The 116 Best Cybersecurity Tools & Tactics (2021)

By Benjamin Eidam

Proudly presented by the
Global Cyber Security Forum

If you want the best cybersecurity tools and tactics all in one place, you will love this guide.

Below are the best 116 tools and tactics to keep your business digitally secure.

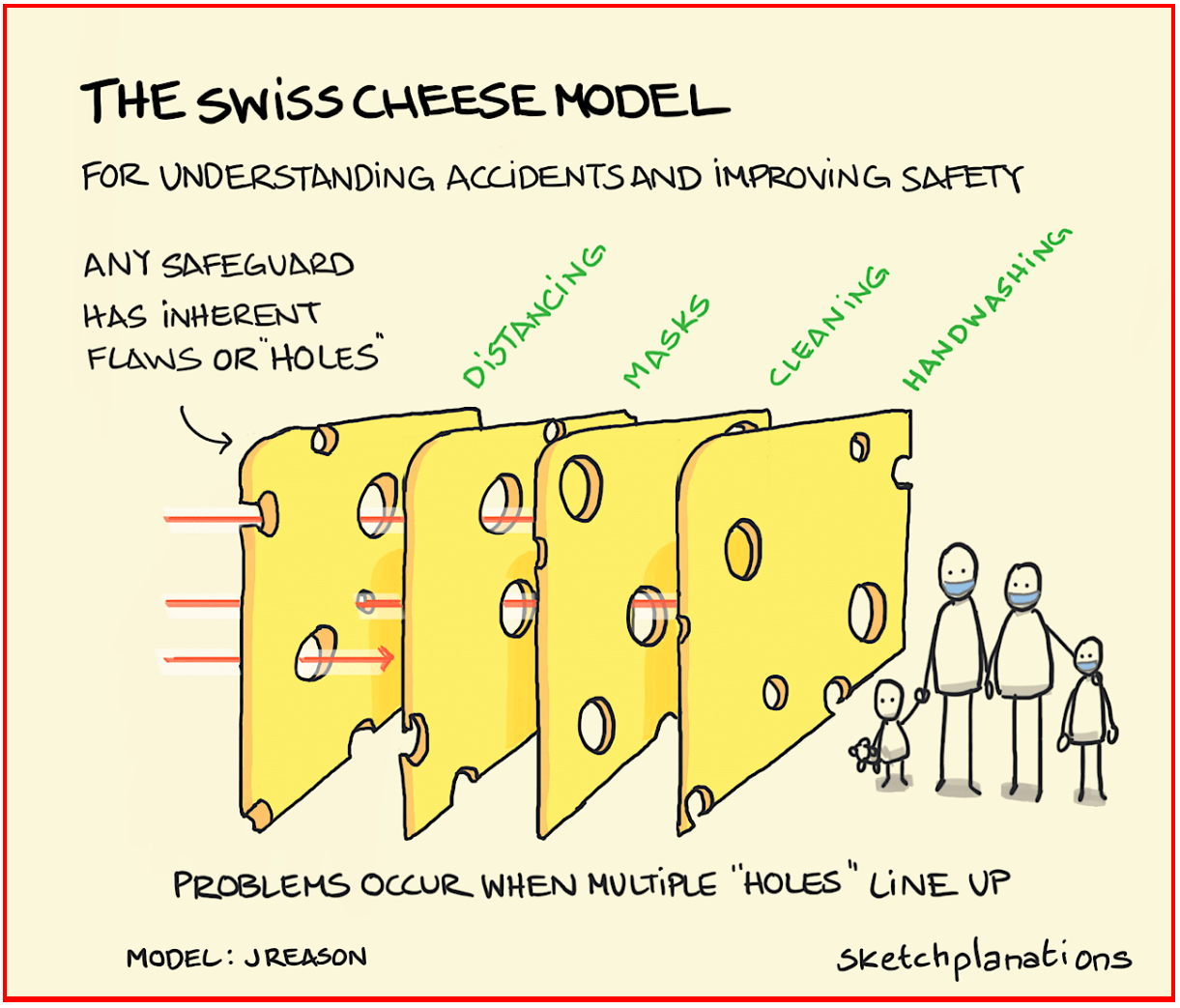
Let's get started:

What is cybersecurity?

For most people, cybersecurity sounds quite abstract. Just as “security measures” can mean anything and everything in the “real” world.

Roughly speaking, cybersecurity consists of three interlinked and coordinated areas; Human, Hardware and Software.

Cybersecurity is more than the sum of its parts. You can imagine cybersecurity as the "digital immune system" like a sliced onion or a stack of Swiss cheese slices:



Source and more: https://sketchplanations.com/the-swiss-cheese-model

This e-book is about these layers, the components of cybersecurity. And about the most practical and immediately applicable components of it. Because cybersecurity is such an incredibly complex field that no side in the world can completely map it.

That is why I am showing 116 facets and immediately tangible possibilities that the big term cybersecurity for every section will fill with life.

Why is cybersecurity important?

The greatest digital Threads are:

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	---	---
2	Web-based Attacks	---	↗
3	Phishing	↗	↗
4	Web application attacks	---	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	---	---
9	Insider threat	↗	---
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	---	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Source: https://www.enisa.europa.eu/publications/year-in-review

Every company is attacked, no matter what size or sector, and this table is as impressive as it is meticulous.

According to ENISA, the most common attack strategies are:

The most common attack strategies:

- Attacks on the human element
- Web and browser-based attack vectors
- Internet Exposed objects
- Exploitation of weak points / misconfigurations and errors in cryptography / networks / security protocols
- Attacks via supply chain attacks
- Network spread / lateral movement
- Active network
- Abuse / escalation of privileges or userinformation
- Fileless or memory-based attacks
- Misinformation / disinformation

Source: https://www.enisa.europa.eu / topics / threat-risk-management / threats-and-trends

Tips for optimal implementation

In order to get the most out of the tools and tactics mentioned here, it makes sense to:

1. Double check and deal with the tool / tactic to evaluate which and which Shape works best.
2. Consultation / questions to the relevant responsible. It's not about competencies or paternalism, it's about optimal security. If he can say out of hand how this has already been implemented, great. If not, this can be a good starting point for further security.
3. Each of these notes has been created to the best of our knowledge and belief, however, successes in the individual application must be individually weighed and, if necessary, supervised.

I wish you success!

Software

In principle, many of the cybersecurity options presented here are software.
And since the majority of cyber security takes place in cyberspace, software logically takes up the largest part here.

In this section, however, I am mainly concerned with the “80/20” programs, i.e. the 20% of cybersecurity software that as independently as possible of the occupation achieves 80% of the security results for the user.

In other places I also give software recommendations, but these are section-specific.

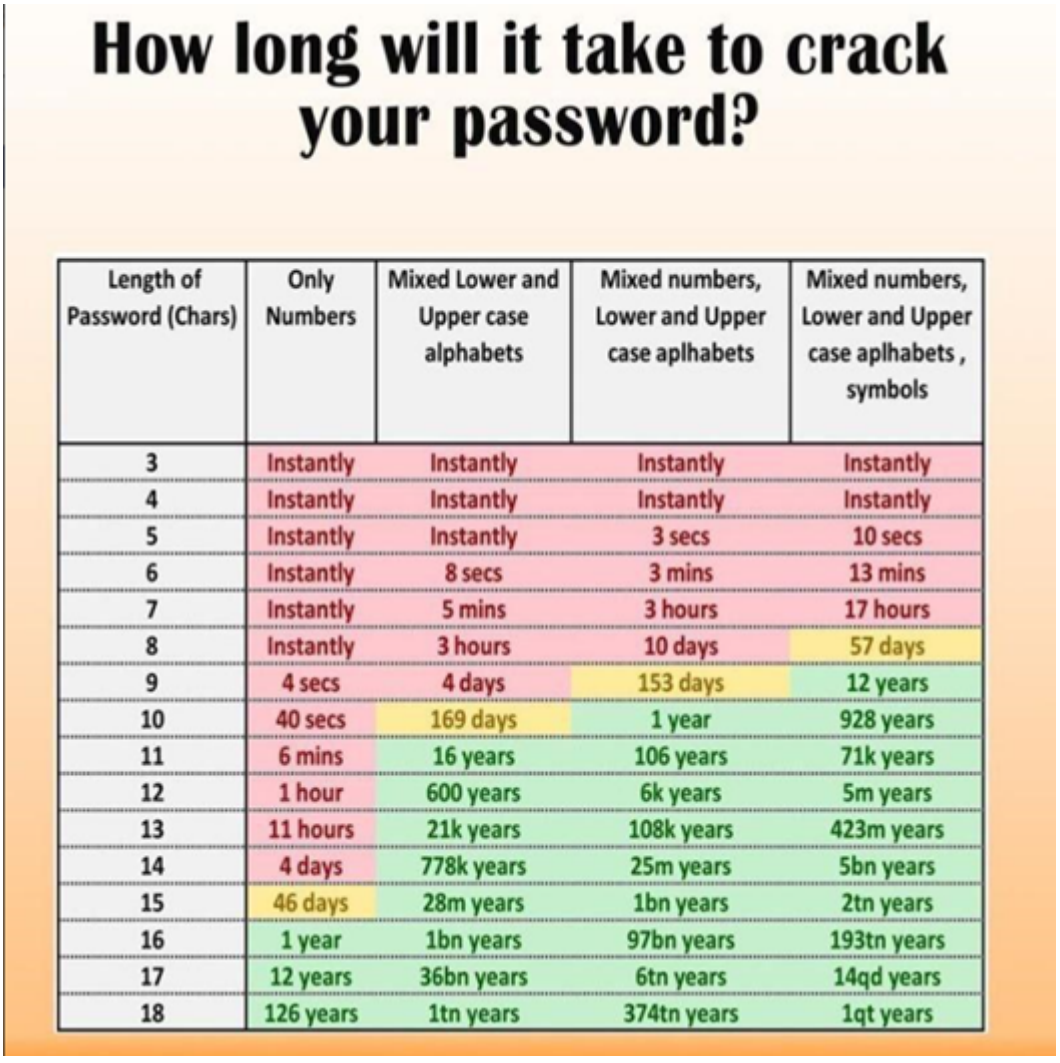
Let’s dive right in:

1. Secure password

For the foreseeable future, passwords will remain the most important security measure in the digital space. While they can be supplemented and framed by other measures, they remain # 1 on the list of defense strategies for now. But not all passwords are the same.

A secure password is characterized by:

- It is > 13 characters long.
- It consists of all categories of the keyboard. (Upper and lower case, numbers and letters, special characters etc.)
- It is not used a second time anywhere else.



Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

Source:
https://cloudnine.com/ediscoverydaily/electronic-discovery/how-long-will-it-take-to-crack-your-password-cybersecurity-trends/

Or, if you want it more precisely:

Estimated Password Recovery Times — 44x Terahash Inmanis (440x Nvidia RTX 2080 SUPER)
Alphanumeric mask attack with Terahash Hashstack

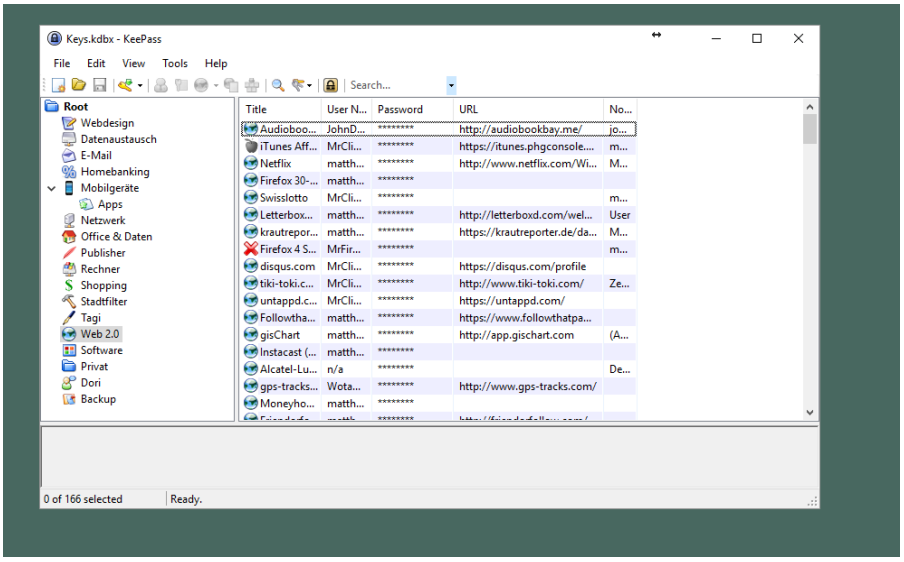
	Speed	Length 4	Length 5	Length 6	Length 7	Length 8	Length 9	Length 10	Length 11	Length 12	Length 13
NTLM	33 TH/s	Instant	Instant	Instant	Instant	Instant	6 mins 51 secs	7 hrs 3 mins	2 wks 4 days	3 yrs 1 mo	192 yrs 0 mo
MD5	17.65 TH/s	Instant	Instant	Instant	Instant	Instant	12 mins 47 secs	13 hrs 12 mins	1 mo 0 wk	5 yrs 9 mos	359 yrs 1 mo
NetNTLMv1 / NetNTLMv1+ESS	16.52 TH/s	Instant	Instant	Instant	Instant	Instant	13 mins 40 secs	14 hrs 6 mins	1 mo 0 wk	6 yrs 2 mos	383 yrs 8 mos
LM	15.53 TH/s	Instant	Instant	Instant	Instant						
SHA1	6.16 TH/s	Instant	Instant	Instant	Instant	Instant	36 mins 40 secs	1 day 13 hrs	3 mos 0 wk	16 yrs 7 mos	1 mil
SHA2-256	2.38 TH/s	Instant	Instant	Instant	Instant	1 min 32 secs	1 hr 34 mins	4 days 1 hr	8 mos 1 wk	42 yrs 11 mos	2.7 mil
NetNTLMv2	1.2 TH/s	Instant	Instant	Instant	Instant	3 mins 3 secs	3 hrs 8 mins	1 wk 1 day	1 yr 4 mos	85 yrs 4 mos	5.3 mil
SHA2-512	787.58 GH/s	Instant	Instant	Instant	Instant	4 mins 38 secs	4 hrs 46 mins	1 wk 5 days	2 yrs 1 mo	129 yrs 9 mos	8.1 mil
descrypt, DES (Unix), Traditional DES	636.03 GH/s	Instant	Instant	Instant	Instant	5 mins 44 secs					
Kerberos 5, etype 23, TGS-REP	203.27 GH/s	Instant	Instant	Instant	Instant	17 mins 55 secs	18 hrs 29 mins	1 mo 2 wks	8 yrs 1 mo	502 yrs 11 mos	31.2 mil
Kerberos 5, etype 23, AS-REQ Pre-Auth	203.08 GH/s	Instant	Instant	Instant	Instant	17 mins 56 secs	18 hrs 30 mins	1 mo 2 wks	8 yrs 1 mo	503 yrs 5 mos	31.2 mil
md5crypt, MD5 (Unix), Cisco-IOS 1 (MD5)	8.23 GH/s	Instant	Instant	Instant	7 mins 8 secs	7 hrs 22 mins	2 wks 5 days	3 yrs 2 mos	200 yrs 4 mos	12.4 mil	770.6 mil
LastPass + LastPass sniffed	1.75 GH/s	Instant	Instant	Instant	33 mins 30 secs	1 day 10 hrs	2 mos 4 wks	15 yrs 2 mos	940 yrs 10 mos	58.4 mil	3618.6 mil
macOS v10.8+ (PBKDF2-SHA512)	329.11 MH/s	Instant	Instant	2 mins 53 secs	2 hrs 58 mins	1 wk 0 day	1 yr 3 mos	80 yrs 9 mos	5 mil	310.8 mil	19270.4 mil
WPA-EAPOL-PBKDF2	272.28 MH/s					1 wk 2 days	1 yr 6 mos	97 yrs 8 mos	6.1 mil	375.7 mil	23292.6 mil
TrueCrypt RIPEMD160 + XTS 512 bit	207.99 MH/s	Instant	Instant	4 mins 34 secs	4 hrs 42 mins	1 wk 5 days	2 yrs 0 mo	127 yrs 10 mos	7.9 mil	491.8 mil	30491.6 mil
7-Zip	178.27 MH/s	Instant	Instant	5 mins 19 secs	5 hrs 29 mins	2 wks 0 day	2 yrs 4 mos	149 yrs 2 mos	9.3 mil	573.8 mil	35575.9 mil
sha512crypt 6, SHA512 (Unix)	117.32 MH/s	Instant	Instant	8 mins 5 secs	8 hrs 20 mins	3 wks 0 day	3 yrs 7 mos	226 yrs 8 mos	14.1 mil	871.9 mil	54055.8 mil
DPAPI masterkey file v1	46.39 MH/s	Instant	Instant	20 mins 25 secs	21 hrs 5 mins	1 mo 3 wks	9 yrs 2 mos	573 yrs 3 mos	35.6 mil	2205 mil	136712.8 mil
RAR5	27.84 MH/s	Instant	Instant	34 mins 15 secs	1 day 11 hrs	3 mos 0 wk	15 yrs 6 mos	962 yrs 1 mo	59.7 mil	3700.5 mil	229431 mil
DPAPI masterkey file v2	27.32 MH/s	Instant	Instant	34 mins 39 secs	1 day 11 hrs	3 mos 0 wk	15 yrs 8 mos	973 yrs 4 mos	60.4 mil	3743.5 mil	232098.3 mil
RAR3-hp	20.47 MH/s	Instant	Instant	46 mins 15 secs	1 day 23 hrs	4 mos 0 wk	20 yrs 11 mos	1.3 mil	80.6 mil	4996.9 mil	309807 mil
KeePass 1 (AES/Twofish) and KeePass 2 (AES)	17.48 MH/s	Instant	Instant	54 mins 10 secs	2 days 7 hrs	4 mos 3 wks	24 yrs 6 mos	1.5 mil	94.4 mil	5851.4 mil	362784 mil
bcrypt $2*$, Blowfish (Unix)	11.17 MH/s	Instant	1 min 23 secs	1 hr 24 mins	3 days 15 hrs	7 mos 1 wk	38 yrs 4 mos	2.4 mil	147.7 mil	9159.6 mil	567896.1 mil
Bitcoin/Litecoin wallet.dat	3.49 MH/s	Instant	4 mins 23 secs	4 hrs 31 mins	1 wk 4 days	1 yr 11 mos	122 yrs 10 mos	7.6 mil	472.7 mil	29305.5 mil	1816938.1 mil

Source: [https : //imgur.com/t/nvidia/GpTYAg8 You can findgeneral information]

More tips and helpful stuff about secure passwords [here].

