

Awareness: Sensibilisierungskampagne zu (Selbst-)Datenschutz und IT-Sicherheit

Dr. Hans Pongratz, pongratz@tum.de
Geschäftsführender Vizepräsident (CIO)
Technische Universität München (TUM)

HRK-Workshop Informationssicherheit als
strategische Aufgabe der Hochschulleitung

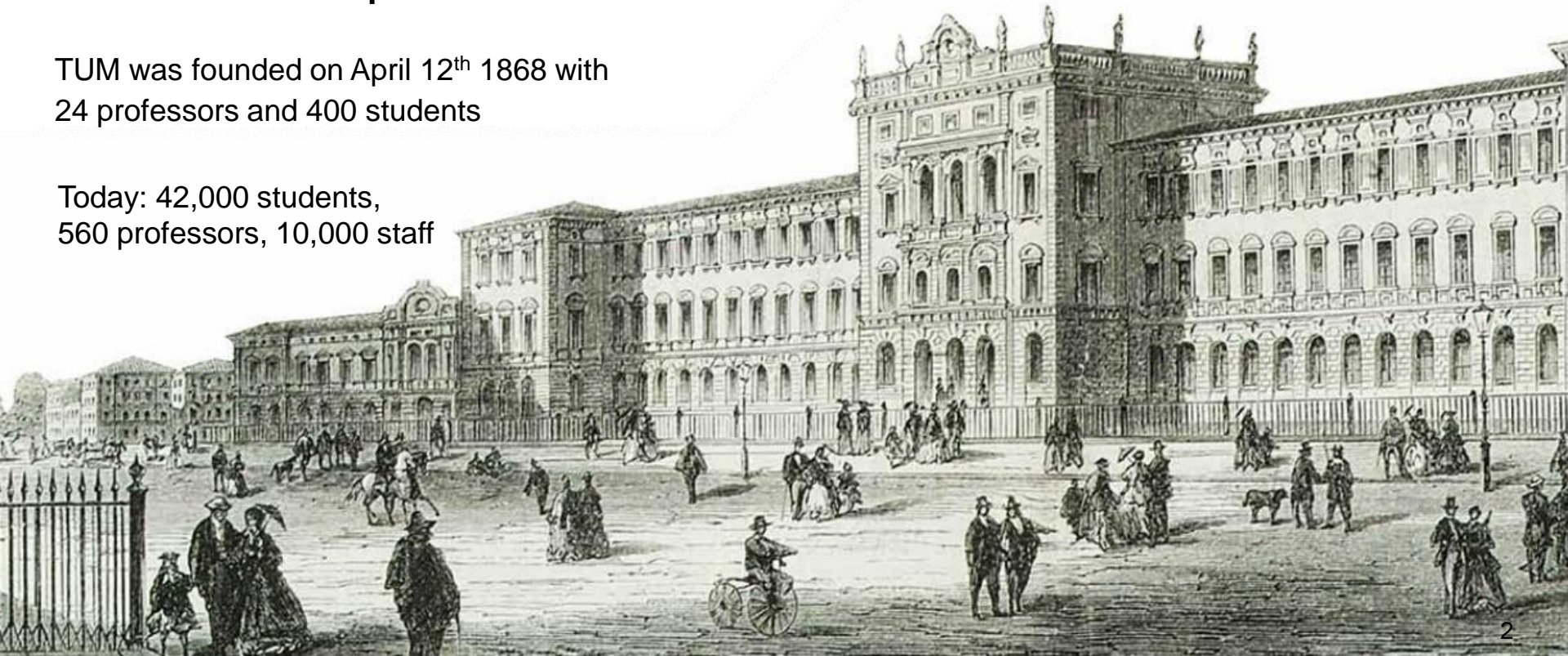
Berlin, 25. November 2019



A look in the past

TUM was founded on April 12th 1868 with
24 professors and 400 students

Today: 42,000 students,
