



Technische
Universität
Braunschweig

Gauß-IT-Zentrum



Awareness Maßnahmen an der TU Braunschweig

Dr. Christian Böttger, 04.05.2021



Technische
Universität
Braunschweig

Agenda

- Warum Awareness-Maßnahmen zur Informationssicherheit?
- Maßnahmen - Überblick
- „analoge“ Maßnahmen
- „digitale“ Maßnahmen
- Einsatz eines Awareness-Tools
- Links





Einführung

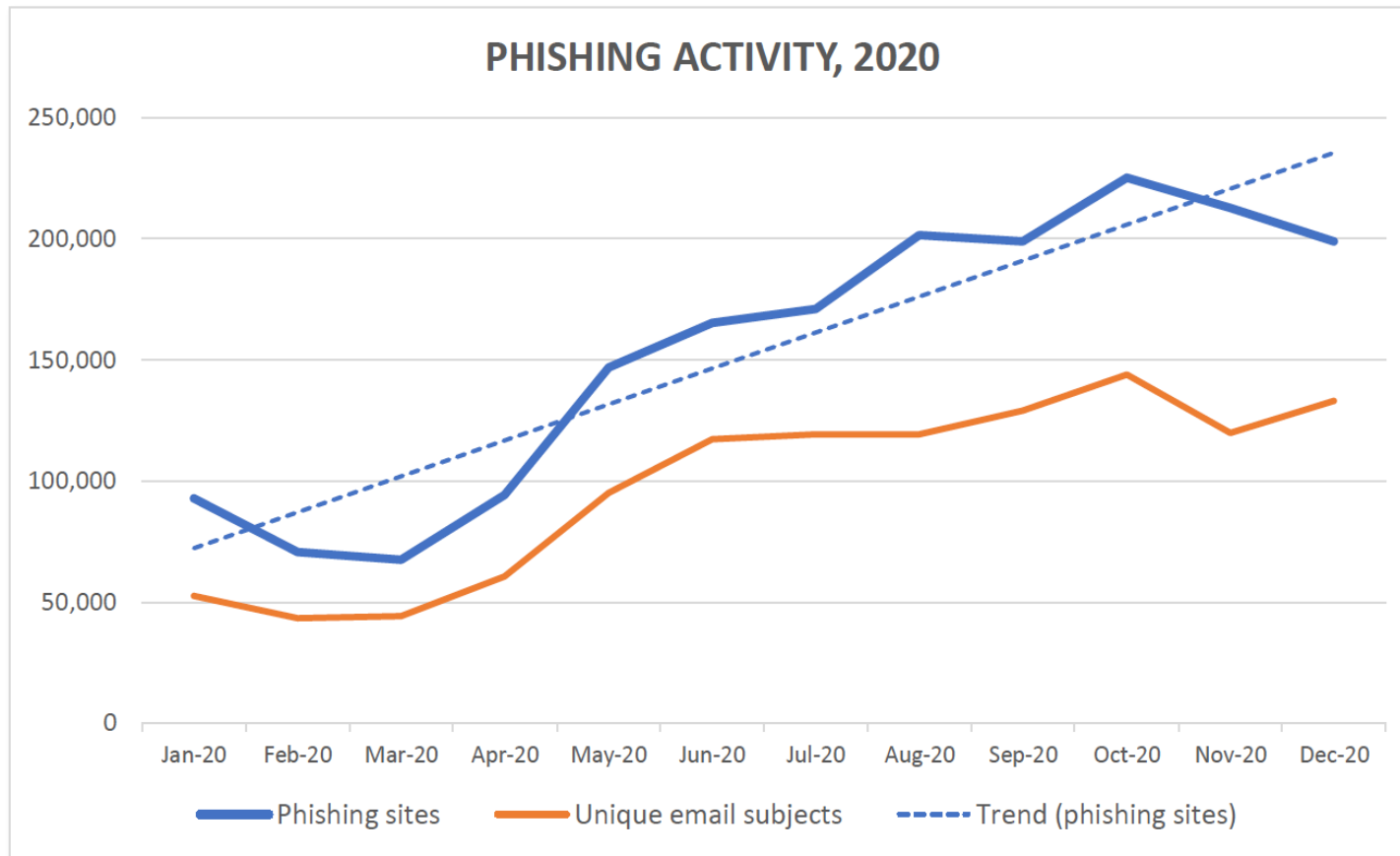
- Informationssicherheit kann man nicht aus dem Regal kaufen. Alle Nutzer/innen müssen sich aktiv beteiligen.
- Informationssicherheit ist ein dauernder Prozess, keine einmalige Installation oder Einrichtung einer Software.
- Angriffe erfolgen zunehmend über den Menschen, nicht mehr nur über die Technik.
- Zusätzlich zu allen weiter nötigen technischen Maßnahmen muss die Aufmerksamkeit aller Mitarbeitenden ständig aktiv gehalten werden.
- Auch dies ist ein dauernder (Kreislauf-)Prozess.
 - Ähnlich wie jährliche Schulungen zum Datenschutz und zum Unfallschutz.



