„Ich will's sicher“ – Security Awareness Kampagnen an der Technischen Universität München (TUM)

Angelika Müller
Referentin IT-Sicherheit & Datenschutz
mueller@tum.de

Hans Pongratz
Geschäftsf. Vizepräsident & CIO
pongratz@tum.de

24. September 2015, 10. Cyber-Sicherheits-Tag der ACS, Hamburg

TUM Campus

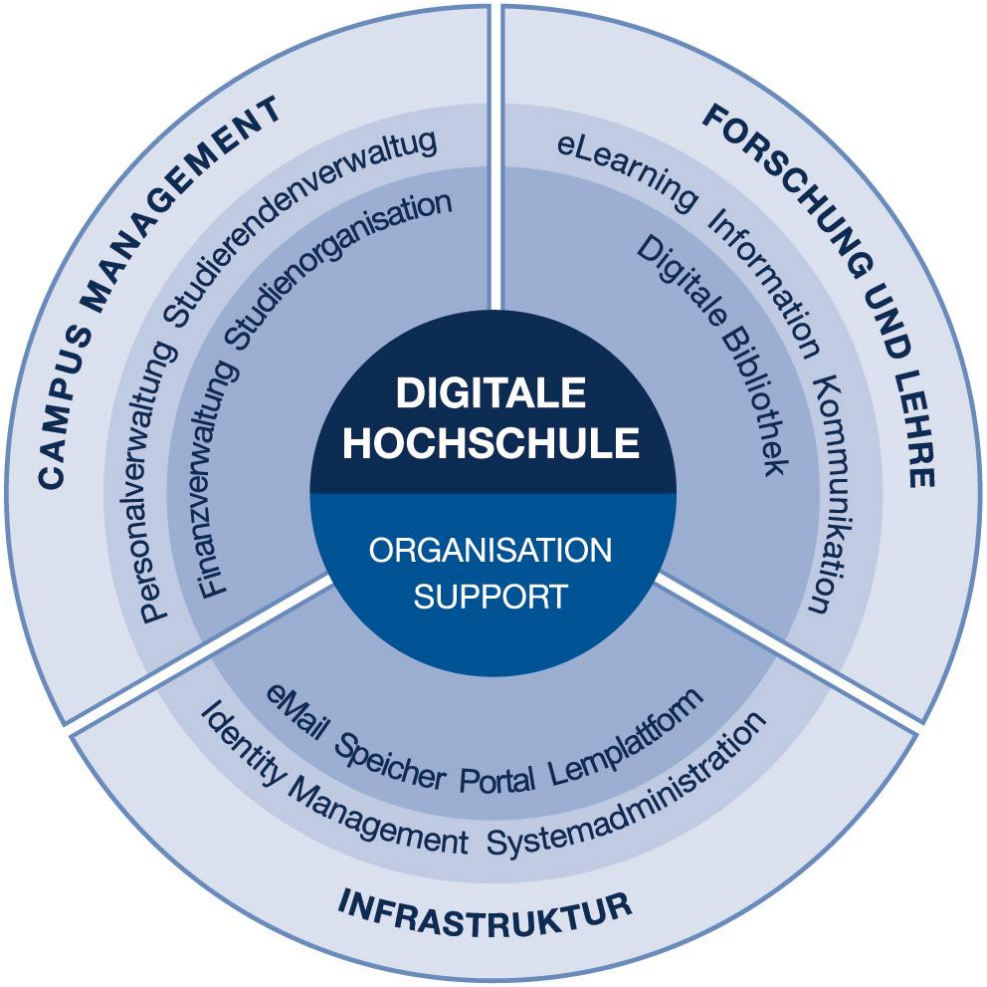
TUM in Zahlen

13	Fakultäten	
411	Gebäude	
154	Studiengänge	
~ 37 300	Studierende	33% Studentinnen 21% Intern. Studierende
~ 511	Professoren (m. Klinikum)	
~ 6 400	Wiss. Mitarbeiter (m. Klinikum)	
~ 3 200	Nichtwiss. Mitarbeiter (o. Klinikum)	
45	ERC Grants	
13	Nobelpreisträger	
17	Leibniz-Preisträger der DFG	
5	Humboldt-Professuren	