560 professors, 10,000 staff



Long-term Leitmotif: The Digitally Enabled University

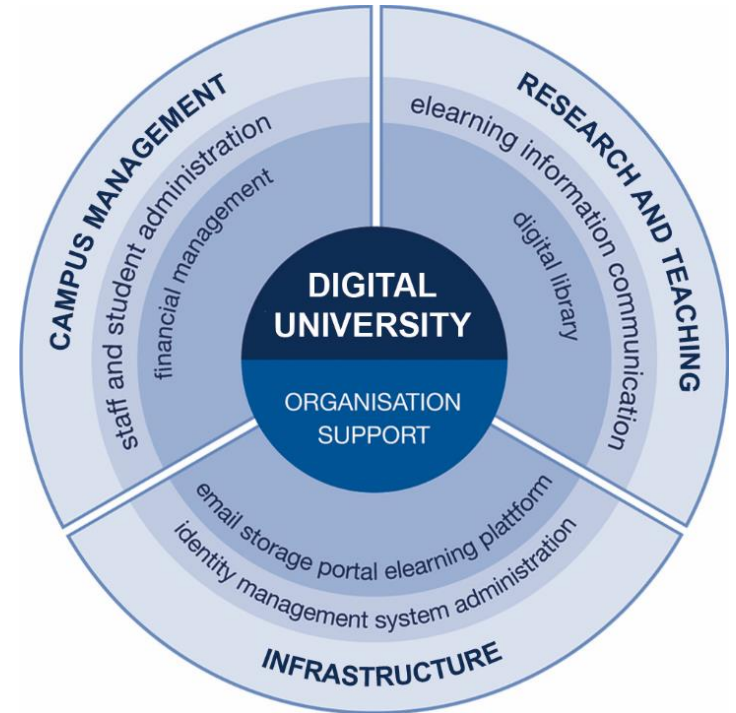
Baseline:

»A customer-friendly and smoothly integrated ICT infrastructure for research, teaching and administration«

Mantras Digital Transformation:

- User-focused (personalized & individualized)
- At any time and from anywhere

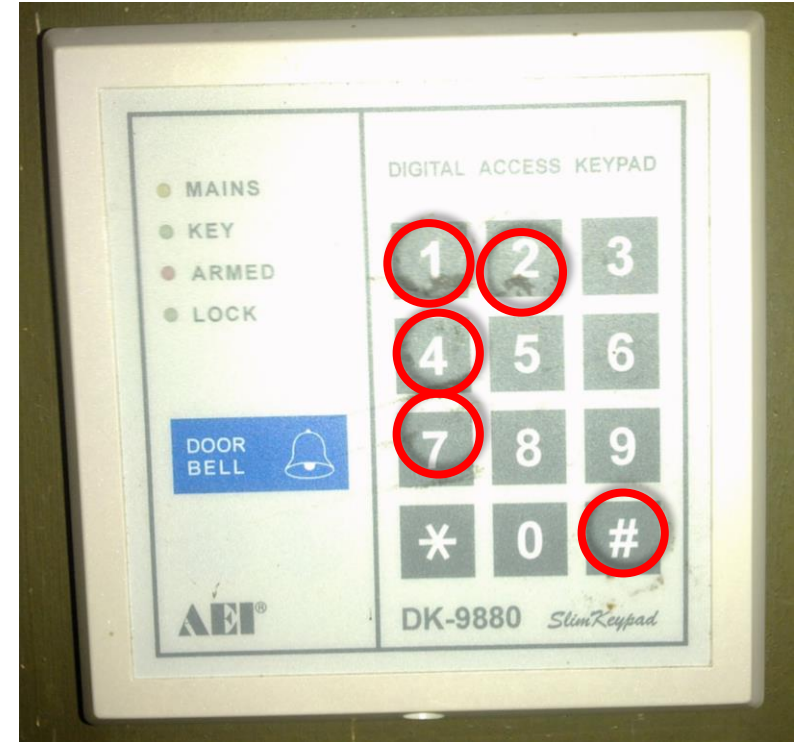
Levels of Digitalization:



IT-Security at HEIs?

