IT-Sicherheit im Studienalltag

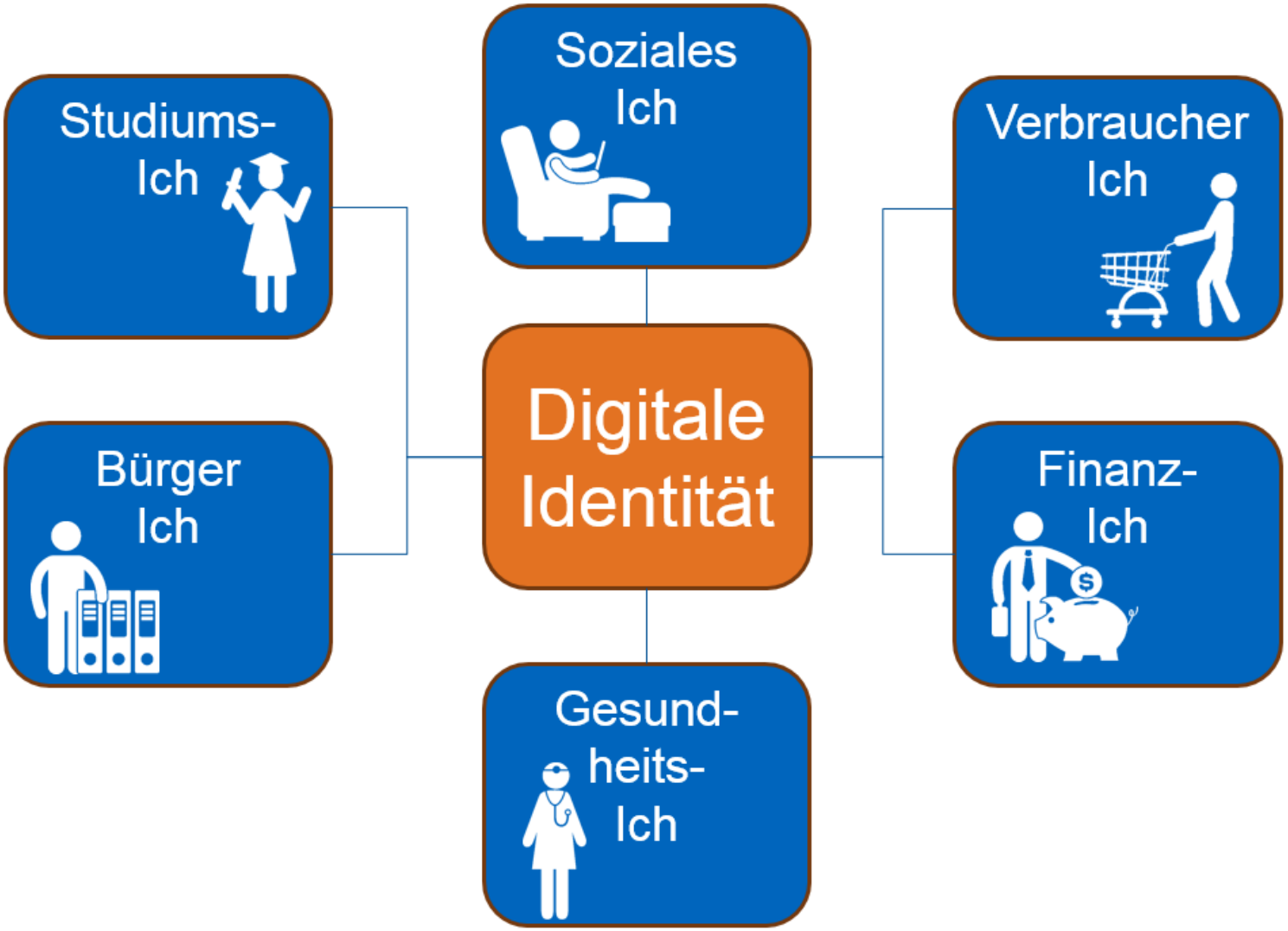
Angelika Müller – Referentin für Datenschutz und IT-Sicherheit

Technische Universität München

IT-Servicezentrum

Oktober 2016

Die digitale Identität – Wer bin ich und wenn ja, wie viele?



Die TUM-Identität

- Wie werden Studierende eindeutig identifiziert?
  - TUM-E-Mailadresse – max.mustermann@tum.de
  - TUM-Kennung – *go42tum*
  - Matrikelnummer – 0123456789
  - StudentCard (Matrikelnummer, Bibiliotheksnummer, Kartennummer) –

Die digitale TUM-Identität: der TUM-Account

Was kann man alles mit dem zentralen TUM-Account tun?

- E-Mails empfangen/verschicken
- Studienangelegenheiten online regeln (*Vorlesungsanmeldung, Prüfungsanmeldung, Ergebnisse einsehen,*…)
- E-Learning-Plattform nutzen
- WLAN und VPN nutzen
- Software beziehen
- Über die Bibliothek: Datenbanken nach Artikeln/Zeitschriften durchsuchen, eBooks downloaden/ausleihen
- TUM-Dateiablage nutzen
- TUM-“DropBox“ (Sync&Share) nutzen
- Uvm.

➔ dies alles mit einer Kennungen und einem Passwort

Schutz der digitale TUM-Identität

- Verwenden Sie ein eigenes Passwort für die TUM-Identität
  ➔ keine Wiederverwendung eines Passworts aus einer anderen digitalen Identität

