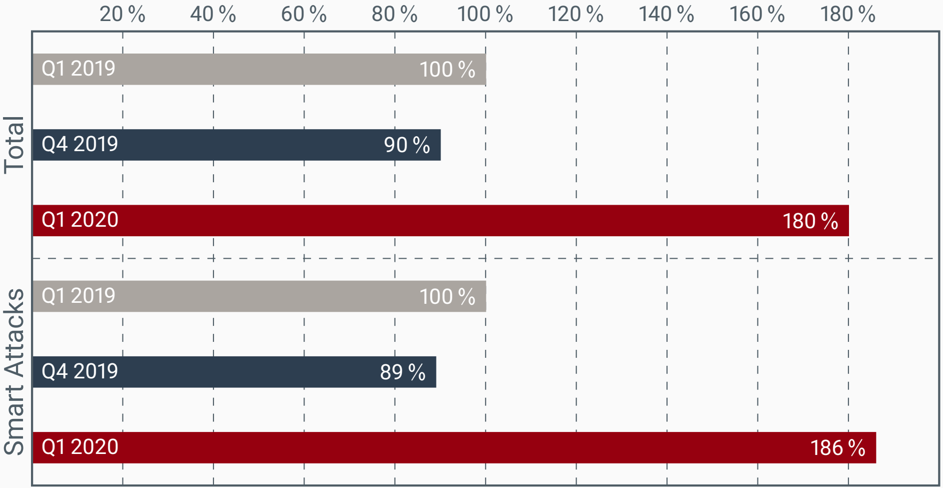
Summary:

- ✘ Credentials stolen
- ✘ Code (IP) stolen
- ✘ Additional expenses
- ✘ Bitcoins for the attacker
- ✘ Damage to company’s image
- ✘ Fines, . . .



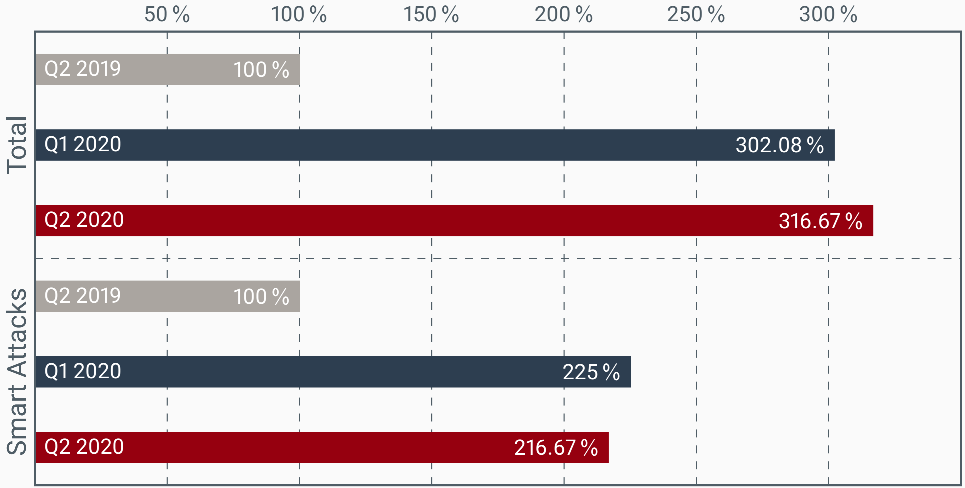
Source: Sophos 2020 Threat Report, p. 21, 2019. URL: `https://www.sophos.com/en-us/labs/security-threat-report.aspx`
Image Sources: Pixabay, `https://www.pixabay.com`, and OpenClipart, `https://openclipart.org`, CC0

DDoS Attacks in Q1 2020



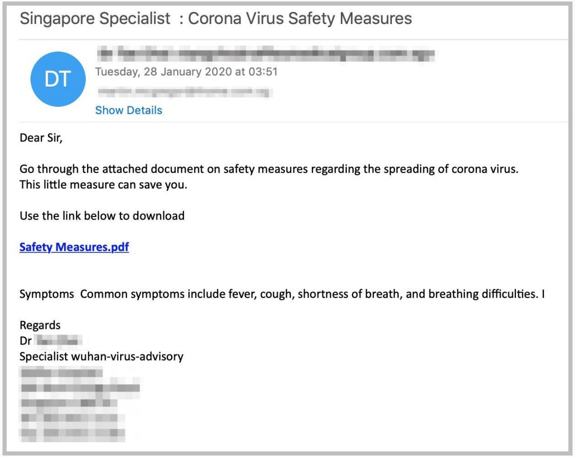
Source: Kupreev O., E. Badovskaya, and A. Gutnikov, *DDoS attacks in Q1 2020*. Kaspersky's securelist.com, 2020-05-06, `https://securelist.com/ddos-attacks-in-q1-2020/96837/`.