- Starke Zunahme von Phishing über die Jahre



• Phishing im Jahr 2020



Quelle: Anti-Phishing Working Group <https://apwg.org/>



- Phishing basiert auf **Emotionen**
 - **Gier, Neugier, Mitleid und Angst – und Mischungen davon**
 - *Respekt vor Autoritäten*: Vorgesetzte, Behörden, ... (Angst), „Konto läuft ab“
 - Künstlich erzeugter (Zeit-) *Druck*: (Angst, Gier)
 - Vorgesetzter braucht bis in 2 Stunden irgendwas
 - „nur die ersten 50 gewinnen einen Preis“
 - *Automatisierte Handlungen* nutzen:
 - „Klicke hier“ auf einem roten Knopf, „Bestätigen Sie“, „Akzeptieren“,
...
 - (hohen) finanziellen *Gewinn* in Aussicht stellen (Gier)
 - *Sex* (Gier)
 - *Apell*: jemand braucht Hilfe (Mitleid, Hilfsbereitschaft)
 - Angebliche *Gehaltsdaten* anderer Menschen (*Neugier*)
 - *Vertraulichkeit*: *Vortäuschen von angeblichem Detailwissen*, gefälschte Absender, Zitat aus echten Mails
 - *Dunning-Kruger-Effekt*: *alle Menschen überschätzen ihre eigenen Fähigkeiten, besonders dann, wenn sie auf dem jeweiligen Gebiet real wenig Fähigkeiten haben*

Grundsätze

- Maßnahmen müssen regelmäßig wiederholt werden
- Aufmerksamkeit lässt schnell wieder nach
- Problem: Integration in den Arbeitsablauf
- Positive Fehlerkultur ist zwingend notwendig.
- IT/Informationssicherheit ist nicht die primäre Aufgabe der Mitarbeitenden!
- Mitarbeitende müssen „abgeholt“ werden.
- Wichtig: niemals Vorwürfe machen – sondern immer Hilfe und Unterstützung anbieten!
- Ohne aktiven Rückhalt aus den Leitungsebenen geht gar nichts!



Es gibt keine „Silver Bullet“

- Viele kleine sich ergänzende Maßnahmen sind nötig.
 - Menschen lernen auf verschiedenen Wegen.
- Analoge Maßnahmen
- Digitale Maßnahmen
- Online Maßnahmen und Offline-Maßnahmen
- Und immer: wertschätzend!

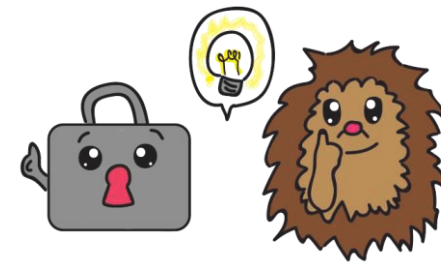


Analoge Maßnahmen an der TU Braunschweig

- Mousepads kostenfrei verteilen
- Info-Aufsteller in den PC-Pool-Räumen
- Bei Präsenzbetrieb: wechselnde Plakate
- Informations-Flyer (z.B. bei Einführungsveranstaltungen und im Service Desk)
- Seminare (z.B. über die Personalweiterbildung)
- Vorträge
 - z.B. Beteiligung am European Cyber Security Month
- Seminare und Vorträge nicht in der Freizeit, sondern als Arbeitszeit
- Gastbesuche in Gremien