TUM IT-Strategie: Digitale Hochschule

„Effiziente Nutzung von Informations- und Kommunikationstechnik zur Verbesserung der Leistungen in Forschung, Lehre und Verwaltung“

- Prozesse
- Organisation
- Technik und Support



IT-Sicherheit: 2012 Einführung zentrales Meldewesen (1/2)

IT-sicherheitsrelevante Vorfälle und Schwachstellen werden zentral dokumentiert und koordiniert, dazu gehören:

- Verlust von elektr. Geräten, auf denen sensible Daten gespeichert sind;
- Einbruch von Hackern in IT-Systeme der TUM;
- Verbreitung von Schadcode durch von der TUM betriebene IT-Systeme;
- Kompromittierung von Zugangsdaten;
- sicherheitskritische Schwachstellen bei im Einsatz befindlichen IT-Geräten und IT-Systemen.

➢ Abwicklung erfolgt über zentralen IT-Support

(it-support@tum.de bzw. 289-17123)

IT-Sicherheit: 2012 Einführung zentrales Meldewesen (2/2)

- Zentrale Hilfestellung zur Wiederherstellung des Betriebs nach einem sicherheitskritischen Vorfall;
- CIO wird regelmäßig informiert, bei schwerwiegenden Fällen unverzüglich;
- Bei Bedarf Einbindung von HSP, Datenschutzbeauftragten, Sicherheitsbeauftragten und Personalrat;
- Neue Referentin IT-Sicherheit & Datenschutz im IT-Management des IT-Servicezentrums der TUM;
- Flankierende Informationskampagnen, um Sensibilität für IT-Sicherheit und IT-Sicherheitsbewusstsein zu fördern.

Zwei Kampagnen zur Sensibilisierung

Zielgruppen: Studierende & Beschäftigte

Maßnahmen (u.a.)

- Ideenwettbewerb
- Vorträge
- Infostände mit Postern, Flyern, Passwortkarten, Give-aways
- Webseite
- Newsletter
- Phishing-Beratung

www.it.tum.de/it-sicherheit

Ideenwettbewerb – Sensibilisierung zur IT-Sicherheit

Zielgruppe: hauptsächlich Studierende

Ausschreibung / Infos: www.it.tum.de/wettbewerb/

Einsendeschluss: 31. Mai 2014

Anzahl Einreichungen: 19

Gewinnervorschlag:

„Ich will‘ sicher. Mach‘s mit. Gib Computerviren keine Chance“

Logo:

Beispiele & Impressionen

Und wie schützt du dein bestes Stück?

Schutz vor Apps
Nicht benötigte Apps gelöscht?
Unbekannte Installationsquellen verboten?
Welche Berechtigungen will die neue App?

…tz vor Zugriff von außen
…S ausgeschalten?
…ffentlichen WLANs?

… Verlust
…ng eingerichtet?
…macht?

…eines
…s eingespielt?
…ysperre aktiviert?

…ormier dich unter
www.it.tum.de/sicher

mach's mit.

ICH WILL'S SICHER!

Schütze dein Smartphone.

Artikel in Studierenden-zeitschriften

Themen

- Das Passwort – der Schutz der digitalen Identität
- Warum ich einen Virenscanner habe? Weil Bodyguards sexy sind!
- Und wie schützt du dein bestes Stück?
- In Vorbereitung: Selbstdatenschutz: Was tun gegen Tracking?

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 unbekannten 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 den 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.

Flyer

Zur Verteilung an die Erstsemester, z.B. in den anfangs ausgeteilten Erstsemestertaschen und zum Verteilen bei Aktionen

- Tipps für den richtigen Umgang mit dem Rechner
- Der richtige Umgang mit Passwörtern
- Schütze 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!

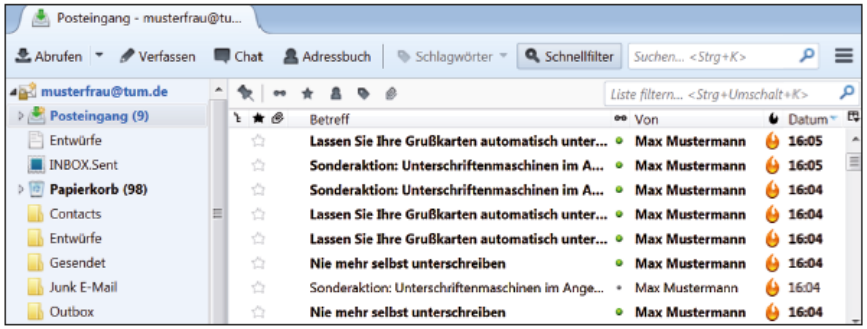
Schütze dein Smartphone.

