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 DAta Collection On Resilient System Architectures (ADACORSA)**

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

**Intelligent Security 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
<table>
<thead>
<tr>
<th>Rank</th>
<th>Top Threats</th>
<th>Change in Percentage</th>
<th>2019 Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cyber incidents</td>
<td>39%</td>
<td>37% (2)</td>
</tr>
<tr>
<td>2</td>
<td>Business interruption</td>
<td>-2%</td>
<td>37% (1)</td>
</tr>
<tr>
<td>3</td>
<td>Changes in legislation and regulation</td>
<td>27%</td>
<td>27% (4)</td>
</tr>
<tr>
<td>4</td>
<td>Natural catastrophes</td>
<td>-6%</td>
<td>21% (3)</td>
</tr>
<tr>
<td>5</td>
<td>Market developments</td>
<td>21%</td>
<td>23% (5)</td>
</tr>
<tr>
<td>6</td>
<td>Fire, explosion</td>
<td>-4%</td>
<td>20% (6)</td>
</tr>
<tr>
<td>7</td>
<td>Climate change</td>
<td>17%</td>
<td>13% (8)</td>
</tr>
<tr>
<td>8</td>
<td>Loss of reputation or brand value</td>
<td>15%</td>
<td>13% (9)</td>
</tr>
<tr>
<td>9</td>
<td>New technologies</td>
<td>-2%</td>
<td>13% (7)</td>
</tr>
<tr>
<td>10</td>
<td>Macroeconomic developments</td>
<td>11%</td>
<td>8% (13)</td>
</tr>
</tbody>
</table>

Source: Allianz Global Corporate & Specialty, 2020-01-14.

© Andreas Aßmuth: "Cybersecurity Education"
Business as Usual: Ransomware

AIDS Trojan, Reveton, Sypeng, Koler, CTB-Locker, Ransomware32, SamSam, Ryuk, BitPaymer, LockerGoga, Matrix, MegaCortex, Dharma, ...


© Andreas Aßmuth: “Cybersecurity Education”
Summary:
- Credentials stolen
- Code (IP) stolen
- Additional expenses
- Bitcoins for the attacker
- Damage to company's image
- Fines, ...

DDoS Attacks in Q1 2020

DDoS Attacks in Q2 2020


© Andreas Aßmuth: “Cybersecurity Education”
Singapore Specialist: Corona Virus Safety Measures

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.

Regards
Dr. [Name]
Specialist Wuhan Virus Advisory

[Attached document]


© Andreas Aßmuth: “Cybersecurity Education”
COVID-19 Phishing Scams II

New programme against COVID-19

GOV UK Notify <michael.hns@deedeedraz.com>

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.


© Andreas Aßmuth: “Cybersecurity Education”
COVID-19 Themed Android Malware

Attacks Against Hospitals During COVID-19 Pandemic

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...](https://interpol.int/News-and-Event...)

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...](https://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
- Hacked devices
- Stolen accounts
- Personal information exposure
- Professional information exposure
- Cyber addiction

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

© Andreas Aßmuth: "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.”


Cybersecurity Education For whom?

Private individuals?  Executives?  Computer Scientists and Engineers?  Security Professionals?

Cybersecurity Education At what age should we start?

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

© Andreas Aßmuth: “Cybersecurity Education”
Cybersecurity Education

Passwords

Official Password Best Practice

Why Passwords?
1. Protect valuable assets
2. Confirm claimed identity

Password Issues
1. Shoulder Surfing
2. Phishing
3. Keylogging
4. Social Engineering
5. Password Guessing
6. Written down passwords
7. Forgetting a password
8. Network Sniffing
9. Reused passwords cracked

Password Leakage Consequences
1. Impersonation

Password Creation
1. Match strength to value
2. Use passphrases
3. Don't choose complex passwords
4. Choose memorable passwords
5. Don't choose predictable passwords
6. Don't reuse passwords
7. Choose easy to type passwords

Password Retention
1. Don't write passwords down
2. Don't change regularly
3. Don't share passwords
4. If hacked change password

Password Entry
1. Prevent observation
2. Verify URL before entering
3. Ensure HTTPS is used
4. Check for a physical keylogger

Password Tools
1. Password Managers
2. Two Factor Authentication

Sources:


