

IT security in everyday student life

Angelika Müller – Referentin für Datenschutz und IT-Sicherheit

Technische Universität München

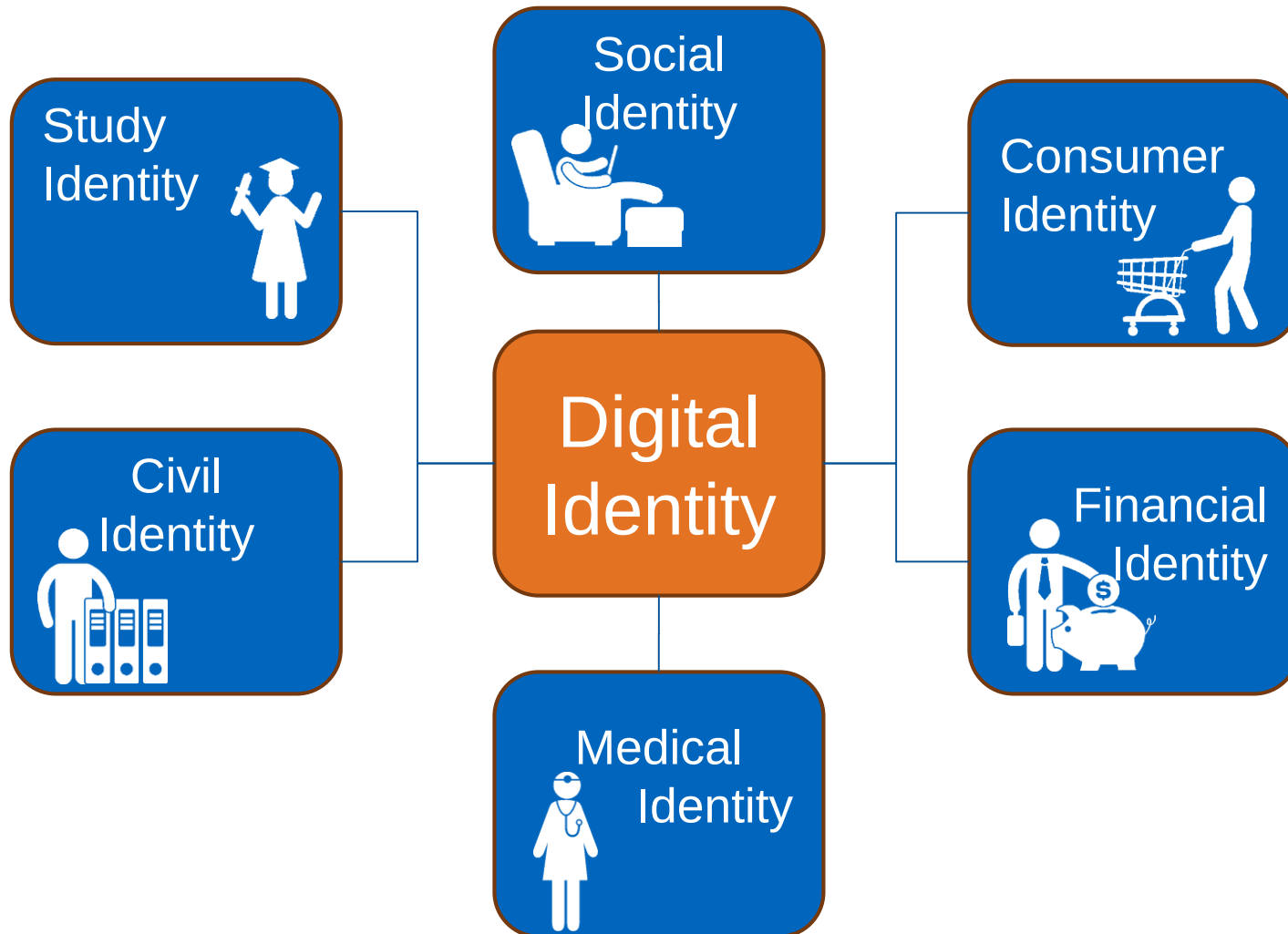
IT-Servicezentrum

Oktober 2016



**ICH WILL'S
SICHER!**

Your Digital Identity – Who am I - and if so, how many?



Your TUM-Identity

- Identification of TUM students
 - TUM email address
 - TUM ID
 - Student number
 - StudentCard (Student number, library number, Card number)
- John.doe@tum.de
- *go42tum*
- 0123456789



Your TUM-Identity: TUM Account

Capabilities of the TUM Account

- Write and send emails
- Administer study matters (*registration for lectures and exams, find grades,...*)
- Use Moodle
- Use Wi-Fi and VPN
- Download software
- library services: search for articles and journals, download eBooks
- Use TUM Storage
- Use TUM-“DropBbox” (Sync&Share)
- etc.

➔ You can use all these services with one ID and one password.



Protection for your digital TUM identity

- Use a separate password for your TUM identity
→ no reuse of passwords of another digital identity

Adobe's Hackers Release Top 100 Most Common Passwords

Posted by Mersad On November 9th, 2013 / Comments Off on Adobe's Hackers Release Top 100 Most Common Passwords

