



Technische
Universität
Braunschweig

Gauß-IT-Zentrum



Phishing – und was Sie dagegen tun können

Dr. Christian Böttger, 13.11.2018



<https://secuso.aifb.kit.edu/NoPhish.php>

<https://secuso.aifb.kit.edu/642.php>

- Betrugsversuch per E-Mail oder Messenger
- Nachricht wirkt seriös
- Links führen zu unseriösen Websites
- Bösartige Anhänge

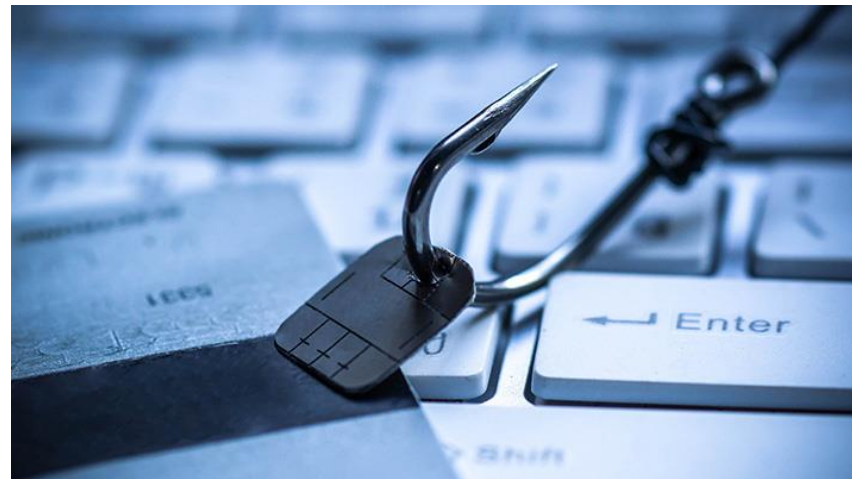


Bild: 1

- Bankdaten



Bild: 2

- Bankdaten
- Benutzerkonten mit den dazugehörigen Passwörter



Bild: 2

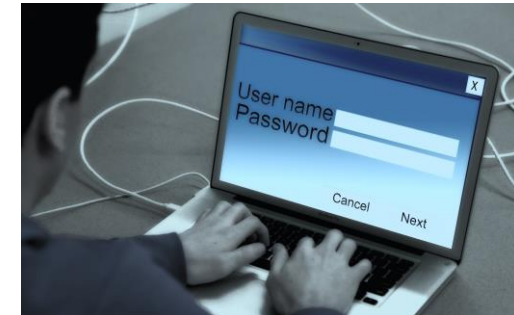


Bild: 3

- Bankdaten
- Benutzerkonten mit den dazugehörigen Passwörter
- Namen (Freunde, Familie, Arbeitskollegen)
- Telefonnummer



Bild: 2

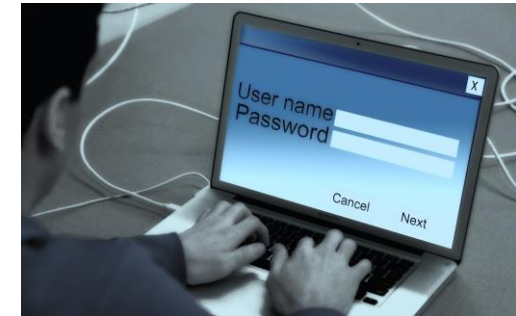


Bild: 3



Bild: 4

- Daten verkaufen



Bild: 6

- Daten verkaufen
- Vermögensschäden

Überweisungsprotokoll		Hauptmenü
Dies sind Ihre letzten 16 Transaktionen		
gestohlen		-\$5,000.00 DB
gestohlen		-\$108.00 DB
gestohlen		-\$113.00 DB
gestohlen		-\$480.00 DB
Für Kontaktdienstleistungen ausgegeben		-\$500.00 DB
gestohlen		-\$480.00 DB
Von OMI erhalten	\$880,000.00 CR	
Für Fahrzeuge & Wartung ausgegeben		-\$410.00 DB
gestohlen		-\$600.00 DB
gestohlen		-\$5,000.00 DB
gestohlen		-\$108.00 DB
Kauf		-\$108.00 DB