Plakate - Beispiele



Aufsteller - Beispiele



IT-Sicherheit
Gauß IT Zentrum



IT-Sicherheit
Gauß IT Zentrum



IT-Sicherheit
Gauß IT Zentrum



Mousepads – Beispiel 2

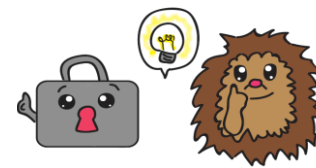


Technische
Universität
Braunschweig

Gauß-IT-Zentrum



<http://it-sicherheit.tu-braunschweig.de/>




Technische
Universität
Braunschweig

Digitale Maßnahmen an der TU Braunschweig

- Informationssicherheits-Blog / Webseite
 - Informationen und Warnungen
- Nutzung von Mailverteilern: DV-Koordinierende, ...
 - Warnungen – Achtung, nicht zu viel!
- Videos zum Abrufen
 - Einbindung ins Lernmanagementsystem der TU (Stud.IP)
- Vorträge (PDF) zum Abruf
- Online-Quiz / Online-Kurse
- Online- Vorträge und Seminare
 - ECSM, Personalweiterbildung
 - IT-SAD 7.-18.6.2021 (öffentlich)
- Meldeadresse (E-Mail, Formular) für Vorfälle und Spam




Online-Kurs: Beispiel



Technische
Universität
Braunschweig

WILLKOMMEN ZUM
E-LEARNING-KURS
TU BRAUNSCHWEIG



KURSTITEL:
Geführter Kurs: Grundlagen der IT-Sicherheit

DAUER:	15-20 Minuten
Komplexität:	Mittel
Zielgruppe:	Alle
Interaktiv:	Ja

KURS STARTEN ▶

Erstellungsjahr: 2021
Version: 1.0



Digitale Maßnahmen an der TU Braunschweig: Links

- https://studip.tu-braunschweig.de/seminar_main.php?auswahl=bc863707104006d8b2c63d11f6a60ed0
- <https://blogs.tu-braunschweig.de/it/category/informationssicherheit/>
- <https://blogs.tu-braunschweig.de/it/it-sad-it-security-awareness-days-sommersemester-2021/>
- <https://blogs.tu-braunschweig.de/it/videos-zur-informationssicherheit-zum-selbstlernen/>
- <https://blogs.tu-braunschweig.de/it/vortraege-zu-themen-rund-um-informationssicherheit/>
- <https://blogs.tu-braunschweig.de/it/screencast-trau-keinen-phishen/>
- <https://blogs.tu-braunschweig.de/it/informationssicherheit-online-materialien-zum-selberlernen/>



Einsatz eines Awareness-Tools

- Methoden
 - „Fake-Spam“-Kampagnen mit anschließenden Kursen
 - per Mail, aber auch mit z.B. USB-Sticks
 - Aufklärungskampagnen mit Quiz, Kursen, Vorträgen, Videos (ohne „Fake-Spam“)
 - Multimediale Kurse zum Selber lernen im dauerhaften Zugriff
 - bald: Spam-Meldeknopf in Outlook (evtl. Thunderbird)
 - Optional: Test der technischen Spam-Abwehrmaßnahmen
- In 2020: gemeinsames Projekt mit der RUB
- Eingesetztes Tool: LUCY
 - <https://lucysecurity.com/de/>



LUCY 1 - Kampagnenübersicht

RUB/OGB/T...