Empfehlen 8

Another Day, Another Hack: 117 Million LinkedIn Emails And Passwords

May 18, 2016 // 04:00 AM EST

Dropbox hack leads to leaking of 68m user passwords on the internet

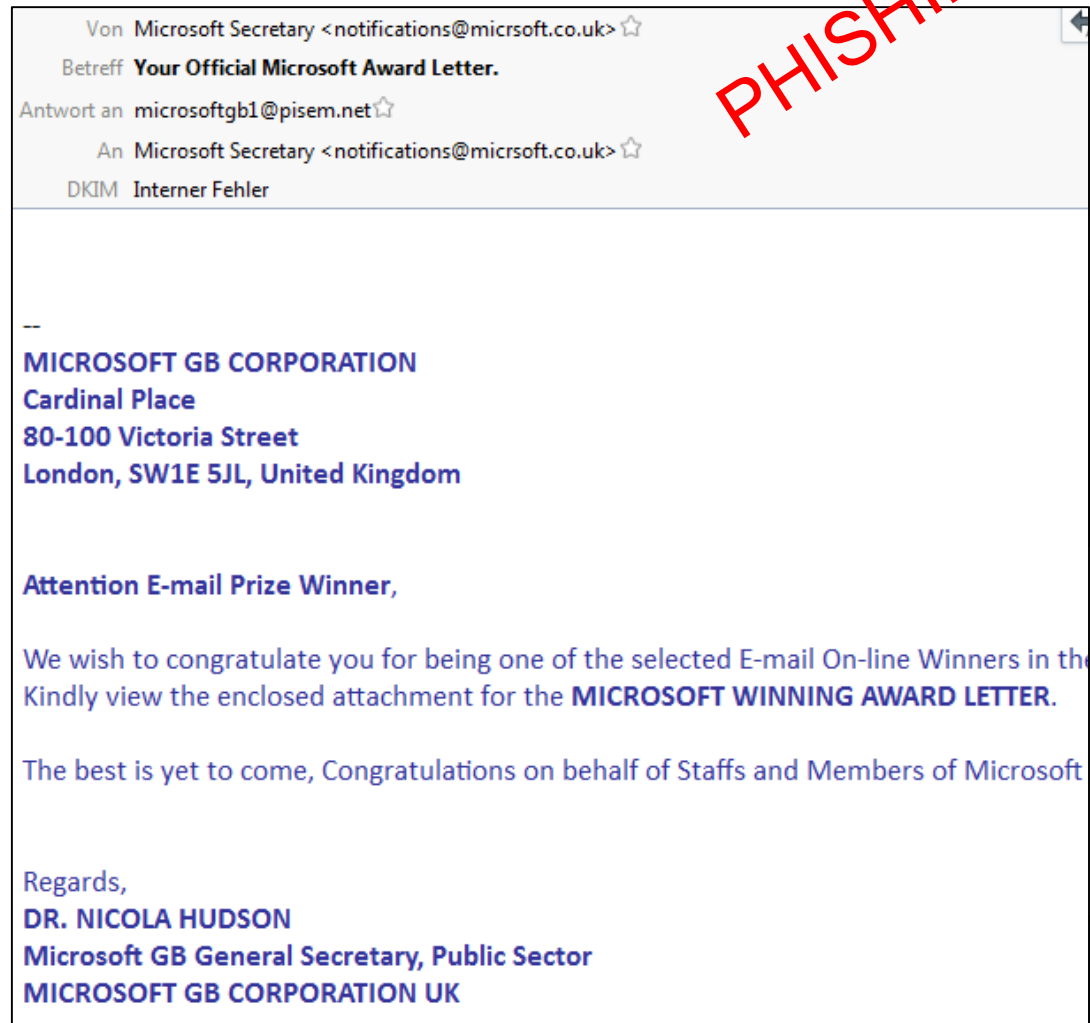
Data stolen in 2012 breach, containing encrypted passwords and details of around two-thirds of cloud firm's customers, has been leaked

Study
Identity



Protection for your digital TUM identity

- Use a separate password for your TUM identity
➔ no reuse of passwords of another digital identity
- Change your password regularly (at least once a year)
- Chose a strong password
- Don't share your password.



Protection for your digital TUM identity

- Use a separate password for your TUM identity
➔ no reuse of passwords of another digital identity
- Change your password regularly (at least once a year)
- Chose a strong password
- Don't share your password.



Do's and Dont's

- Use your TUM email address for official TUM emails
 - This ensures that the recipient knows, that you are you
john.doe@gmail.com
↑↓
john.doe@tum.de
- Don't share your student number. Even not with parents, friends and fellow students.
 - Student numbers are often used as pseudonym such as grade announcement or to verify your identity in telephone calls.
- Don't post pictures of your student card at Instagram or other social platforms („Hooray! I got my student card! “)
 - Everyone knows your name, birthdate and student number



Secure Passwords

Video of the Federal Office for Information Security (BSI) to explain the sentence method

<https://www.youtube.com/watch?v=BEyW39by8KQ>

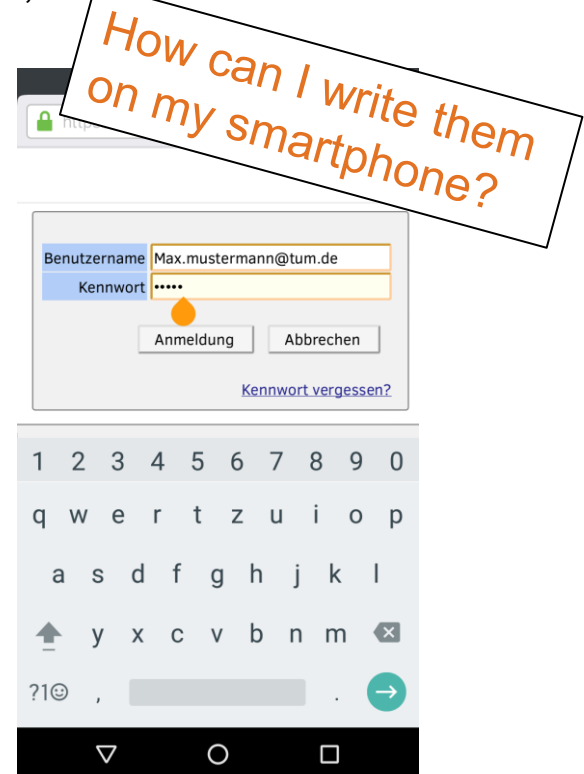
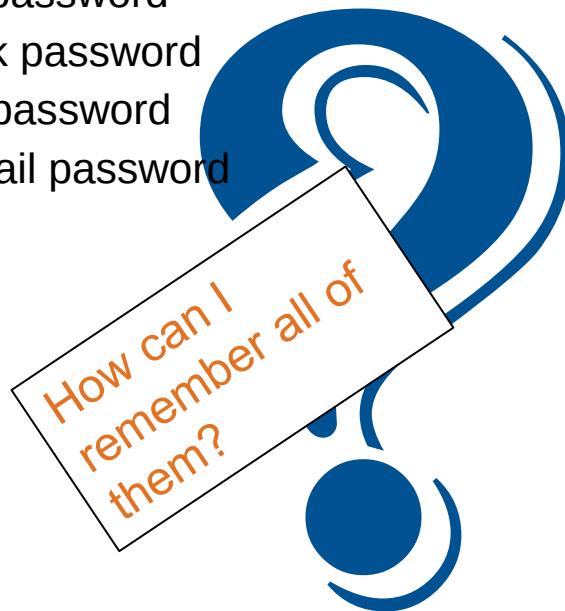
Secure Passwords