DDoS Attacks in Q2 2020



Source: Kupreev O., E. Badovskaya, and A. Gutnikov, *DDoS attacks in Q2 2020*. Kaspersky's securelist.com, 2020-08-10, `https://securelist.com/ddos-attacks-in-q2-2020/98077/`.

COVID-19 Phishing Scams I



Singapore Specialist : Corona Virus Safety Measures

[redacted]

Tuesday, 28 January 2020 at 03:51

[redacted]

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

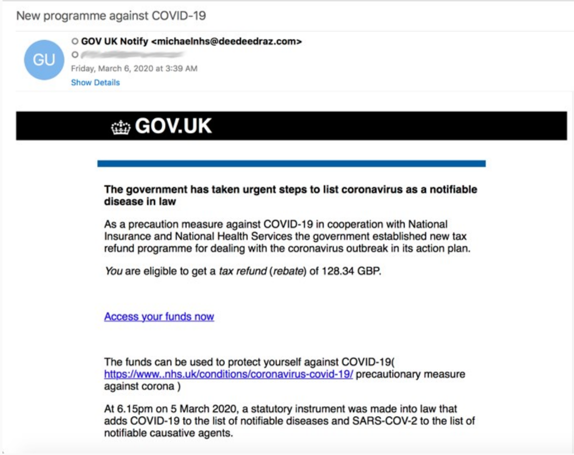
Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

Image Source: Lily Hay Newman, *Watch Out for Coronavirus Phishing Scams*. wired.com, 2020-01-31, `https://www.wired.com/story/coronavirus-phishing-scams/`.

COVID-19 Phishing Scams II



New programme against COVID-19

GU

○ GOV UK Notify <michaelnhs@deedeedraz.com>

○ [redacted]

Friday, March 6, 2020 at 3:39 AM

Show Details

GOV.UK

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund* (*rebate*) of 128.34 GBP.

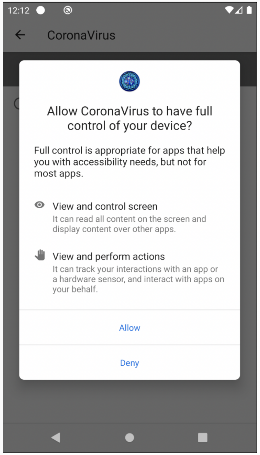
[Access your funds now]

The funds can be used to protect yourself against COVID-19(https://www..nhs.uk/conditions/coronavirus-covid-19/ precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

Image Source: Adrien Gendre, *Hacker nutzen die Coronavirus-Pandemie für die aktuellsten, auf Ereignis basierenden E-Mail-Angriffe*. VadeSecure, 2020-04-02, `https://www.vadesecure.com/de/hacker-nutzen-die-coronavirus-pandemie-fur-die-aktuellsten-auf-ereignis-basierenden-e-mail-angriffe/`.

COVID-19 Themed Android Malware

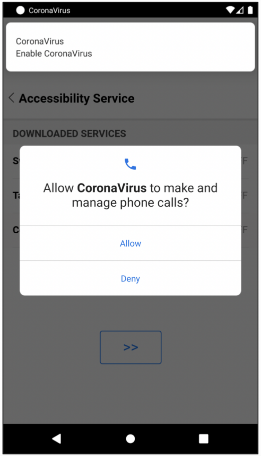


Allow CoronaVirus to have full control of your device?

Full control is appropriate for apps that help you with accessibility needs, but not for most apps.

View and control screen
It can read all content on the screen and display content over other apps.

View and perform actions
It can track your interactions with an app or a hardware sensor, and interact with apps on your behalf.