2. Password manager

Since very few people can remember many different long character combinations,managers are convenient, automatic and secure solutions for password safes or passwords. Examples are [KeePassX] or [1Password].



KeePass Source: [https://blog.clickomania.ch/2017/09/21/ein-uberfalliger-umstieg/]

3. Passphrases

Passphrases are combinations of different words and characters to form memorable “password sentences”.

A few tips to make the most of passphrases:

- Use an easy-to-remember but unusual phrase. For example, “Luke Skywalker is eating pink rose petals, haha”
- Add spaces.
- Use capital letters and / or type certain words IN ALL CAPS.
- Add punctuation marks like “!.,;) Etc.
- Use unusual or abbreviated spellings for words. Such as MRT for magnetic resonance tomography.
- If necessary, replace some l3tt3rs with numb3r5. More on this in the “Password Phrases” section.

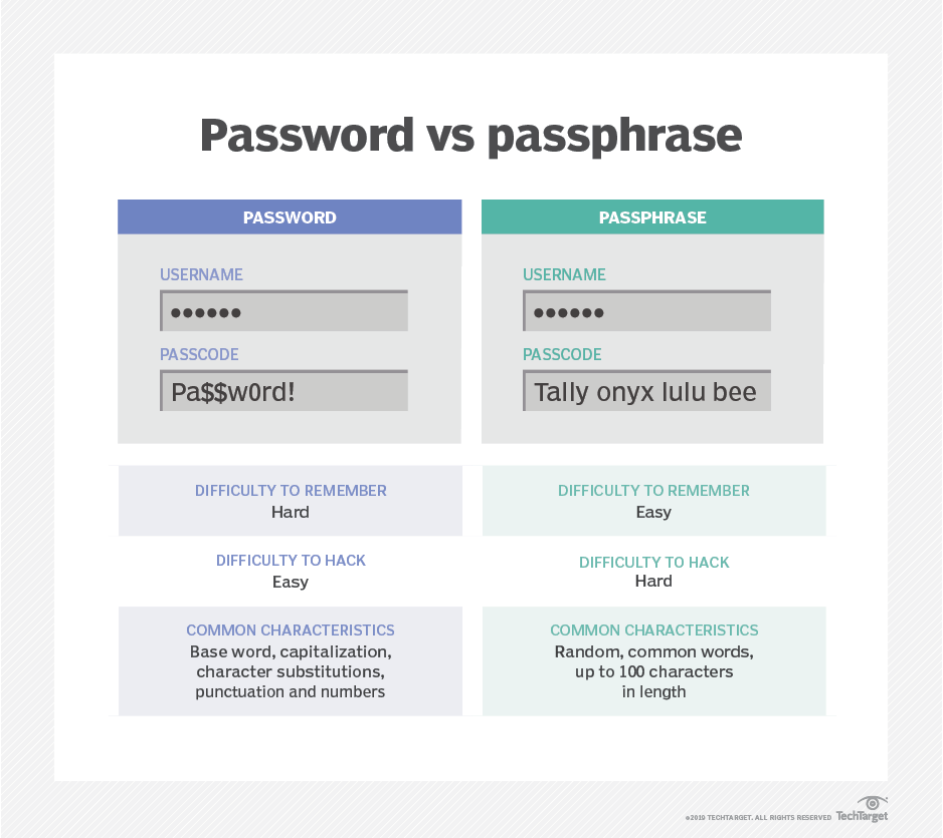


Image source: https://searchsecurity.techtarget.com/definition/passphrase

4. Password cards

Passwordcards convert passwords into sequences of steps. With a password card, you only remember the starting point, the pattern (e.g. always one field diagonally downwards for example) and the end point. Your password card will do the rest.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
1	G	p	6	C	w	6	O	n	7	N	g	3	1	y	5	G	e	1	T	l	5	G	y	4	J	r	1
2	9	i	0	0	&	F	1	I	Y	8	#	W	8	I	H	0	§	9	4	b	H	0	%	v	X	4	2
3	S	3	$	Z	8	&	8	5	%	F	3	§	Z	1	§	T	1	&	E	8	@	5	4	@	Z	7	3
4	#	&	J	5	#	V	l	a	N	4	#	y	6	1	E	m	o	#	4	#	i	W	j	&	0	#	4
5	r	P	u	1	t	W	z	1	j	7	u	5	j	B	v	6	n	U	s	2	n	L	d	7	u	B	5
6	4	z	9	C	y	3	F	w	4	W	g	3	E	e	6	3	j	1	S	p	9	M	e	9	I	p	6
7	1	r	L	6	#	3	6	r	V	6	§	G	2	y	T	3	&	Z	0	k	4	5	§	o	C	0	7
8	0	5	@	N	2	#	T	9	#	5	2	@	K	9	%	N	9	#	H	4	&	T	3	%	3	6	8
9	#	@	A	7	#	X	d	c	Z	2	§	i	5	S	9	d	x	%	2	@	o	A	y	§	6	&	9
10	g	Y	a	1	i	D	y	6	k	V	i	1	x	8	v	8	s	B	f	1	u	P	q	6	w	Q	10
11	E	r	7	3	z	5	B	m	7	E	c	6	D	d	0	O	h	8	5	c	8	N	c	7	I	w	11
12	3	f	I	8	&	U	4	r	3	7	#	V	2	j	T	2	@	R	6	m	Y	3	$	g	6	6	12
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	

Image source and further information: https://www.sicherheit-im-netz.de/dsin-passwortkarte

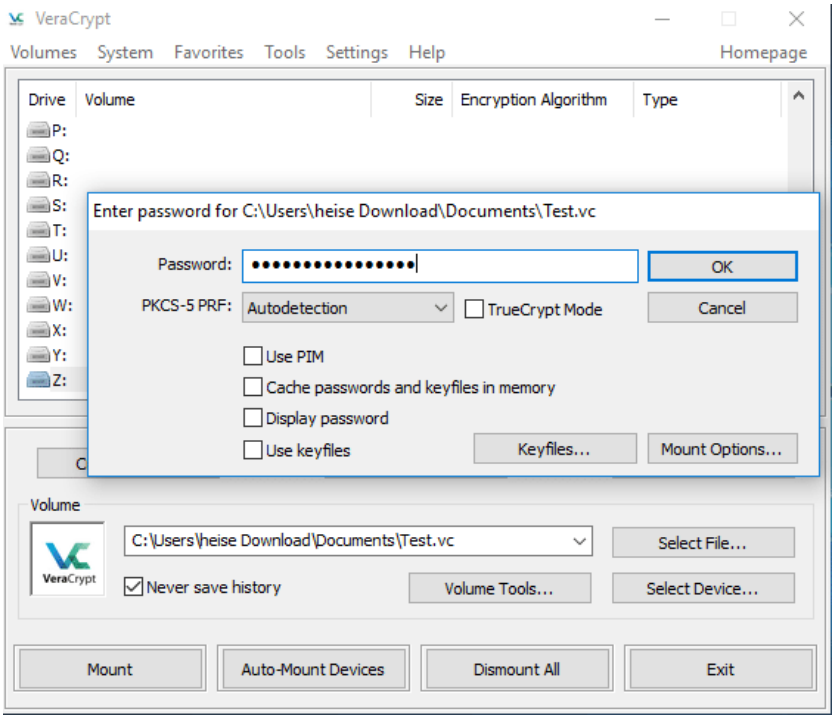
5. Password phrases

With password phrases you only memorize one key phrase and, for example, only enter the first letters of each word in this phrase.
E.g .: I've lived at home alone since I was 10. = IlahsIw10b.

Password sentences are made even more effective by combining them with “Leetspeak” (replacing letters with similar-looking digits and / or special characters).
Example: Wikipedia = w!K!P3d!4

6. Encryption Software

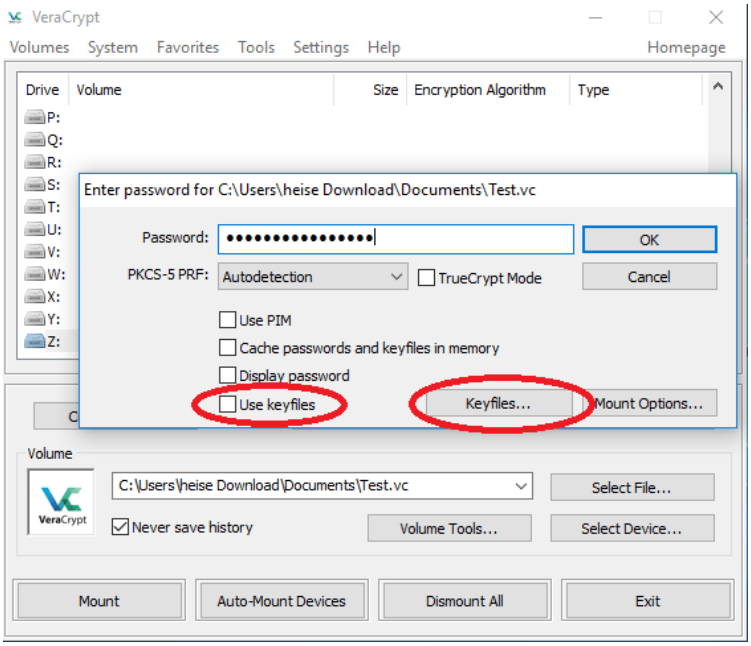
Encryption is useful for both data and hard disk drives. The best tool to start with is Veracrypt.



Download and further information about VeraCyrypt as well as image source:
https://www.heise.de/download/product/veracrypt-95747

7. Keyfiles

Keyfiles increase the security of tools password and encryption enormously. They are like a key in addition to the password. But be careful: once lost or only corrupted by one bit, the access files can never be restored and are irretrievably lost.



Further information and image source:
https://www.heise.de/download/product/veracrypt-95747

8. Firewall

A firewall shields a computer from some types of external attacks. There are different types of firewall and providers.

9. Antimalware

Malware is any malicious code that is intended to infect, infiltrate and destroy systems. On the one hand, there is "classic" malware, i.e. malware written by humans. And on the other hand "intelligent", i.e. reactive / adaptable malware. The latter is made possible by machine learning and artificial intelligence.

Malware includes, for example,

- computer viruses,
- trojans,
- ransomware,
- keyloggers, etc.

10. OSINT

OSINT stands for Open Source Intelligence Tools, roughly translated as “publicly usable information-collection tools”. These are mainly used by secret services, but are also used to prepare for large-scale attacks. Knowing which data can be found out and how is an enormous help in defending against social engineering attacks. You can find example tools in my article on internet research or in this framework.

11. Becoming invisible / TOR, VPN & Mesh-Nets

Tools such as TOR for VPN or mesh network connections ensure that your own data flow on the Internet is difficult or impossible to trace. Combined with tools such as TAILSunauthorized viewers , a very high level of security can be achieved. The easiest, fastest and most convenient way to access TOR is through the Brave browser. (increases your own online security in other ways at the same time) The simplest use of mesh nets / mesh networks is via Freifunk or tools like Firechat (the latter was unfortunately so effective that it was switched off).

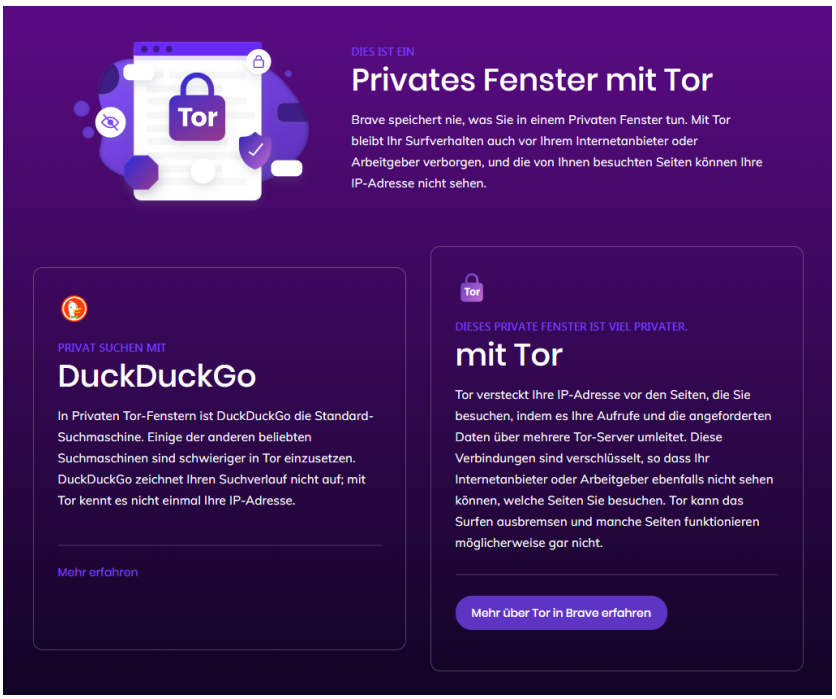
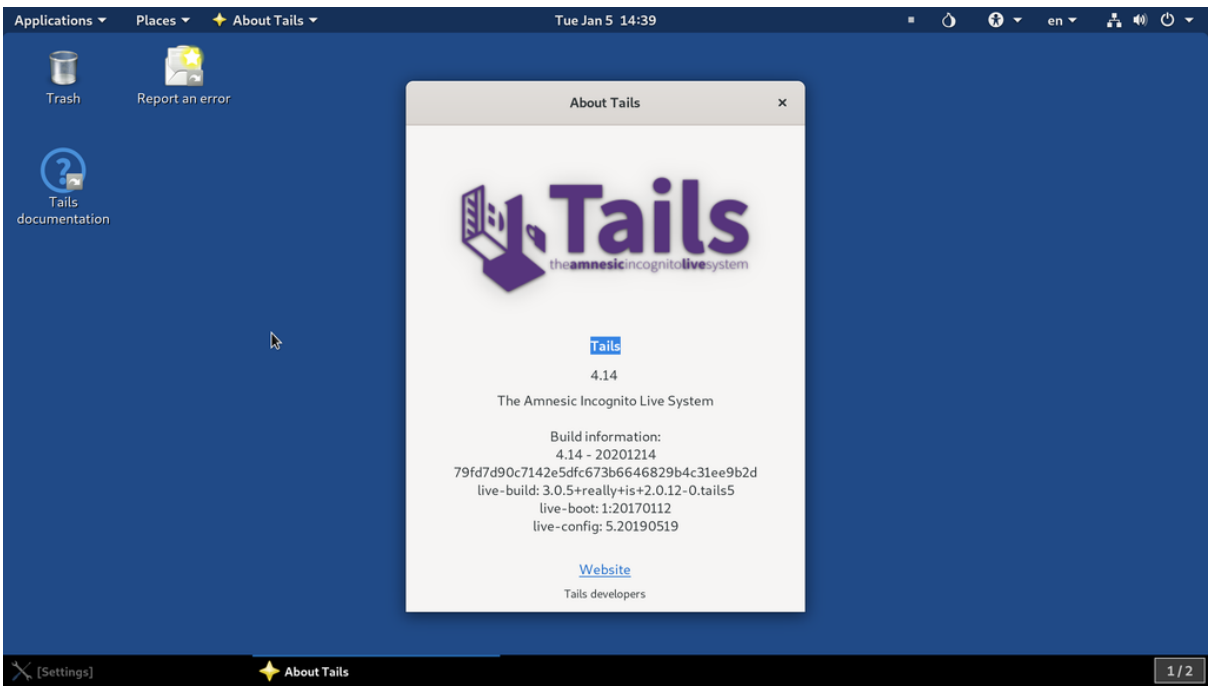


Image source: own screenshot

12. Simulated Environment / Virtual Systems

Virtual systems simulate a real PC environment. As a result, the user leaves fewer / less traceable / different traces and / or can check programs in a secure environment. Virtual systems include everything from the sandbox (more on this in the sections “Sandboxes” and “AI sandbox” to the completely hardened system. TAILS is the safest and easiest to use virtual “all in one” system.



Further information and image source :
https://en.wikipedia.org/wiki/Tails_(operating_system)

13. Security / penetration

Tools such as Kali Linux or Metasploit tests are pen test tools, “penetration test tools”, with which systems can be attacked in order to find weak points in order to fix them. But be warned: Depending on the country, some of the tools within these toolkits can be used semi-illegally or even illegally. So check before you test please.