A secure password consists of

- At least **10** characters (unfortunately the spot is a little bit old... but still nice)
- Mixed with numbers, characters (Upper and lower case) and special characters.

Actually, one should use a separate password for each service, but

- TUMonline password
- Banking password
- Facebook password
- Amazon password
- Gmail password



How to remember passwords

The sentence method

We learned today how to create and remember good passwords.

We learned **2**day how to **c**reate and **r**emember **g**ood **p**asswords.

Leads to the password: **Wl2dhtcargp.**

individualized:

- TUMonline password
- Banking password
- Facebook password
- Amazon password
- Gmail password

W**TUM**2dhtcargp.

-

W**FAC** 2dhtcargp.

W**IAMA** 2dhtcargp.

W**IGOO** 2dhtcargp.

Another method: The password card

for strong passwords not daily in use

e.g. Amazon-Password **YJRRvq/D)qm**

	ABC	DEF	GHI	JKL	MNO	PQR	STU	VWX	YZ	.
0	Y	I5	3bZ	Co	U,b	F	k	2Hu	ct	OIX
1	4XB	Z	Lkl	w4	J	TK	ho	x	!0	j
2	RR	E+	OLn	kB	T+	DBe	YA	UI	JW	K
3	Hk	4a	bG	bf	W	=	JZ	gQY	vq	j
4	b	zjN	fB	T	/D	p	vM	uiN	Db	gX
5	K=r	A	31k	XqG	)gm	cA	Py	ZU	sV	ml
6	Sw	a)	Q/	M/	hEZ	FBQ	nKA	tNm	ge	wk
7	G(j	v3O	)W	0Ea	9GA	L6	8w	/j0	,	P
8	qr	H	VU	gl3	(M	c2	hN/	y5	NZ	S9
9	dk(	kp	fF	FNe	g:	+8/	.e1	4!	M	D1p
10	=	rh	Y0	UR	:	R	M	7Je	1f	IWa

The password card

This is the method for the wallet. You can use the card to generate a good password for each service (Facebook, Amazon, Google, TUMonline...) and not have to worry about how you are supposed to remember it..

The basic idea is to be able to read the password by means of a table. The simplest method is to utilize the name of the service. For AMAZON as an example, the A corresponds to the entry in the first row, the M in the second row...The corresponding entries in each of the rows then yield the password.

You don't need to "translate" the entire name of the service of course, but the password should contain at least 10 characters.

With this method your password remains secret as long no one gets their hands on your password card.

You can make the password even more secure by creating a unique method for reading the card that only you know.

Write passwords on the smartphone

- TUMonline Password: WITUM2dhtcargp.
Write on an iPhone:
 - 15 characters
 - Switch to Upper Case: 4 x
 - Switch to digits/special characters: 2 x
- Conflict: comfort vs. security
- Decide consciously to use easy or strong passwords.
- Basis for your decision:
 - How important is security in this special case?

More Password Tipps

On www.it.tum.de/en/passwords/

Or print your personal password card after this lecture.



Deine persönliche Passwortkarte

Deine persönliche Passwortkarte hilft dir für jeden einzelnen Dienst ein gutes Passwort festzulegen und dieses nicht zu vergessen.

Halte deine Karte geheim, gib Sie niemanden, denn Sie ist der Schlüssel zu deinen Passwörtern.

Wenn du dir eine eigene Methode zum Ablesen der Passwörter ausdenkst, die nur du kennst, wird niemand deine Passwörter herausfinden, auch nicht, wenn du diese Karte verlierst.

Hebe deine Backup-Karte an einem sicheren Ort auf. Sie hilft dir, falls du deine Karte verlierst.

Viele weitere Passworttipps oder auch andere Sicherheitstipps für deinen Rechner, dein Smartphone oder Tablet findest du unter:

www.it.tum.de/sicher

mach's mit.

Werde Passwortkünstler.



ICH WILL'S SICHER!

	ABC	DEF	GHI	JKL	MNO	PQR	STU	VWX	YZ	.
0	Nj	b	dGI	yq	/	8:	z7c	cC	L2u	f
1	@G	i	gL	;	TsI	Pe	07R	z4	@p	Mv
2	REf	GU	Fh:	l8	ewg	CJ	3T	3m	/U	?eI
3	Pq	G	V	Kd	sOV	Q	Yw	,lv	.lr	l
4	5k	C(	L	vV	pM	F	uI	pr	ZP	iH
5	x	hR	0V	za	wC	e8	v	5HT	J9	pl
6	Y	j	SZ	Mq6	I	jW	5	xb	vWl	hhZ
7	2B	V0O	90	R	aO	*S	PK	!m	6l	iHg
8	S	sc	PG	a	TQo	(I	x	q	ic	ZM
9	3y	cD	yT	Plk	L	wY	W	4u	Tm	iG
10	YS	=P	2dr	q:	mM	B3	t	Wh;	/	*