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 Virenscanner 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 seinen (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 Virenscanner. Beim LRZ kannst du dir kostenlos Sophos Antivirus für Windows, Mac OS X und Linux herunter laden.
- 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

Personalisierte Passwortkarte für Studierende

	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	.1r	1
4	5k	C(	L	vV	pM	F	u1	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
										ZM
										iG
										*

Deine persönliche Passwortkarte

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

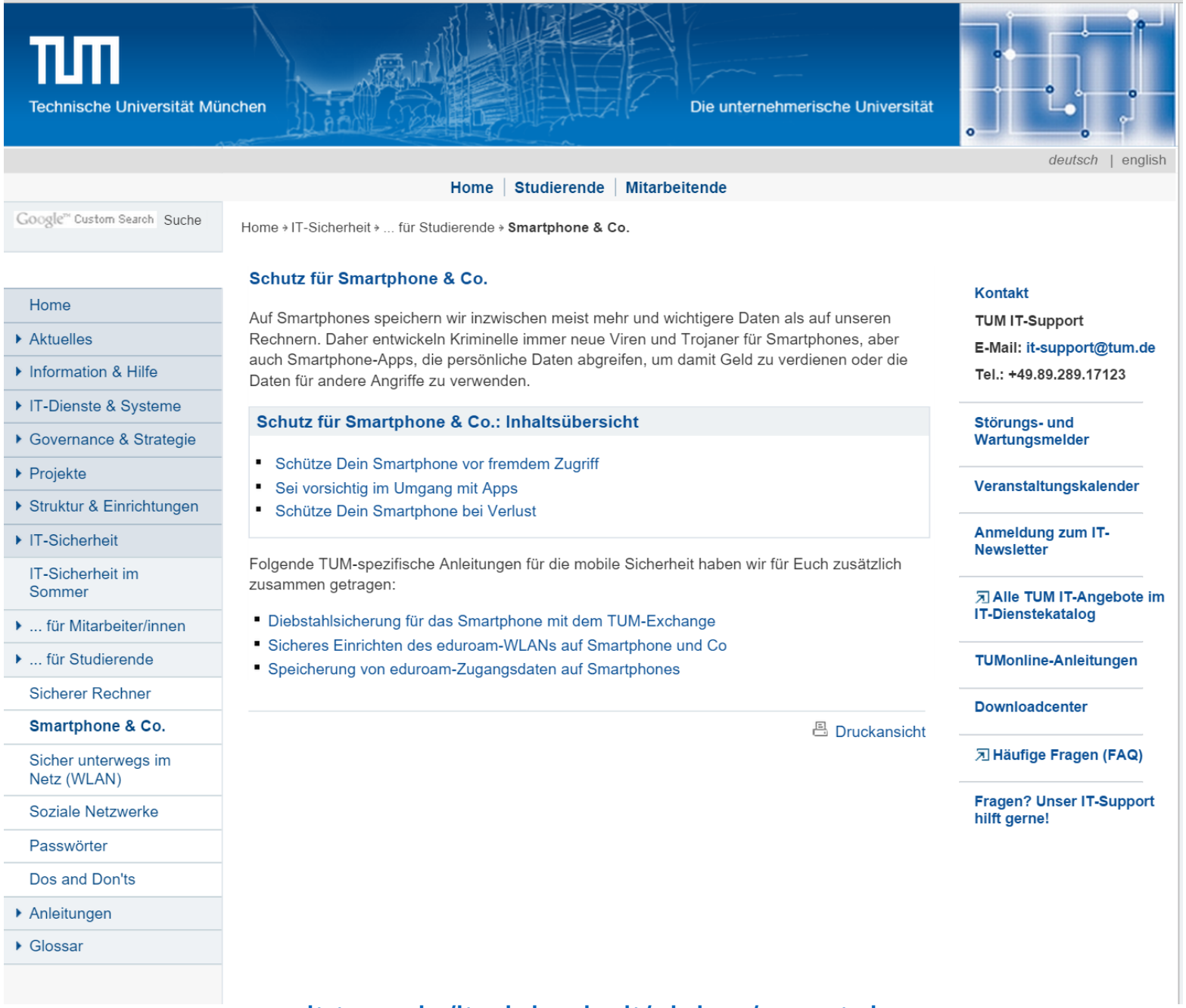
Halte deine Karte geheim, gib Sie niemanden, denn Sie ist der Schlüssel zu deinen Passworten.