© Andreas Aßmuth: "Cybersecurity Education"
4... 5 Year Old Children’s Password Best Practice

### Understanding

- **4** Someone knowing your password (other than Mummy, Daddy, your carer or teacher)
- **7** You might not be able to play a game if you forget your password

### Application

- **8** Always ask your teacher, carer, Mummy or Daddy if you’re not sure about anything
- **1** Before you enter your password have a quick look that no one is peeking

Sources:

6…7 Year Old Children’s Password Best Practice

**Why Passwords?**
1. Stopping others from getting into your computer
2. Tell the computer, tablet or smartphone that you are you

**Password Issues**
1. Someone watching as you enter your password
2. Someone knowing your password (other than Mummy, Daddy, your carer or teacher)
3. Someone guessing your password
4. Someone finding your written down password
5. You might not be able to play a game if you forget your password

**Password Leakage Consequences**
1. Someone telling the computer that they are you

**Password Creation**
1. Make up a silly sentence
2. Make sure you can remember your password
3. Doors have different keys. You should also use different passwords
4. Choose a password that doesn’t muddle you when you’re typing
5. Always ask your teacher, carer, Mummy or Daddy if you’re not sure about anything

**Password Retention**
1. Remember your password
2. If someone knows your password, change it

**Password Entry**
1. Before you enter your password have a quick look that no one is peeking

Sources:


© Andreas Aßmuth: “Cybersecurity Education”
Cybersecurity Education for Kids

Passwords III

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

Why Passwords?

1. Stopping others from getting into your computer
2. Tell the computer, tablet or smartphone that you are you

Password Issues

1. Someone watching as you enter your password
2. Someone knowing your password (other than Mummy, Daddy, your carer or teacher)
3. Someone guessing your password
4. Someone finding your written down password
5. You might not be able to play a game if you forget your password
6. If you use the same password everywhere, you’re giving a hacker the key to your world

Password Leakage Consequences

1. Someone pretending to be you

Password Creation

1. If someone could you your password to change something you care about, choose a longer password
2. Make up a silly sentence
3. Make sure you can remember your password
4. Choose a password that doesn't muddle you when you're typing
5. Always ask your teacher, carer, Mummy or Daddy if you're not sure about anything

Password Retention

1. Remember your password
2. If someone knows your password, change it

Password Entry

1. Before and while you enter your password have a quick look that no one is peeking
2. Check for a small lock at the top of the screen before entering your password

Sources:


© Andreas Aßmuth: “Cybersecurity Education”
Cybersecurity Education

Passwords

- **Tr0ub4dor & 3**
  - **Difficulty to Guess:** Easy
  - **Difficulty to Remember:** Hard

- **correct horse battery staple**
  - **Difficulty to Guess:** Hard
  - **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/

© Andreas Aßmuth: "Cybersecurity Education"
Cybersecurity Education for Kids

Further information:
Professor Karen Renaud
Professor in Cyber Security

🔗 https://karenrenaud.com/
✉️ cyber4humans@gmail.com
Cybersecurity Education for Adults in General Germany

https://www.cyberfibel.de/

© Andreas Aßmuth: “Cybersecurity Education”
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

Cybersecurity Education at Universities

1. Teach security topics according to the subject of study and the students requirements!
2. Teach the fundamentals first!
3. Do not just teach concepts! Let the students get their hands dirty!
4. Practice, practice and... (guess what?)... practice!
5. Keep your lectures and course material up to date!
**Cybersecurity Education at OTH Amberg-Weiden**

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td><strong>Practical Semester</strong></td>
</tr>
<tr>
<td>5</td>
<td>Algorithms &amp; Data Structures, Computer Networks, Mobile &amp; Ubiquitous Computing, Data Analytics, Control Engineering, Software Engineering 1, Embedded Systems, Fundamentals of Coding Theory &amp; Cryptology</td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

© Andreas Aßmuth: “Cybersecurity Education”
Practical Exercises  Example: ANSKo

Further Information:
Prof. Dr. Rudolf Hackenberg, OTH Regensburg, rudolf.hackenberg@oth-regensburg.de
Cybersecurity Training Lab at Weiden

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
Special Track “Cybersecurity Education”:

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