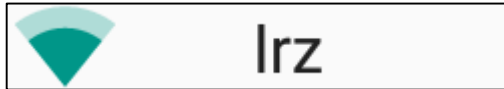
WiFi– at university and underway



By Shutterstock.com/Gorobets

WiFi at University

- LRZ



- WiFi to connect without password
- Without VPN: only www.lrz.de
- Good idea for downloads of configuration files, antivirus software Sophos, ...
- With VPN enabled: browse the whole web

- Eduroam



- available on all locations of the TUM, in the Munich city center and at various German and European universities
- Login with your TUM-ID@eduroam.mwn.de and your TUM-Password

Install eduroam securely

A secure configuration is not as easy as you think:

Use instructions on http://www.lrz.de/services/netz/wlan_en/ → **eduroam** :

- Linux: download script to install
- iPhone/iPad/Mac OsX : download profile for automatic installation
- Android: use the App eduroam-Cat and the LRZ-profile
- Windows: download installation program

WiFi underway: public WiFi

Public WiFi – unencrypted

- Generally visible
- No lock symbol 
- Anyone can connect
- anyone can read the communications traffic

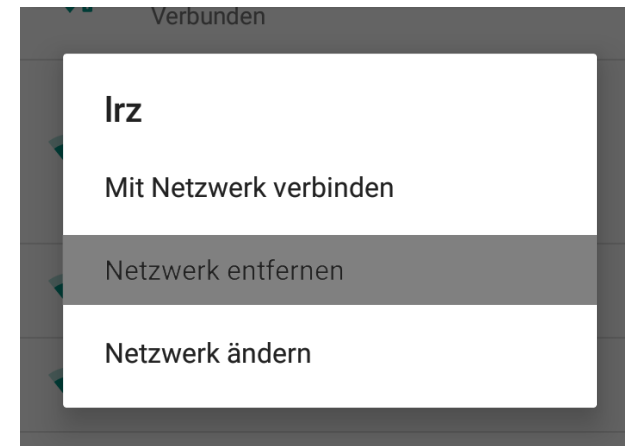
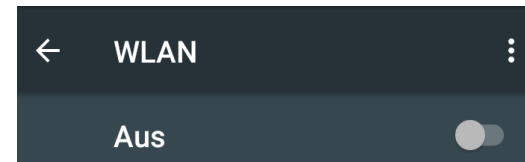
Public WiFi – encrypted

- Generally visible
- With lock symbol 
- Only certain people can connect
- The network operator can read the communications traffic.

WiFi underway: public WiFi

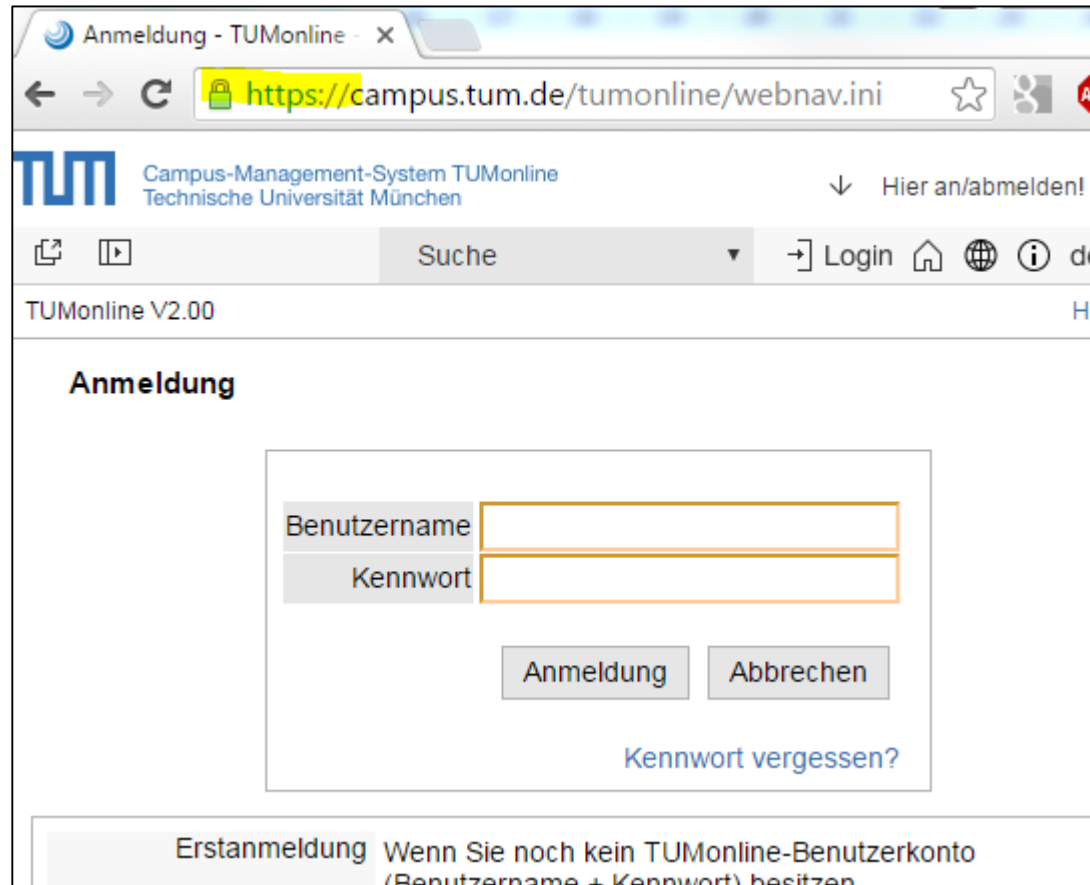
Some security tips for being underway

- Enable / disable WiFi on your smartphone consciously
 - No unintended connection possible
- Use mobile network if possible
- Delete WiFi if you don't want to use it anymore
 - No unintended connection possible