CoronaVirus
Enable CoronaVirus

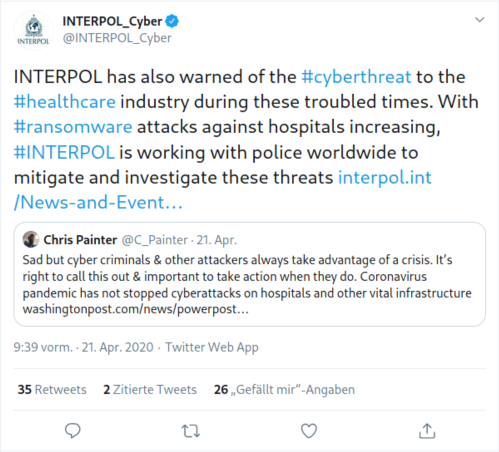
Accessibility Service

DOWNLOADED SERVICES

Allow **CoronaVirus** to make and manage phone calls?

Image Source: Avira Protection Labs, *Malware Threat Report: Q2 2020 Statistics and Trends*. avira.com, 2020-09-29, `https://www.avira.com/en/blog/malware-threat-report-q2-2020-statistics-and-trends`.

Attacks Against Hospitals During COVID-19 Pandemic



INTERPOL_Cyber
@INTERPOL_Cyber

INTERPOL has also warned of the #cyberthreat to the #healthcare industry during these troubled times. With #ransomware attacks against hospitals increasing, #INTERPOL is working with police worldwide to mitigate and investigate these threats interpol.int/News-and-Event…

Chris Painter @C_Painter · 21. Apr.
Sad but cyber criminals & other attackers always take advantage of a crisis. It's right to call this out & important to take action when they do. Coronavirus pandemic has not stopped cyberattacks on hospitals and other vital infrastructure washingtonpost.com/news/powerpost…

9:39 vorm. · 21. Apr. 2020 · Twitter Web App

35 Retweets 2 Zitierte Tweets 26 „Gefällt mir"-Angaben

Cyber Threats for Individuals

cybercrime

cyberbullying

cyber addiction

hacked devices

personal information exposure

stolen accounts

professional information exposure

Image Source: Pixabay, https://www.pixabay.com, CC0

Cybersecurity Education

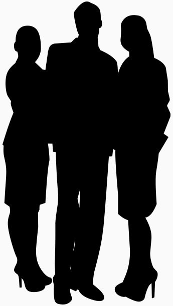
Matthew McNulty and Houssain Kettani:

> *“Much of the existing research focuses on the need to train professionals in cybersecurity or related disciplines, rather than expanding the knowledge base of individuals who are not attempting to learn about these areas directly.”*

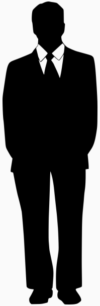
McNulty M., and H. Kettani (2020). *On Cybersecurity Education for Non-Technical Learners*. Proceedings of the 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA. Piscataway, NJ: IEEE. `https://doi.org/10.1109/ICICT50521.2020.00072`

European Union Agency for Network and Information Security (ENSIA). (2019). *ENISA threat landscape report 2018: 15 top cyberthreats and trends*. Heraklion: ENISA. `https://doi.org/10.2824/622757`

Cybersecurity Education For whom?

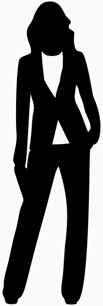


Private individuals?



Executives?

Computer Scientists and Engineers?



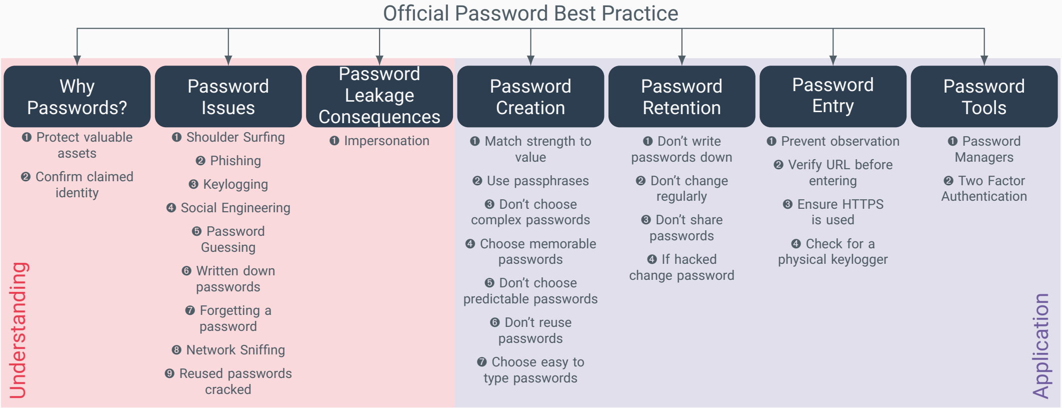
Security Professionals?