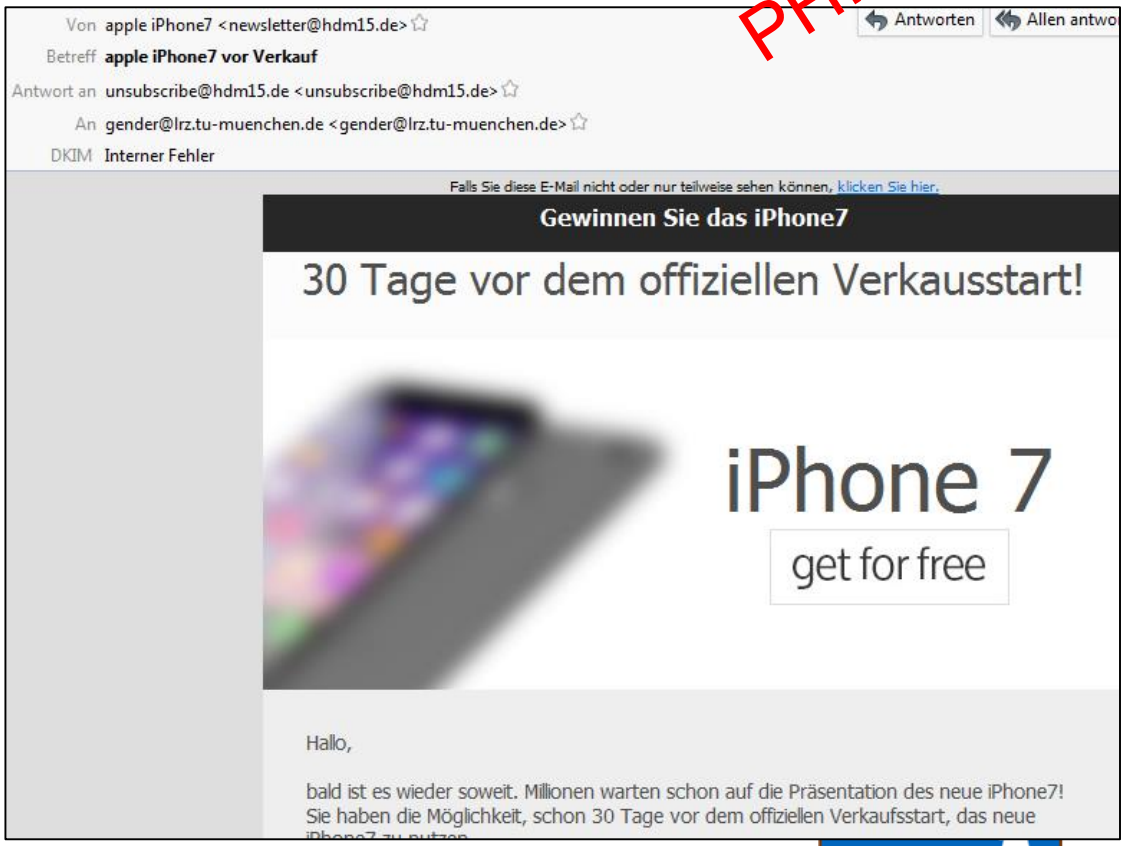
Studiums-Ich

Schutz der digitale TUM-Identität

- Verwenden Sie ein eigenes Passwort für die TUM-Identität
  ➔ keine Wiederverwendung eines Passworts aus einer anderen digitalen Identität

- Ändern Sie Ihr Passwort regelmäßig (mindestens einmal im Jahr)

PHISHING



Schutz der digitale TUM-Identität

- Verwenden Sie ein eigenes Passwort für die TUM-Identität
  ➔ keine Wiederverwendung eines Passworts aus einer anderen digitalen Identität
- Ändern Sie Ihr Passwort regelmäßig (mindestens einmal im Jahr)
- Wählen Sie ein starkes Passwort (später mehr hierzu)
- Keine Passwortweitergabe!

Do‘s and Dont‘s

- Verschicken Sie E-Mails an offizielle Stellen der TUM am besten von Ihrer TUM-Adresse aus

➢ So ist sicher gestellt, dass der Empfänger weiß, dass Sie Sie sind…
max.mustermann@gmx.de
⇅
max.mustermann@tum.de

- Geben Sie Ihre Matrikelnummer nicht weiter, auch nicht an Eltern, Kommilitonen, Freunde

➢ Matrikelnummern werden an der TUM häufig als Pseudonym verwendet, z.B. bei Notenaushängen oder auch zur Verifizierung der Identität am Telefon.

- Posten Sie keine Fotos der Studentcard bei Instagram oder ähnlichen Diensten („Hurra meine Studiausweis ist da!“)

➢ So kennt jeder Ihren Namen, Ihr Geburtsdatum, Ihre Matrikel-nummer

Sichere Passwörter

Kurzvideo zur Erläuterung der Satzmethode des BSI (Bundesamt für Sicherheit in der Informationstechnik

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

Sichere Passwörter

Wie sieht ein sicheres Passwort aus?

- Mindestens **10** Zeichen (der Spot ist leider schon etwas älter…. ☹)
- Zufällige Mischung aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen

Eigentlich sollte man Passwörter nicht wiederverwenden, aber

- TUMonline-Passwort
- Bank-Passwort
- Facebook-Passwort
- Amazon-Passwort
- Googlemail-Passwort

Passwörter merken

Satzmethode
Am zweiten Vorlesungstag waren ganz schön viele Erstsemester im Hörsaal, die alle schon sehr müde waren wegen der vielen Informationen, die sie gehört haben.

Am **2.V**orlesungstag **w**aren **g**anz **s**chön **v**iele **E**rstsemester **i**m **H**örsaal**, d**ie **a**lle **s**chon **s**ehr **m**üde **w**aren **w**egen **d**er **v**ielen **I**nformationen**, d**ie **s**ie **g**ehört **h**aben**.**

Ergibt das Passwort: **A2.VwgsvEiHdassmwwdvI,dsgh.**
Hier übertreiben wir etwas, um die Sache anschaulicher zu machen, 10 Zeichen reichen)

Und nun individualisiert:

TUMonline-Passwort	A2.V**TUM**wgsvEiHdassmwwdvI,dsgh.
Bank-Passwort	--
Facebook-Passwort	A2.V**FAC**wgsvEiHdassmwwdvI,dsgh.
Amazon-Passwort	A2.V**AMA**wgsvEiHdassmwwdvI,dsgh.
Googlemail-Passwort	A2.V**GOO**wgsvEiHdassmwwdvI,dsgh.

Weitere Passwortmethode: Passwortkarte

für Passwörter, die gut sein müssen, aber nicht mehrmals täglich verwendet werden.

z.B. Amazon-Passwort YJRRvq/D)qm

	ABC	DEF	GHI	JKL	MNO	PQR	STU	VWX	YZ	.
0	Y	l5	3bZ	Co	U,b	F	k	2Hu	ct	OlX
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

Erläuterungen zur Passwortkarte

Die Passwortkarte ist der Passwortsafe für den Geldbeutel. Anhand der Karte kann man für jeden Dienst (Facebook, Amazon, Google, TUMonline, usw.) ein eigenes, gutes Passwort ablesen.

Mit Hilfe der Tabelle kann man sein Passwort ablesen und zusammenstellen. Die einfachste Methode dafür ist es anhand des Dienstnamens vorzugehen. Möchte man z. B. dein Passwort für AMAZON ablesen, liest du in der Spalte ABC in Zeile 0 den Eintrag ab. Danach geht es in Spalte MNO in Zeile 1 weiter, usw. So setzt sich dein individuelles Passwort pro Anbieter zusammen.

Natürlich muss man nicht den ganzen Dienstnamen „übersetzen“, dennoch sollte ein Passwort mindestens 10 Zeichen haben.
Mit dieser Methode bleibt das Passwort geheim, solange niemand die Passwortkarte in die Finger bekommt.

Zusätzliche Sicherheit erhält man mit einer eigenen Ablesemethode, die man nur selbst kennt.

Passwörter am Smartphone tippen?

- TUMonline-Passwort: A2.VTUMwgsvEiHdassmwwdvI,dsgh. am Smartphone?
- Eingabe am iPhone:
  - 30 Zeichen
  - Umschalten auf Großschreibung: 7 x
  - Umschalten auf Zahlen/einfache Sonderzeichen: 3 x
  - Umschalten auf Buchstaben: 3x

➢ Konflikt Bequemlichkeit vs. Sicherheit

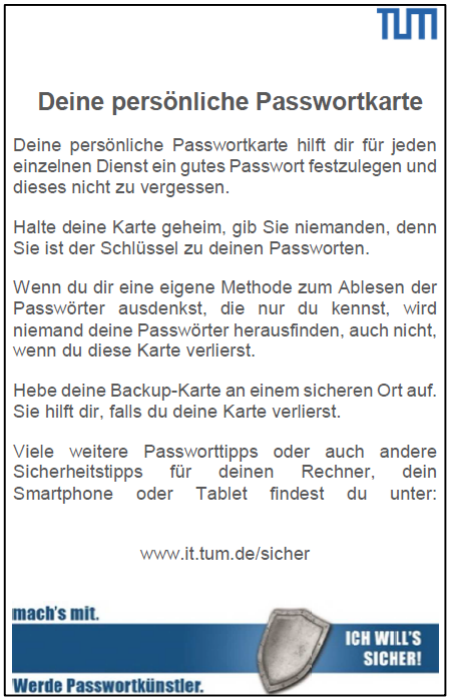
- Entscheiden Sie bewusst, welche Passwörter Sie vereinfachen und wie stark Sie das Passwort auf Grund der Bequemlichkeit vereinfachen.