Secure Communication

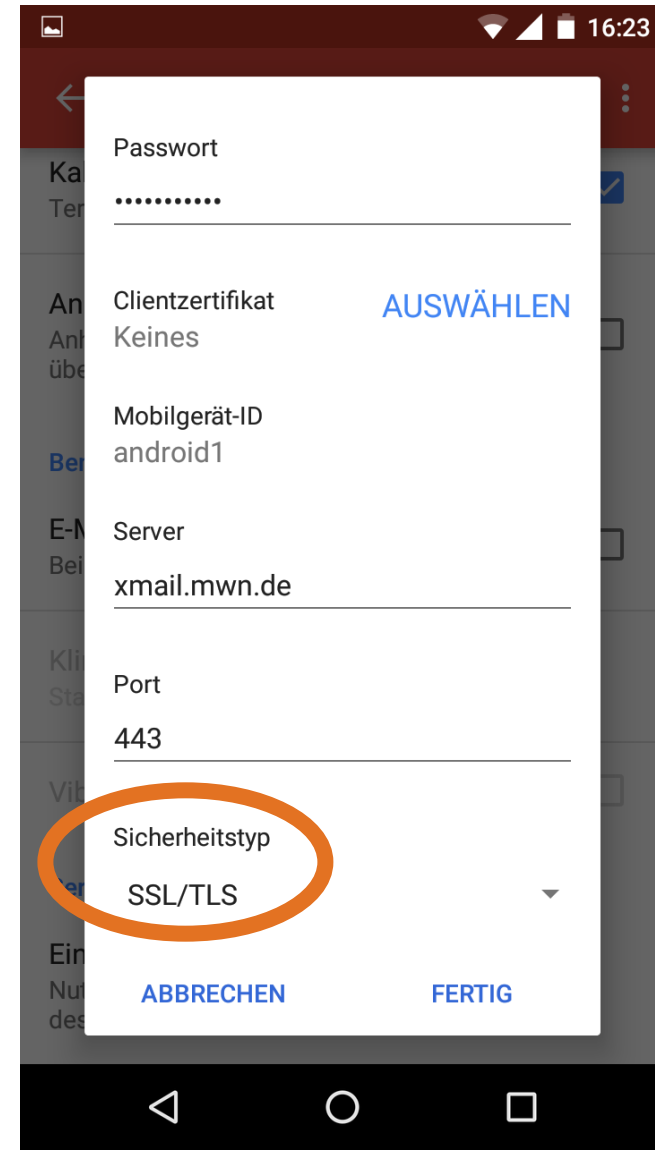
- Activate encryption
 - Websites: see if **https://** is enabled, especially if you have to enter personal data.



The screenshot shows a web browser window titled "Anmeldung - TUMonline". The address bar displays a secure connection: **https://campus.tum.de/tumonline/webnav.ini**. The page header includes the TUM logo and the text "Campus-Management-System TUMonline Technische Universität München". A search bar with the text "Suche" and a "Login" button are visible. The main content area is titled "Anmeldung" and contains a login form with two input fields: "Benutzername" and "Kennwort". Below the fields are two buttons: "Anmeldung" and "Abbrechen". A link "Kennwort vergessen?" is also present. At the bottom, a message states: "Erstanmeldung Wenn Sie noch kein TUMonline-Benutzerkonto (Benutzername + Kennwort) besitzen".

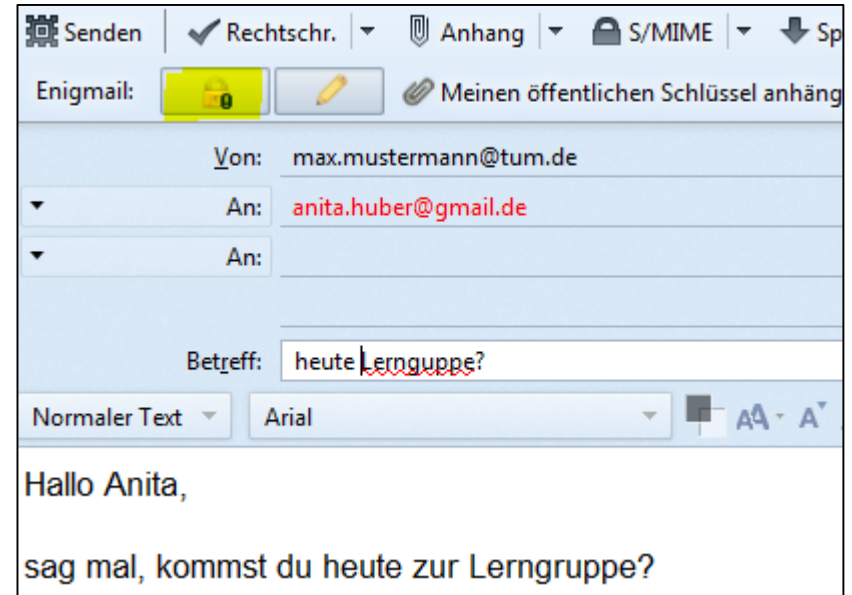
Secure Communication

- e-mail
 - Within apps/programs for e-mail:
enable transport encryption
(SSL/TLS or StartTLS)



Secure Communication

- e-mail
 - Within apps/programs for e-mail:
enable transport encryption
(SSL/TLS or StartTLS)
 - Use end-to-end encryption



e-mail encryption: transport encryption and end-to-end encryption

- Not encrypted



- transport encryption



- end-to-end encryption



End-to-End-Encryption?

Visit a Cryptoparty!