Kampagnen Status: Gestoppt

🔄 Statistiken leeren

📄 Bericht

📁 Als Vorlage speichern

📄 Exportiere ▾

▶ Start

Ergebnisse

Zusammenfassung

Statistiken

Berichte

Exporte

Automatischer Export

Konfiguration

Basiseinstellungen

Sensibilisierungskurs
Einstellungen

Einstellungen Angriffssimulation

Zeitplan

Empfänger

Erweiterte Einstellungen

Benutzereinstellungen

Filter

Benutzerdefinierte Felder

Kampagne	Laufzeit	Erstellt von
RUB/OGB/TUBS Studis	2 Monate, 25 Tage	leonard-jari.zurek@tu-braunschweig.de

Angriffsübersicht



Highcharts.com
24788 Nachrichten
gesendet

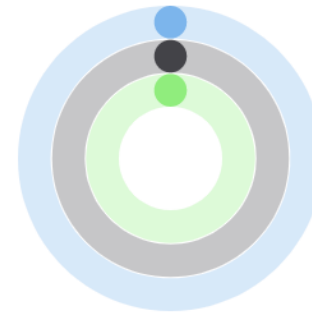
Highcharts.com
60.62% aller
Empfänger öffneten die
Nachricht

Highcharts.com
27.48% aller
Empfänger klickten den
Link

Highcharts.com
7.81% aller Attacks
waren erfolgreich

Köder gesendet	24785 of 24799	99.94%
Nachrichten gesendet	24788 of 24799	99.96%
Nachrichten geöffnet	15034 of 24799	60.62%
Klicks	6816 of 24799	27.48%
Erfolgreiche Attacks	1938 of 24799	7.81%
Anfällige Opfer	31 of 24799	0.13%
Fehler	11 of 24799	0.04%

Sensibilisierungskurs



Training gesendet

Training geöffnet

Trainingswertung (%)

Zur Aktionsübersicht anklicken – mit Anzahl der E-Mails

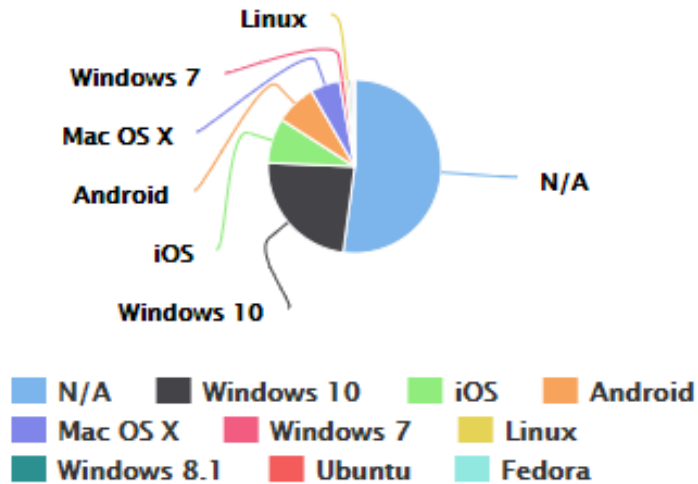
E-Mails insgesamt 24788



Technische
Universität
Braunschweig

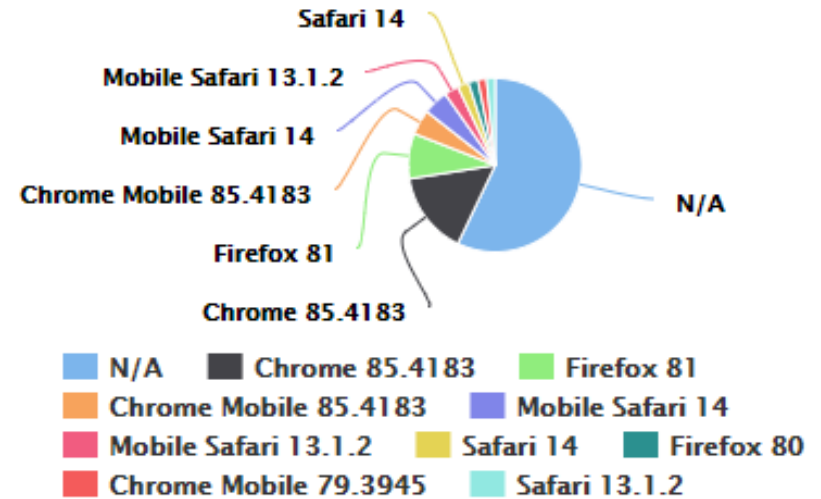
LUCY 2 – technische Statistiken

Betriebssysteme



Highcharts.com


Browser









Highcharts.com









LUCY 5 - Vorlagen




 A request to reset the password from Booking.com is sent to the user
25.07.2019 11:15:16