- Entscheidungsgrundlage:
  - Wie wichtig ist es im speziellen Fall ein besonders sichere Passwörter zu haben?

Mehr zu Passwörtern

Weitere Tipps für gute Passwörter:
www.it.tum.de/sicher/passwoerter

Oder Sie drucken sich Ihre Passwortkarte….



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 Passworten.

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

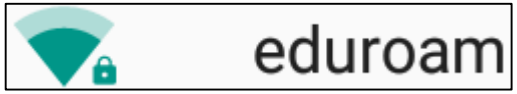
	ABC	DEF	GHI	JKL	MNO	PQR	STU	VWX	YZ	.
0	Nj	b	dGI	yq	/	8:	z7c	cC	L2u	f
1	@G	i	gL	;	Ts1	Pe	07R	z4	@p	Mv
2	REf	GU	Fh:	l8	ewg	CJ	3T	3m	/U	?eI
3	Pq	G	V	Kd	sOV	Q	Yw	,lv	.lr	l
4	5k	C(	L	vV	pM	F	ul	pr	ZP	iH
5	x	hR	0V	za	wC	e8	v	5HT	J9	pl
6	Y	j	SZ	Mq6	I	jW	5	xb	vW1	hhZ
7	2B	V0O	90	R	aO	*S	PK	!m	6l	iHg
8	S	sc	PG	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;	/	*

WLAN – an der Uni und unterwegs

By Shutterstock.com/Gorobets

WLAN an der Uni

- LRZ 

  - WLAN zugänglich ohne Passwort
  - Ohne VPN: nur Seiten unter www.lrz.de erreichbar.
    Nützlich für Downloads von Konfigurationsdateien, Virenscanner, Zertifikaten vom LRZ (Leibniz-Rechenzentrum – Rechenzentrum der Münchner Hochschulen)
  - Mit aktiviertem VPN: freies Surfen möglich
- Eduroam 

  - WLAN an den TUM-Standorten, einigen zentralen Plätzen in München (z.B. Sendlinger Tor, Marienplatz,…) und europaweit an anderen Hochschulen
  - zugänglich mit TUM-Kennung und zugehörigen Passwort.

Eduroam richtig einrichten

Eine manuelle Konfiguration kann zu erheblichen Sicherheitsproblemen führen.
Deshalb wird empfohlen nach Anleitung unter www.lrz.de/wlan ➔eduroam vorzugehen:

- Linux: Skript zum Download für die sichere Konfiguration
- iPhone/iPad/Mac OsX : Profil zum Anklicken, Installation wird automatisch durchgeführt
- Android: unbedingt über App eduroam-Cat installieren (aus dem Playstore)
- Windows: Installationsprogramm zum Download

Haben Sie eduroam bereits manuell eingerichtet, können Sie das WLAN löschen und erneut einrichten.

WLAN unterwegs: öffentliche WLANs

Öffentliches WLAN – unverschlüsselt

- Allgemein sichtbar
- Kein Schloss-Symbol 
- Jeder kann sich verbinden
- Es ist möglich, die Daten der anderen WLAN-Nutzer mitzulesen

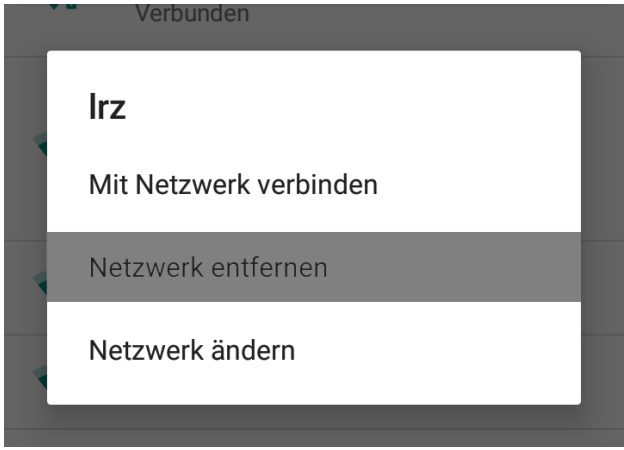
Öffentliches WLAN – verschlüsselt

- Allgemein sichtbar
- Mit Schloss-Symbol 
- Nur bestimmte Leute können sich verbinden
- Betreiber kann u.U. mitlesen