Offered by

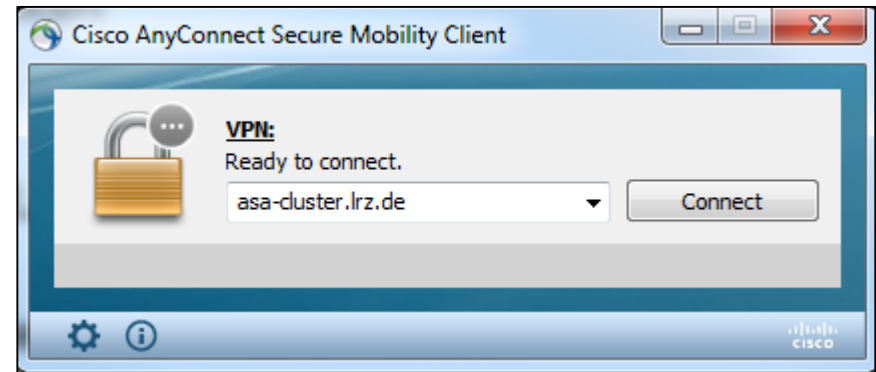
- Chaos Computer Club
- TUM: expected to be held on 9 December ab 16:00 at Leibniz Rechenzentrum (German)

You want a Cryptoparty held in English?

➔ Write an e-mail to it-sicherheit@tum.de

Secure Communication

- Activate VPN and the whole communication will be encrypted
... until LRZ / Munich Scientific Network.



VPN (Virtual Private Network)

3 Features:

1. Connect to Munich Scientific Network (e.g. if you are at home)
 - Download and update antivirus software Sophos
 - Search for free in fee-based databases
 -
 2. Browse the web if connected to the LRZ WiFi
 3. Security in public WiFis
 - ➔ The network operator can not read the communications traffic.
- Use „!go42tum“

Summary: Secure Communication

Encrypt! Encrypt! Encrypt!

- HTTPS while browsing the web
- transport encryption and end-to-end encryption for e-mails
- VPN for public WiFis

More WiFi at www.it.tum.de

www.it.tum.de/en/wlan/

Security tips for your computer

Some basic rules will help to protect your computer, smartphone and digital identity.

Security tips for your computer

Install antivirus software

You can download the free Sophos Antivirus program for

- Windows
- Mac OS X
- Linux

from LRZ.

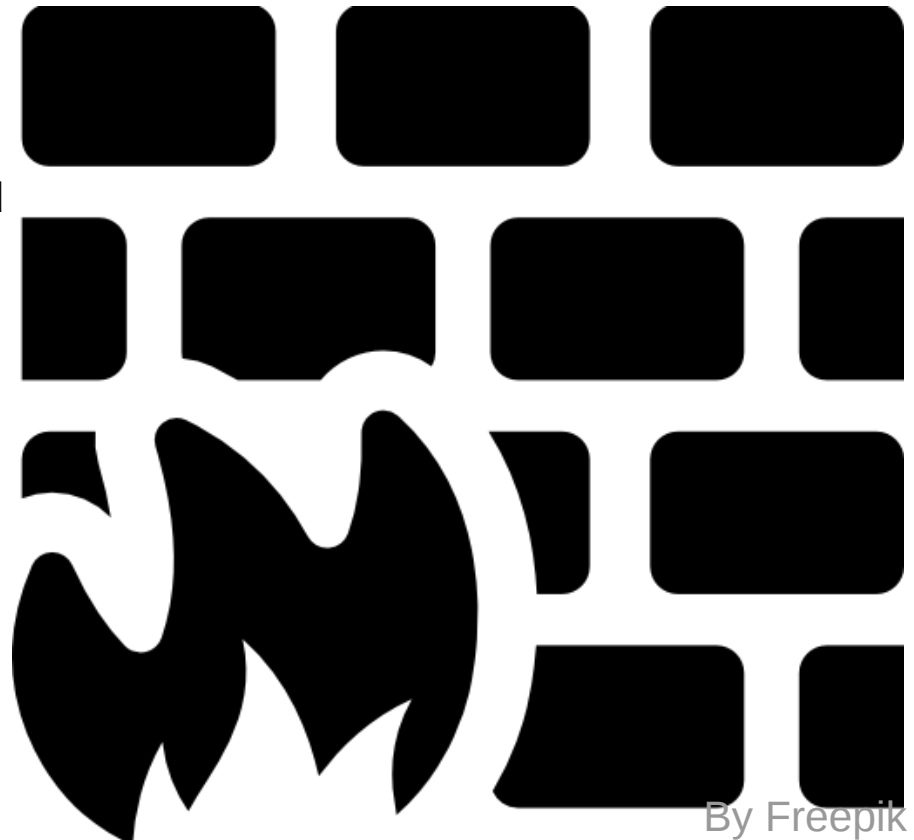


by Vectors Market

Security tips for your computer

Use a firewall

- A firewall can protect you against malicious software or hacker attacks.
- Mac OS X and Windows have an integrated firewall enabled by default.