Image Sources: Pixabay, `https://www.pixabay.com`, and OpenClipart, `https://openclipart.org`, CC0

Cybersecurity Education At what age should we start?

Image Source: Pixabay, `https://www.pixabay.com`, CC0

Cybersecurity Education Passwords



Official Password Best Practice

Understanding

Why Passwords?

❶ Protect valuable assets

❷ Confirm claimed identity

Password Issues

❶ Shoulder Surfing

❷ Phishing

❸ Keylogging

❹ Social Engineering

❺ Password Guessing

❻ Written down passwords

❼ Forgetting a password

❽ Network Sniffing

❾ Reused passwords cracked

Password Leakage Consequences

❶ Impersonation

Application

Password Creation

❶ Match strength to value

❷ Use passphrases

❸ Don't choose complex passwords

❹ Choose memorable passwords

❺ Don't choose predictable passwords

❻ Don't reuse passwords

❼ Choose easy to type passwords

Password Retention

❶ Don't write passwords down

❷ Don't change regularly

❸ Don't share passwords

❹ If hacked change password

Password Entry

❶ Prevent observation

❷ Verify URL before entering

❸ Ensure HTTPS is used

❹ Check for a physical keylogger

Password Tools

❶ Password Managers

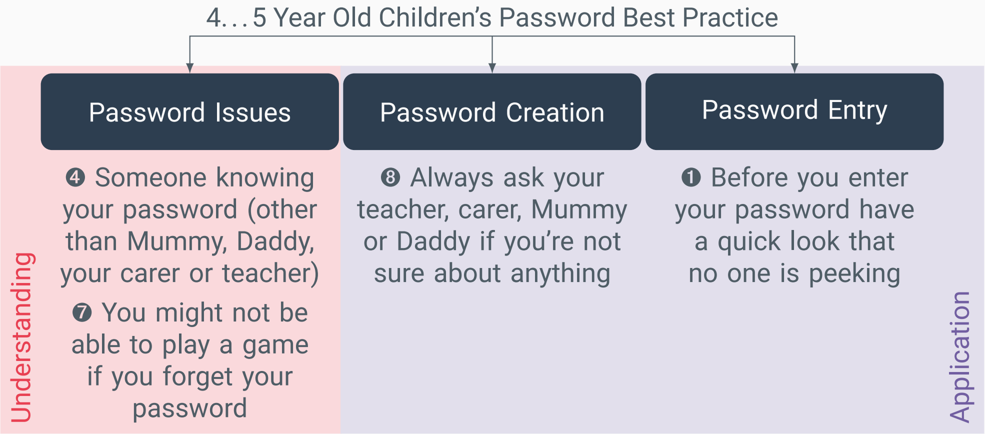
❷ Two Factor Authentication

Sources:

Suzanne Prior, and Karen Renaud. *Age-Appropriate Password "Best Practice" Ontologies for Early Educators and Parents*. International Journal of Child-Computer Interaction. Volumes 23-24, June 2020. `https://doi.org/10.1016/j.ijcci.2020.100169`

Karen Renaud, and Suzanne Prior. *Children's Password-Related Books: Efficacious, Vexatious and Incongruous*. Early Childhood Education Journal, July 2020. `https://doi.org/10.1007/s10643-020-01067-z`

Cybersecurity Education for Kids Passwords I



4…5 Year Old Children's Password Best Practice

Understanding

Password Issues

❹ Someone knowing your password (other than Mummy, Daddy, your carer or teacher)

❼ You might not be able to play a game if you forget your password

Password Creation

❽ Always ask your teacher, carer, Mummy or Daddy if you're not sure about anything