WLAN unterwegs: öffentliche WLANs 2

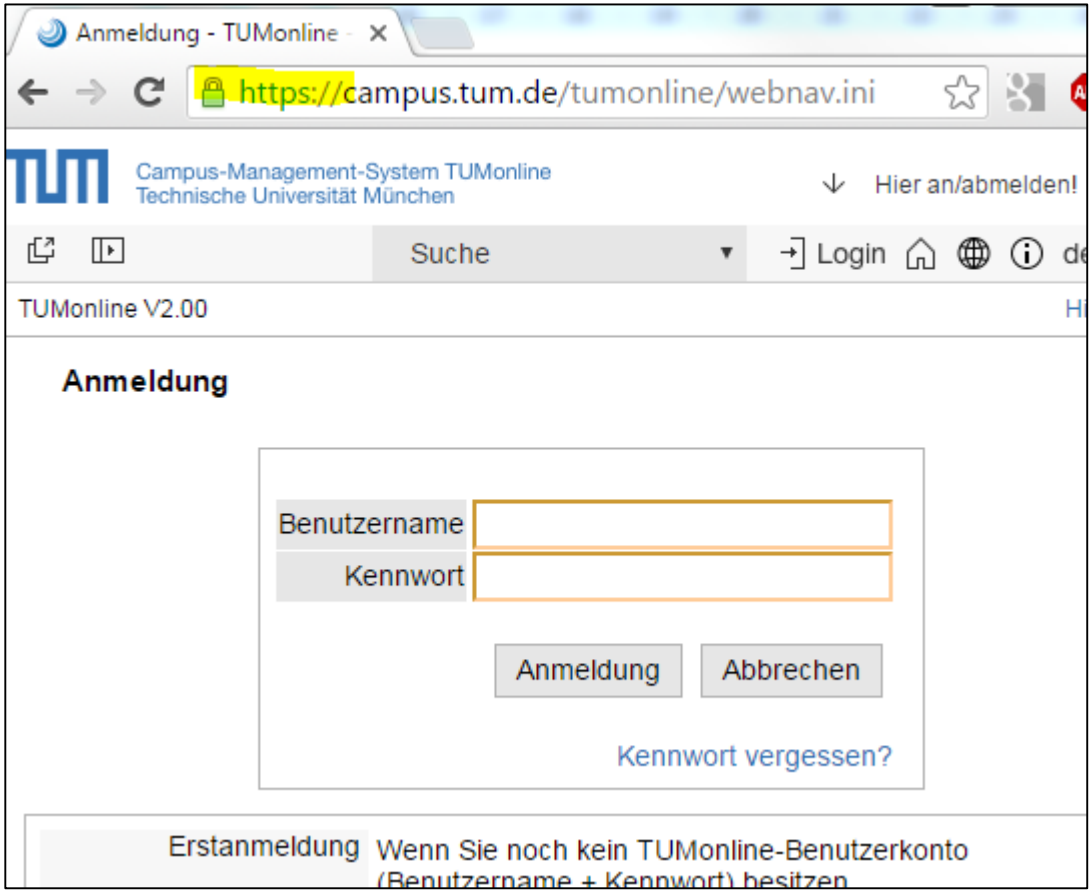
Sicherheitstipps für Unterwegs

- WLAN am Smartphone bewusst an- und ausschalten
  - ➢ Somit wird ein ungewolltes automatisches Verbinden unterbunden.
- Unterwegs Mobilfunknetz nutzen, falls möglich.
- Nach Nutzung: WLAN löschen/blockieren/ignorieren.
  - ➢ Somit wird ein ungewolltes automatisches Verbinden unterbunden.



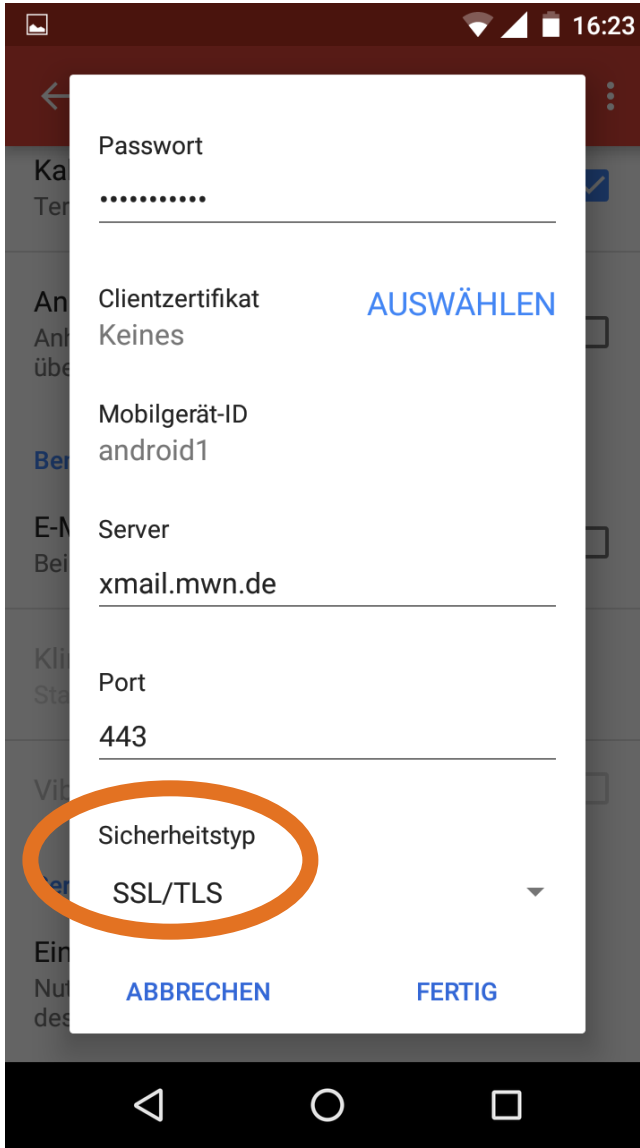
Kommunikation absichern

- Aktivieren der Verschlüsselung bei Diensten, z.B.
  - Bei Webseiten auf http**s**:// achten, besonders, wenn Daten eingegeben werden sollen!



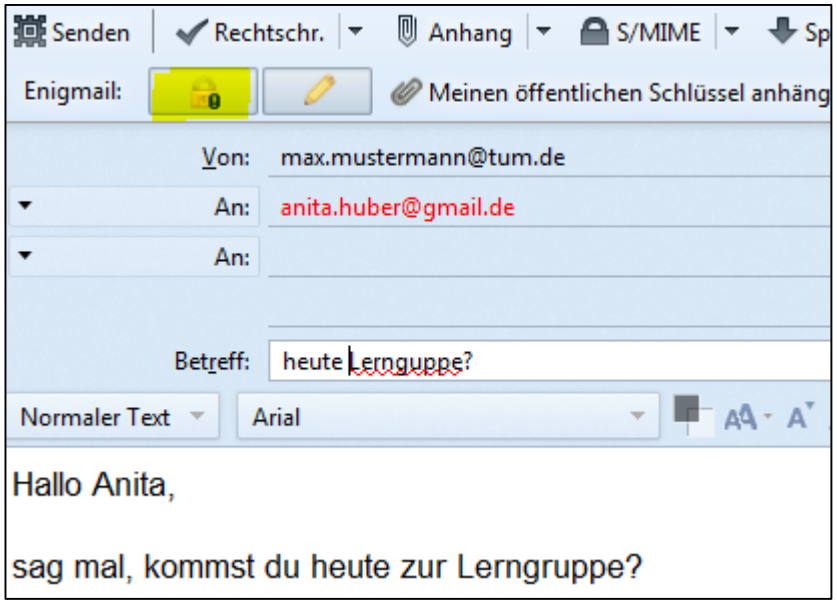
Kommunikation absichern

- E-Mail
  - Bei E-Mai-Apps/Programmen: Transportverschlüsselung in den Einstellungen einschalten (Punkte: SSL/TLS und/oder StartTLS)