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



www.it.tum.de/it-sicherheit/sicher/smartphone

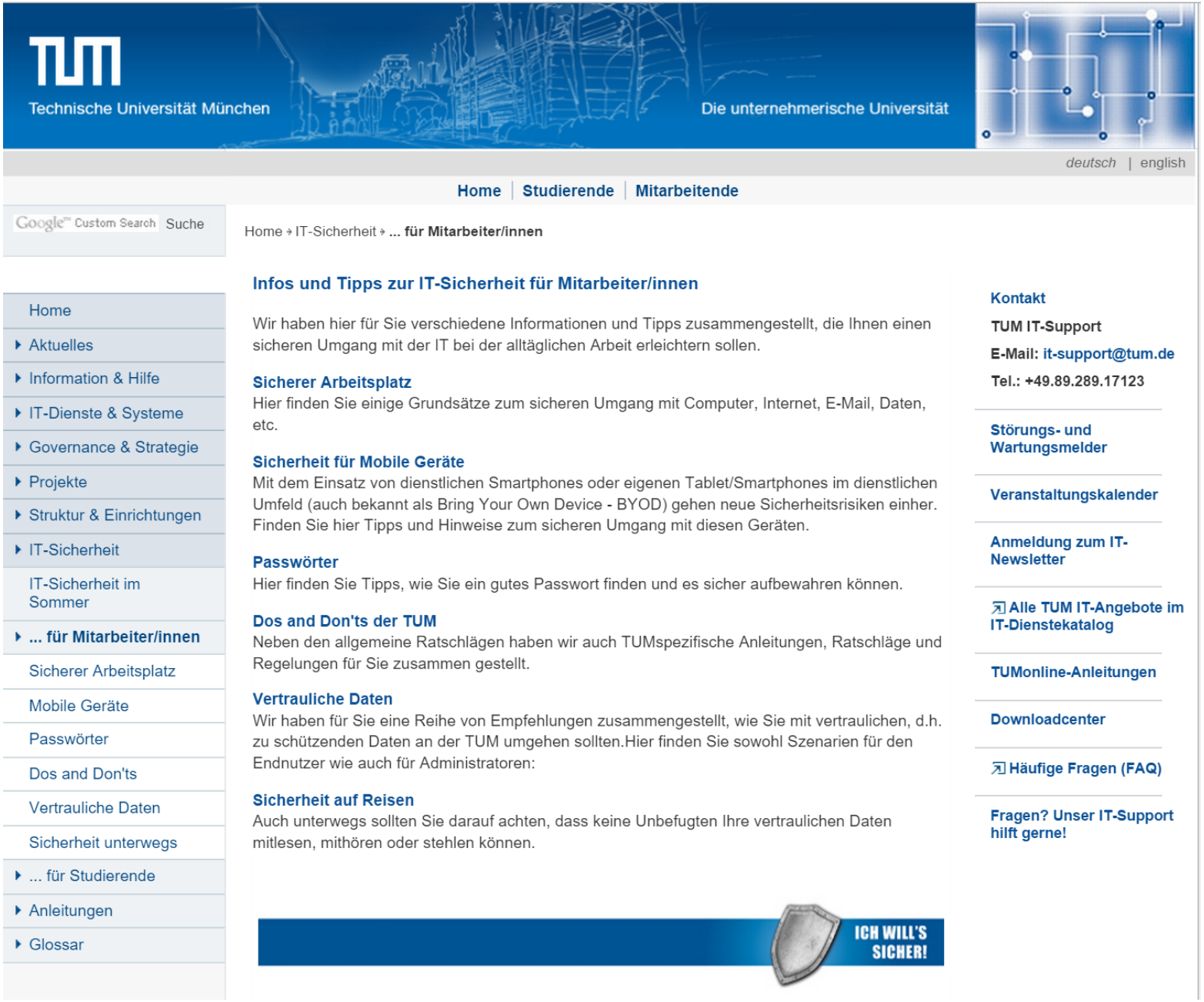
Sensibilisierung der Mitarbeiterinnen und Mitarbeiter