Password Entry

❶ Before you enter your password have a quick look that no one is peeking

Application

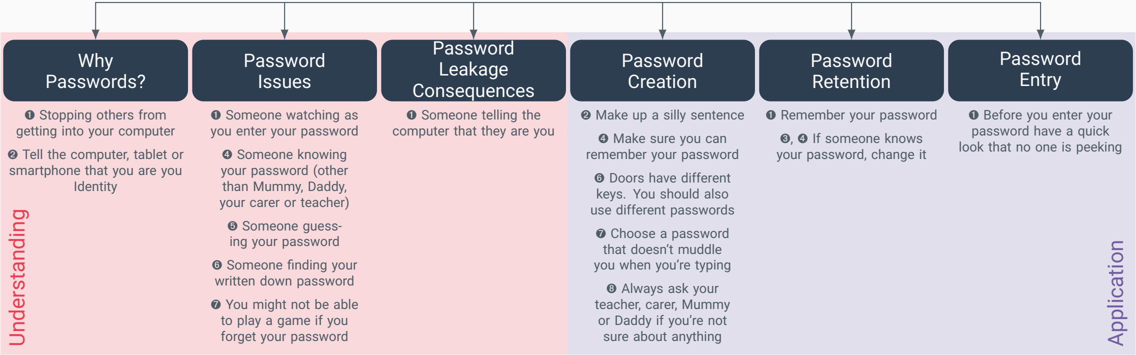
Sources:

Suzanne Prior, and Karen Renaud. *Age-Appropriate Password "Best Practice" Ontologies for Early Educators and Parents*. International Journal of Child-Computer Interaction. Volumes 23-24, June 2020. `https://doi.org/10.1016/j.ijcci.2020.100169`

Karen Renaud, and Suzanne Prior. *Children's Password-Related Books: Efficacious, Vexatious and Incongruous*. Early Childhood Education Journal, July 2020. `https://doi.org/10.1007/s10643-020-01067-z`

Cybersecurity Education for Kids Passwords II

6. . . 7 Year Old Children’s Password Best Practice



Understanding

Why Passwords?

❶ Stopping others from getting into your computer

❷ Tell the computer, tablet or smartphone that you are you Identity

Password Issues

❶ Someone watching as you enter your password

❹ Someone knowing your password (other than Mummy, Daddy, your carer or teacher)

❺ Someone guessing your password

❻ Someone finding your written down password

❼ You might not be able to play a game if you forget your password

Password Leakage Consequences

❶ Someone telling the computer that they are you

Application

Password Creation

❷ Make up a silly sentence

❹ Make sure you can remember your password

❻ Doors have different keys. You should also use different passwords

❼ Choose a password that doesn’t muddle you when you’re typing

❽ Always ask your teacher, carer, Mummy or Daddy if you’re not sure about anything

Password Retention

❶ Remember your password

❸, ❹ If someone knows your password, change it

Password Entry

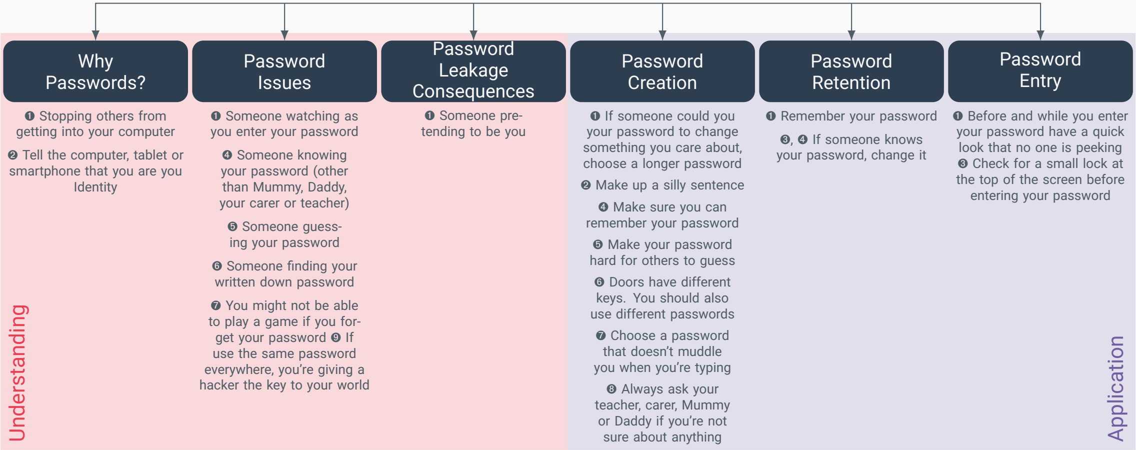
❶ Before you enter your password have a quick look that no one is peeking

Sources:

Suzanne Prior, and Karen Renaud. *Age-Appropriate Password “Best Practice” Ontologies for Early Educators and Parents*. International Journal of Child-Computer Interaction. Volumes 23-24, June 2020. `https://doi.org/10.1016/j.ijcci.2020.100169`

Karen Renaud, and Suzanne Prior. *Children’s Password-Related Books: Efficacious, Vexatious and Incongruous*. Early Childhood Education Journal, July 2020. `https://doi.org/10.1007/s10643-020-01067-z`

Cybersecurity Education for Kids Passwords III



8. . . 9 Year Old Children’s Password Best Practice

Why Passwords?