Bild: 7

- Daten verkaufen
- Vermögensschäden
- Rufschädigung



Bild: 8

- Vorab: Sammeln von Informationen
 - Name, Position
 - Firma
 - Ausschreibungen



Bild: 9

- Vorab: Sammeln von Informationen
 - Name, Position
 - Firma
 - Ausschreibungen
- Clone Phishing:
 - Kopie einer E-Mail mit ersetzten Links



Bild: 9

- Vorab: Sammeln von Informationen
 - Name, Position
 - Firma
 - Ausschreibungen
- Clone Phishing:
 - Kopie einer E-Mail mit ersetzten Links
- Whaling:
 - Ziel sind "größere Fische" wie Führungskräfte



Bild: 9

- Meist per Kurznachrichten verschickt
- Probleme mit dem Konto klären
- Telefonnummer anrufen



Bild: 10

Tippfehler, Zeichenverdreher und andere Tricks lassen Link seriös wirken

<https://faecbook.com/login>

<https://vvetter.com/deutschland/EUDE.html>

<https://microsoft.com.secure-update.com/...>

<https://tu-braunschweig-it.de>

<https://arnazon.de>



https://www.tu-braunschweig.de/it

Achten Sie auf den Domain-Bereich!



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

Achten Sie auf den Domain-Bereich!

Häufige Muster:

- <https://faecbook.com/login>
- <https://vvetter.com/deutschland/EUDE.html>
- <https://microsoft.com.secure-update.com/...>
- <https://tu-braunschweig-it.de>
- <https://arnazon.de>



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

Achten Sie auf den Domain-Bereich!

Häufige Muster:

- <https://facebook.com/login>
- <https://vvetter.com/deutschland/EUDE.html>
- <https://microsoft.com.secure-update.com/...>
- <https://tu-braunschweig-it.de>
- <https://arnazon.de>



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

Achten Sie auf den Domain-Bereich!

Häufige Muster:

- <https://facebook.com/login>
- <https://vvetter.com/deutschland/EUDE.html>
- <https://microsoft.com.secure-update.com/...>
- <https://tu-braunschweig-it.de>
- <https://arnazon.de>



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

Achten Sie auf den Domain-Bereich!

Häufige Muster:

- <https://facebook.com/login>
- <https://vvetter.com/deutschland/EUDE.html>
- <https://microsoft.com.secure-update.com/...>
- <https://tu-braunschweig-it.de>
- <https://arnazon.de>



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

Achten Sie auf den Domain-Bereich!

Häufige Muster:

- <https://facebook.com/login>
- <https://vvetter.com/deutschland/EUDE.html>
- <https://microsoft.com.secure-update.com/...>
- <https://tu-braunschweig-it.de>
- <https://arnazon.de>



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

Achten Sie auf den Domain-Bereich!

Häufige Muster:

- <https://facebook.com/login>
- <https://vvetter.com/deutschland/EUDE.html>
- <https://microsoft.com.secure-update.com/...>
- <https://tu-braunschweig-it.de>
- <https://amazon.de>