 **Booking: Reset your password**  
A request to reset the password from Booking.com is sent to the user
18.12.2020 16:47:17




 **Booking: Reset your password (hyperlink)**  
A request to reset the password from Booking.com is sent to the user
18.12.2020 16:46:12




 **Booking: Reset your password (hyperlink)**  
A request to reset the password from Booking.com is sent to the user
25.07.2019 11:12:44




 **Booking (Petya Ransomware) ver.2.2**  
The recipient gets a booking confirmation "Your Booking Berlin Novut Hotel is confirmed". After the link click the user gets redirected to a landing page where he can authenticate with his credentials and download an Word Document. The Word File is required to cancel the reservation and refund the money. Office files containing a filearc are the typical entry point for malware (seen in attacks like Petya).
25.07.2019 11:07:10




 **BYOD - Open VPN Access**  
In this scenario, employees can use a new web based SSL VPN login portal to get access with their personal devices to all internal business applications.
25.07.2019 11:10:16




« 1 2 3 4 ... 6 »




 **Identity theft video (close caption)**  
This video is dedicated to the topic "identity theft". The content (animation, language, script) is customizable. The video has subtitles. More info about customization can be found here: <https://goo.gl/HXNWSG>. Duration: 5:27 Minutes | Skill Level: Low | Audience: All | Interactive: No
22.04.2021 14:36:07

 **Identity Theft (Whiteboard Video)**  
In this 5-minute identity theft video we talk about identity theft risk. We have put together a few security tips about best practices and policies. The content (animation, language, script) is customizable. More info about customization can be found here: <https://goo.gl/HXNWSG>. Duration: 5 Minutes | Skill Level: Low | Audience: All | Interactive: Yes
12.01.2021 10:48:53

 **Identity Theft (Whiteboard Video) (close caption)**  
In this 5-minute identity theft video we talk about identity theft risk. We have put together a few security tips about best practices and policies. The content (animation, language, script) is customizable. More info about customization can be found here: <https://goo.gl/HXNWSG>. Duration: 5 Minutes | Skill Level: Low | Audience: All | Interactive: Yes
12.01.2021 10:48:53

 **Incidents Exam**  
In this short quiz, the participant is asked five multiple choice questions in order to test their knowledge regarding incidents. At the end of the quiz the participant can create a certificate with the exam results.
Duration: 10-15 Minutes | Skill Level: Low | Audience: All | Interactive: Yes
12.01.2021 10:48:53

 **Interactive Email Awareness Video**  
In this video the participant will learn about the risks that come with using email. The participant will be exposed to the various risks involved in handling email and at the same time receive tips on how to better protect the company's data. This interactive video also allows the participant to prove their knowledge by completing a short exam.
12.01.2021 10:48:53

 **Interactive Password Awareness Video**  
In this video the participant will learn the importance of Password Security. This video talks about the importance of password security. How do hackers hack passwords, and how can you make your password secure? The video contains questions to help the participant test their knowledge.
12.01.2021 10:48:53

« 1 2 3 4 »