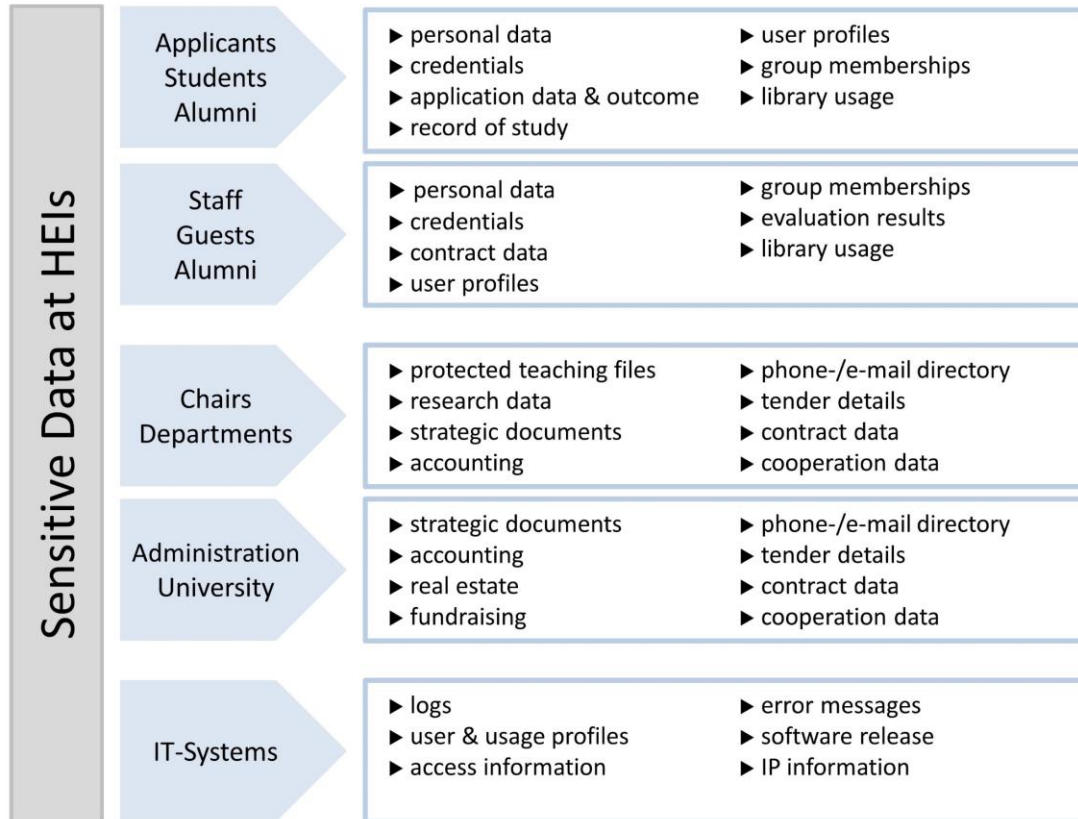


Quelle: unbekannt



Quelle: Pongratz

Sensitive Data at HEIs - categorization model



Fraud: TUM edX Certificate

Supplier Verification Request (14124-7301792-3)





Contact Us



996284301



996284301

Mon ~ Sat (GMT+8)
am. 08:00 ~ 12:00
pm. 14:00 ~ 18:00

Free Email Sample

[Click Here](#)

[Click to Email](#)

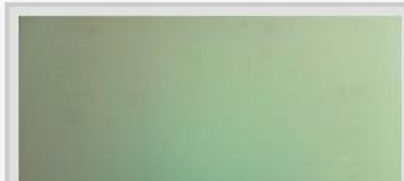
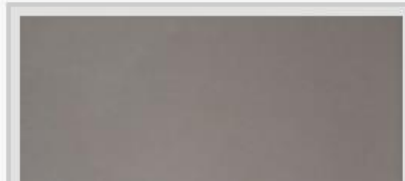
Frequently Asked Questions

- Why Choose fakecertificatemall?
- No Substitution of Schools or D
- What's the guarantee that I will
- How long will I receive the cer
- How Does This Work?

Real Customized Raised and Embossed Seals



Papers





';--have i been pwned?

Check if you have an account that has been compromised in a data breach

<https://haveibeenpwned.com/>



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)

416

pwned websites

9,138,980,630

pwned accounts

104,344

pastes

123,501,318

paste accounts

Why Campaigns? Our story in a nutshell ...

More than 50 universities hacked (~ 2012):

servers from universities worldwide got hacked (e.g. Harvard, Stanford).

Bold phishing mails:

... lost my bag, please send money for ticket home ...

Lots of more examples, e.g. remote shells and defacements on websites

Our approach:

- **New position of IT security and privacy officer**
- **Security Incident reporting, handling and support**
- **Cybersecurity Awareness Campaigns**

How did we start?

- small, very motivated team
- lots of brainstorming & stocktaking
- lots of talking to faculty and students

⇒ Proposal with concrete awareness-raising measures, estimated costs, and potential outreach.

Vorschläge für Maßnahmen zur Sensibilisierung im Bereich IT-Sicherheit

Ziel	1
Maßnahmen	2
Kostenabschätzung	3
Nächste Schritte	3
Darstellung der Maßnahmen	4
Maßnahme: IT-Sicherheitshirts	4
Maßnahme: Haftnotizzettel	5
Maßnahme: IT-Pursuit	6
Maßnahme: Revolverblatt	8
Maßnahme „Frauenzeitschriftentest“	10
Maßnahme Alltagsvergleiche	11
Maßnahme: IT-Sicherheitszahl der Woche	13
Maßnahme Handyreinerpads	15
Maßnahme Ideenwettbewerb	17
Maßnahme Verlosung	17

Ziel

Ziel der Vorgeslagenen Maßnahmen ist die Sensibilisierung von Mitarbeitern und Studierenden für die Bereiche IT-Sicherheit und Datenschutz im universitären wie auch privaten Umfeld.