- Nov. 2014: Veranstaltung „Die Hacker kommen“ mit Unterstützung des IT-Planungsrates im völlig ausgebuchten Audimax

- Vortragsreihe IT-Sicherheit im Sommer 2015, s. https://www.it.tum.de/it-sicherheit/it-sicherheit-im-sommer/

- Newsletter, Webseiten und „Aktionen“

Veranstaltung: Die Hacker kommen.



www.it.tum.de/it-sicherheit/fuer-mitarbeiterinnen/

Hilfe zur Selbsthilfe

Home › IT-Sicherheit › Glossar › Phishing-Mails › **Selbstlerntest Phishing**

Phishing Selbstlerntest

Leider werden immer wieder betrügerische E-Mails an TUM-E-Mail-Adressen verschickt - sogenannte Phishing-Mails. Da eine technische Abwehr hier meist nicht möglich ist, ist die TUM darauf angewiesen, dass die Empfänger von Phishing-Mails besonders vorsichtig sind.

Auf den folgenden Seiten finden sie einen kleinen Selbsttest mit dem Sie Ihre eigenen Kenntnisse und Fähigkeiten zum Thema Phishing testen können.

Zu ihrer eigenen Sicherheit wurden sämtliche schadhafte Links unbrauchbar gemacht. Außerdem wurden persönliche Daten der Empfänger unkenntlich gemacht.

Betrachten Sie sich selbst als Max Mustermann, der alle diese E-Mails erhalten hat.

Hier geht's zur ersten E-Mail

Aufmerksam machen

Home › IT-Sicherheit › Glossar › **Social Hacking**

An wen verschicken Sie vertrauliche Daten?

Angenommen Sie erhalten von Ihrem Chef eine Mail wie die Folgende:

Von: Hans Pongratz <HansPongrats@gmx.de>
An: Max Mustermann <max.mustermann@tum.de>
Betreff: Eilig: Mitarbeiterliste benötigt

Sehr geehrter Herr Mustermann,
der Präsident bat um eine Zusammenstellung über die Mitarbeiter des Campus-Management-Teams.
Leider habe ich von meinem Urlaubsort nur beschränkten Zugriff auf die Systeme der TUM, deshalb bitte ich Sie mir eine Liste dieser Mitarbeiter mit Namen, Mitarbeiternummer, Telefonnummer, Mailadresse, Eingruppierung und Vertragsende zu übermittelt.
Wie üblich ist die Sache dringend, so dass ich Sie bitten muss, mir die Daten noch heute zuzuschicken.
Besten Dank,
Hans Pongratz
--
Dipl.-Inf. Hans Pongratz
Vizepräsident IT-Systeme & Dienstleistungen (CIO) der Technischen Universität

Lessons learned

- Interesse an Kampagnen und Aktionen größer als erwartet
- Nutzung verschiedener Kanäle (online und offline) und Fokussierung auf verschiedene Zielgruppen, Einsatzbeispiele und Orte (Büro, Mensa, Hörsaal, …) ist sehr wichtig
- Aktuelle Vorfälle und Pressemeldungen sind gute Aufhänger und Ideengeber für den nächsten Newsletter bzw. die nächste Aktion.
- Besonders wichtig: regelmäßige Aktionen und Wiederholung wichtiger Themen, Motto „steter Tropfen höhlt den Stein“.
- Nach der Kampagne ist vor der nächsten Kampagne

Sensibilisieren ist Überzeugungsarbeit leisten, nicht Vorschriften machen

Wir würden uns über einen Ideen- und Erfahrungsaustausch sehr freuen!

Angelika Müller

Referentin IT-Sicherheit & Datenschutz

mueller@tum.de

Hans Pongratz

Geschäftsf. Vizepräsident & CIO

pongratz@tum.de