LUCY 6 – Dashboard für gemeldete Phishing-Vorfälle

✉ Missbrauchsmeldung senden

✕ Löschen

✕ Alle löschen

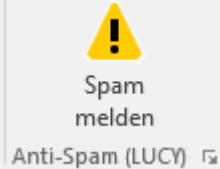
Status ändern ▾

📄 Plugin herunterladen ▾

Phishing Vorfall Berichte

Filter ▾

Statistiken ▾



<input type="checkbox"/>	Zeit	E-Mail	Klient	Kampagne	Wertung	Status	
<input type="checkbox"/>	01.03.2021 09:36	c.boettger@tu-braunschweig.de	LUCY@GITZ	N/A	0.00	Öffnen	⚠️ ✉️ 📄 ✕
<input type="checkbox"/>	01.03.2021 09:36	c.boettger@tu-braunschweig.de	LUCY@GITZ	N/A	10.00	Öffnen	⚠️ ✉️ 📄 ✕
<input type="checkbox"/>	19.02.2021 16:33	l.zurek@tu-braunschweig.de	LUCY@GITZ	N/A	0.00	Öffnen	✉️ 📄 ✕
<input type="checkbox"/>	19.02.2021 15:53	l.zurek@tu-braunschweig.de	LUCY@GITZ	N/A	0.00	Öffnen	✉️ 📄 ✕
<input type="checkbox"/>	19.02.2021 15:41	l.zurek@tu-braunschweig.de	LUCY@GITZ	N/A	0.50	Echtes Phishing	✉️ 📄 ✕
<input type="checkbox"/>	19.02.2021 13:35	l.zurek@tu-braunschweig.de	LUCY@GITZ	N/A	0.00	Öffnen	✉️ 📄 ✕
<input type="checkbox"/>	19.02.2021 13:20	l.zurek@tu-braunschweig.de	LUCY@GITZ	N/A	1.20	Öffnen	✉️ 📄 ✕
<input type="checkbox"/>	19.02.2021 13:12	c.boettger@tu-braunschweig.de	N/A	N/A	0.00	Öffnen	✉️ 📄 ✕
<input type="checkbox"/>	19.02.2021 13:12	c.boettger@tu-braunschweig.de	N/A	N/A	0.00	Öffnen	✉️ 📄 ✕
<input type="checkbox"/>	19.02.2021 13:11	leonard-jari.zurek@tu-braunschweig.de	N/A	N/A	0.00	Öffnen	✉️ 📄 ✕

« 1 2 3 4 5 ... 8 »

10 Zeilen pro Seite.



Awareness-Tool Einsatz

- LUCY ist selbst gehostet
 - Solche Tools gibt es auch als externen Service.
- Nicht zu häufig, nicht zu selten
 - Wirkung lässt jeweils schnell nach
 - Aber: Eindruck vermeiden „ach, das ist nur wieder ein Test“
- Niemals die „Hereingefallenen“ maßregeln!
- Hilfe und Information anbieten
- Kampagnen vorher ankündigen und auch das Ende bekannt geben!
- Leitung und Help Desk mit einbeziehen!



Fazit

- Es gibt nicht die eine richtige Maßnahme.
- Die Vielfalt macht's.
- Immer am Ball bleiben!
 - Also: als Daueraufgabe anlegen!
- Leitungsebenen müssen dahinter stehen!
- Der Aufwand ist beträchtlich – genügend personelle Kapazitäten einplanen!
- Mitarbeitende dürfen sich nicht kontrolliert fühlen:
 - Wertschätzung
 - Hilfe anbieten
 - Nicht maßregeln



Links

- <https://www.tu-braunschweig.de/it-sicherheit>
- <https://www.tu-braunschweig.de/it-sicherheit/kurztipps>
- <https://www.tu-braunschweig.de/it-sicherheit/pwsec>
- <https://doku.rz.tu-bs.de/doku.php?id=it-sec:it-sec>
- <https://blogs.tu-braunschweig.de/it/category/informationssicherheit/>
- https://studip.tu-braunschweig.de/seminar_main.php?auswahl=bc863707104006d8b2c63d11f6a60ed0
- <https://www.bsi-fuer-buerger.de/>
- <https://zac-niedersachsen.de/inhalte.php>
- <https://www.polizei-praevention.de/aktuelles.html>





Weitere Infos:

<https://doku.rz.tu-bs.de/doku.php?id=it-sec:it-sec> und
<http://it-sicherheit.tu-braunschweig.de/>

und beim IT-Service-Desk des Gauß-IT-Zentrums
Tel. +49.531.391.5555

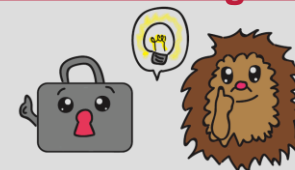
it-service-desk@tu-braunschweig.de

<https://www.tu-braunschweig.de/it/service-desk>

Vielen Dank für Ihre Aufmerksamkeit!



<https://pixabay.com/de/baby-lernen-laptop-frage-2709666/>
CC0 Lizenz



Geschafft!



**Vielen Dank für die
Aufmerksamkeit!**

Einfache Fragen? ;-)