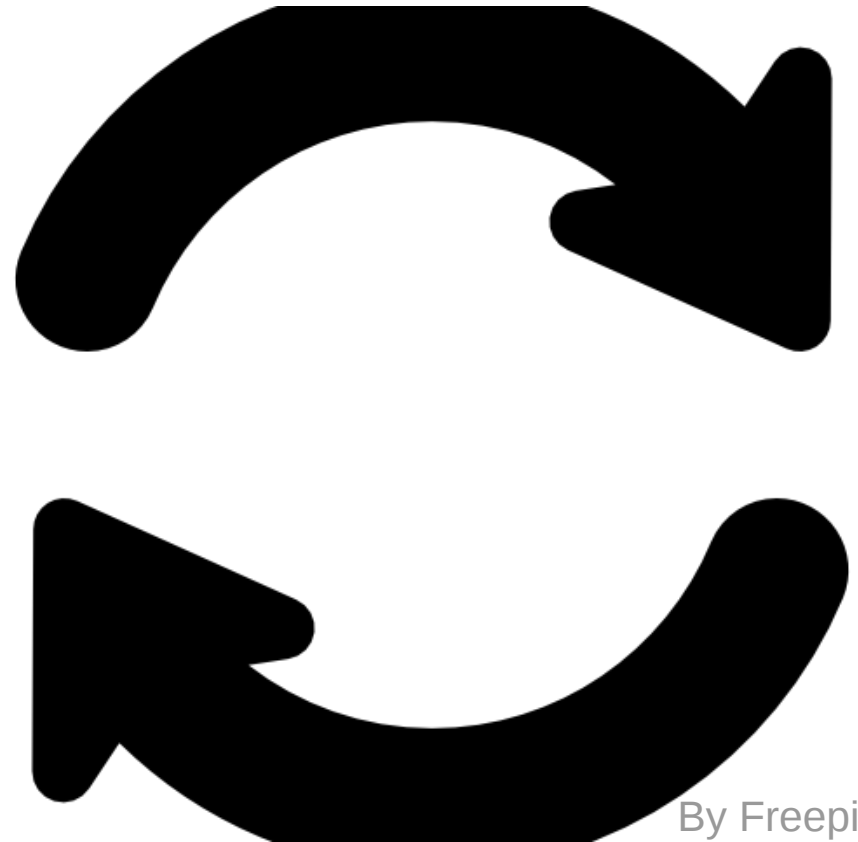
By Freepik

Security tips for your computer

Keep your software up-to-date

Updates are mandatory. Security gaps can be close and new security features can be implemented.

Most operating systems can be configured to automatically install important updates or to be notified about available imported updates.



By Freepik

Security tips for your computer

Work with restricted rights

- Do not work with administrator rights.
- Instead, create a normal user account for your day-to-day activities.
- Set up separate passwords for the administrator and user accounts.

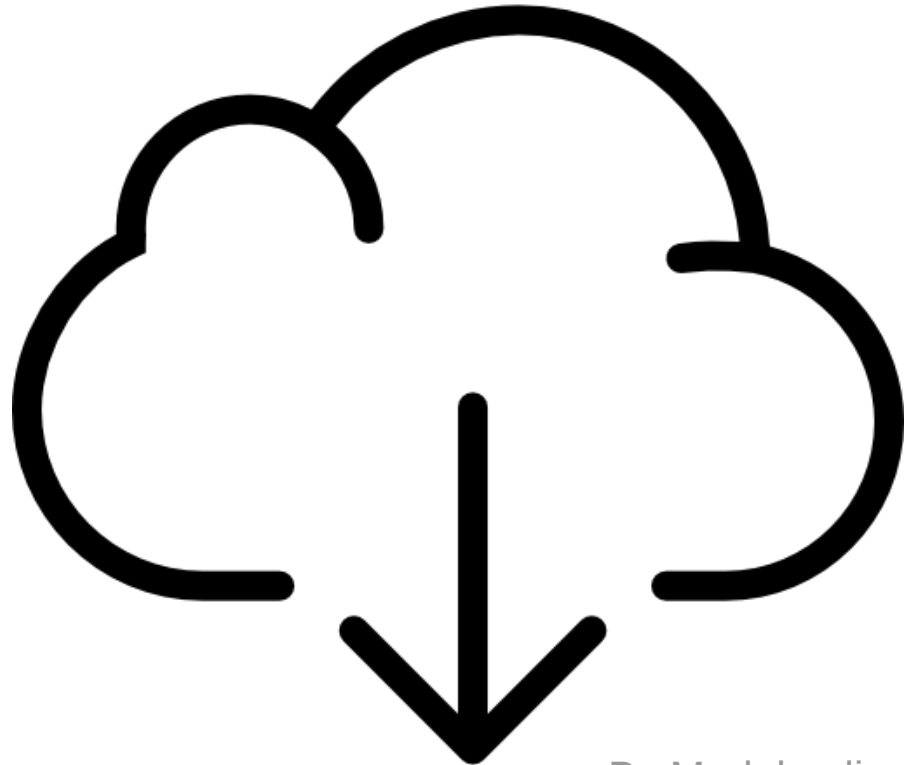


By Freepik

Security tips for your computer

Avoid dubious software sources

- Never install programs from untrustworthy sources.
- Sources you can trust include software directories from well-known IT publishing houses that scan the programs for viruses before making them available for download.

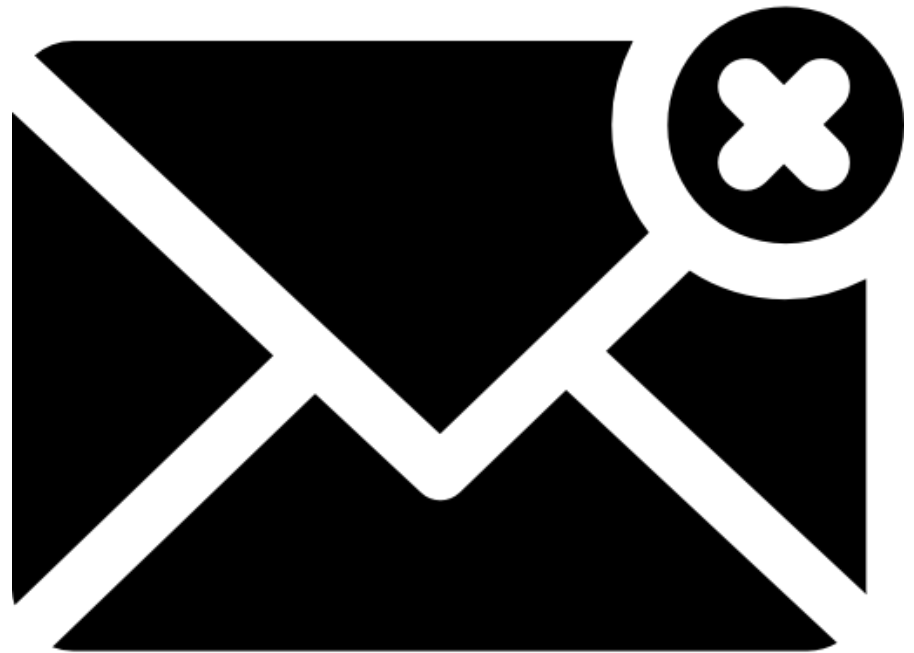


By Madebyolive

Security tips for your computer

Use caution with suspicious e-mails

- Never open suspicious mails or attachments, so that no one can invade your computer from the outside
- Recognizing suspicious mails:
 - You don't know the sender
 - Grammatically-incorrect and/or misspelled text
 - Great things are promised
 - The sender tries to exert time pressure.
 - You should click on suspicious links.