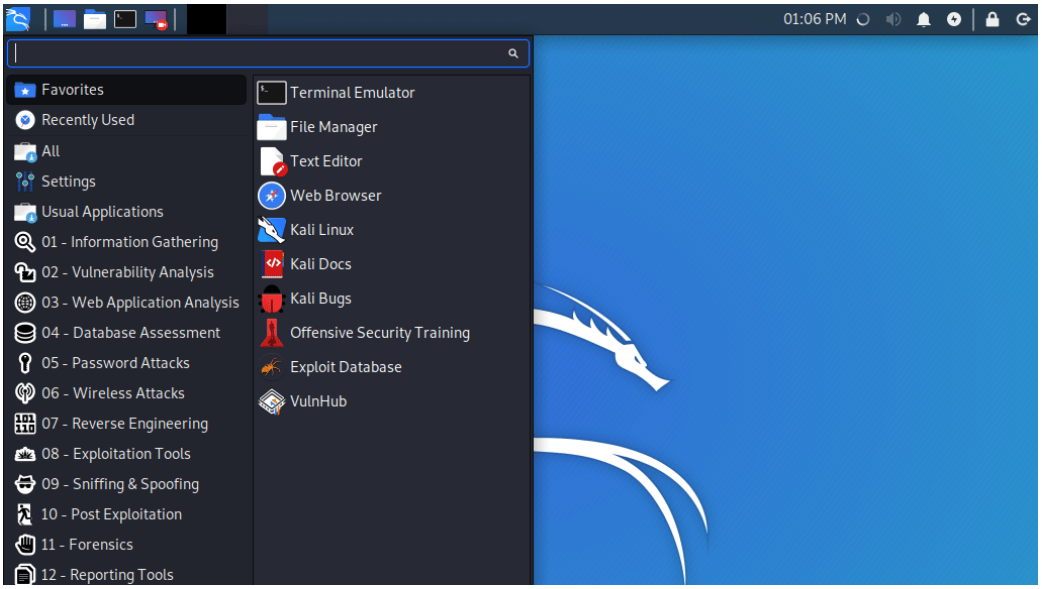


Image source and further information on Kali: https://www.heise.de/security/ message / Kali-Linux-2020-1-updated-boot-media-selection-and-samples-standard-root-from-4648751.html

14. Honey Pots

Honeypots or “honey pots” are systems or machines that attract attacks in order to protect the real goal and to analyze attacks from a safe distance. For example, you can find honeypot tools here and here.

15. Early warning systems / sentiment analysis tools

Sentiment analysis is automatic searches for set keywords and phrases. Mainly used for mood detection and shitstorm prevention, these tools help to monitor also and prepare for potential large-scale attacks in real time.

Tool overview and image source:
https://www.talkwalker.com/de/blog/die-besten-sentiment-analyse-tools

16. Controlled demolition / sandbox test areas

Sandboxes are isolated from the rest of the system, in which the effectiveness of software is safe and can be tested. If malware tries to attack a system within a sandbox, for example, it is simply deleted along with the sandbox. Most antivirus software will automatically deploy sandboxes; separate tools can be found here.

17. Secure email providers

Mails and programs are one of the greatest gateways and starting points for attacks of all kinds. In addition to the dangerous content of emails, phishing, it is also important to choose a mail provider that is technically secure.
My personal favorite has been for many years Protonmail, but there are also other recommended providers, for example here from Germany.

You can find a great Talk about Protonmail here.

18. Limit email history on mobile devices to a maximum of 30 days.

This Tip is particularly helpful against theft or loss of the mobile device. If the device can be accessed for any reason, the outflow of data remains limited.

19. Use secure messengers

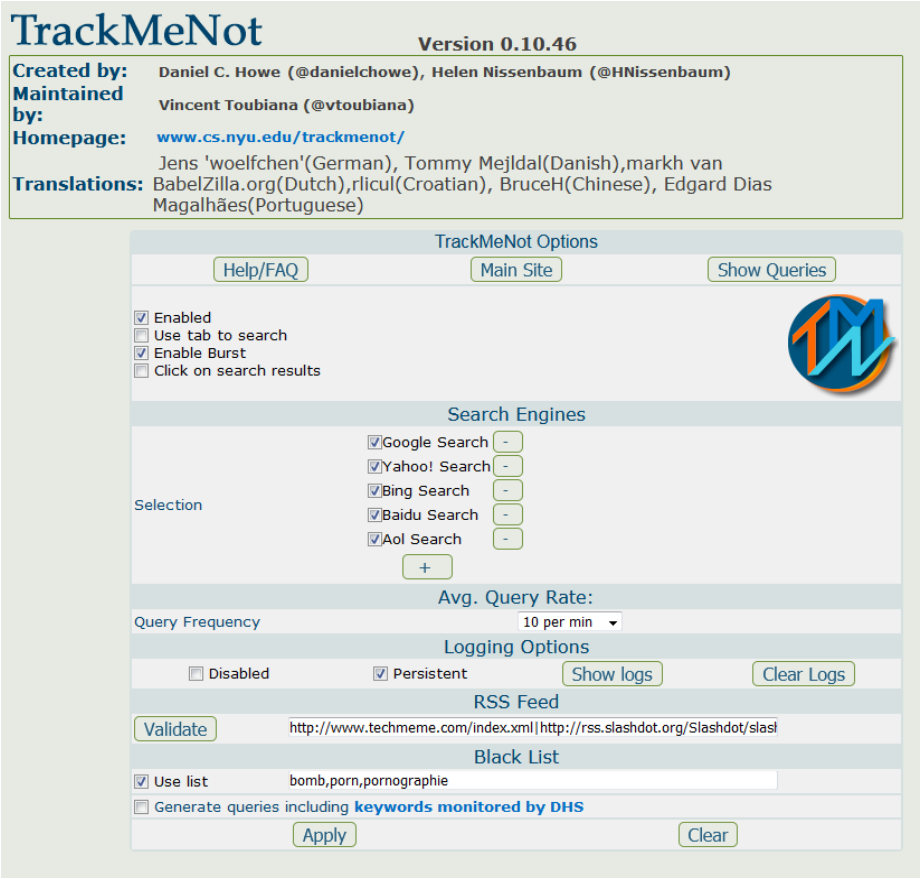
Especially in hacking and secret service circles one hears again and again that one should generally avoid emails as best as possible. And use secure messengers instead. So programs like WhatsApp, just in a safe way build. My personal favorite is Wire.

	Google Messages	Apple iMessage	Facebook Messenger	Element / Riot	Signal	Microsoft Skype	Telegram	Threema	Viber	Facebook Whatsapp	Wickr Me	Wire	Session
Overview													
Is the app recommended to secure my messages and attachments?	No	No	No	No	Yes	No	No	Yes	No	No	No	Yes	No
Main reasons why the app isn't recommended **Improvements to apps that are recommended** More details	Named as NSA partner in Snowden revelations Makes money from personal data Data not protected, not all data protected No independent & recent code audit and security analysis Closed source	Named as NSA partner in Snowden revelations Data not protected, not all data protected No independent & recent code audit and security analysis Closed source	Named as NSA partner in Snowden revelations Encryption not enabled by default Makes money from personal data Data not protected, not all data protected No independent & recent code audit and security analysis Closed source	No independent & recent code audit and security analysis	Remove the mandatory requirement for users to sign up with a mobile number Provide more comprehensive independent assessments of security/privacy	Named as NSA partner in Snowden revelations Encryption not enabled by default Makes money from personal data Data not protected, not all data protected Closed source	Bespoke cryptography Encryption not enabled by default Data not protected, not all data protected	Make APIs and server code open source Implement perfect forward secrecy at the end-to-end encryption layer Provide more comprehensive independent assessments of security/privacy	Data not protected, not all data protected No independent & recent code audit and security analysis Closed source	Named as NSA partner in Snowden revelations Makes money from personal data Data not protected, not all data protected No independent & recent code audit and security analysis Closed source	Recent security audits are not public Closed source	Further limit metadata storage and logging Provide more comprehensive independent assessments of security/privacy	No independent & recent code audit and security analysis Data not protected

Image source and further information on the overview:
https://www.securemessagingapps.com/

20. Automatic counter information

The concept of counter information comes from the military and the secret services. False traces are simply deliberately placed, through which it is no longer possible to understand from the outside which trace is real and which is not. This makes it more difficult to create detailed profiles. Can be used as a supplement to separated data streams. Browser plugins such as TrackMeNot can be used here quickly and easily to start.



Source: Own screenshot

21. Private tabs as default

Private tabs do not give any protective real additional value. (depending on the respective browser) But no data such as passwords, pages visited etc. are stored within them. In other words: With the right expectations, it is a good idea to use them.

22. Using different locks / multi-factor authentication

“x-factor authentication”, also called “multi-factor authentication”, is the use of different keys in order to be able to open a lock.
This makes it more difficult for attackers to break into a system. Because they always need all the keys used to open the door.
Factors / keys can be, for example:

1. PhotoTAN
2. Enter SMS code
3. Clicking on an additional link
4. etc.

23. Shortlink Checker

Even if you can read links, shortlinks, i.e. services that turn long links into short, easy-to-remember ones, such as bit.ly or similar services, effectively hide the actual link source. If you click on the shortlink, however, it may already be too late. Shortlink reviewers help by clicking the link and viewing the result from a safe distance. Similar to a virtual system.

A shortlink review tool. Source: Own screenshot

24. Exif Data

Exif files are specifying data that are made around a photo. For example, deleting the location, time, etc. Exif data prevents anyone who has access to the picture from finding out when, where, by which device etc. the picture was taken. It is to prevent this data from being generated, not easy it is to be deleted but fortunately.

25. Remove the doorbell on the computer / randomize the MAC address

The MAC address is the doorbell of a network interface. Using the MAC address, your device can be assigned exactly anywhere in the world. To prevent this, it is worth the randomizingMAC address. On any device connected to the internet.

26. 1-click check if own visibility

Infosniperyour or similar tools can show at a glance how well the obfuscation of your own location data works. Here you can find a lot of them also sorted by popularity.

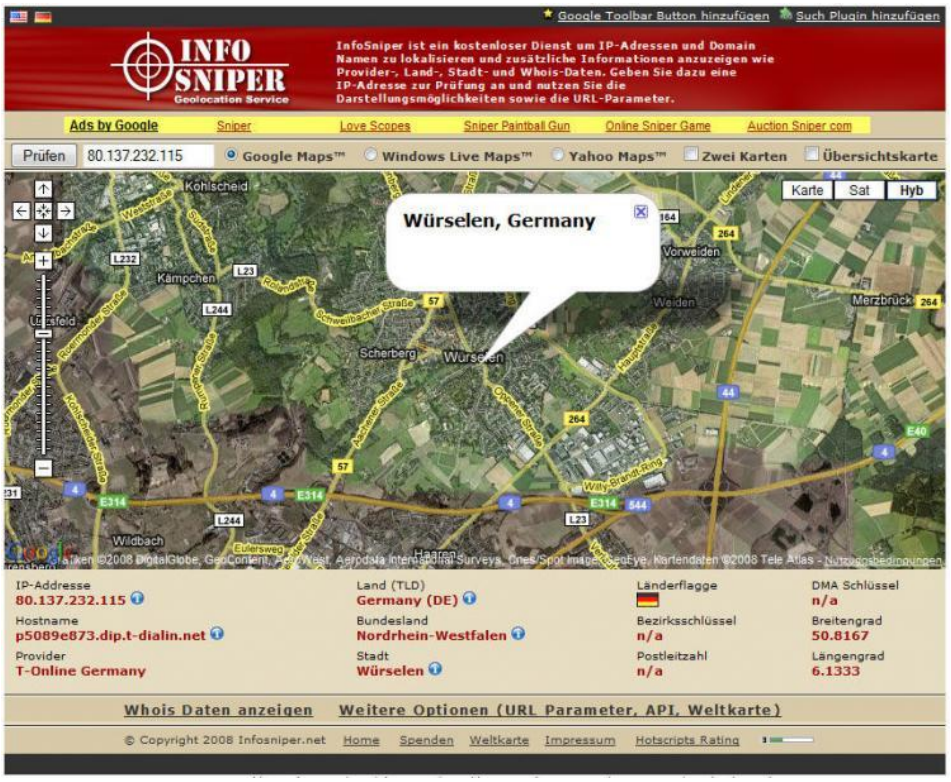


Image source and further information:
https://www.heise.de/download/product/infosniper-ip-adressen-lokalisierung-55629

27. Security status

Tools such as CheckHaveIBeenPwned or the Identity Leak Checker from HPI are ideally suited to see at a glance which data and access information from one's own online activities are already flying through the network, accessible to everyone. Quick action is then the order of the day.

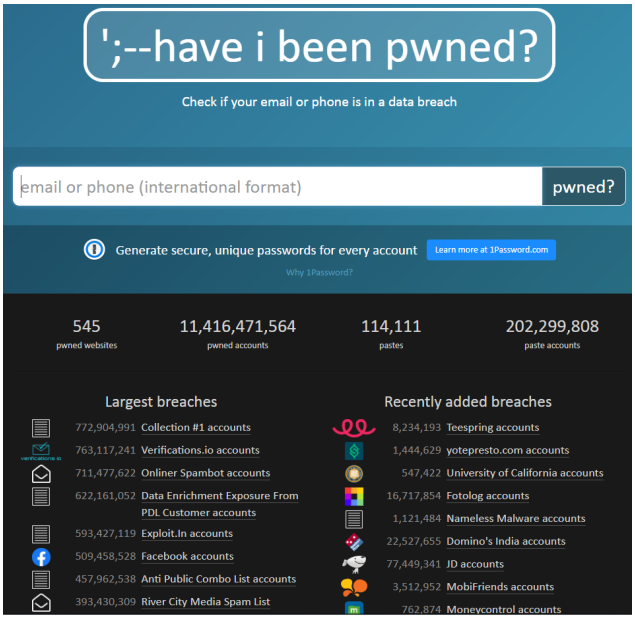


Image source: Own screenshot

28. Securing Wordpress

Since Wordpress hosts almost 65% of all websites, it makes sense to give a few short recommendations for helpful tools for WP security.

My personal top 3 to start are:

- Sucuri (system security)security
- ReCaptcha (accessand bot blockade)
- UpdraftAttacking (automatic backups)

Hardware

Hardware is not as easy as attacking software and by far not as easy as manipulating a person. Still, this is a popular vector to break into systems.

The minimum rule of thumb applies to hardware: The sender device, the receiver device and the connection between the two devices must be secured.

For example, when surfing the Internet: the user's computer, the Internet connection and the server of the website called up.

The rest is (roughly simplified) on the software side.

1. Hardware firewall

A hardware firewall works very similarly to its software sister, but it can also provide additional security.
With a hardware firewall, the device (the hardware) compares the various data streams and makes it even more difficult for attackers to penetrate a system due to the fact that it is different from software. Especially since an attack on the target computer, which can be leveraged by a software firewall, does not affect the hardware firewall, as it is separated from the computer. The AVM hardware firewall is a good starting point.

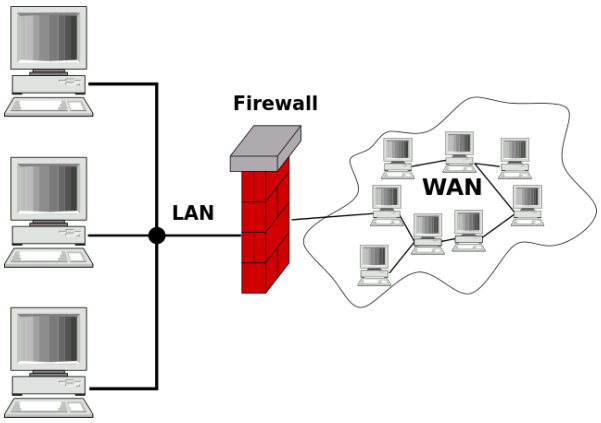


Image source and further information: https://de.malwarebytes.com/

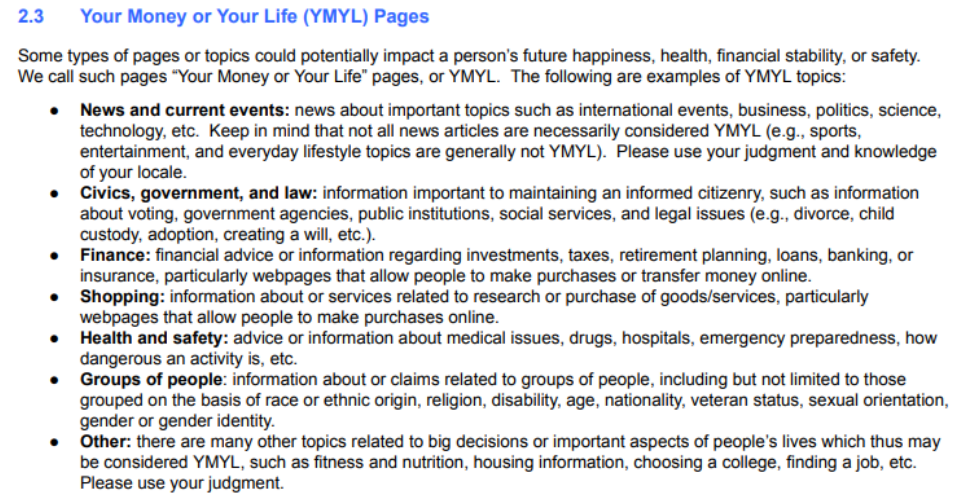
2. Hardware Key

Hardware keys are an excellent part of multi-factor authentication and make it extremely difficult to break into a computer. These hardware keys, also called FIDO sticks, make it difficult for anyone to get into the “apartment” (the target computer) without a key, just like a classic house door. A good starting point is the Titan Security Key from Google.
Here is a list of other good hardware keys.