Mitarbeiter und Studierende sollen über die Gefahren informiert werden, die in der digitalen Welt auf sie warten. Außerdem sollen Tipps und Tricks, sowie Gegenmaßnahmen, die sie ergreifen können dargestellt werden, so dass sie in der Lage sind sich sicher im Internet zu bewegen, ob nun beim Online-Banking, Online-Einkauf, Umgang mit der IT am Arbeitsplatz oder mit dem Smartphone.

IT-unerfahrene Mitglieder der TUM sollen dabei grundsätzlich für IT-Sicherheitsthemen sensibilisiert werden, um den „Grundgefahren“ des Netzes besser gerüstet entgegen treten zu können.

IT-erfahrene Mitglieder der TUM sollen über witzige Marketingmaßnahmen gebracht werden, wichtige IT-Sicherheitsthemen erneut zu bedenken. Da IT-Sicherheit häufig zugunsten der Bequemlichkeit vernachlässigt wird, sollen die Maßnahmen durch Humor das Thema präsen-ter machen und über die eigene Bequemlichkeit nachdenken lassen.

Neben Texten für Newsletter und Informationen unter www.it.tum.de/sicherheit sollen Werbemittel eingesetzt werden, um die Aufmerksamkeit auf das Thema IT-Sicherheit zu lenken. Studierende sowie Mitarbeiterinnen und Mitarbeiter sollen auf obige Webseite aufmerksam gemacht werden und regelmäßig auf dort beschriebene Themen aufmerksam gemacht werden.

The golden rules

Les règles d'or

Die goldenen Regeln



Keep your password safe!
 Protégez votre mot de passe!
 Bewahren Sie Ihr Passwort sicher auf!



Avoid printing sensitive data unless necessary!
 Évitez d'imprimer des données sensibles si ce n'est pas nécessaire!
 Vermeiden Sie das Ausdrucken sensibler Daten!



Going for a coffee? Lock your computer first!
 Passez café? Verrouillez d'abord votre ordinateur!
 Kaffeezeit? Sperren Sie erst Ihren Desktop vor unbedingtem Zugriff!



Did you lose your PDA? Report it to your IT department immediately!
 Avez-vous perdu votre PDA? Prévenez immédiatement votre support technique!
 PDA verloren? Benachrichtigen Sie sofort Ihre IT-Abteilung!



Visitors should be badgeged and escorted in the building at all times!
 Des visiteurs devraient avoir un badge et être escortés dans le bâtiment à tous les moments!
 Die Besucher Ihres Gebäudes sollten Besucherweises tragen und immer begleitet werden!



...Don't make your organization's confidential information available to everyone!
 ...Ne laissez pas les informations confidentielles de votre organisation disponibles à chacun!
 ...Machen Sie sensible Informationen Ihrer Organisation nicht für jeden zugänglich!



Secure sensitive data by locking your desktop screen!
 Protégez les données sensibles en ne les laissant pas accessible!
 Sperren Sie sensible Daten und halten Sie Ihren Schreibtisch in Ordnung!



Going home? Log off from your computer!
 C'est le fin de journée? Fermez votre session!
 Peterabend? Ausloggen nicht vergessen!