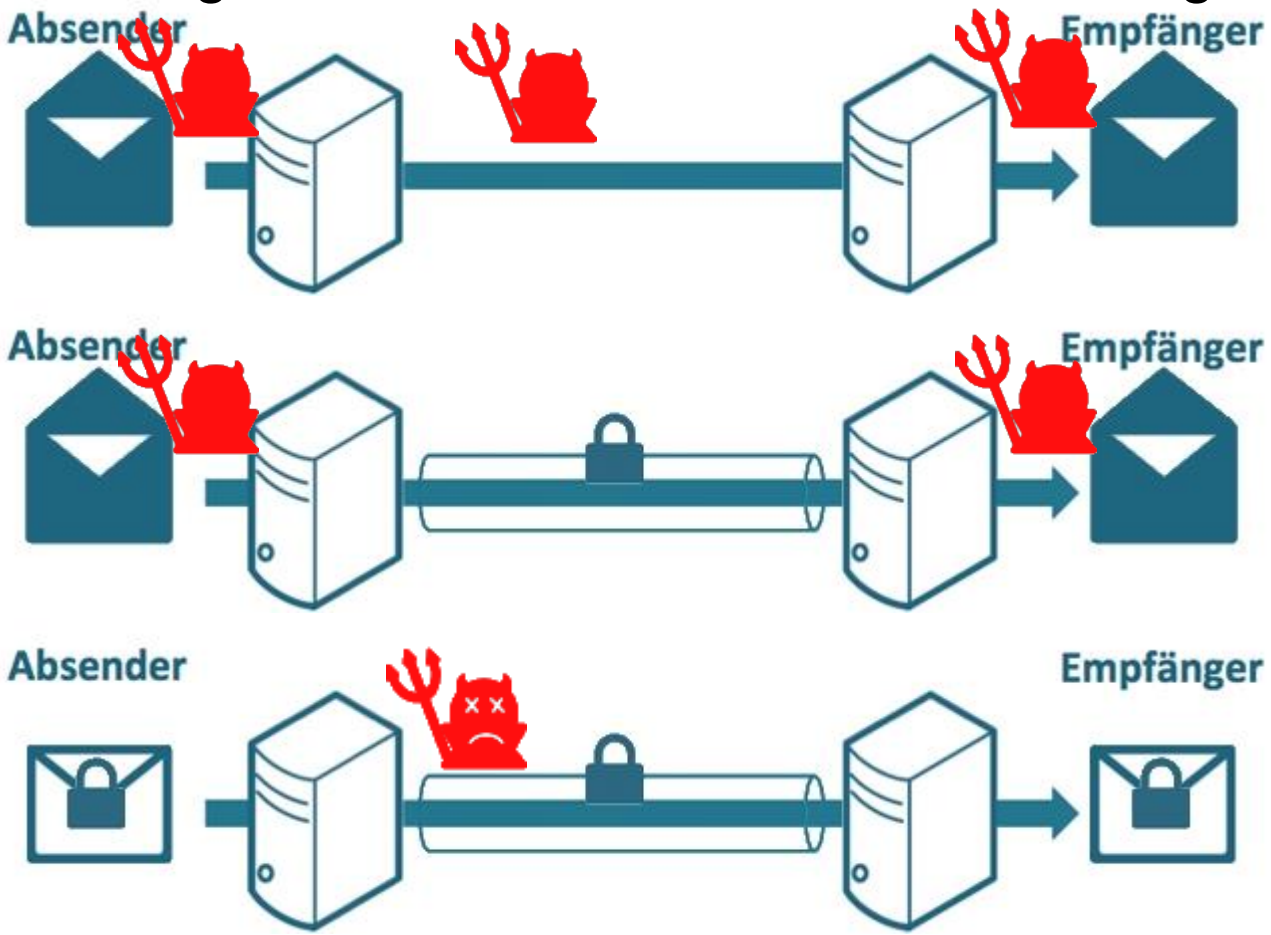
Kommunikation absichern

- E-Mail
  - Bei E-Mai-Apps/Programmen: Transportverschlüsselung in den Einstellungen einschalten (Punkte: SSL/TLS und/oder StartTLS)
  - Ende-Zu-Ende Verschlüsselung für E-Mails



E-Mail:
Transportverschlüsselung ↔ Ende zu Ende Verschlüsselung

- Unverschlüsselter Versandt
- Transport-verschlüsselung
- Ende zu Ende Verschlüsselung



Ende-Zu-Ende-Verschlüsselung?

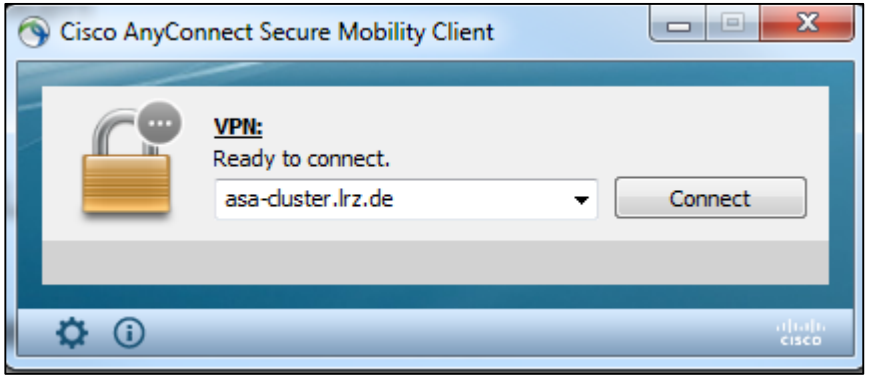
Besuchen Sie eine Cryptoparty!

Anbieter, z.B.

- Chaos Computer Club
- TUM, siehe www.it.tum.de/veranstaltungen

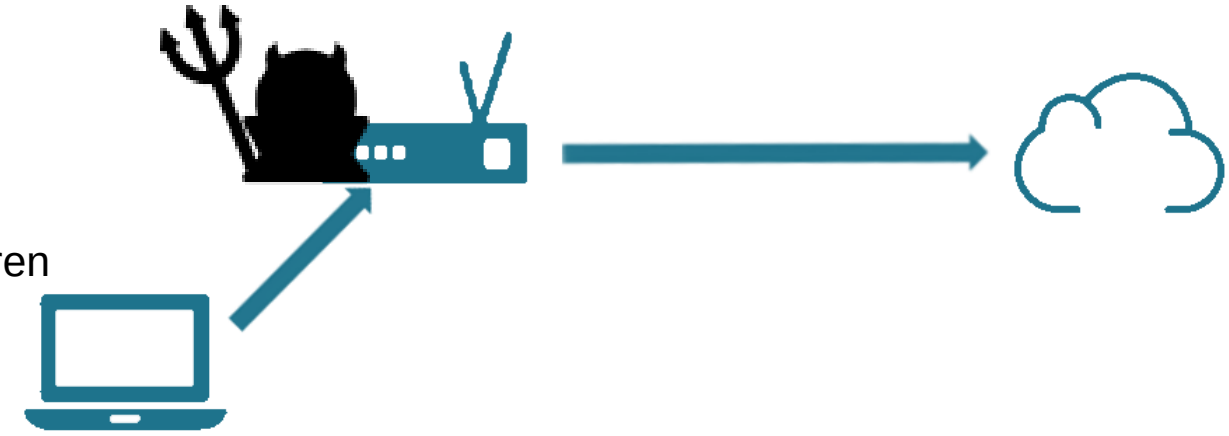
Kommunikation absichern

- VPN-Verbindung zum LRZ aufbauen → jegliche Kommunikation wird verschlüsselt… bis zum LRZ / Münchner Wissenschaftsnetz



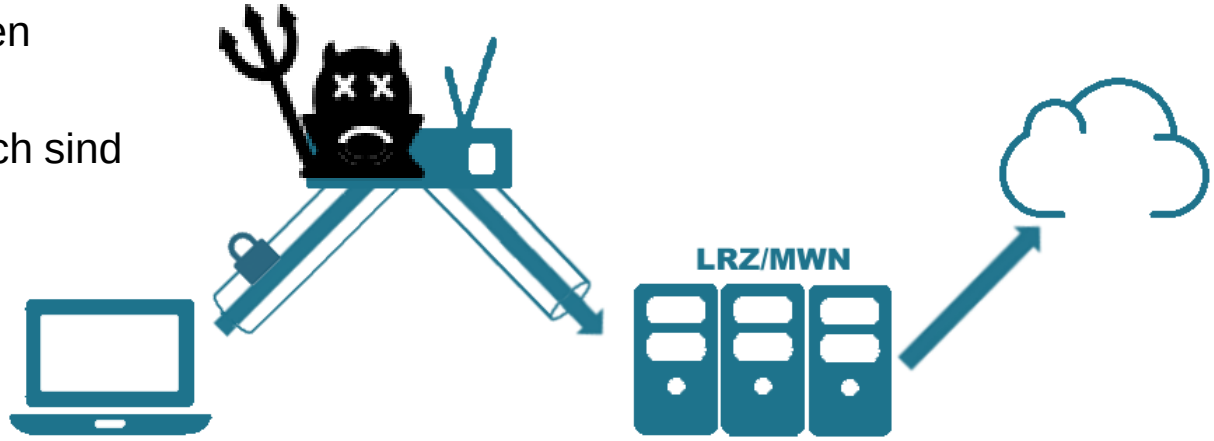
VPN

- Verbindung ohne VPN
  - wenig Schutz gegen Abhören



- Verbindung mit VPN zum LRZ: verschlüsselt bis ins Hochschulnetz
  - Angreifer kann nicht Abhören
  - Dienste nutzen, die nur im Hochschulnetz zugänglich sind
  - Für Schutz der kompletten Kommunikation:

    Anmelden mit „!go42tum“



VPN (Virtual Private Network)

3 Funktionen:

1. Von zu Hause aus in das MWN (Münchner Wissenschaftsnetz) einwählen
   - Aktualisieren Sophos Antivirus
   - Recherche in kostenpflichtigen Datenbanken
   - ….

2. Freies Surfen, wenn man mit dem LRZ-WLAN verbunden ist

3. Schutz in öffentlichen Netzen
   ➔ Netzanbieter kann nicht mitlesen

   Für Schutz der kompletten Kommunikation: Anmelden mit „!go42tum“

Zusammenfassung: Kommunikation absichern

Verschlüsseln! Verschlüsseln! Verschlüsseln!

- HTTPS bei Webseiten
- Transportverschlüsselung und Ende-zu-Ende Verschlüsselung für E-Mails
- VPN für unsichere WLANs

WLAN auf unseren Webseiten

www.it.tum.de/wlan/

Allgemeines Sicherheitstipps

Einige Grundregeln helfen den Rechner und das Smartphone vor Schadsoftware und Ihre Online-Identität vor Angriffen zu schützen.

Allgemeines Sicherheitstipps

Installieren Sie einen Virenscanner

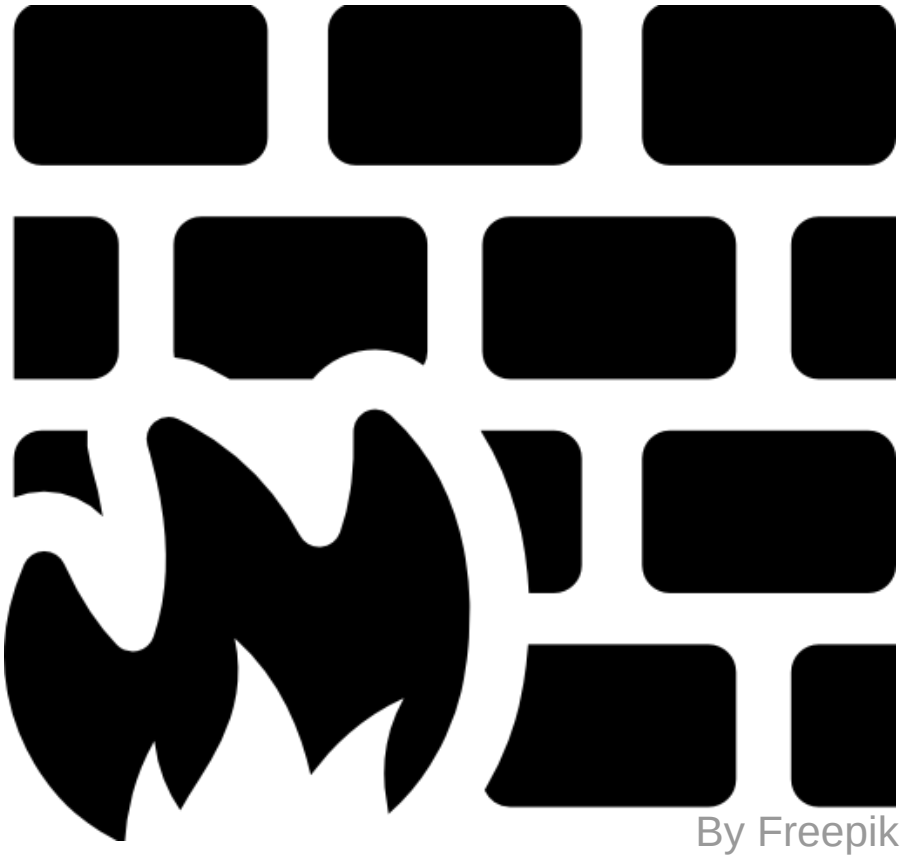
Als Studierender erhalten Sie kostenlos den Virenscanner von Sophos für

- Windows
- Mac OS X
- Linux

Allgemeines Sicherheitstipps

Schützen Sie den Rechner mit einer Firewall

- Eine Firewall kann vor Hackern oder Schadsoftware schützen.
- Mac OS X und Windows haben diese bereits integriert und standardmäßig aktiviert.



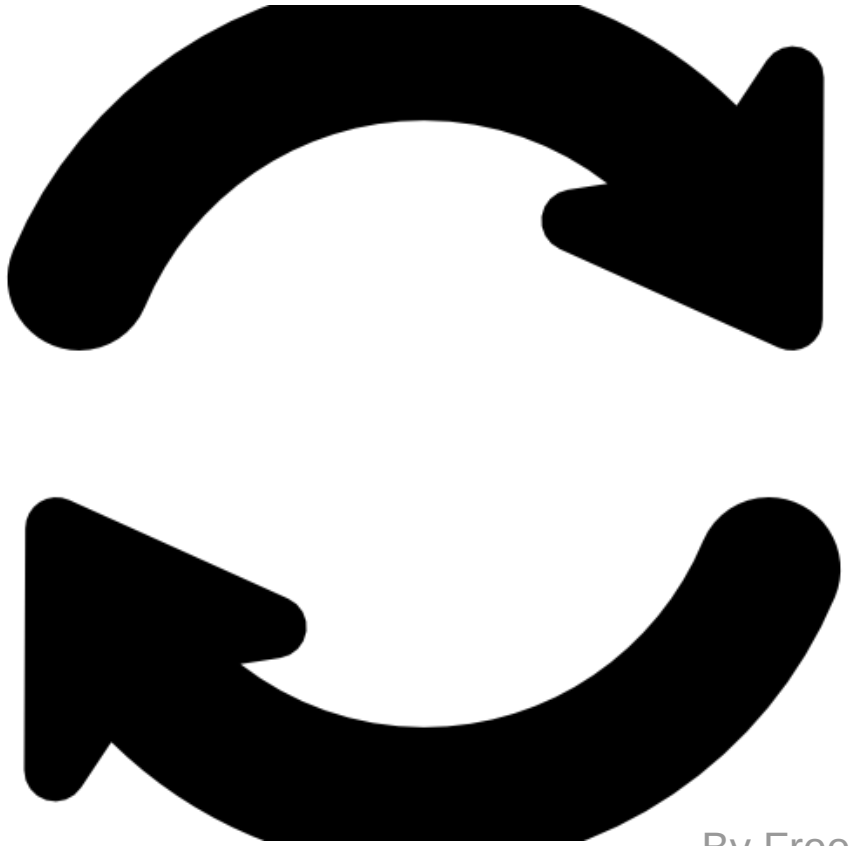
By Freepik

Allgemeines Sicherheitstipps

Spiele Sie Updates ein

Updates sind heute wichtiger denn je. Häufig werden Sicherheitslücken damit geschlossen oder neue Sicherheitsfeatures eingestellt.