Source and further information: https://store.google.com/de/product/titan_security_key?hl=de

3. Never save (YMYL) login data on (mobile) devices

YMYL stands for “Your Money Your Life” and describes all data that are related to your money and your life / health. Securing access to this particularly sensitive data has top priority. Therefore, if possible, no login data should be saved, especially on mobile, i.e. easily movable devices.



2.3 Your Money or Your Life (YMYL) Pages

Some types of pages or topics could potentially impact a person's future happiness, health, financial stability, or safety. We call such pages "Your Money or Your Life" pages, or YMYL. The following are examples of YMYL topics:

- **News and current events:** news about important topics such as international events, business, politics, science, technology, etc. Keep in mind that not all news articles are necessarily considered YMYL (e.g., sports, entertainment, and everyday lifestyle topics are generally not YMYL). Please use your judgment and knowledge of your locale.
- **Civics, government, and law:** information important to maintaining an informed citizenry, such as information about voting, government agencies, public institutions, social services, and legal issues (e.g., divorce, child custody, adoption, creating a will, etc.).
- **Finance:** financial advice or information regarding investments, taxes, retirement planning, loans, banking, or insurance, particularly webpages that allow people to make purchases or transfer money online.
- **Shopping:** information about or services related to research or purchase of goods/services, particularly webpages that allow people to make purchases online.
- **Health and safety:** advice or information about medical issues, drugs, hospitals, emergency preparedness, how dangerous an activity is, etc.
- **Groups of people**: information about or claims related to groups of people, including but not limited to those grouped on the basis of race or ethnic origin, religion, disability, age, nationality, veteran status, sexual orientation, gender or gender identity.
- **Other:** there are many other topics related to big decisions or important aspects of people's lives which thus may be considered YMYL, such as fitness and nutrition, housing information, choosing a college, finding a job, etc. Please use your judgment.

The topics listed in the picture offer a good orientation as to which login data should not be saved. Image source and further information about YMYL: https://static.googleusercontent.com/media/guidelines.raterhub.com/en//searchqualityevaluatorguidelines.pdf

4. If necessary, switch off the smartphone and remove the battery.

To avoid passive data collection / tracking, can It Be useful to turn off his smartphone and remove the battery.

5. Resetting mobile devices to factory settings regularly

This simple trick avoids malware that has spread to the smartphone without the user's knowledge. By deleting it every time you root. (Root process = the device is to its original state)

6. Masking off cameras

Mark Zuckerberg does it, the head of the FBI as well and everyone about your safety mask off the cameras and microphones on your devices. Because these are often proven direct spy tools.

A fundamental alternative can be a “hardened device”, i.e. cyber-secure devices such as crypto cell phones .

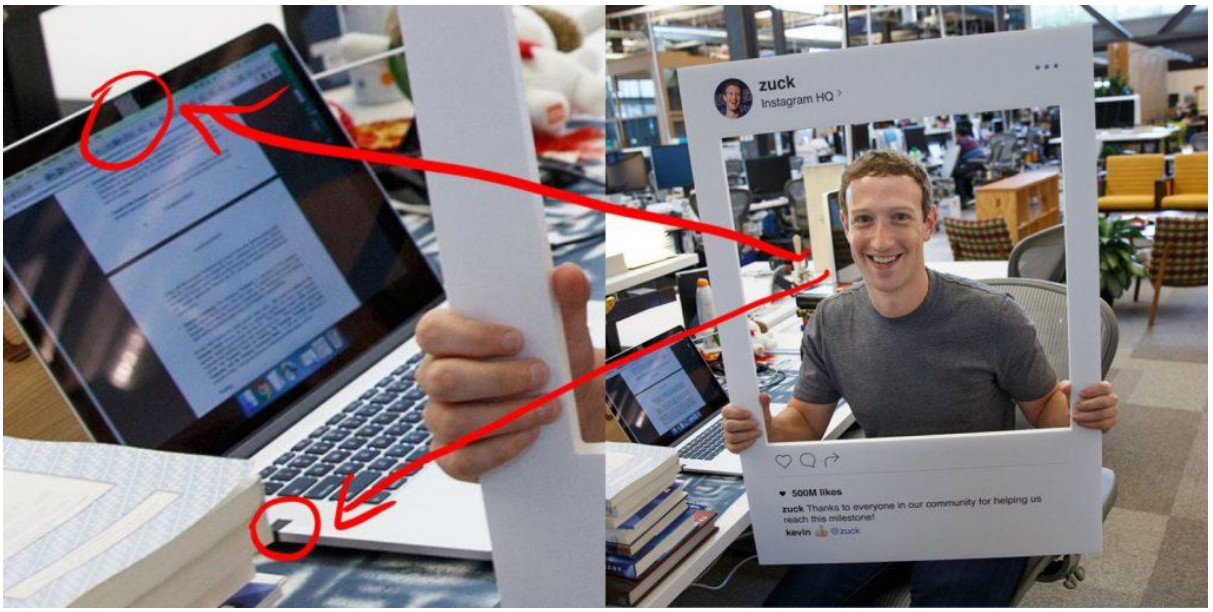


Image source and further information:
https://9to5mac.com/2016/06/21/facebook-mark-zuckerberg-tape-over-camera/

7. Encrypt entire hard disk

Hard disc encryption can be a good first line of defense against attackers. Even more important than already: create regular backups! Hard disk encryption can be used hand in hand with partition encryption and encrypted containers. Bitlocker is a good tool to start on Windows, FileVault on Mac OS.

8. NEVER connect USB sticks that you do not trust!

With infected USB sticks Nuclear power plants were switched off.
Therefore: No matter what happens, never connect a third-party USB stick to a computer with sensitive data. Never. Ever. No matter how fancy it looks.

Sweet but dangerous. Image source:
https://www.entertainmentearth.com/product/MC10375___16GB

9. WLAN Securing

A wireless network is no easy task. Because: Anyone with a device that can log into the WLAN can in principle attack it.
Here are a few basic tips for WLAN security:

1. Activate (WPA2) encryption
2. Use a secure password for encryption, router and access (use different passwords for each point)
3. all software Always keep up to date.
4. If possible, use cable instead of WiFi.
5. Deactivate file and printer sharing Deactivate
6. SSID broadcasting

You can find more tips here and here.

10. Smartphone Hardening

Smartphones are a land of milk and honey for cyber attackers. Because they are mobile, i.e. easy to steal, they connect to various networks via WLAN, are mobile spy devices thanks to their sensors, cameras and microphones and very often store potentially compromising material. That is why it is very important to secure your smartphone. In technical jargon one speaks of “hardening”. As already mentioned above, crypto cell phones or at least hardened operating systems like this make sense, otherwise these and these instructions help very well.

CHECKLIST

Checklist

Step	√	To Do	CIS	UT Note	Cat I	Cat II/III
		Basic Security				
1		Update operating system to the latest version	1.1.1	§	!	!
2		Do not Root the device		§	!	
3		Do not install applications from third party app stores	1.1.17	§	!	
4		Enable device encryption	1.1.15	§	!	
5		Disable 'Developer Actions'	1.1.16	§	!	!
6		Use an application/service to provide remote wipe functionality	3.2	§	!	
7		Enable Android Device Manager		§		
8		Erase all data before return, repair, or recycle	1.1.11	§	!	!
		Authentication Security				
9		Set a PIN and automatically lock the device when it sleeps	1.1.2	§	!	!
10		Set an alphanumeric password	1.1.3	§		
11		Set Auto-Lock Timeout	1.1.4	§	!	!
12		Disable 'Make Passwords Visible'	1.1.14	§		
13		Erase data upon excessive passcode failures		§	!	
		Browser Security				
14		Show security warnings for visited sites	1.2.2	§	!	!
15		Disable 'Form Auto-Fill'	1.2.3	§		

Image source and complete checklist:
https://security.utexas.edu/handheld-hardening-checklists/android

Employees

In > 99% of the cases, humans are the greatest and simplest weak point of any system.

For this reason, many hackers no longer deal with technologies, because manipulating users is almost always child's play in comparison.

Hacks against people are called "social engineering".
Security measures on the other hand are subsumed under “Security Awareness”.

1. Secure your own brain / Amygdala hijacking

One of the most effective strategies in social engineering is to put the target in a strong emotion such as fear or stress. This switches the target's brain from “complex thinking” to “fight or flight” mode. The target of the attack can then hardly / no longer think abstractly and, for example, carry out calculations but only react in a “quasi-panic” manner. From this moment on you are literally the attacker's plaything.
And that doesn't happen in your mind. With this attack, your perception changes the “place of residence” from the prefrontal cortex from your higher hemispheres to the amygdala, your brain stem. Unprepared, you literally cannot do anything (meaningful) against an “amygdala hostage-taking”.

An awareness of this possibility, standard protocols and strategies as well as stress tests can help effectively. You can find more options here.

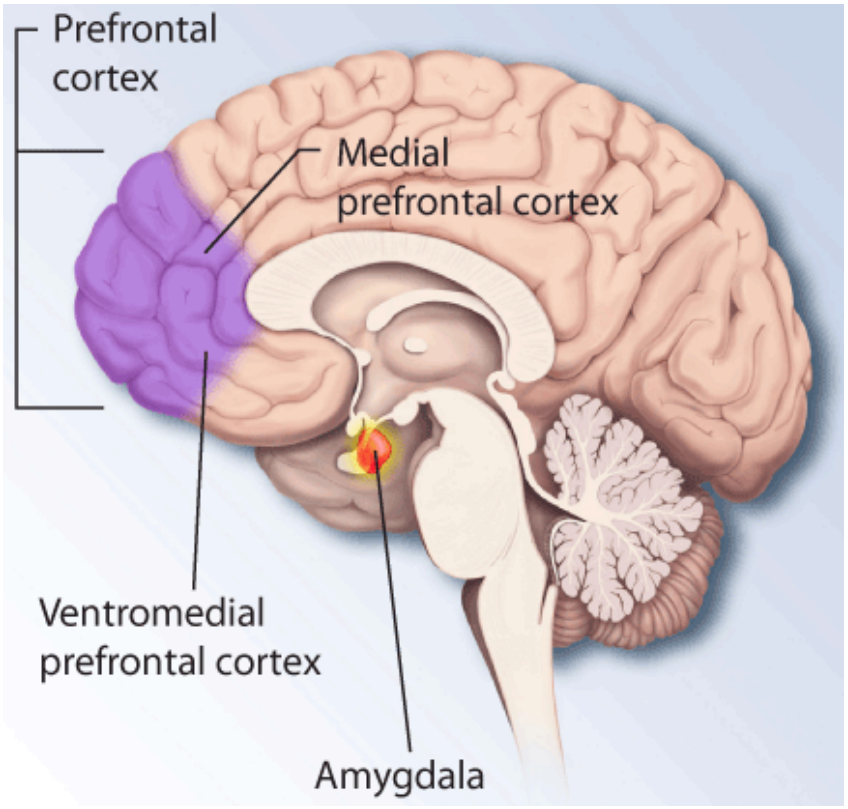


Image source: https://commons.wikimedia.org/wiki/File:Ptsd-brain.gif Further information: https://benjamineidam.com/phishing-anruf

2. Regular training courses and tests

As the: saying goes: “*You only learn boxing by boxing*”. It's the same with cybersecurity: you can only find out about security holes by attacking your walls. And the weak points that are revealed as a result are exposed and deliberately remedied. There are good opportunities to do this for the whole company Stress and / or pentests. For employees in particular, however, the best option is to make the secure option the standard option. So adjust the habits in a targeted manner. The easiest way to do this is through environment design.

3. No lethal data in public

A Lethal piece of data is any information which, if put into the wrong hands, can lead to serious or even devastating damage. Depending on the situation, for example, passwords, key cards, access codes, etc. A good rule of thumb is: "***Would you feel comfortable speaking to a group of people using a megaphone?***" If this thought of it turns your stomach upside down, make the phone call in the next room, think twice about writing down your password, etc.

4. Awareness of attack surfaces

Everyone is vulnerable, especially with virtual aids. Nothing new so far. But the specific weak points differ individually and according to personality type. An excellent introduction to the topic is this article by IT expert Philipp Schaumann. The best and at the same time fastest personality analysis as a starting point can be found here.

Ihr persönliches Profil
Was sind meine Prioritäten?
Was sind meine Angriffsflächen?

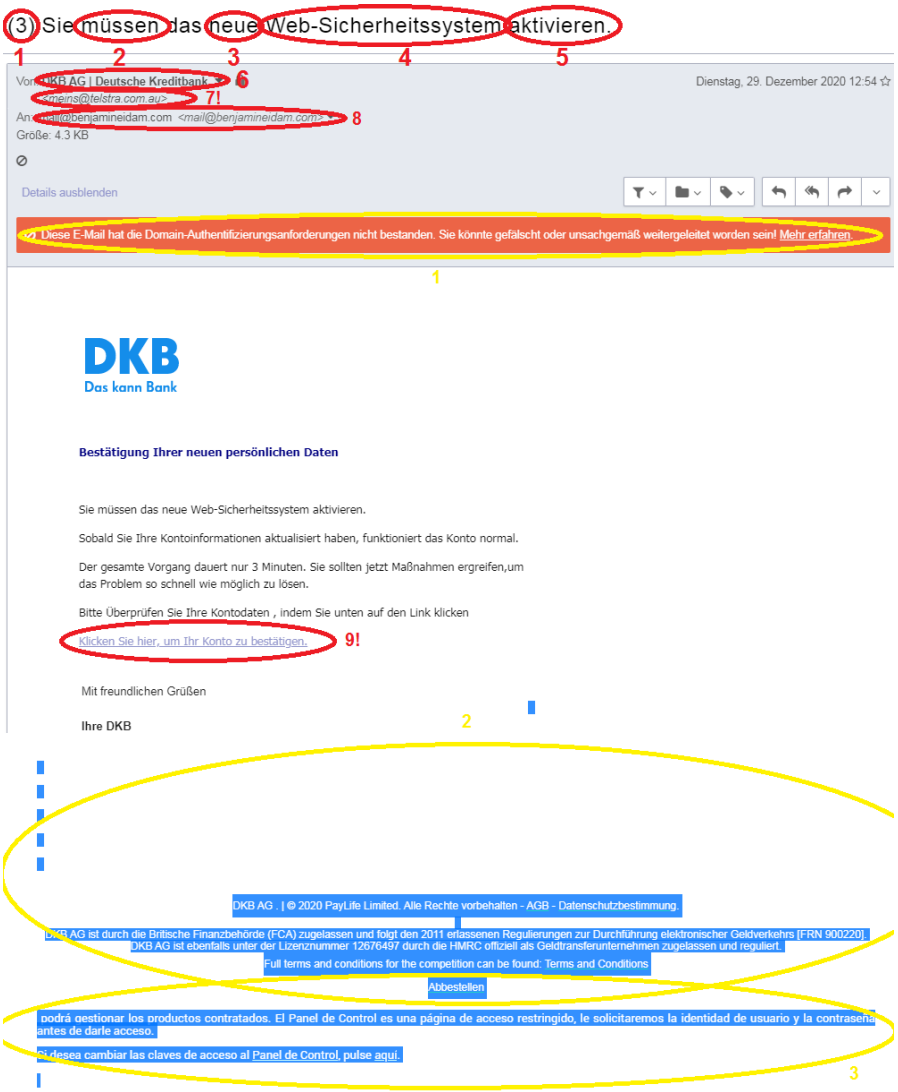
	Ihre Punkte	
A		Hilfsbereitschaft, emotionale Erpressung
B		Versprechen (gegenüber Kunden) muss man halten
C		Team-Player, Solidarität mit den Kollegen
D		Lob, Anerkennung, Schmeichelei
E		Unsicherheit, Schüchternheit
F		Konflikt- und Aggressionsvermeidung (Autoritäten)
H		Strikte Regeleinhaltung

Vulnerability profiles can be a good starting point for security awareness. Image source and further information: https://www.sicherheitskultur.at/social_engineering.htm

5. Avoiding the Biggest Danger on the Internet / Phishing

Phishing is the best digital crime weapon. Because it is extremely successful, very easy to adapt, easily scalable and if done correctly, not traceable. You can find out more about the disproportion and importance of phishing here.

You can find a complete guide to phishing mails here, the same about phishing calls here, more information about phishing, its types and much more here and a good quiz for checking your own knowledge here.



Anatomy of a phishing email. Image source and further information: https://benjamineidam.com/phishing-mails

6. Identity Abuse

The abuse of digital identities is another asymmetrical attack method. Depending on the scenario, the effort is almost negligible. The damage, however, can be gigantic. Job loss, divorce, stress with the personal environment and high loss of money are the relatively harmless effects. Suicide the worst.

The topic is very complex and has to be treated individually but two good starting points to see at a glance whether you are in danger or your own sensitive data is already in the wrong hands are these two pages:

- https://haveibeenpwned.com/
- https://sec.hpi.de/ilc/search?lang=de

In addition to the “classic” identity abuse, there is also the “synthetic” identity theft / abuse. With this, an artificial identity is made from one's own digital identity and thus damage is caused.

7. Mental Models

Mental models are contextual perspectives on situations.
For example, a botanist sees a biological treasure in a forest and thinks about protection strategies. An agricultural speculator, on the other hand, sees a monetary treasure in the same forest and thinks about sales.
Mental models can be extremely effective in solving cybersecurity problems, especially social engineering challenges.