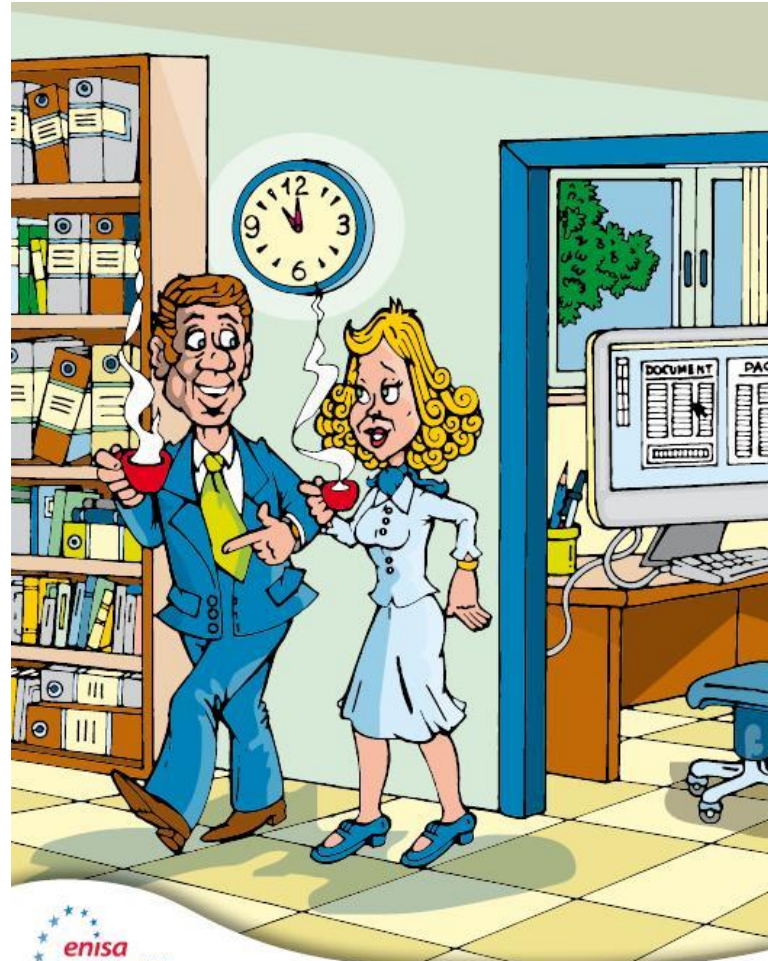
Don't leave your laptop on view in the car!
 Ne laissez pas votre ordinateur portable visible dans votre voiture!
 Lassen Sie Ihren Laptop nicht sichtbar im Auto liegen!



Working while travelling? Be it safely!
 Travail à distance? Faites-le sans risque!
 Arbeiten unterwegs? Richten Sie vorsichtig!



Avoid printing sensitive data unless necessary!



**Going for a coffee?
Lock your computer first!**

Video clips on raising awareness by ENISA



e.g. on shoulder surfing

23 languages available!

Our agenda

- Idea Contest
- Talks and seminars
- Live hacking event
- Giveaways
- Flyer & articles
- Website
- Phishing helpdesk
- European Cyber Security Month

Our mantra:

***»Recommend instead of prescribe,
convince instead of force,
make curious instead of bore.«***

IT Idea Contest:

Tired of boring IT security notices?



Sicherheitshinweise von gestern? Machen Sie mit beim Ideenwettbewerb. (Foto: Martin Jäschke/Photocase.de)


14.04.2014

Are you tired of boring IT security notices such as "Remember to change your password regularly!" or "Use an anti-virus software!"? Help us to improve – you can win a personalized T-shirt! Take part in the IT-security awareness contest.

We are looking for slogans or designs that appeal to you and your fellow students, that are funny and that might even cause IT-noobs to give a thought to IT security. If you have an idea that could catch your fellow students' attention as a T-shirt design, a flyer or some other

marketing object, please send it in by **May 31, 2014**.

We will reward any idea we can use with a T-shirt that has your idea printed on it. You can choose the shirt colour and size yourself.

For more information concerning the competition and how to take part please visit www.it.tum.de/wettbewerb/ 



mach's m
Gib Computerviron keine Cha
www.it.tum.de/s



And how do you protect your pride and joy?

Protect yourself against malicious apps

- Unnecessary apps deleted?
- Unknown installation sources avoided?
- What kind of rights does the app want?

Protect against loss

- Remote wipe configured?
- Backup performed?

Protect your private sphere

- Are Bluetooth, GPS and WiFi activated only when needed?
- Do you trust public WiFi networks?

General

- Security updates installed?
- Screen lock activated?



Learn about IT security at www.it.tum.de/en/safe

Do your part.



Protect your smartphone.

Und wie schützt du dein bestes Stück?

Auf Smartphones speichern wir inzwischen meist mehr und wichtigere Daten als auf unseren Rechnern. Das weiß nicht nur die NSA, sondern das wissen auch Kriminelle. So entstehen Viren und Trojaner für Smartphones, aber auch Smartphone-Apps, die persönliche Daten abgreifen um damit Geld zu verdienen oder die



Daten für andere Angriffe zu verwenden.