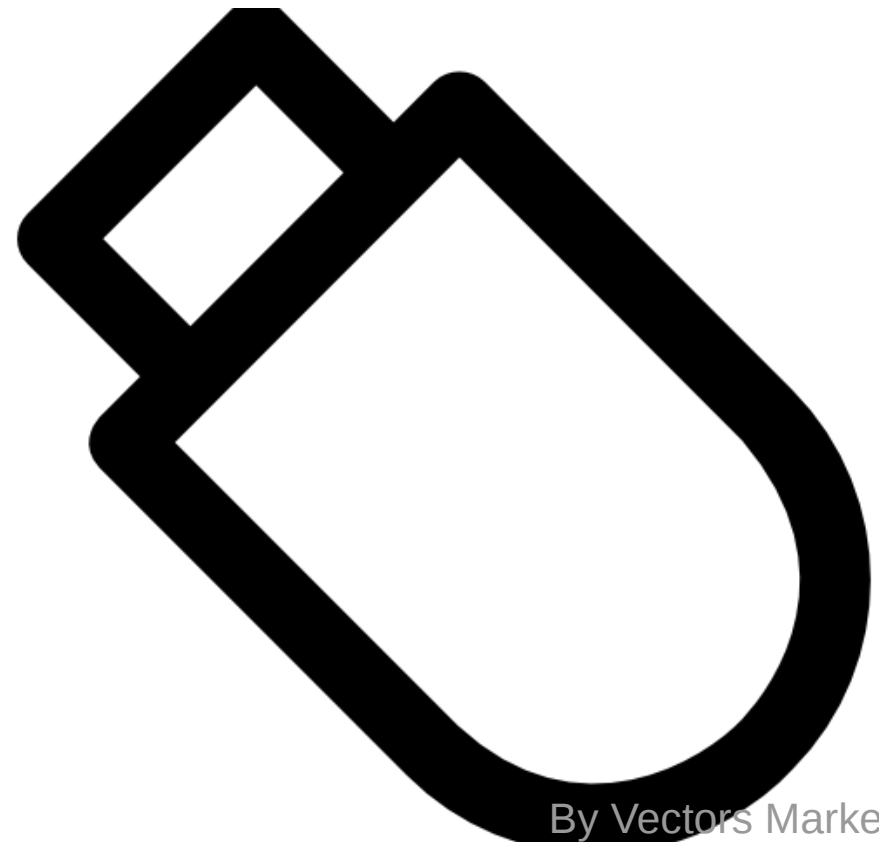


By Schnittstelle

Security tips for your computer

Don't use USB sticks from unknown sources

- Unknown USB sticks can contain malicious software.
- Never plug in USB sticks unless you know where they come from.
- Even don't plug in your fellow student's USB stick. Do you know if his/her computer is not infected?

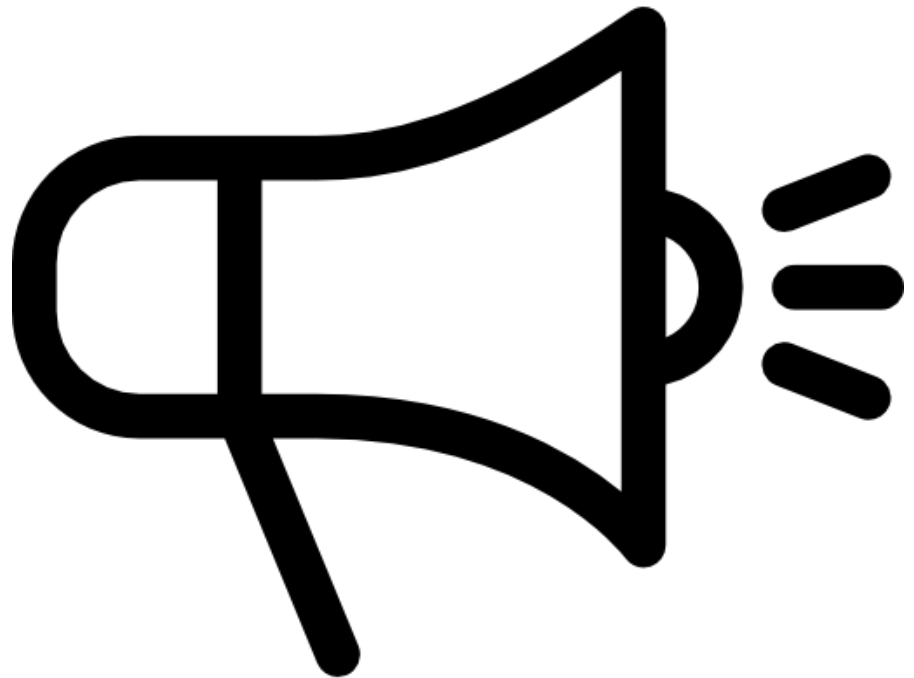


By Vectors Market

Security tips for your computer

Beware of browser ads

- Browser ads can also be misused to distribute malware.
- Malvertising means that malicious ads are placed on trustworthy websites.
- You can protect your computer or smartphone with an adblocker (see www.it.tum.de/en/adblocker)



By Gregor Cresnar

Security tips for your computer

All these tips help to protect you and your digital identity.

But you can never be **protected** 100%.

For that reason: Put mind in gear, before clicking a link!

More tips:

www.it.tum.de/en/computer

www.it.tum.de/en/smartphone

Thanks for your attention!