❶ Stopping others from getting into your computer

❷ Tell the computer, tablet or smartphone that you are you Identity

Password Issues

❶ Someone watching as you enter your password

❹ Someone knowing your password (other than Mummy, Daddy, your carer or teacher)

❺ Someone guessing your password

❻ Someone finding your written down password

❼ You might not be able to play a game if you forget your password ❾ If use the same password everywhere, you’re giving a hacker the key to your world

Password Leakage Consequences

❶ Someone pretending to be you

Password Creation

❶ If someone could you your password to change something you care about, choose a longer password

❷ Make up a silly sentence

❹ Make sure you can remember your password

❺ Make your password hard for others to guess

❻ Doors have different keys. You should also use different passwords

❼ Choose a password that doesn’t muddle you when you’re typing

❽ Always ask your teacher, carer, Mummy or Daddy if you’re not sure about anything

Password Retention

❶ Remember your password

❸, ❹ If someone knows your password, change it

Password Entry

❶ Before and while you enter your password have a quick look that no one is peeking

❸ Check for a small lock at the top of the screen before entering your password

Understanding

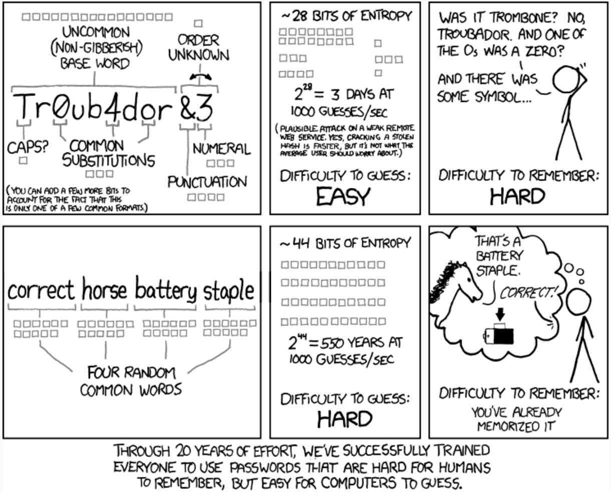
Application

Sources:

Suzanne Prior, and Karen Renaud. *Age-Appropriate Password “Best Practice” Ontologies for Early Educators and Parents*. International Journal of Child-Computer Interaction. Volumes 23-24, June 2020. `https://doi.org/10.1016/j.ijcci.2020.100169`

Karen Renaud, and Suzanne Prior. *Children’s Password-Related Books: Efficacious, Vexatious and Incongruous*. Early Childhood Education Journal, July 2020. `https://doi.org/10.1007/s10643-020-01067-z`

Cybersecurity Education Passwords

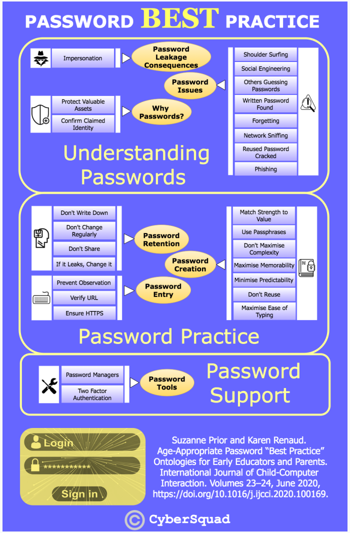

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Source: Randall Munroe, `https://xkcd.com/936/`

Cybersecurity Education for Kids

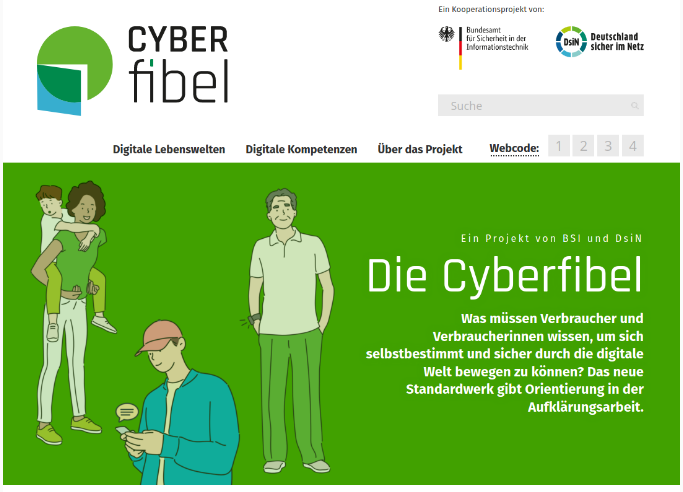
Further information:
Professor Karen Renaud
Professor in Cyber Security