Expert-Interview: Sai Krishna

Founder of the Global Cybersecurity Forum
Sai on LinkedIn

1.What are the 3-5 biggest mistakes newcomers make when they start cybersecurity?
- Influenced by the vendors, trainers and research papers
- Choosing a product from external recommendation, endorsement instead of looking at it from his / her own use case
- Missing key success criteria during poc (Proof Of Concept)

2. What mistakes are also common among professionals?
- Heavily dependent on technology
- Poor focus on people and processes
- Considering it as a cost center than a value creation center

3. What 3-5 actions bring the greatest impact to cybersecurity?
- Continuous upskilling
- Finding a right mentor
- Periodic assessment of skills applied VS only learned

Management

Managers, CEOs and bosses in various areas, groups and departments are a cybersecurity category in themselves.

From a technical point of view, they are also people and employees, so they are just as vulnerable.

In practice, however, it looks different: For people with responsibility and authorizations within companies, there is a separate “universe of attack”

Accordingly, the defense strategies must be fundamentally reconsidered / adapted here.

1. Regular training / test

For people with responsibility, security clearance and access to sensitive information, the tipps above apply even more for the management than for “the rest” of the workforce: Hardening one's own behavior is very important for the cybersecurity of the entire company. The 1½ approach works very well: Confident and routined action should either be ranked first or, at most, second, depending on the activity. For YMYL areas in first place, for all others to be decided individually. In other words: Before a bank manager can go about his daily routine, he must first of all be cyber-secure. Otherwise, he simply cannot do his job safely.

2. Stress- and Pentests as Routine

Due to the trivium of responsibility, releases and access, not only training courses but also regular simulation of the digital emergency are very important and even more important than for “normal” employees.
A good rule of thumb can be derived from the “effect proportion”: The results and regularity of stress tests must be proportional to the maximum effect of one's own action. For example, if the average employee has a maximum control over $ 10,000 before cross-checking, but a manager has $ 1,000,000, the results should be accordingly.
From a factor of ≥ 10, the results should be at least 90% in the last > 3 tests. From a factor of ≥ 100 even > 95% in the last> 3 tests.

3. No lethal data in public

Opening secret documents on a computer with its screen facing a public place or speaking data like credit card information loudly into the phone. There are situations that can quickly turn into sources of danger. Social media as a whole is like a giant honeypot and an invitation to it.

Rule of thumb: Use and edit YMYL data only behind closed doors, meaning in a secure environment.

4. Awareness of attack surfaces

There are literally an infinite number of attack possibilities on any digital target. For example, a computer can be attacked via the Internet, local network, storage media, inputs, programs, hardware hacks, etc. And computers are literally everywhere these days, as the “trend aloneSmart Home”shows.

A good rule of thumb to identify and contain attack vectors:

1. The honest and as completely as possible answered question: "What is important to me?" This can be anything from your own family to a new car or investment fund.
2. The answer to the question "What am I currently doing to protect the answer to 1.?"

3. The answer to the question "What can I do to protect the answer to 1.?" (For the widest possible range of answers you have this page)
4. The answer to the question “Does it make sense to take further measures? And if so, which ones? "

Here it almost always makes sense to look at and implement options and measures together with a professional. e.g. via individual training and coaching.

5. The stab in the heart / phishing

The difference between seldom priority targets and “normal” employees is as clear as it is with phishing. Because phishing + company VIPs = spear or whale phishing.
Spear or whale phishing also means e-mails which, if treated incorrectly, allow attackers into the target system. But spearphishing emails are a different matter. While normal phishing emails are more or less generic, sometimes have incorrectly translated attachments, sometimes the sender does not match the content, etc., spear phishing emails are insidious. Often with weeks or even months of preparation and precise tailoring to your goal.
Usually the preferences and preferences of the target are spied on, trustworthy proxies are hacked and the mail is sent from there, etc.

Distinguishing a phishing mail from a mail is like distinguishing a flower from a bush. For most people it is relatively easy and quick to do.

A whalephishing email, on the other hand, is like a blue flower to be distinguished from another blue flower. Feasible if you have a little background in botany. Otherwise potentially toxic.

You can find my guide on phishing mails here and on phishing calls here. For more information about phishing, its species and more can be found here.

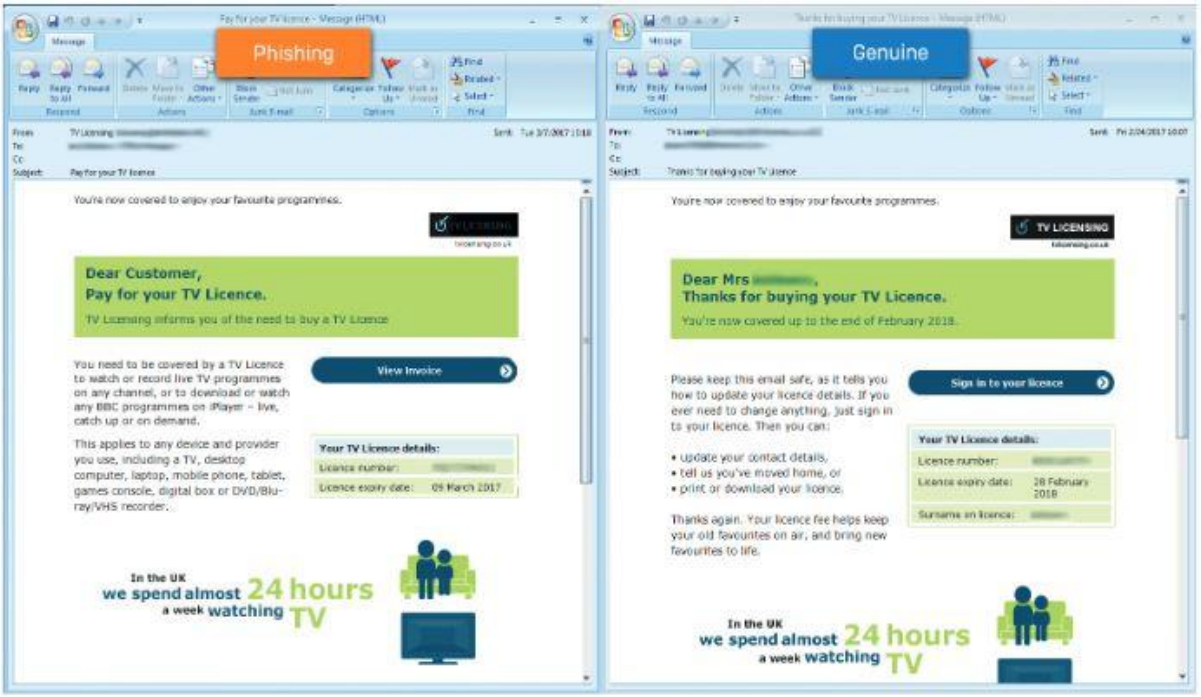


Image source and further information:
https://www.wud.de/it-security/7-gefaehrliche-phishing-angriffsmlösungen-die-sie-kennen-muessen/

6. Identity abuse

As already mentioned above, identity abuse is an important part of cyber warfare. And logically, an identity with more reputation, for example a manager, managing director or even a celebrity, is a more worthwhile goal than a “normal” employee, right?

When the big ones are hacked. Source:
https://twitter.com/tibor/status/1283502215039201282

Almost. That cannot be said in general terms. Here the “Goldilocks-Conditions” of cybersecurity apply:
The “digital nobody” is vulnerable and worthwhile. Celebrities and similar lucrative destinations as well. But dominating one's own digital brand makes it extremely difficult for attackers to succeed, especially in character assassination campaigns, stalking and similar attempts at identity abuse.

7. Mental Models

As already mentioned above, the correct mental assessment, attitude and the resulting options for action in the area of cybersecurity are essential for survival.

Two special rules apply to the most important employees of a company:

1. The person you talk to must be particularly trustworthy on all work-related topics. There are different schemes and checklists for this, a solid gut feeling with enough experience is a good start.
2. The potentially more productive and / or weapon-capable one 's own level of knowledge and workplace, the more likely an attack on the owner of it.

Mental models are extremely helpful tools in the cybersecurity context.

Companies

Companies are the main targets of cyber attacks because they are the main value-adding company of the economy.

3 rules of thumb apply here:

1. The higher the utility value, the more lucrative an attack.
2. The further away from cybersecurity expertise, the more lucrative an attack.
3. The closer to critical infrastructures, the more lucrative an attack.

1. Knowing and using security levels Controlling

Access sensibly can be a simple but asymmetrically effective security method. A good starting point and / or balance it maythe the DIN-Standardization Roadmap.Designing these together with all (relevant) employees can also the safety help culture.

TLP-Stufen

Stufe	Bedeutung	Bestimmungen
TLP-White	Unbegrenzt	Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP-White ohne Einschränkungen frei weitergegeben werden.
TLP-Green	Organisations-übergreifende Verteilung	Informationen in dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Information darf jedoch nicht veröffentlicht werden.
TLP-Amber	Organisationsinterne Verteilung	Informationen in dieser Stufe dürfen innerhalb der Organisationen der Empfänger weitergegeben werden, jedoch nur auf der Basis „Kenntnis nur wenn nötig". Der Ersteller der Information muss zusätzlich beabsichtigte Einschränkungen der Weitergabe klar spezifizieren.
TLP-Red	Persönlich, nur für benannte Empfänger	**TLP-Red-Informationen** sind auf den Kreis der Anwesenden in einer Besprechung oder einer Video-/Telefonkonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. In den meisten Fällen werden Informationen der Stufe TLP-Red mündlich oder persönlich übergeben.

The Traffic Light Protocol (TLP) levels of the Alliance for Cybersecurity are another good framework for orienting your own security sections. Image source and further information: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/_/merkblatt_verarbeitung_vertraulicher_informationen.html?nn=145680#download=1

2. Working with professionals

This point is probably (hopefully) not an insider tip: It makes sense, especially when it comes to the cybersecurity of your own company, to work with experts from different areas of focus. Or to have their updates on the screen. The CCC is a good starting point in Germany, the Security Googleblog is international.

3. Turning the Equation upside down

Many of the actions outlined here add up to more than the sum of their parts. As written in the chapter intro, the following applies: The less worthwhile a target is because it is comparatively too hardened, the less likely an attack is, because there are almost infinitely many other, simpler targets.
In other words: Every security measure increases security even without an actual attack, simply because it increases the attack effort and thus reduces the probability of an attack. (Of course, this does not apply to targeted attacks explicitly against your company based on an order, etc.)

4. Knowing the vocabulary

The technical vocabulary list is endless and hopefully the most important words are already covered here. When it comes to social engineering attacks, there are still a few key terms:

- DLP (Data Loss Prevention)
- UBA (User Based Analytics)
- SIEM (Security Information and Event Management)
- BRI (Business Risk Intelligence)
- IaaS (Infrastructure as a Service)
- PAM (Privileged Accounts Management)
- XDR (eXtended Detection and Response)
- XSS (Cross-Site-Scripting)

Of course, this list does not claim to be complete. Rather, it can be viewed as a helpful, conceptual addition and inspiration.

5. Follow the “Krebs-Rules”

If I had to choose only one cybersecurity expert that would bring the greatest, continuous and understandable value, it would be Brian Krebs.

He also wrote the three wonderful “Krebs-Rules”:

- **“If you didn't go looking for it, don't install it!”**
- **"If you installed it, update it."**
- **"If you no longer need it, remove it."**

If you're looking for an instantly actionable 80/20 starting point, these three rules are likely to be. Source of the 3 rules and more about them:
https://krebsonsecurity.com/2011/05/krebss-3-basic-rules-for-online-safety/

6. Basic knowledge for everyone in the company

The most important terms and their properties and meaning should be known to everyone with access authorization to a device with a display. This also applies to exclusive access rights in an emergency.
A good starting point is the BSI's cyber glossary.

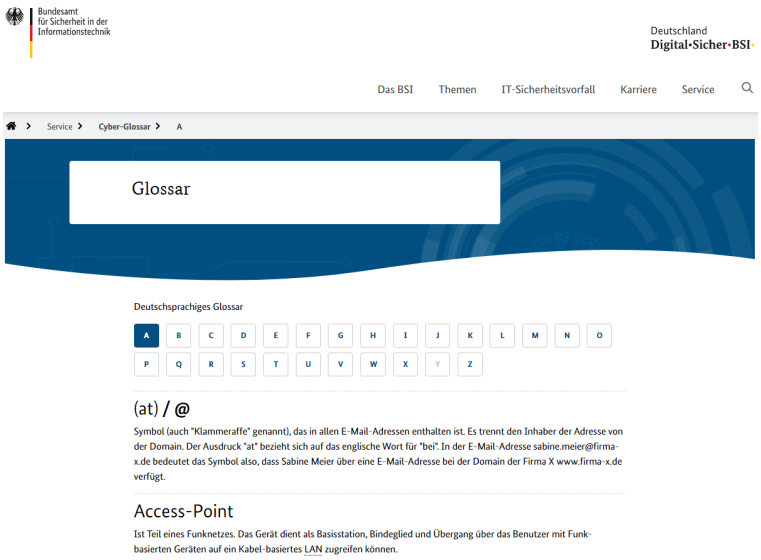


Image source and further information on the BSI's cyber glossary: https://www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/cyber-glossar_node.html

7. Recommendations from Edward Snowden

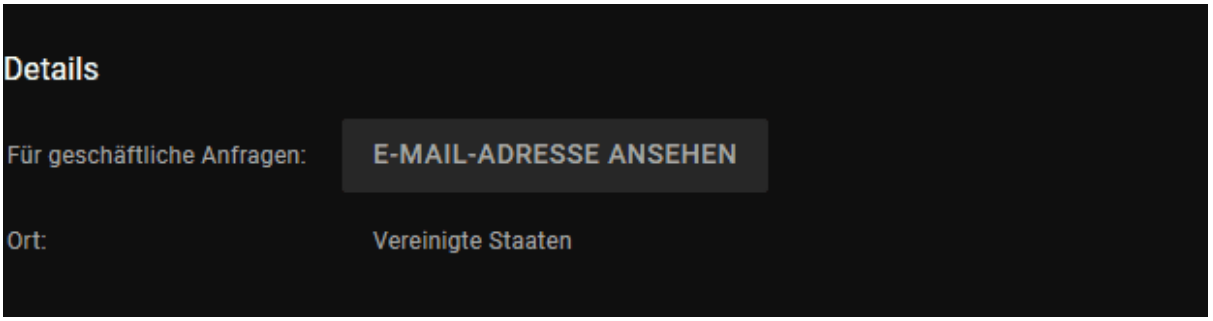
Another good impetus for improvement or review can be of internal processes and actions This short guide including tool recommendations and justifications from Edward Snowden. What makes these recommendations more trustworthy than those of other security professionals? This precise answer.

8. Security against Bot-mails

You want to prevent company addresses from being automatically collected, linked and then attacked by programs. For this purpose, it is worthwhile to harden them on your own websites (and generally to post on the net as rarely as possible). Possible ways to do this are, for example:

- Replace “@” with “(at)” or something similar. Example: xyz (ät) abc.de.
- Add additional characters to disguise the email address. Example: xyz@remove-this.abc.de.
- Only show the address as an image. Example: picture below.
- Upstream a captcha or encryption. Example: YouTube as seen in the .gif below.

One possibility to secure your email addresses against bots: choose a different display format.



Captchas can be good hurdles against bots.

9. Knowing and using security frameworks / NIST framework

The NIST framework is the best framework as a starting point for testing your own security processes. You can find the most important other frameworks here.

Source and further information: https://www.nist.gov/cyberframework/framework

10. Check the own defense (professional)

On penetration testing or simply "pen test" I continued already as discussed above. For larger companies / special attention to security, such tests by external service providers make sense. As far as you can come up with toolboxes and tools like Kali, a “real” pentest needs experts from outside the company. Combined with the continuous exchange with experts , this achieves a very good level of security.

11. Testing password strengths

Often referred to as “password auditing”. Cain & Abel and John the Ripper are the top addresses for it.

12. Network Security

This is where internal audits, stress tests and / or tests with tools such as CheckNetstumbler, Aircrack or KisMAC can be used .

13. Restricting access rights

As with the key words already mentioned and other points, it makes sense to implement “bulkheads”. So that not every employee, guest etc. has the same access. Can sometimes be a hindrance or even annoying, but it may save the company. Because an infected area is better than having the whole ship on fire. You can learn a lot from the Navy here.

14. Person controls / locks

Random, unannounced bag, system and person controls can be very effective. The sheer probability of these possibilities changes the feeling of security.
Depending on the scope, this tactic should be tested with caution and only further implemented after positive results. Because in almost every culture outside of Russia or China, this type of surveillance and interference with personal rights is not part of everyday life.

15. Use up to date Hardware

NASA cannot operate correctly thanks to problems with the hardware compatibility of older and current systems. However, this problem is not purely interstellar; mostly terrestrial systems are affected. Outdated hardware may not be able to run updated software, introduces vulnerabilities into inhomogeneous systems and leads to additional work that automatically leads to further vulnerabilities.
Since hardware is the basis for all activities and backups, fundamental work should be done here accordingly.

16. Digital Hailstorm / DDOS

DDoS, the “Distributed Denial of Service” is one of the easiest ways for attackers against unprotected systems to attack a company. A company's systems that are connected to the Internet, usually its websites, are attacked. The attackers “garbage” the systems until they capitulate and are no longer available. The most popular service for protection against DDOS attacks is Cloudflare.