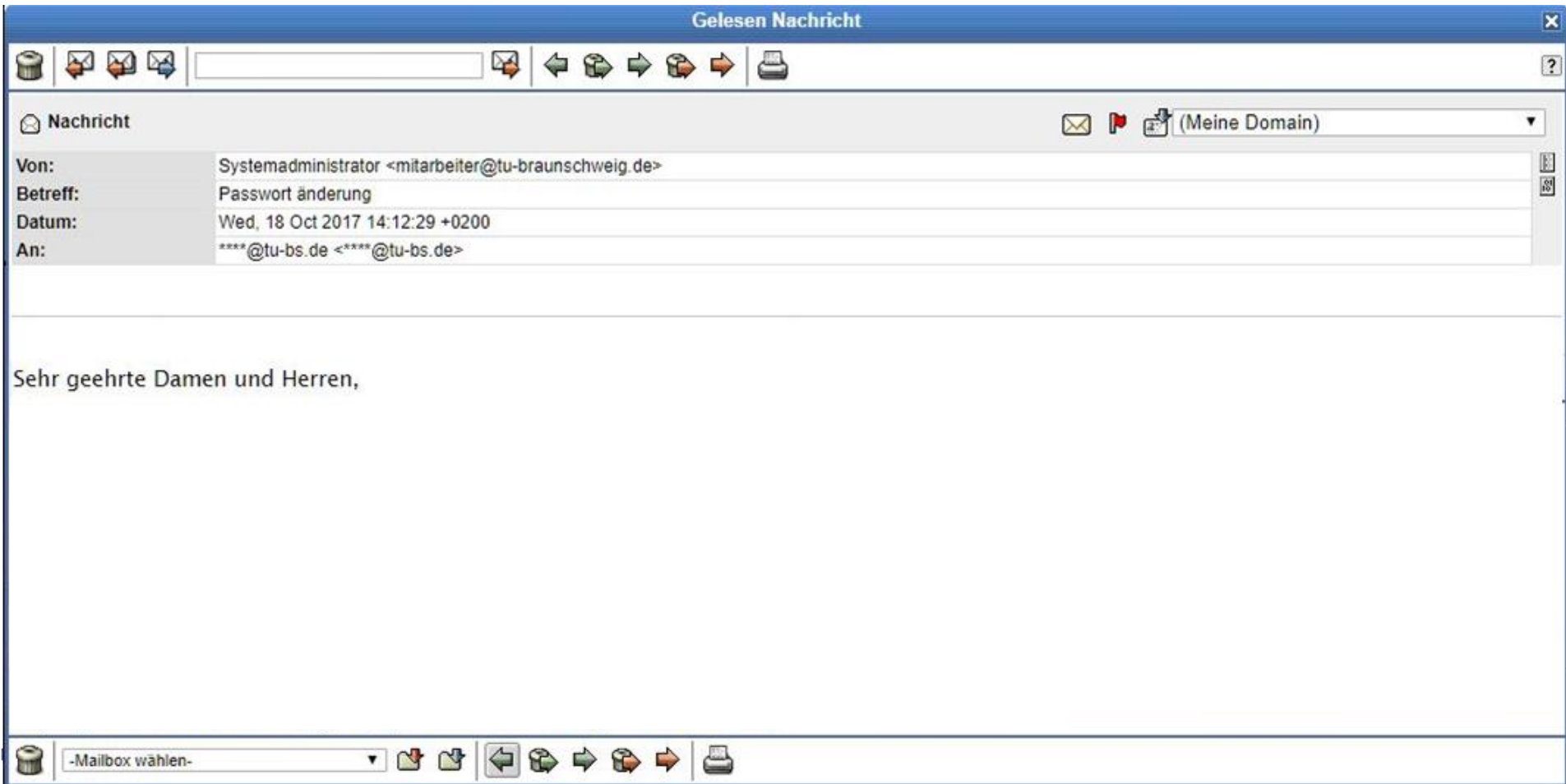


Bild: 11