Um dein Smartphone zu schützen gibt es ein paar einfache Tipps, die wir dir hier vorstellen wollen. Ausführlicher findest du die Tipps unter

www.it.tum.de/sicher/smartphone

- Allgemeines**
 - Spiele Betriebssystemupdates ein. Damit werden oft Sicherheitslücken geschlossen.
 - Richte eine Displaysperre ein. So kann niemand auf die Schnelle auf dein Smartphone zugreifen.
- Apps**
 - Für Android: Installiere nichts aus unbekanntem Installationsquellen.
 - Vor der Installation einer App: Prüfe die Berechtigungen. Ist eine App zu gierig, installiere lieber eine Alternative.
 - Lösche nicht benötigte Apps. So wird Speicherplatz frei und eventuelle Sicherheitslücken stellen kein Risiko mehr dar.
- Schutz vor Zugriff von außen**
 - Schalte nicht benötigte Dienste wie Bluetooth, WLAN und GPS aus. So kann dein Smartphone nicht von extern auf Lücken gescannt werden und du sparst Strom.
 - Sei vorsichtig bei der Einwahl in öffentliche WLANs. Alle Daten werden im Klartext übertragen. Passwörter für E-Mails und Banking-Apps können so, vorausgesetzt es handelt sich um keine sichere Verbindung, ausgespäht werden. An der Uni kannst du aber bedenkenlos das eduroam-WLAN verwenden.
- Schutz bei Verlust**
 - Bei Verlust solltest du sofort deine SIM-Karte sperren lassen, damit niemand auf deine Kosten telefonieren kann.
 - Es gibt viele Tools, um die Daten von Smartphones aus der Ferne zu löschen, falls dein Handy gestohlen wurde. Auch über den TUM-Exchange kannst du dir so eine Möglichkeit einrichten.
 - Mache regelmäßig ein Backup, so bleiben dir z.B. deine Fotos auch bei Verlust deines Smartphones erhalten.

mach's mit.



ICH WILL'S SICHER!

Schütze auch dein Smartphone.

Schütze Dein Smartphone vor fremdem Zugriff



Gerät einstecken

Lass Deine mobilen Geräte niemals unbeaufsichtigt, um unbefugte Zugriffe und Manipulationen zu verhindern.

Displaysperre einrichten

Richte Dir eine Displaysperre ein. So kann niemand auf Deine Daten zugreifen, falls Du das Gerät verlierst oder es unbeaufsichtigt liegen lässt. Hierfür gibt es viele unterschiedliche Varianten: Von Passwort über PIN und Muster bis zum Face Unlock (Gesichtserkennung).

Sicherheitsupdates einspielen

Spiele immer alle Sicherheitsupdates ein. Egal ob Android-Phone, iPhone, Blackberry oder Windows-Phone!

Drahtlose Schnittstellen und Ortungsdienste deaktivieren

Schalte nicht benötigte Dienste wie Bluetooth, WLAN und GPS aus. So kann Dein Smartphone nicht von extern auf Lücken gescannt werden, zu neugierige Apps können weniger über Deinen Standort erfahren und der Akku hält auch länger.

Öffentliche WLANs meiden

Sei vorsichtig bei der Einwahl in öffentliche WLANs, die z.B. von Cafés angeboten werden. Dort ist das Mitlesen Deines Datenverkehrs häufig recht einfach möglich. Passwörter für E-Mails und Banking-Apps können so evtl. ausgespäht werden. Tipps zur Nutzung findest Du unter www.it.tum.de/sicher/wlan/.

An der Uni kannst Du übrigens bedenkenlos das eduroam-WLAN verwenden.

Tipps zum richtigen Umgang mit Apps und Vorkehrungen für den Fall von Verlust findest Du unter www.it.tum.de/sicher/smartphone

mach's mit.



ICH WILL'S SICHER!

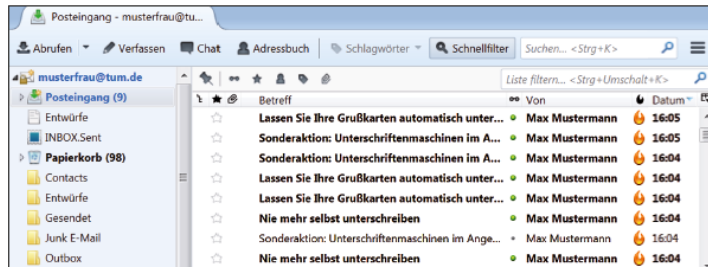
Schütze dein Smartphone.

Rechner gehackt- Student wird zu Computerkurs verknackt

Ein Student der TU München wurde zum Besuch eines Computerkurses verurteilt, weil Hacker in seinem Rechner eingedrungen waren.

München, 22.08.2014

Der Student Max M. soll laut eines Urteils des Landesgerichts Münchens für die Überflutung von Millionen E-Mailpostfächern mit Werbe-E-Mails für Unterschriftenmaschinen verantwortlich sein.



Die Flut an Werbemails war unglaublich.