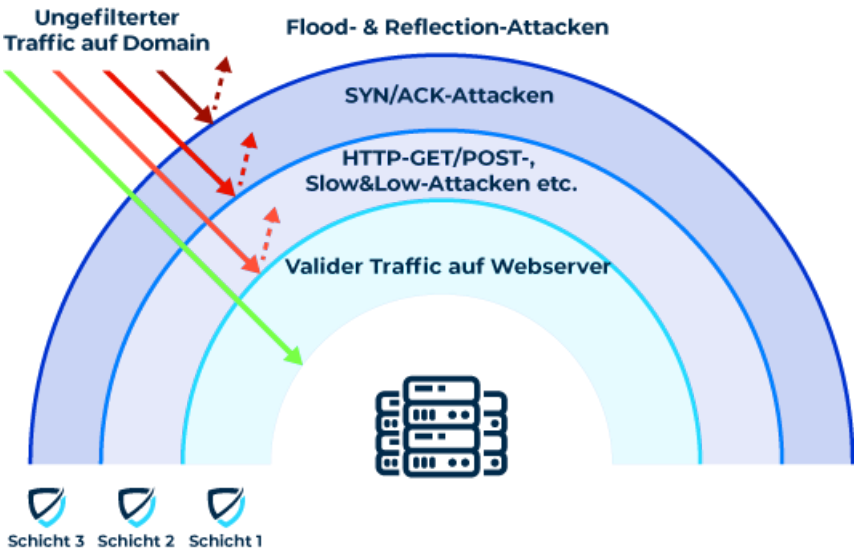


Image source and further information:
https://www.myrasecurity.com/de/was-ist-ein-ddos-angriff/

17. Injections

Injections, above all SQL injections, in short “SQLi's” are the misuse of programs by the Smuggling in foreign code / commands. Injections have been at the top of the list for years OWASP Top 10 Application Security Risks. You can find more about injections and measures against them here.

Threat Agents / Attack Vectors		Security Weakness		Impacts	
App. Specific	Exploitability: 3	Prevalence: 2	Detectability: 3	Technical: 3	Business ?
Almost any source of data can be an injection vector, environment variables, parameters, external and internal web services, and all types of users. Injection flaws occur when an attacker can send hostile data to an interpreter.		Injection flaws are very prevalent, particularly in legacy code. Injection vulnerabilities are often found in SQL, LDAP, XPath, or NoSQL queries, OS commands, XML parsers, SMTP headers, expression languages, and ORM queries. Injection flaws are easy to discover when examining code. Scanners and fuzzers can help attackers find injection flaws.		Injection can result in data loss, corruption, or disclosure to unauthorized parties, loss of accountability, or denial of access. Injection can sometimes lead to complete host takeover. The business impact depends on the needs of the application and data.	

Image source and further information:
https://owasp.org/www-project-top-ten/2017/A1_2017-Injection

Corporate Culture

A "quasi-dictatorial leadership with a climate of fear" in a company is the dream scenario for every attacker.

But "quasi-anarchy working" is also useless.

Long story short: Only if the company acts as a team, it is difficult for someone to drive a wedge into it from the outside. Otherwise, it is child's play to play employees at any level off against each other and manipulate them.

1. Idea Meritocracy

An idea meritocracy describes the principle that the best idea always wins. No matter who it comes from.
Thisby investor Ray Dalio and his company Bridgewater idea of idea meritocracy, coined and lived, is also a cybersecurity measure. Because nonsensical and security-endangering phenomena such as bullying, power games etc. are fundamentally defused. And esteemed employees hold no grudges and are not ignorant of potential dangers.

From a cybersecurity perspective, a shitstorm is one of the easier scenarios that employees can lead to. Image source and further information:
https://www.talkwalker.com/de/blog/krisenmanagement-wie-man-sich-auf-einen-shitstorm-vorready

2. Basic understanding of evolutionary biology

People act humanly. No sensation as far as that goes. But what this actually means in everyday (work) life is not yet scientifically known for a long time. And on the other hand, it is even less frequently taken into account.
This can prove to be a danger not only in terms of organization, but also in terms of safety.

Things like:

- decision fatigue (the more decisions made, the less energy for each further decision)
- tribal affiliation (humans are a group animal, which can be exploited)
- collective guilt (transfer of responsibility when performing an action)
- etc.

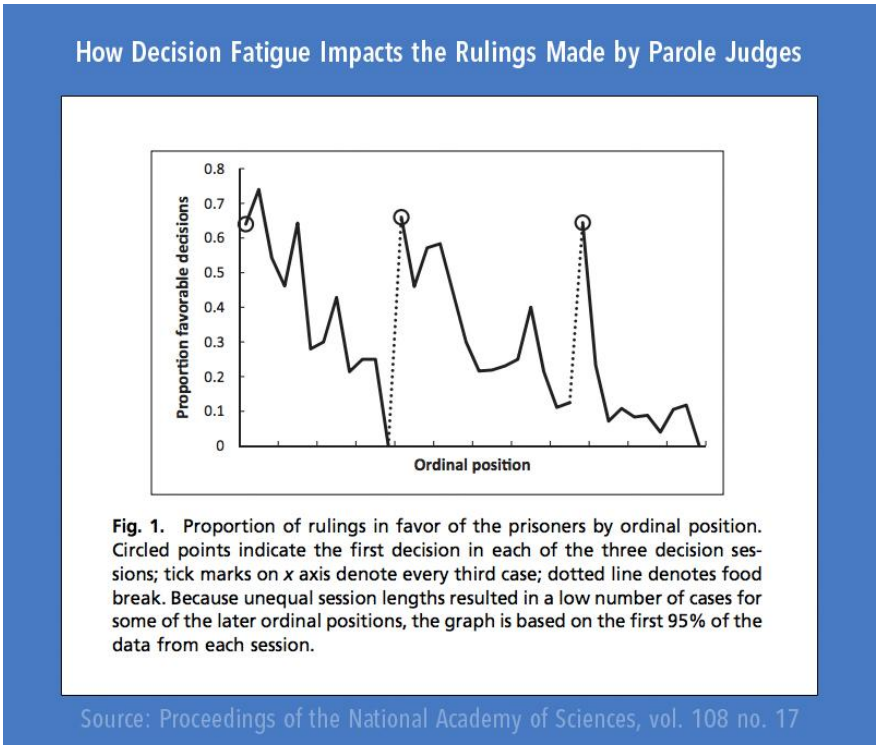


Image source and further information: https://jamesclear.com/willpower-decision-fatigue

3. Extreme Ownership

Extreme Ownership means that every employee behaves as if he were the owner of the company. It can roughly be translated as “extreme responsibility”. A company where this is lived alone is much safer against social engineering etc. due to proactivity, self-evident and mutual support, root cause control directly at the source etc.

Here you find Extreme Ownership brilliantly explained.

4. The group as a unit / team building

Cyber war at the latest inevitably makes a team out of thrown together employees. Or more precisely: it should be better.
Because the team is being attacked whether it feels like a team or not.
If one cannot ask the other or share his or her thoughts, an essential layer of protection against any social engineering attack is missing. Therefore: team building is a cybersecurity measure.

Expert-Interview: Kyle Lai

Kyle Lai is a Security Advisor, Investor and President, CISO & Head of Services of KLC Consulting, Inc.
Kyle on LinkedIn

1. What are the 3-5 biggest mistakes newcomers make when they start cybersecurity?

1) Start planning cybersecurity projects without understanding the company's business and without involving business teams.
   Different businesses have different attack vectors and threat actors. For example, you need to protect the user's privacy, user identity, access, and transaction integrity if you are in banking. If you are in the defense industry, your priority will be protecting intellectual property, sensitive government information, supply chain security, and manufacturing facilities. There are also regulations to comply with.
2) Communicate to business people without a common language.
   Newcomers tend to use many technical terms with business people, which degrades the relationships with business groups. New cybersecurity professionals should learn to simplify the technical terms to a common language that business people will understand. It is a better way to build trust and show that you are helpful to them.
3) Not ask questions when getting stuck with a problem - Ask for help. People are willing to help. The worst thing a professional can do is NOT ask questions when getting stuck with a problem, then make up excuses on why they can't complete a project.

2. What mistakes are also common among professionals?

1) Security pros tend to make too many assumptions when working with business teams and not ask questions. For example, assuming business people will like the new security solutions to be put in place, only to find out that business teams hated it after the deployment.
2) Stop learning is a big mistake. Technologies are advancing very fast. Security professionals must keep up with the technologies and trends; otherwise, they will get left behind.

3. What 3-5 actions bring the greatest impact to cybersecurity?

1) Conduct short and frequent security awareness training to all employees.
2) Do regular independent vulnerability assessment and penetration testing to address the company's unknown risks.
3) Enforce multi-factor authentication on all systems, on-prem and cloud. ID and Password alone are not sufficient.

4) Enhance identity and access management. Remove unnecessary privileges after a job transfer. Terminate accounts after job termination.
5) Get threat intelligence. The company should assign at least one security team member to track daily security news for new vulnerabilities, new threats and exploits, new emergency patches, etc.

Suppliers

An often overlooked part of the safety chain is the “before” and “after”.

There is no point in the thickest fortress if the caravan from the neighboring village brings a Trojan horse behind the walls.

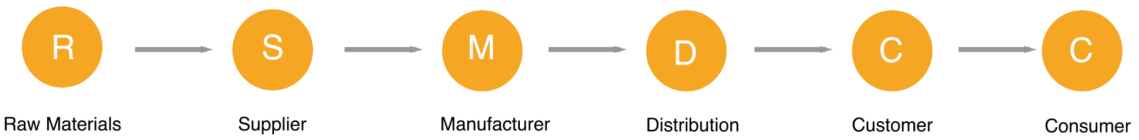
1. Security from start to finish / SSL

SSL certificates turn websites into “pipes” between sender and recipient that cannot be looked into. So you secure the connection from one end to the other.

This follows a similar principle to Quantum cryptography. Although theoretically unbreakable because it is based on the laws of nature, it still needs some development time to become practicable. For security planning, however, it makes sense to have this on the screen.

2. Interfaces / APIs

APIs, Application Programming Interfaces, are interfaces between your own software and the software of other users, programmers or companies. To secure this is a high priority, since the other side of the interface can not be controlled.



Example stations that must be secured all around. Image source and further information: https://en.wikipedia.org/wiki/Supply_chain_attack

3. External access- and roles (manage)

Almost every (larger) company has supply chains, “preparatory work” or similar links with other companies. Everything from the “classic” supplier to software testers following development. Since these links can add security gaps to a self-contained fortress, you should have them on your screen and implement appropriate measures. A good starting point is to record all contact points and then brainstorm about possible safety measures.

Environment

The environment and its effects are not adequately considered and taken into account in almost all areas of life.

In cybersecurity, this failure can create profound problems.

Let’s look at them:

1. Insert special glass

Your password can be read from your window: every click on a keyboard and every spoken word generates a specific frequency. This frequency is picked up by some surfaces, e.g. window panes, and generates a specific, measurable and interpretable vibration. These speaking and typing vibrations can be collected and processed under the right circumstances.

2. Use non-identifiable rooms

There are signal sources such as power lines that generate individual and clearly assignable patterns. For example, locations can be determined from the background noise of video messages.

3. Environment design / decision

“First you design your environment, then your environment designs you”.
What works by swapping a bowl of biscuits for one with apples also has an impact on cybersecurity. Posters, desk pads, easily visible storage locations for hardware keys , etc. can make the secure option the easiest option. And thus make cybersecurity the standard without any additional effort.

A good place to start when designing the decision architecture is “*What was this space designed for?*“ You can find instructions and more information here.

4. Understanding the depths of the Internet

Stolen data, accounts etc. very often end up in the Darknet and are sold there. Some data is stolen from the deep web and then offered on the darknet.
But what are the dark and deep web anyway? In a nutshell:

- Darknet: Internet section that can only be accessed with special software. (TOR etc.)
- Deep Web: Internet sections to which no link leads. If you know the link, you have access, otherwise the respective page is (theoretically) invisible.

The subject is very complex, but understanding these two key terms is already of great benefit.

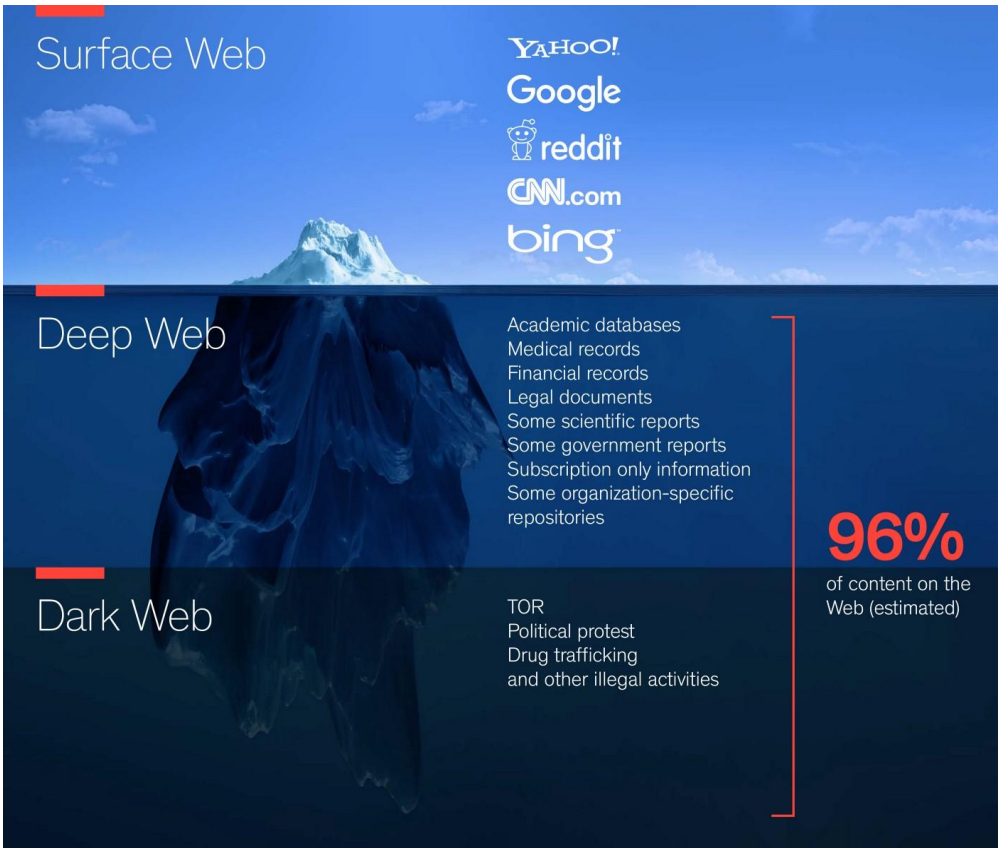


Image source and further information:
https://medium.com/@smartrac/the-deep-web-the-dark-web-and-simple-things-2e601ec980ac Using

5. Mapping services

Programs such as Google Maps or Open Street Maps are extreme in everyday life practically. But they can be used in the context of an OSINT analysis to find out targeted attack routes. Here it makes sense to discuss possible measures with experts.

6. Use “security corridors”

Especially in military and secret service systems there are sometimes “security corridors”. These are corridors full of high-tech equipment such as deep retina scanners, gait analysis tools, body heat scanners, etc. The aim of these corridors is to be able to identify the respective person in real time and with almost 100% certainty. The idea: Everything that is individual is suitable for identification. And the bigger the combination, the harder it is to forge anything. (Apart from direct hacking of the software)your
You don't have to use it in your own company. But it is good to know the possibilities to make decisions.

7. Security by Design

Security by Design is a holistic, i.e. holistic approach to the construction of software, especially apps. The best starting point I know of is this free, which lasts just a few minutes mini-course from Google.

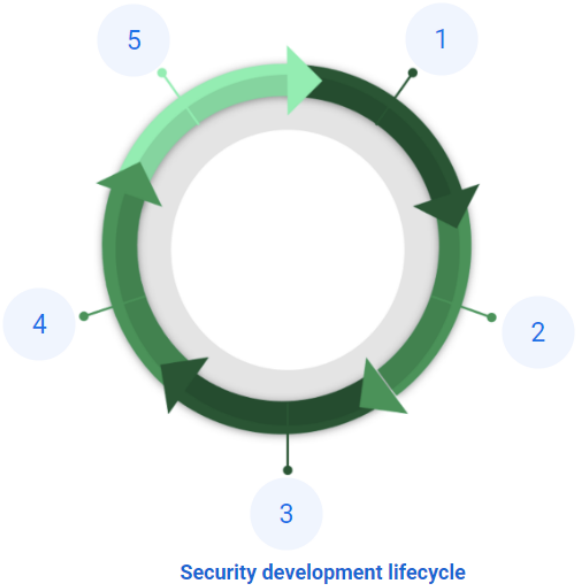


Image source and further information:
https://playacademy.exceedlms.com/student/path/63550-security-by-design

Expert-Interview: Cedric Mössner

Germany's most famous cybersecurity-teacher, computer scientist and lecturer in Barcelona and Frankfurt.
Cedric on LinkedIn

1. What are the 3-5 biggest mistakes newbies make when starting out in cybersecurity?

- When doing security, I think it's extremely important to set priorities. Because if you are given a budget that is far too small, as usual, there is no point in dealing with a secondary application in detail, but leaving the main application open to everything. Of course, a higher budget would be nicer, but that's rarely the case.
- In addition, it is often noticeable that checks are only made once (if at all). That is not enough, in the best case one has to search continuously.
- And that brings us to the third point: not from AI, but above all from humans. Tools are nice and good and allow a quick automated check during build, but it cannot be compared to a manual pentest, which should be done at least once a year.

2. Which mistakes are common among professionals?

- Unfortunately, I think that many professionals are too convinced of their own competence. You have to admit that you can't do everything and that one person always finds less than two.
- It is therefore important to get external help as well. The more you switch, the more different skills you pick up.