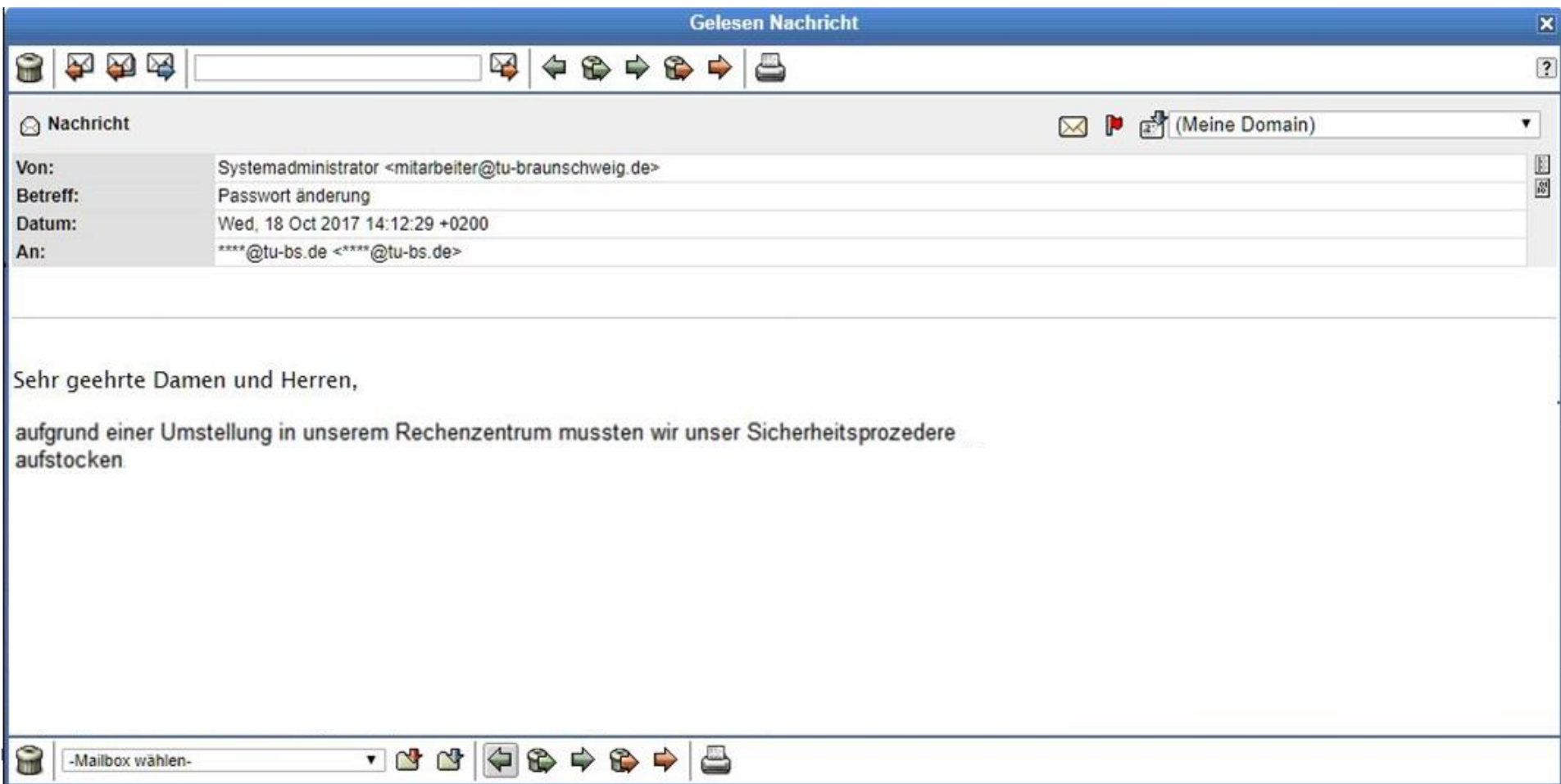


Bild: 11



Bild: 11