Laut Recherchen des Cyberfachdezernats des Polizeipräsidiums München wurden diese Werbe-E-Mails vom MacBook des Studenten Max M. versandt. Obwohl Max M. vor Gericht seine Unschuld beteuerte, musste er zugeben, dass er weder einen Virenschanner noch die anstehenden Updates installiert hatte.

Der Staatsanwalt warf Max M. grobe Fahrlässigkeit vor, da man von jungen Menschen, die in der digitalen Welt bereits aufgewachsen seien (sogenannten Digital Natives), mehr Fachkenntnis erwarten könnte. Der Richter folgte der Argumentation des Staatsanwalts und verpflichtete den Studenten zum Besuch eines Kurses zur IT-Sicherheit.

Sicherheitstipps für deinen Rechner

Egal ob Windows, Mac OS X oder Linux, dein Rechner will vor Schadsoftware und Hacker-Angriffen geschützt sein. Hier haben wir die wichtigsten Tipps für dich zusammengestellt.

- Installiere einen Virenschanner. Beim LRZ kannst du dir kostenlos Sophos Antivirus für Windows, Mac OS X und Linux herunterladen.
- Aktualisierungen sind Pflicht. Alle Betriebssysteme verfügen über Einstellungen, so dass automatisch wichtige Updates installiert werden. Auch viele Softwarepakete verfügen über diese Einstellungen, andere musst du manuell aktualisieren.
- Installiere keine Programme aus unsicheren Quellen. Vertrauenswürdig sind z.B. Softwareverzeichnisse von renommierten IT-Verlagen, die die angebotene Software auch auf Viren prüfen (z.B. www.heise.de/download oder www.chip.de/Downloads).
- Arbeite nicht mit dir einen normalen Benutzer für die tägliche Nutzung an. Vergib sowohl für den Administrator wie für den normalen Benutzer ein eigenes Passwort.
- Nutze eine Firewall. Eine Firewall kann dich vor Schadsoftware oder auch Hacker-Angriffen schützen. Sowohl Mac OS X wie Windows haben eine integrierte Firewall, standardmäßig ist diese aktiviert.
- Öffne keine verdächtigen E-Mails oder Anhänge, damit niemand von außen in deinen Computer eindringen kann.
- Schließe keine USB-Sticks an, deren Herkunft du nicht kennst. Auch diese können Schadsoftware enthalten.

Mehr Infos zur IT-Sicherheit (z.B. auch für dein Smartphone) findest du unter: www.it.tum.de/sicher

mach's mit.

Gib Viren keine Chance.



**ICH WILL'S
SICHER!**

Security tips for your computer

Whether you have Windows, Mac OS X or Linux, you want your computer to be protected against malicious software and hacker attacks. To help, we have put together a collection of the most important tips.

Install antivirus software

Install a virus scanner. You can download the free Sophos Antivirus program for Windows, Mac OS X and Linux from LRZ (www.lrz.de/antivirus).



by Vectors Market

Keep your software up-to-date

Updates are mandatory. All operating systems can be configured to automatically install important updates. While many software programs offer this feature as well, some have to be updated manually.



by Freepik

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 (i.e. www.heise.de/download).



by Madebyolive

Work with restricted rights

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



by Freepik

icons from www.flaticon.com

Security tips for your computer

Use a firewall

Use a firewall, which can protect you against malicious software or hacker attacks. Both Mac OS X and Windows have an integrated firewall enabled by default.



by Freepik

Use caution with suspicious e-mails

Never open suspicious e-mails or attachments, so that no one can invade your computer from the outside.



by Schmittstelle

Beware of browser ads

Browser ads can also be misused to distribute malware. To learn what "malvertising" is and how you can protect your system against it, read the article www.it.tum.de/en/adblocker.



by Gregor Cresnar

Don't use USB sticks from unknown sources

Never plug in USB sticks unless you know where they come from. Unknown USB sticks can also contain malicious software.



by Vectors Market

You can find additional information about IT security, including for your smartphone, at: www.it.tum.de/en/safe



Personalized password cards for students

	ABC	DEF	GHI	JKL	MNO	PQR	STU	VWX	YZ	.
0	Nj	b	dGI	yq	/	8:	z7c	cC	L2u	f
1	@G	i	gL	;	Tsl	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	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;	/	*

e.g. password for EDUCAUSE:

1. E i
2. D GU
3. U Yw
4. C 5k
5. A x
6. U 5
7. S PK
8. E sc

iGUYw5kx5PKsc

[Manual](#) and [Generator](#)

April Fools' 2016

- our employees via email
- designed to raise awareness
- opportunity to apply knowing about handling malicious emails
- website we lured them, offers lots of information on data protection, privacy, and IT security

[Link to email](#)

Dear Colleagues,

The TUM ID (still frequently known as the LRZ ID) has been a key aspect of the TUM IT system, particularly for central identity management. Because the format of the TUM ID (i.e. "gu42abc") is neither user-friendly, nor compatible with TUM's new corporate design, the IT Service Center and the Leibniz Supercomputing Center (LRZ) have been working hard to create a new, user-friendly and secure solution for you.