Eine Erleichterung ist es, das jeweilige System so zu konfigurieren, dass Updates automatisch eingestellt werden oder man benachrichtigt wird, wenn Updates anstehen.

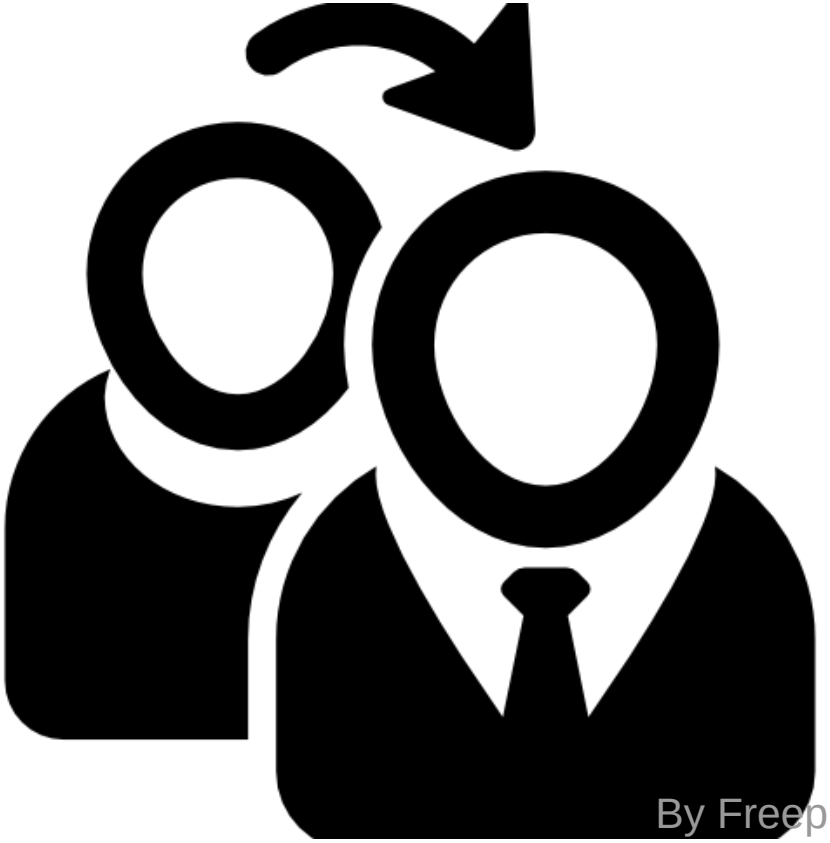


By Freepik

Allgemeines Sicherheitstipps

Arbeiten Sie mit eingeschränkten Rechten

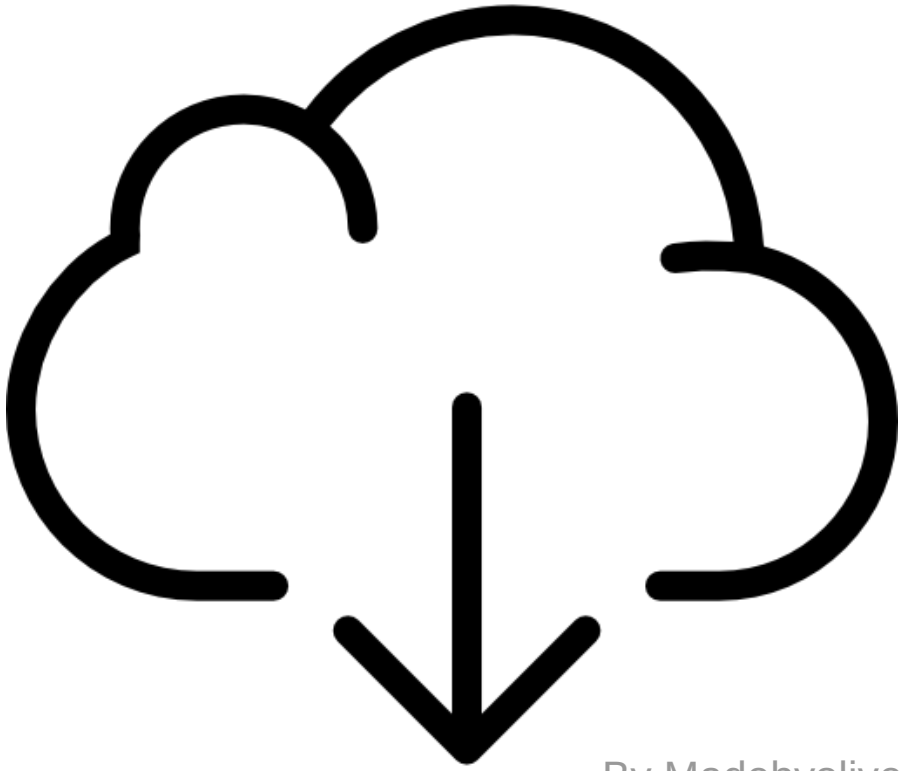
- Richten Sie einen eigenen Administratoraccount ein und nutzen Sie diesen nur zur Administration.
- Für die tägliche Arbeit: arbeiten Sie mit normalen Nutzerrechten.



Allgemeines Sicherheitstipps

Vermeiden Sie zweifelhafte Softwarequellen

- Laden Sie kostenlose Software nicht von beliebigen Seiten herunter.
- IT-Zeitschriftenverlage stellen z.B. häufig auf Viren geprüfte Programme zum Download zur Verfügung.
- Smartphone-Apps: als sicher gilt nur der jeweilige Store (Play Store und App Store).



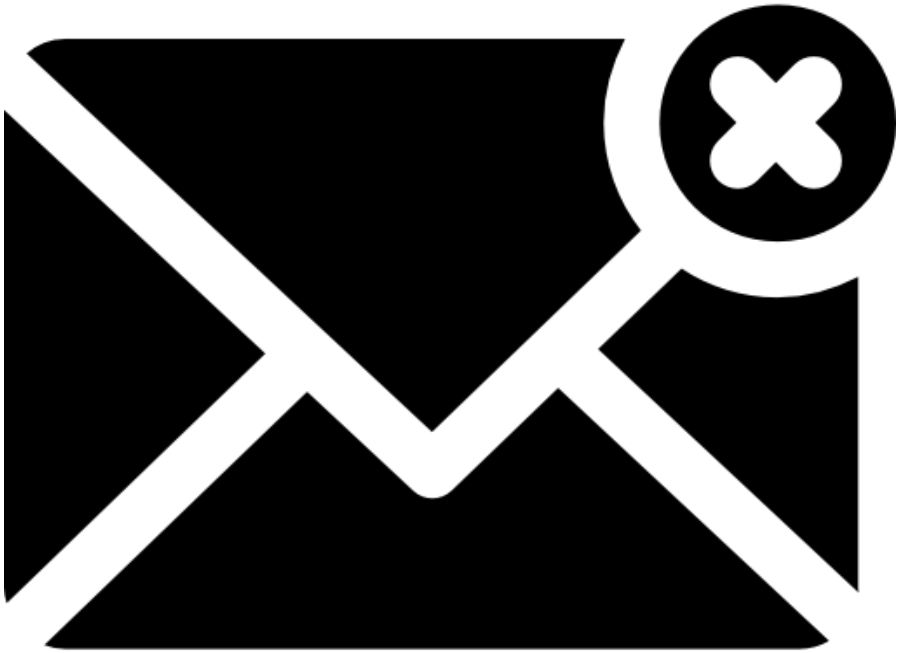
By Madebyolive

Allgemeines Sicherheitstipps

Seien Sie vorsichtig bei verdächtigen E-Mails

- Öffnen Sie keine Links oder Anhänge aus verdächtigen E-Mails.