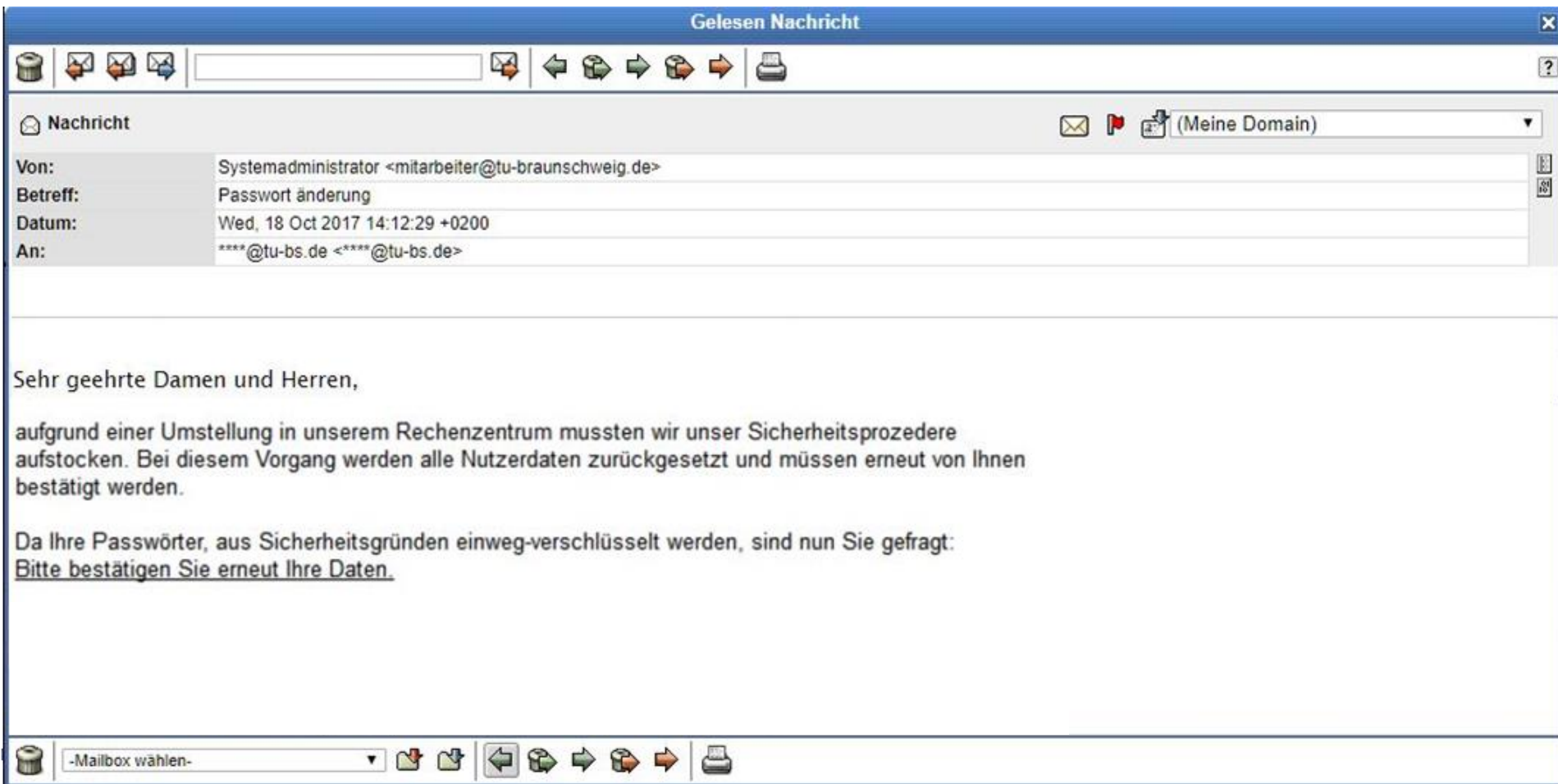


Bild: 11