3. Which 3-5 actions have the greatest effects on cybersecurity?

- The employees are still considered to be the greatest gateway for malware. Therefore, the most important thing is often a good employee policy with a mandatory security key and training in social engineering.
- Constant monitoring and regular tests are another fundamental component, but one must not forget that malware can also penetrate from partners.
- That means that partners and suppliers are safe is almost as important as your own safety - even if it doesn't seem so.

Artificial Intelligence

Artificial intelligence (AI) has been on everyone's lips and active in almost every device for several years.

AI is probably the most important technology of this century and will accordingly revolutionize cybersecurity more than once.

1. Automated fraud detection

Artificial intelligence is getting better and better at detecting fraud, misappropriation and false statements and acting accordingly. Regardless of whether it is phishing, credit card fraud, forgery of ID cards, fake accounts, etc. AI can help with all of these and other areas. A good start is this article.

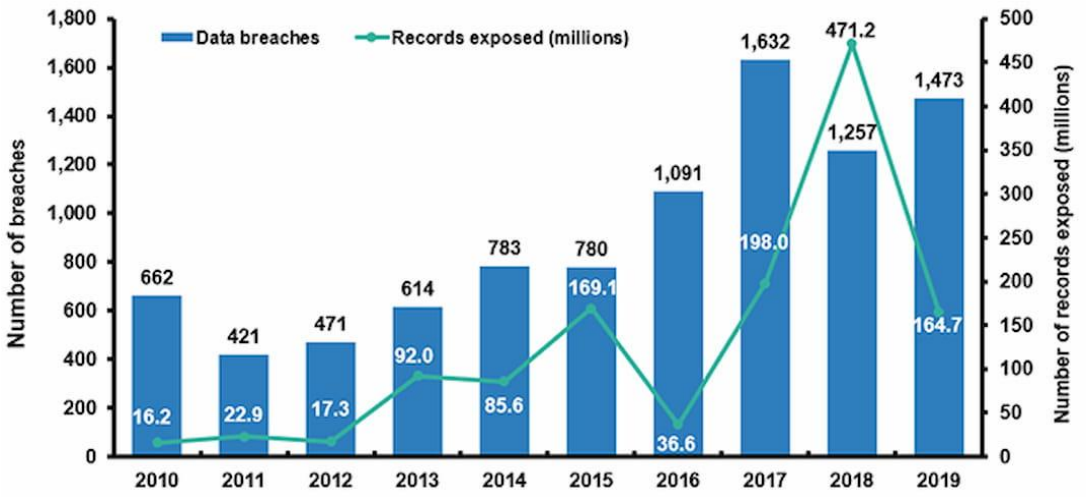


Image source and further information:
https://spd.group/machine-learning/fraud-detection-with-machine-learning/

2. Detecting data leaks at the speed of light

Machine learning in particular learns from (large) amounts of data and filters out patterns from them. Either with the help of a person (supervised learning) or independently (unsupervised learning).
In the case of large, complex data streams, AI can help detect data leaks and sound an alarm in real time.

3. Modeling of user behavior

People are creatures of habit. And artificial intelligences work great with patterns. If you combine these two variables with intelligent sensors such as gyroscopes, the evaluation of data streams and monitoring such as by cameras, etc., you have a high level of security against manipulation and forgery.
Regardless of whether it is checked in real time whether the real user is working on the device and document x. Or whether suspicious behavior is automatically evaluated and forwarded.

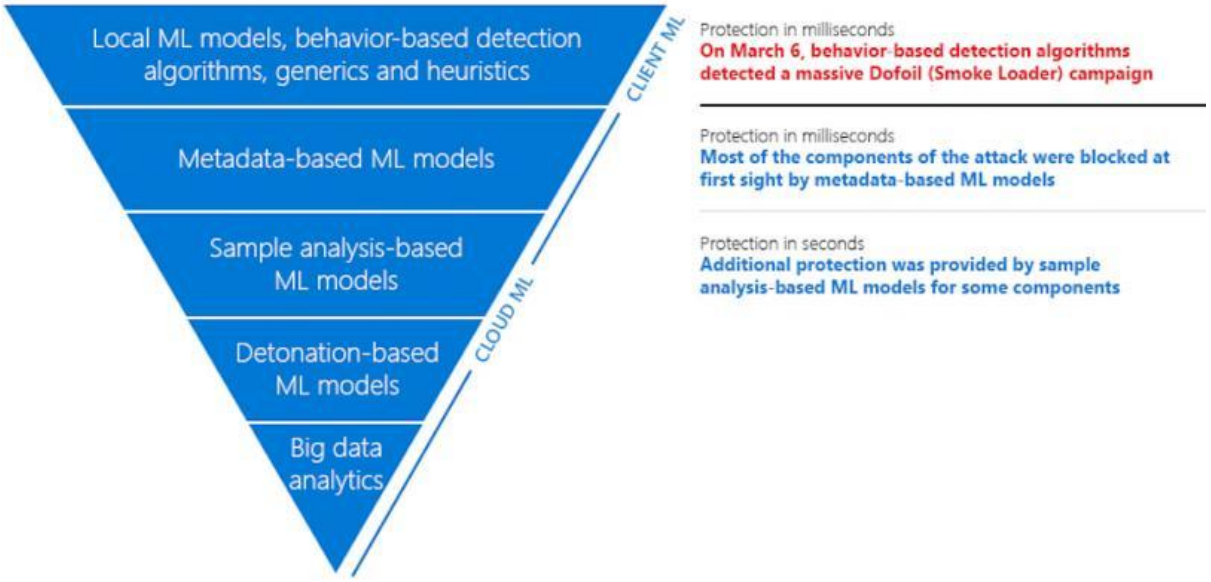


Image source and further information:
https://www.microsoft.com/security/blog/2018/03/07/behavior-monitoring-combined-with-machine-learning-spoils-a-massive-dofoil-coin-mining-campaign /

4. AI-powered anti-virus software / Endpoint protection

Most current anti-virus software is based on checking signatures in software. New malware is then simply checked against these signatures. But this does not work with, for example, reactive, i.e. self-changing code.
Artificial intelligence can play a crucial role in real-time protection here. Ransomware for example, can also be defused before it encrypts systems. The first larger providers such as Blackberry's Cylance are filling this exciting market.

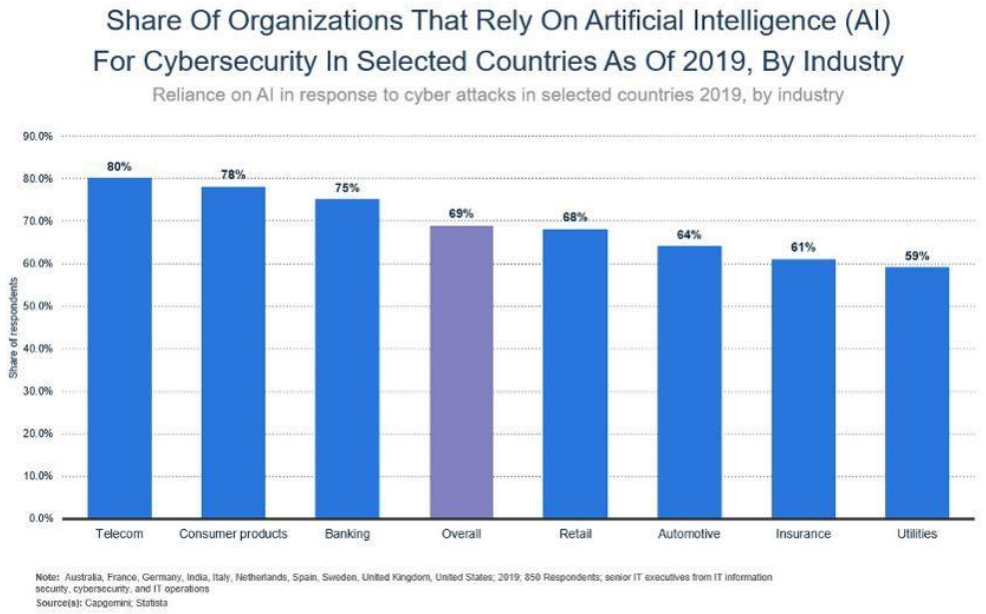


Image source and further information:
https://usmsystems.com/ai-ml-in-cybersecurity-use-cases-examples/

5. Vulnerability

Companies are faced with the challenge of managing and prioritizing the large number of new vulnerabilities they encounter every day. Traditional vulnerability management techniques only respond to incidents after hackers have exploited the vulnerability.

AI and machine learning techniques can enhance vulnerability databases and improve vulnerability management. This can help protect companies even before vulnerabilities are officially reported and patched.

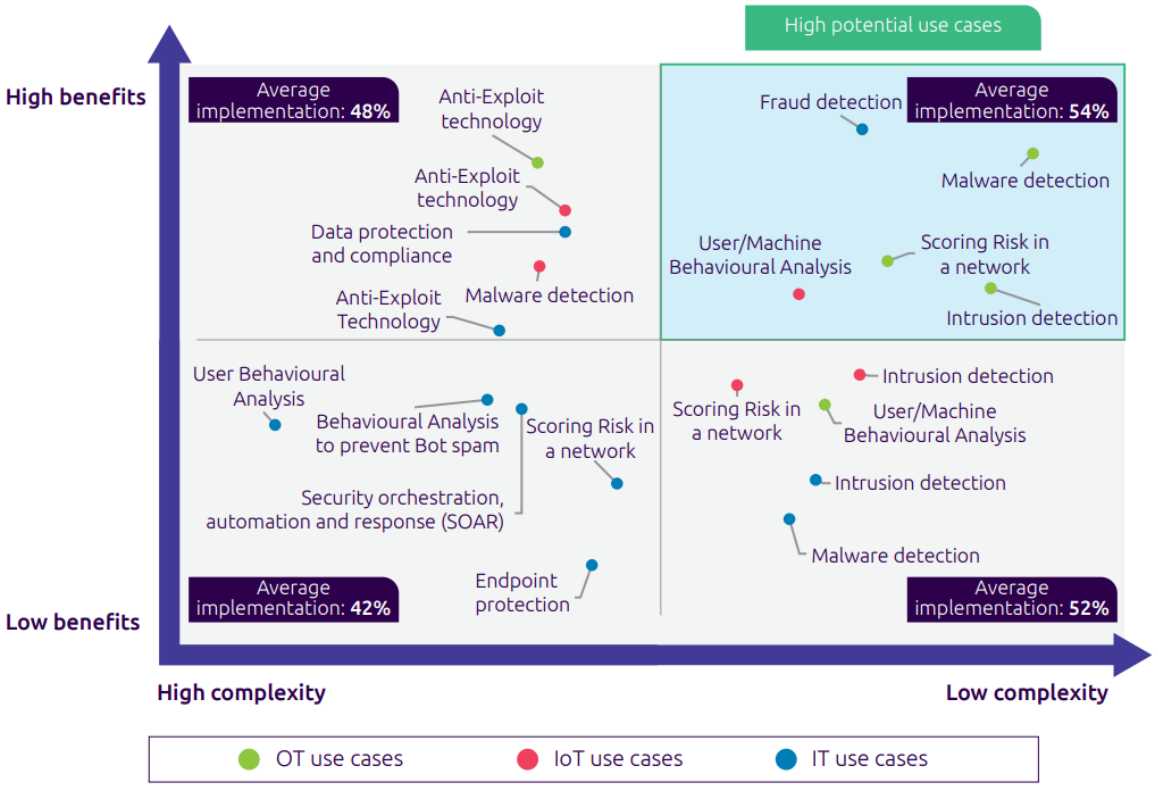


Image source and further information:
https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf

6. Identification of network threats

It takes a lot of resources to monitor all the data streams flowing in and out of the company. Not to mention the evaluation.

Finding out which data packets are dangerous and reacting in good time is one of the greatest challenges of cybersecurity. Artificial intelligence can provide better and better support here.
Companies like Esentire are increasingly specializing in these fields with AI.

7. E-mail monitoring

As already mentioned in the sections on phishing, the flow of conversations via e-mail is one of the central sticking points of cybersecurity. Machine learning can support recognition to increase speed and accuracy and to analyze texts via natural language processing. Coupled with hardened employees, such an attack is then almost impossible.

8. Fighting bots

Automated threats can no longer be countered with manual measures alone. AI and machine learning help build a thorough understanding of website traffic and differentiate between good bots (like search engine crawlers), bad bots, and people.

AI enables the analysis of a huge amount of data and allows cybersecurity teams to adapt their strategy to an ever-changing landscape.
Companies like Netacea are working on such services.

9. Predicting burglary risks

Artificial intelligence can monitor the number, usage and other vectors of devices, users, software and more in real time. And at the same time compare with the permitted accesses and protocols and, if necessary, submit a report.
This constant digital inventory enables algorithms to identify and report weak points and targets.
For example, if there are computers with high access levels on the street side of a building in which people outside the company regularly go in and out.

10. Shortening the reaction time

Artificial intelligences are (way) faster than humans. That is why we have autonomous driving.
In times of AI-supported attacks, it is no longer possible to register, categorize and ward off attacks almost in real time. Companies like AtoS are working on such solutions.

Table 1. Labor hours spent containing cyber exploits each week	Not facilitated by AI	Facilitated by AI	Difference in hours and cost
Organizing and planning approaches to cyber defense	25.32	16.05	9.27
Capturing actionable intelligence about cyber exploits and malware infections	80.20	41.11	39.09
Investigating and detecting application vulnerabilities	195.88	70.48	125.40
Investigating actionable intelligence about cyber exploits or malware	66.28	24.23	42.05
Cleaning, fixing and/or patching networks, applications and devices (i.e., endpoints) damaged/infected by cyber exploits or malware	212.89	39.63	173.26
Documenting and/or reporting upon the cyber event (in conformance with policies or compliance mandates)	25.07	15.91	9.16
Time wasted by security staff members chasing erroneous or false positives	400.83	41.42	359.41
Unplanned downtime due to cleaning, fixing or patching of malware-infected networks, applications and devices	3.95	1.90	2.05
Total hours per week	1,010.42	250.73	759.69
Total hours per year	52,541.84	13,037.96	39,503.88
Estimated total cost per year	$3,283,865.00*	$814,872.50*	$2,468,992.50*

*IT and IT security fully loaded pay rate is $62.50 (source: Ponemon Institute).

Image source and further information: https://www.ponemon.org/

11. Improvement of the (data center) architecture

Artificial intelligence has already led to incredible optimizations in the energy consumption of data centers. Itdesigns the most complex structures automatically.
AI can also make a major contribution to optimizing security architecture such as floor plans, equipment such as cameras, etc.

Google's data centers are AI-optimized. Image source and further information: https://www.wired.com/2012/10/ff-inside-google-data-center/

12. Automated counterattacks

Artificial intelligence can bring the possibilities of digital defense from pure defensive and reaction to offensive action . In this way, attackers can be learning algorithms spied on using and their identity can be decrypted. And the results can be forwarded directly to the responsible authorities with a little bit of additional code. Real time.

In the story of “sword against shield, burglar against defender”, in which the defender 's side was always condemned to react, something changes for the first time.

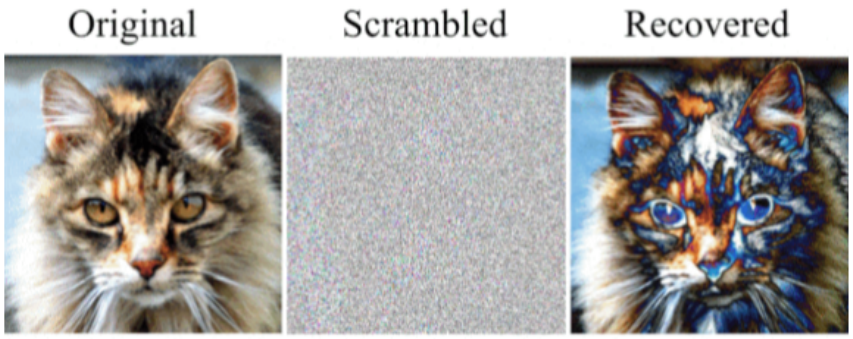
13. AI sandboxes

As I mentioned above and go deeper in an article for Societybyte, “AI sandboxes” are becoming more and more important.

Because only an intelligent simulated environment can keep up with intelligent, self-changing algorithms.

14. Reverse Blackbox

AI can also test intelligent algorithms and climb "backwards up the waterfall" to see if there are any weak spots. If there is access to the attacker AI, its own AI can go backwards along its layers of the neural network and thus decipher the attack algorithm. Based on this, it is then easy to take countermeasures.



Source and further information: https://read.deeplearning.ai/the-batch/

15. Identity

Artificial intelligence canfor example through Imagereverse image search, sentiment tools such as assurance analysis virality maps prevent one's identity from being digitally misused,. Regardless of whether it is classic, i.e. the “original identity”, or synthetic, in which real data are mixed with artificial data in order to achieve a result.

This person does not exist and probably never will. Image source and further information: https://thispersondoesnotexist.com/

16. Cyber-Security

With the right algorithms and the right training data, it is possible to secure against physical attacks in an automated way.

Image source and further information: https://read.deeplearning.ai/the-batch/issue-75/

17. AI as a helping hand

Artificial intelligence can be used as a permanent partner in one's own digital defense. For example, to find sources of errors in one's own code, to make suggestions for hacks / vulnerabilities or to give hints about potential problems.

Habits

Most non-technical cybersecurity tips and approaches have a sub-optimal starting point. They assume that enough fear and / or understanding will automatically lead to the right action.

But people are efficient. They always routinely do what is easiest, most energy efficient.

That is why it is of fundamental importance to harden habits in a targeted manner.