- Verdächtig sind Sie häufig dann, wenn
  - Sie den Absender nicht kennen
  - Die sprachlichen Formulierungen schlecht sind
  - Ihnen tolle Dinge versprochen werden
  - Zeitlicher Druck ausgeübt wird
  - Sie auf dubiose Seiten gelockt werden und dort Ihre Daten eingeben sollen.

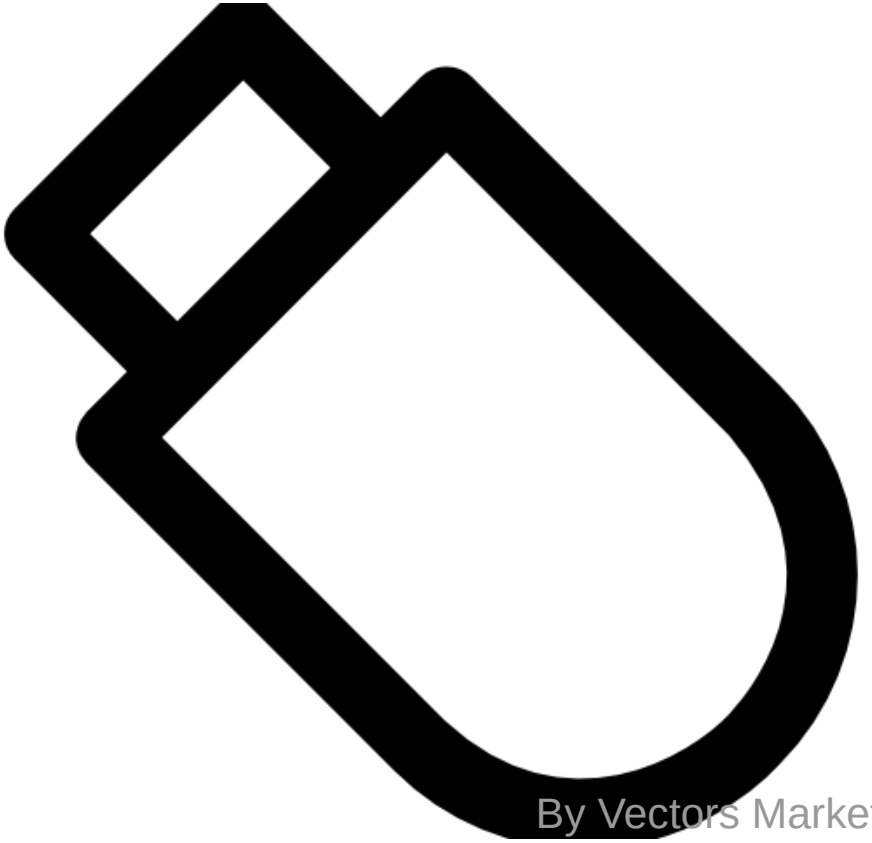


By Schnittstelle

Allgemeines Sicherheitstipps

Vertrauen Sie nicht blind USB-Sticks

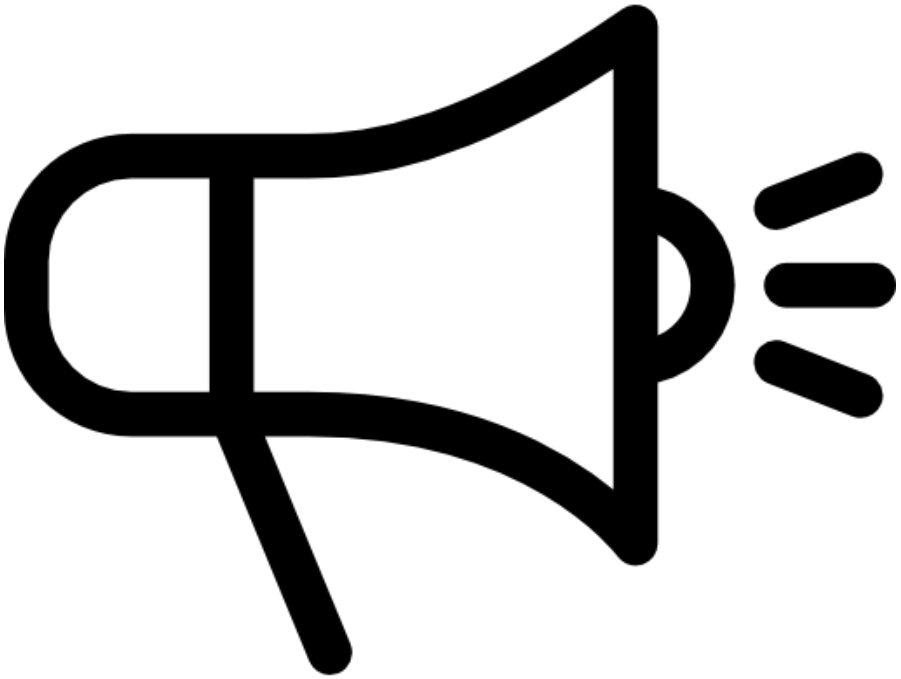
- Ein Einfallstor für Schadsoftware ist der USB-Stick.
- Gefundene USB-Sticks können absichtlich verloren gegangen sein, damit der Rechner des Finder infiziert wird.
- Aber auch der USB-Stick des Kommilitonen kann gefährlich sein. Ist dessen Rechner verseucht, können Sie Ihren Rechner über den USB-Stick infizieren.



Allgemeines Sicherheitstipps

Schützen Sie sich vor Werbung im Browser

- Malvertising ist das Ausliefern von Schadsoftware über Werbenetzwerke. Damit werden schädliche Anzeigen auf eigentlich vertrauenswürdigen Webseiten geschalten, die sofort den Rechner infizieren.
- Abhilfe schaffen hier Werbeblocker (siehe auch www.it.tum.de/sicher/adblocker).



By Gregor Cresnar

Allgemeines Sicherheitstipps

Alle diese Tipps helfen dabei, das mobile Leben sicherer zu machen.

Ein 100%iger Schutz ist dies allerdings nicht.

Deshalb: immer mitdenken und nachdenken, was man gerade online tut.

Sie wollen noch mehr Tipps?
www.it.tum.de/sicher/rechner
Und
www.it.tum.de/sicher/smartphone

Oder nehmen Sie unsere Flyer mit!

Danke für Ihre Aufmerksamkeit!