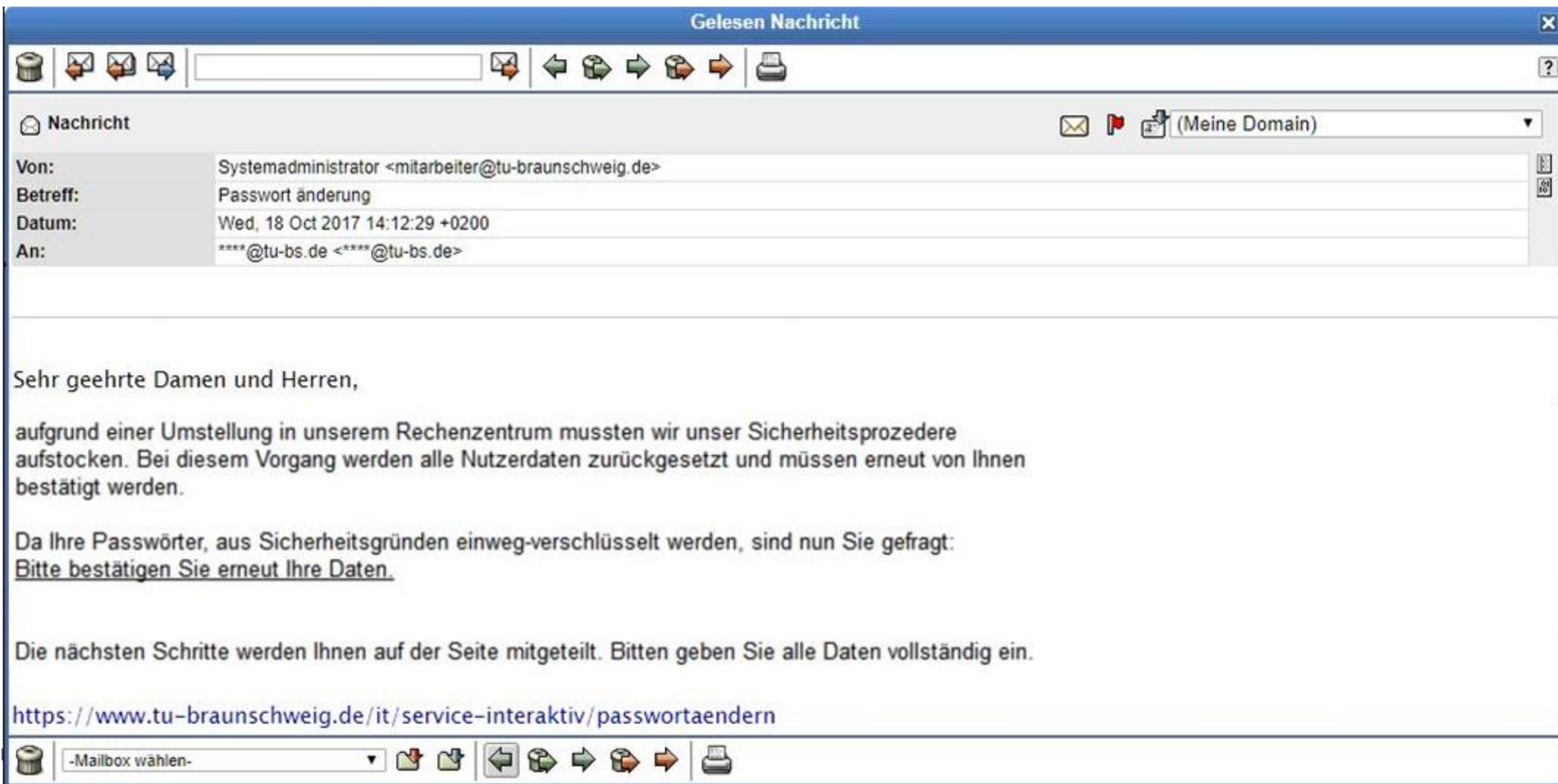


Bild: 11

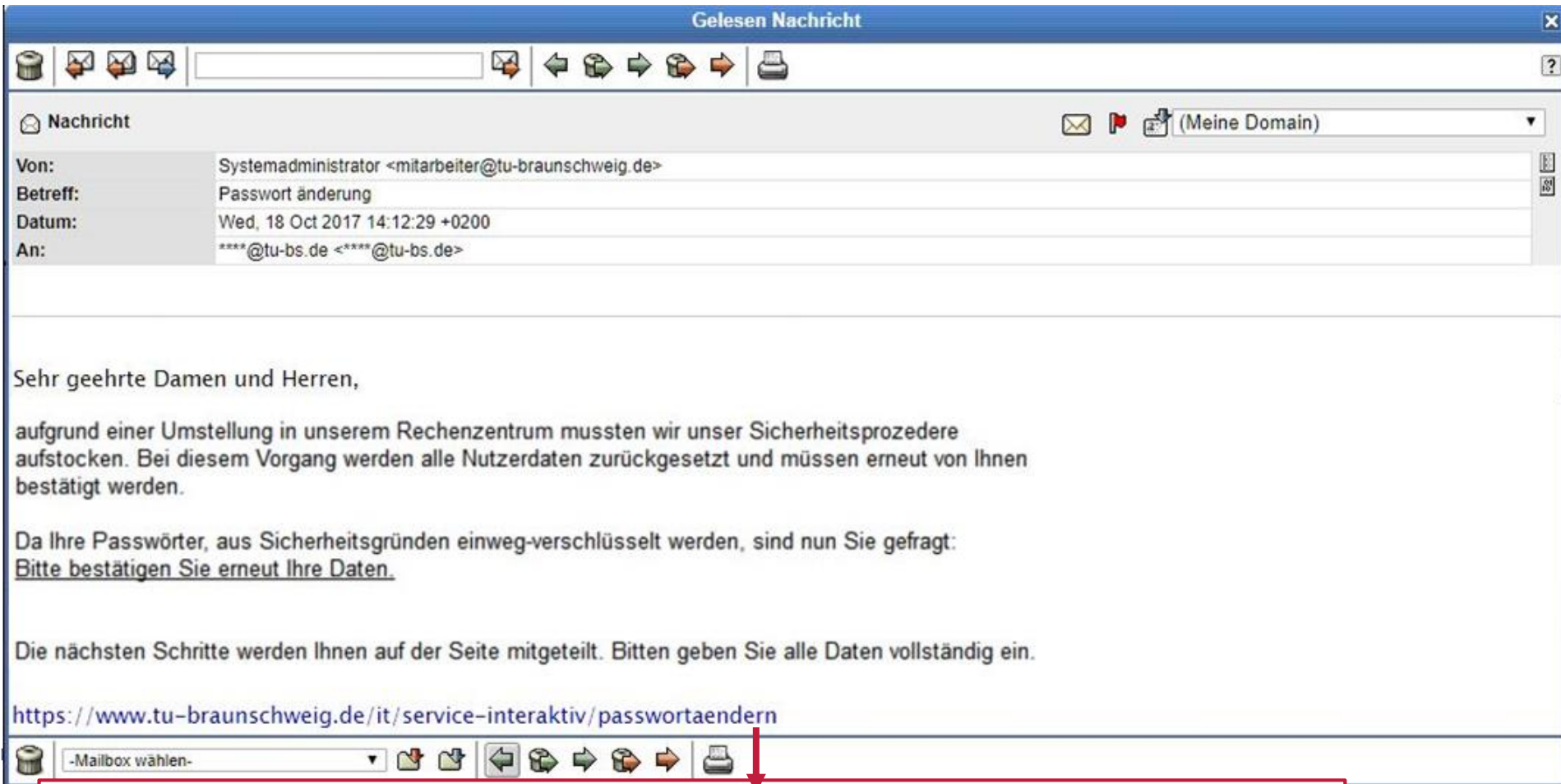