THE MOST IMPORTANT CHANGES

- The TUM ID will no longer be valid effective July 1, 2016.
- In the future, the Facebook ID will be used instead of the TUM ID.
- To prevent data loss, please link your TUM ID to your Facebook ID. This can be done effective today: April 1, 2016.

Below is additional information on how to proceed.

BENEFITS AT A GLANCE

- By linking to your Facebook account, you have an easy-to-remember user

April Fools' 2016 Reactions

Given that we haven't received any official notice abolishing the humor waiver, I assume this was a genuine attack. Please check your systems thoroughly and issue a corresponding warning to all employees who failed to carefully read the specified website... :)

The shock has set in, especially after a careful analysis of the link which revealed that it actually leads to a TUM page. As a wake-up call though, it was a great idea.

Link to [reactions](#)

Thanks a lot for the information. I have to admit, you got me. It was a brilliant campaign, for which you are to be commended. And many thanks even if I fell for it hook, line and sinker...;-)

+++Breaking News+++

TUM has a new president effective April 1, 2016. With 22 likes, Mark Zuckerberg takes over the helm of the elite university. We look forward to the new face (corporate design) of TUM.

*What a brilliant idea! It did seem rather "fishy" as we would say in British English. I much appreciate the TUM IT Department's efforts to assist and warn TUM staff members in this way. It is all part of "awareness training" opening our eyes to such emails. Those of us who have not "grown up with" the computer urgently need such training!
Thanks for the appropriate April Fool's joke!*

Helping people to help themselves

Phishing self-learning test - Question 1

The first email received via muster.liste@tum.de

From: Lunina@abox-labo.com
Sent: Sunday, 17 November 2013 05:50
To: <muster.liste@tum.de>
Subject: I NEED YOUR HELP P/S

Lunina Augama Nugama,

My name is Miss Lunina Nuguma the only daughter of late Mr. and Mrs John Nuguma. I want you to assist me to transfer my inherited money US\$ 1 .2 M to you and I come over to your country and continue my life there. My father left it in bank the sum of US\$1.2M before his untimely death as a result of food poison.I am an orphan . I will give you 15% if you will assist me and upon your reply I will tell you how this fund will be transferred to you by giving details and contact of the bank, so kindly send me your full name; your country and your telephone number and reply me directly here (Lunina.nugama@mail333.com)

Thanks and God bless!

Raising attention

Who do you send confidential data to?

Assume you receive the following email from your boss

From: Hans Pongratz <HansPongrats@gmx.de>
To: Max Mustermann <max.mustermann@tum.de>
Subject: Urgent: Employee list required

Dear Mr Mustermann,

The president requested that I provide him with a list of all employees of the Campus Management Team.

Unfortunately, I only have restricted access to the TUM systems while on vacation. Please provide me a list of all employees, including their name, employee number, telephone number, email address, pay scale and contract termination date.

As usual, this is an urgent matter, so I need the information today.

Best Regards,
Hans Pongratz

--

Dipl.-Inf. Hans Pongratz
Vice President, TUM IT Systems & Services (CIO)

Lessons learned

- Very good feedback on campaigns
- Use different channels (online and offline) and focus on different target groups,
- Good examples and locations (office, canteen, lecture hall, ...) is very important
- Current incidents and press releases are good hooks
- Regular actions are needed!
- “After the campaign is before the next campaign”
- Raising awareness is persuading, not prescribing

=> Get in touch, we would be happy to discuss further ideas! ponggratz@tum.de

Zusammenarbeit wichtig - Beispiele

Bayern

- Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen
- Stabsstelle IT-Sicherheit & IT-Sicherheitsbeauftragter bayerischer Hochschulen
- Cyberallianz Zentrum beim bay. Verfassungsschutz
- BayernCERT für Behördennetz

Netzwerke

- Allianz für Cybersicherheit
- Bitkom DK Informations- und Cybersicherheit
- (früher ENISA Awareness Raising Community)
- DFN-CERT
- ZKI, HRK, TU9, EuroTech, ...

Einbettung Gesamtkontext einer Hochschule