🌎 https://karenrenaud.com/
✉ cyber4humans@gmail.com



Suzanne Prior and Karen Renaud.
Age-Appropriate Password "Best Practice"
Ontologies for Early Educators and Parents.
International Journal of Child-Computer
Interaction. Volumes 23–24, June 2020,
https://doi.org/10.1016/j.ijcci.2020.100169.

Cybersecurity Education for Adults in General Germany



Ein Kooperationsprojekt von:

Bundesamt für Sicherheit in der Informationstechnik

Deutschland sicher im Netz

CYBER fibel

Suche

Digitale Lebenswelten · Digitale Kompetenzen · Über das Projekt · Webcode: 1 2 3 4

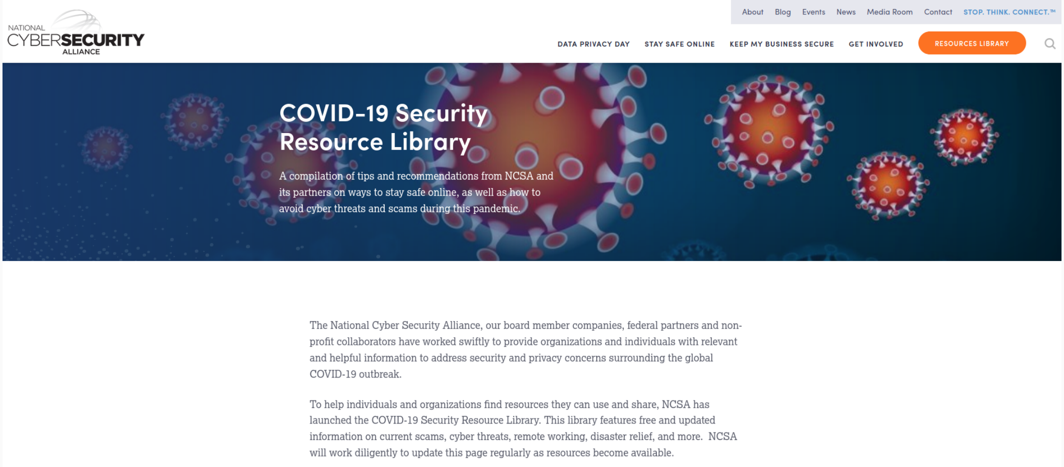
Ein Projekt von BSI und DsiN

Die Cyberfibel

Was müssen Verbraucher und Verbraucherinnen wissen, um sich selbstbestimmt und sicher durch die digitale Welt bewegen zu können? Das neue Standardwerk gibt Orientierung in der Aufklärungsarbeit.

https://www.cyberfibel.de/

Cybersecurity Education for Adults in General USA



COVID-19 Security Resource Library

A compilation of tips and recommendations from NCSA and its partners on ways to stay safe online, as well as how to avoid cyber threats and scams during this pandemic.

The National Cyber Security Alliance, our board member companies, federal partners and non-profit collaborators have worked swiftly to provide organizations and individuals with relevant and helpful information to address security and privacy concerns surrounding the global COVID-19 outbreak.

To help individuals and organizations find resources they can use and share, NCSA has launched the COVID-19 Security Resource Library. This library features free and updated information on current scams, cyber threats, remote working, disaster relief, and more. NCSA will work diligently to update this page regularly as resources become available.

https://staysafeonline.org/
https://www.youtube.com/user/StaySafeOnline1

Cybersecurity Awareness Example: Phishing Campaigns

- ⊕ Information about status quo in terms of phishing awareness
- ⊕ Build-up for awareness seminar
- ⊕ Teachable moment
- ⊕ Evaluation of new security awareness measures

- ⊖ Phishing campaigns might lower security level of organisation
- ⊖ Legal problems
- ⊖ Negative influence on the working atmosphere
- ⊖ Negative influence on trust
- ⊖ Negative influence on error culture

Source:
Melanie Volkamer, Martina A. Sasse, and Franziska Böhm. *Phishing-Kampagnen zur Steigerung der Mitarbeiter-Awareness*. Datenschutz und Datensicherheit (DuD), Vol. 8/2020, pp. 518-521, August 2020.