Because only security that has become routine is really security that earns this title.

1. (Trained / Experience-based) Mindfulness & Skepticism

In the internet and digital space, the “Turkish bazaar” rule applies: In principle, mistrust the entire experience and every interaction with another user.
The more potential value is in the room, the more the presumption of guilt should be considered as “default mode”: someone wants to attack you or at least manipulate you until the opposite is proven.
There are two ways to come to this kind of “experience awareness”:

- Years and decades of experience and learning from it.
- Work with experts.

In addition, a basic understanding of computer and network technology helps enormously.

2. Use a separate password for each input

This rule is as old as it is self-evident and has many advantages:

- Even if a service you use is cracked, all other accesses remain unassailable on the password side.
- Combined with tools such as password safes option, this option is easier than the alternatives.
- In threatening situations, you can credibly deny that you know the access. Because you probably don't know it. (If you work with encryption and password tools)

Of course, **the same rules apply to every single new password**.

3. Choose the correct username

To make counter-information a habit and cover your tracks the more you lay, it makes sense to use separate data for each profile.

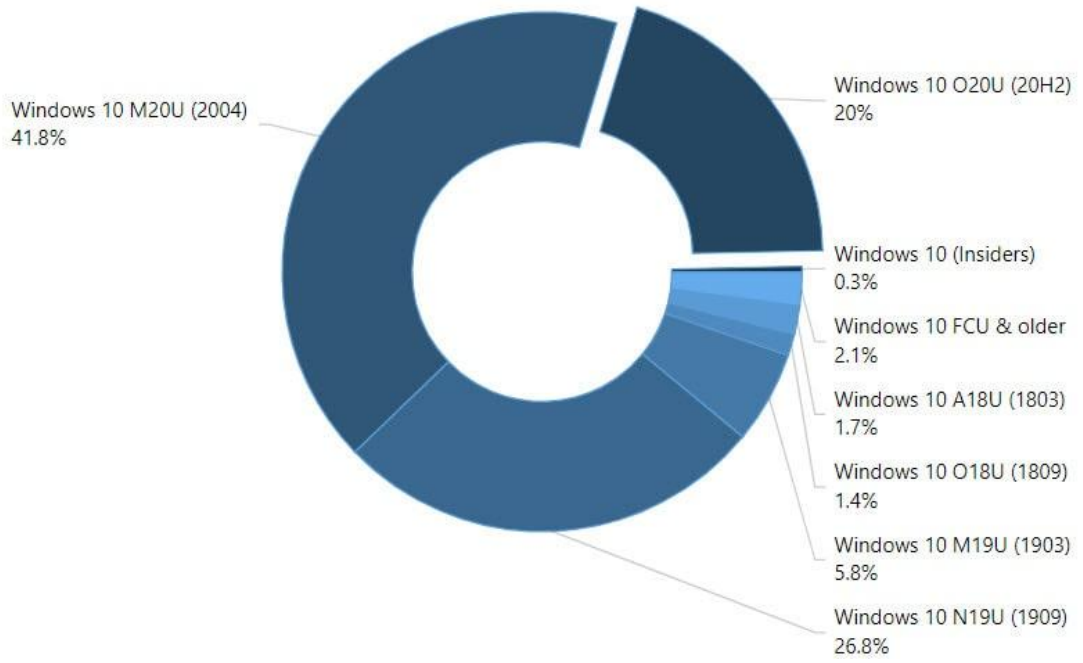
The more independent and confusing / generic, the better:

- For example, on a forum your name is "Archangel789"
- On Facebook you are called "ManfredMüller07".
- On a rating website you are called "Cucaracha_ox" etc.

Important sidenote: **The profiles should have as few common links as possible**. So, for example, share at most one anonymous mail address / [disposable address] independent of your default one, etc.

4. Use updates as soon as possible

As in the “Krebs-Rules” already mentioned, this is one of the habits with little effort but enormous effects. Combined with regular backups, virtual systems etc. for further security, this routine minimizes the attack surface enormously.



Update speed using the example of the operating system. Image source and further information:
https://www.drwindows.de/xf/threads/statistik-windows-10-version-20h2-l%C3%A4uft-jetzt-auf-jedem-f%C3%BCnften-pc.174662 /

5. Regular backups

As already mentioned several times, backups are very important. Because a defective data cluster can destroy all of your work. Therefore, you would like to:

- Have regular (minimum 2x per year),
- happily automated,
- mirrored backups created and
- check them (at least randomly)

You can also outsource this process. However, as always, the rule of thumb applies: What does not happen on your devices is insecure. It doesn't matter whether encrypted etc. or not

6. Stay informed and adapt if necessary

Cyberspace is a world of its own, and in every world the rules of that world apply.
Therefore, it is of central importance to stay up-to-date on your own. Away from and in addition to training courses, etc.
Because everyone has to deal with digital, networked technology all the time. Even if there has just been no training.
Good active starting points in Germany are heise and Golem.
Good passive starting points can be tools like Google Alert for keywords like "cybersecurity" or "hacking". Or individualized tools like search widgets or Google's Discover.

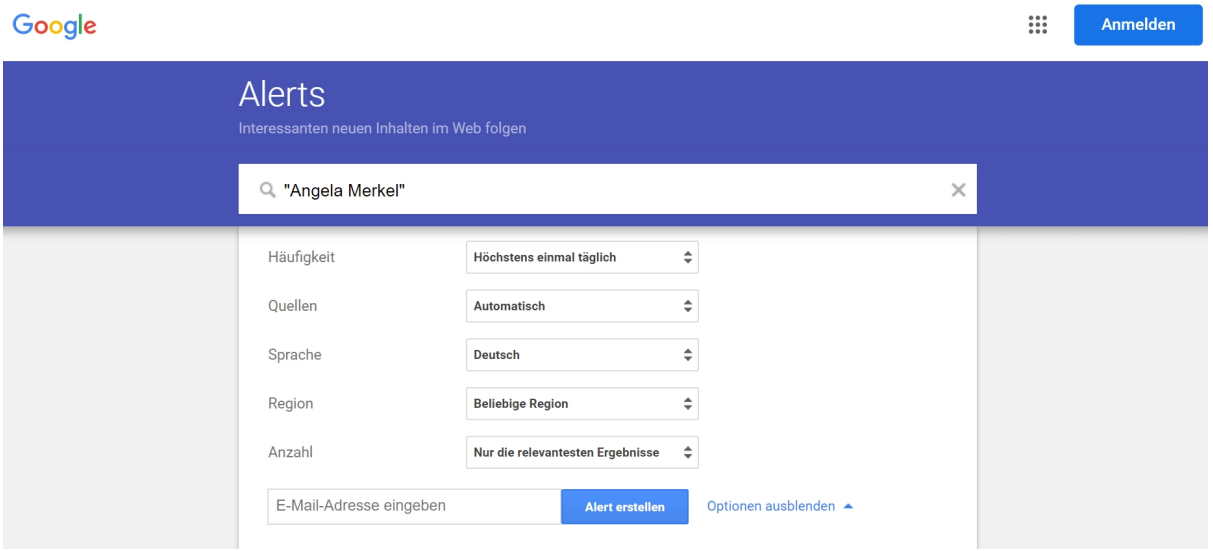


Image source and further information on Google Alerts: https: // reputationup.com/de/google-alerts-leitfaden/

7. Only download things from secure sources

This point is one of the most obvious on this list. It is the digital equivalent of “snacking on nothing in the pharmacy”.
Yet too often it is overlooked or implemented incorrectly.
Safe sources are:

- Always SSL-encrypted (have an httpS in the URL)
- Almost always online for more than 10 years (can be checked with for example this tool)
- Generate a “good gut feeling” (if you have been to more than 100 websites in your life, you will you know what I mean)
- From verifiable and highly reputable sources (e.g. journalists etc.)

Of course, these rules do not always apply, but they are helpful guidelines.

8. Living in a data-saving way

Since the Internet is a network of many computers with hard drives, the network literally forgets nothing. Because every piece of information that exists is “somewhere on a hard drive punched”.
In other words, the less data you generate, the more secure it is. Even counter-information is only the second best strategy. (Just because it means more effort and is never 100% secure)

9. Separating data streams

To further complicate the creation and tracking of profiles, it is worth separating your data streams. The most popular division is between professional and private activities.
This can mean, for example, online banking only via browser A and online shopping only via browser B. Or only carry out online searches via device A and only open via device B, etc.

company accountsCombined with fake accounts, automated counter-information, hardened devices and software, etc., this can be a sensible routine. You can find more on this topic, which is somewhat more complex in detail, in [this article](#).

Same system, different profiles: One way of separating data streams. Image source and further information:
https://blog.everphone.de/geschaeftliche-und-private-daten-trennen-smartphones

10. Change preset passwords on new devices

As already mentioned in the sections on passwords, this measure is very simple and at the same time very effective. With some devices, the passwords are always the same by default. (e.g. place of manufacture, year of manufacture) This means that an attacker may be able to enter passwords that have not been changed correctly on the first attempt.

11. Keeping rights & profiles up to date

What applies to companies in particular also applies to private life. For example, you should never leave access from ex-partners in your own system for longer than necessary.

12. Deleting / destroying not required on a regular basis

data that isSince data carriers can become as already mentioned potential “hostages”,, it makes sense to keep them clean at least using software. Depending on the lethality of the data, the hardware of a hard drive should also be destroyed at the end of its life. My favorite on the software side is Eraser, as it can overwrite data according to military standards.

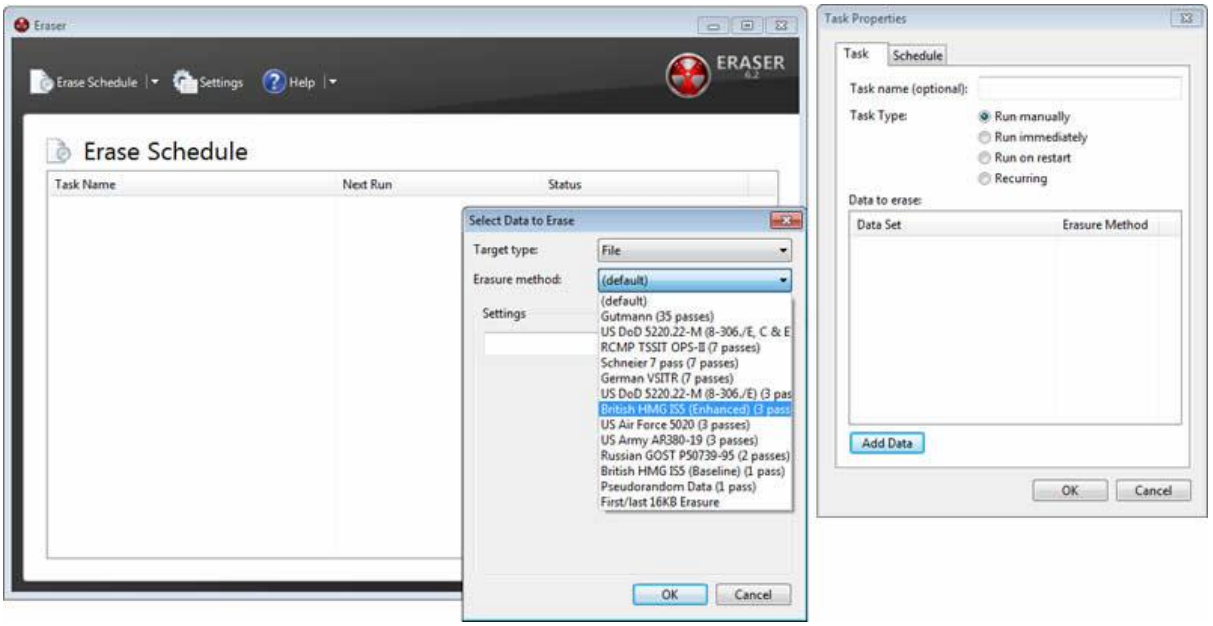


Image source and further information:
https://www.datenrettung-ffekten.de/datenloschung/14-freeware-programme-zur-sicheren-datenloeschung.html

13. Being able to read links Reading

and interpreting links is probably the most important skill for using the Internet safely. You can find out more about this in this article.

14. Avoiding / minimizing cyberbullying

This is one of the most difficult points of this basic guide. Basically, the rules of thumb and rough recommendations apply:

- Live data-sparingly.
- Work with counter-information.
- Retain sovereignty over your digital identity.
- Be mindful of changes that may indicate hacks.
- Be skeptical.
- Use automated tools to notify you of updates about yourself.

Further, active countermeasures are difficult to recommend, as these

- must be weighed up and implemented individually.
- Legally, you can move in the semi-illegal to illegal area,
- require know-how and a defensive personality.

15. Credible denial / ignorance

With the right tools, this tip can very quickly become a subconscious routine that helps especially in (life-threatening) exceptional situations.
Tools like Veracrypt allow so-called “hidden volumes” to be created within an encrypted container.
These hidden volumes allow you to release access to your encrypted container in an emergency without the attacker actually receiving valuable data.
That can save you from dire consequences .

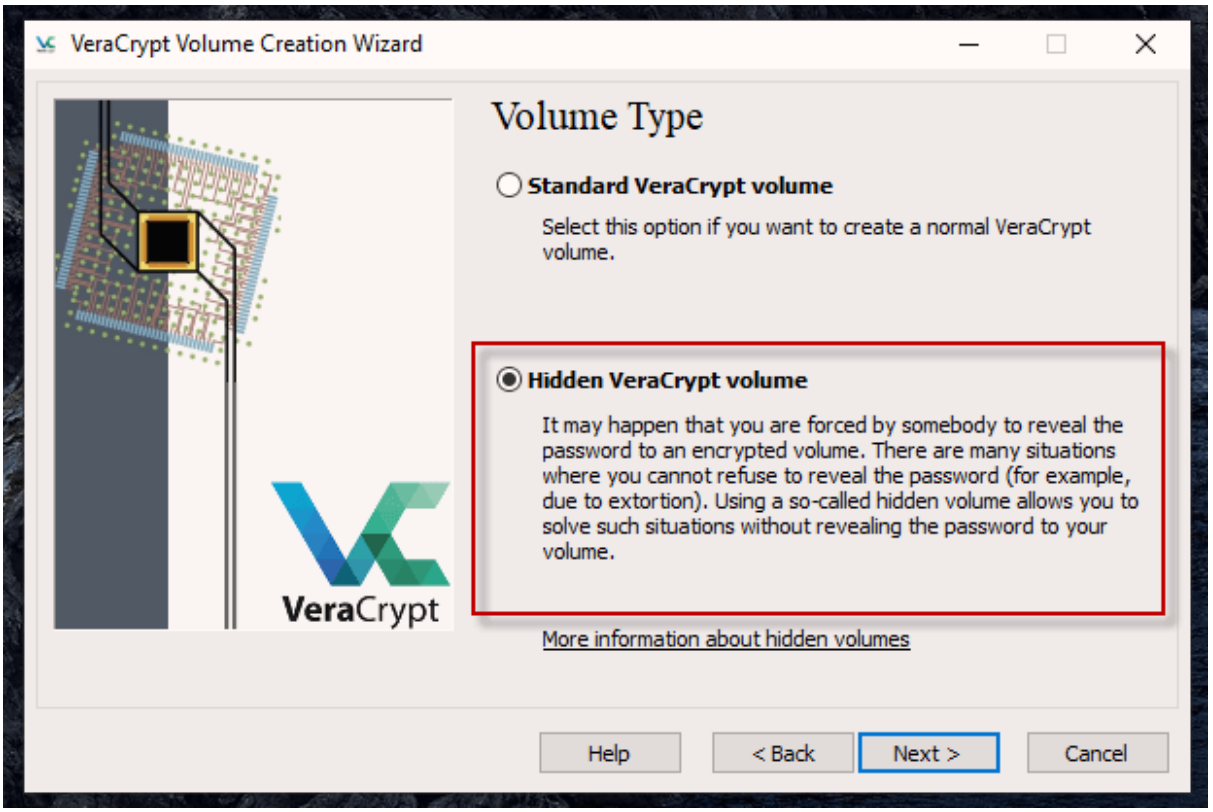


Image source and further information:
https://www.online-tech-tips.com/computer-tips/how-to-add-a-hidden-area-inside-an-encrypted-veracrypt-volume/ Set

16. Social media correctly

Here expediency and sovereignty over one's own digital presence applies. Only post on the Internet what a) a headhunter should see and b) meet your privacy requirements. This can mean that apart from your LinkedIn profile, all others should be private and anonymized. Otherwise OSINT-based attacks are extremely easy.
Here it is worthwhile to check all services about once a year whether all settings are still optimal / something has changed due to updates.

FAQ

1. Why exactly this classification?

From a technical point of view, cybersecurity consists of three components: hardware, software and people, i.e. the user of the first two. In order to make the tools and tactics shown here recognizable at a glance and to make them immediately applicable for every reader, I decided on this categorization. Every device user has to work with hardware and software. But an employee without security clearance and responsibility needs different ways of acting than a corresponding manager. Hence this division.

2. What do I do if I am missing a tool or have a question?

The easiest way is to leave a short comment below this page. I will then update them accordingly or reply to this comment.

3. Where is there more?

There is a good overview of tools here, a good introduction to deepening in this video and a good start to dealing with various helpful tool providers here.

About the Author

Benjamin Eidam is a consultant who secures key employees of innovative companies against hacker attacks and data theft through security awareness coaching and social engineering training.

Web:
benjamineidam.com

Mail:
mail@benjamineidam.com

LinkedIn:
https://www.linkedin.com/in/benjamin-eidam/