Cybersecurity Education at Universities

❶ Teach security topics according to the subject of study and the students requirements!

❷ Teach the fundamentals first!

❸ Do not just teach concepts! Let the students get their hands dirty!

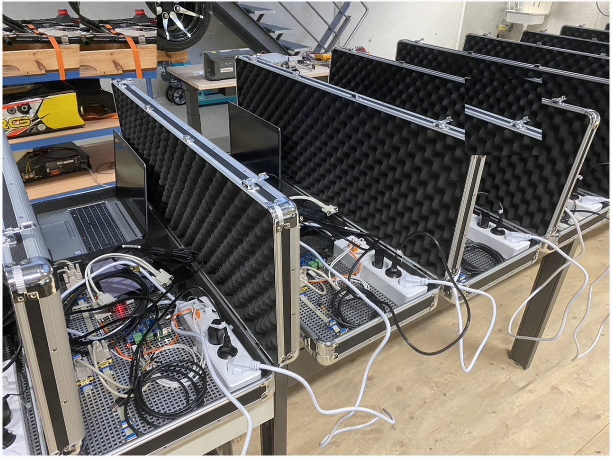
❹ Practice, practice and. . . (guess what?). . . practice!

❺ Keep your lectures and course material up to date!

Cybersecurity Education at OTH Amberg-Weiden Example

7	CPS 2, Software Engineering 2, Software Project, Computer Vision, Real-Time Operating Systems, **Information Security**, Manufacturing Execution Systems, Elective Subjects, Bachelor Thesis	Deepen Knowledge and Practice
6		
5	Practical Semester	
4	Algorithms & Data Structures, Computer Networks, Mobile & Ubiquitous Computing, Data Analytics, Control Engineering, Software Engineering 1, Embedded Systems, Fundamentals of Coding Theory & Cryptology	
3		
2	Mathematics, English, Foundations of Digital Systems, CPS 1, Programming, Theory of Computation, Operating Systems, Stochastics	Fundamentals
1		

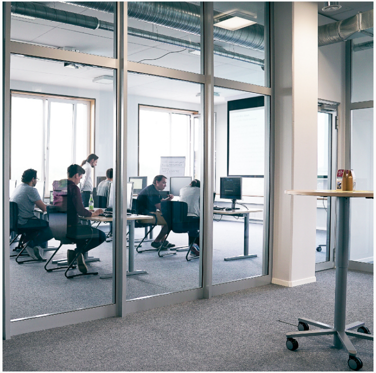
Practical Exercises Example: ANSKo



Further Information:

Prof. Dr. Rudolf Hackenberg, OTH Regensburg, `rudolf.hackenberg@oth-regensburg.de`

Cybersecurity Training Lab at Weiden



Lernlabor **Cybersicherheit**

Cybersecurity Training for Companies

- IT Security: From Prevention to Reaction
- Cryptographic Protocols

Secure Software

- Secure Software Engineering
- Secure Implementations and Testing in C

Hacking

- Pentesting
- Binary Exploitation

Cybersecurity Technologies

- Post-Quantum Security
- Blockchain

Further information: Prof. Dr. Daniel Loebenberger
✉ daniel.loebenberger@aisec.fraunhofer.de

Outlook

SECURWARE 2021

The Fifteenth International Conference on
Emerging Security Information, Systems and Technologies

Special Track "Cybersecurity Education":

- Cybersecurity Education for special target groups
- New concepts
- Ideas for new curricula
- Tools and hardware for Cybersecurity Education
- . . .

Look out for the CfP!

Wordcloud created by Ashashyou, CC BY-SA 4.0

Prof. Dr. Andreas Aßmuth
Professor of Computer Networks and Mathematics

OTH Amberg-Weiden
Department of Electrical Engineering, Media and Computer Science

Kaiser-Wilhelm-Ring 23, 92224 Amberg, Germany
Phone: +49 9621 482 3604
Email: a.assmuth@oth-aw.de
PGP: 0x93E4D0FA
Web: https://www.andreas-assmuth.de