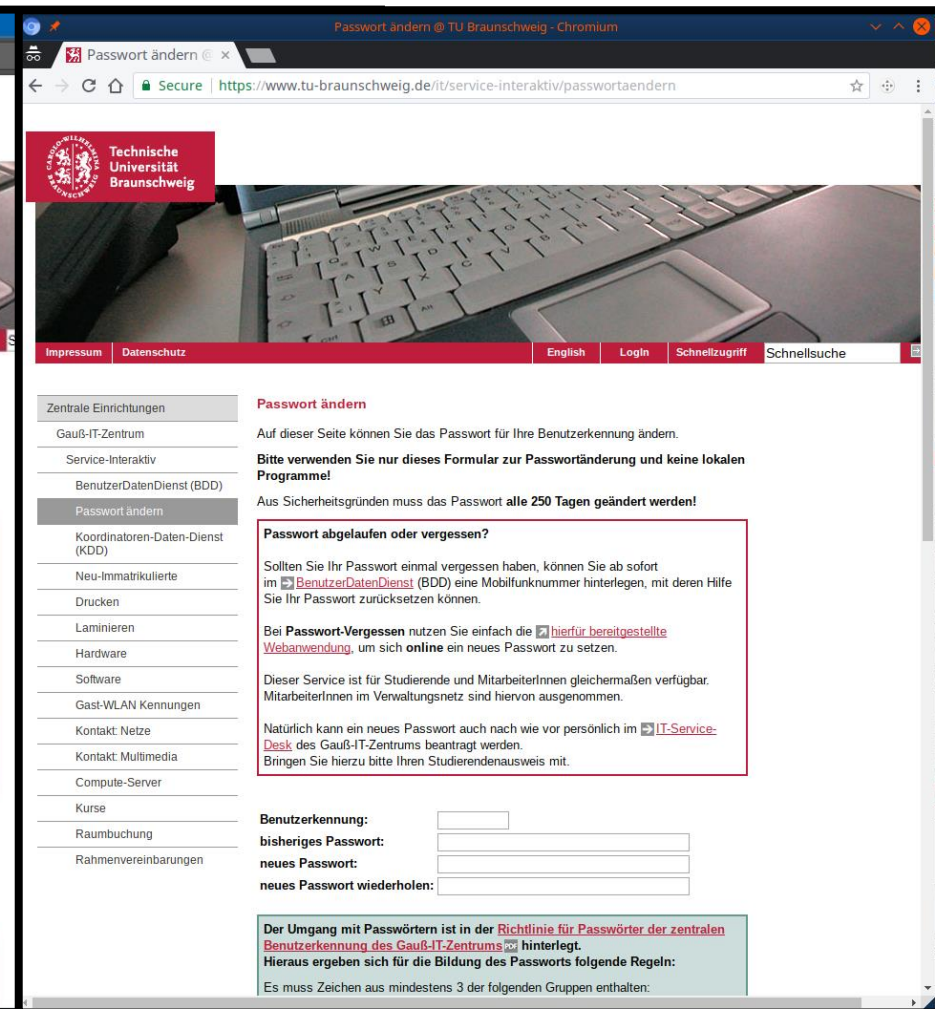
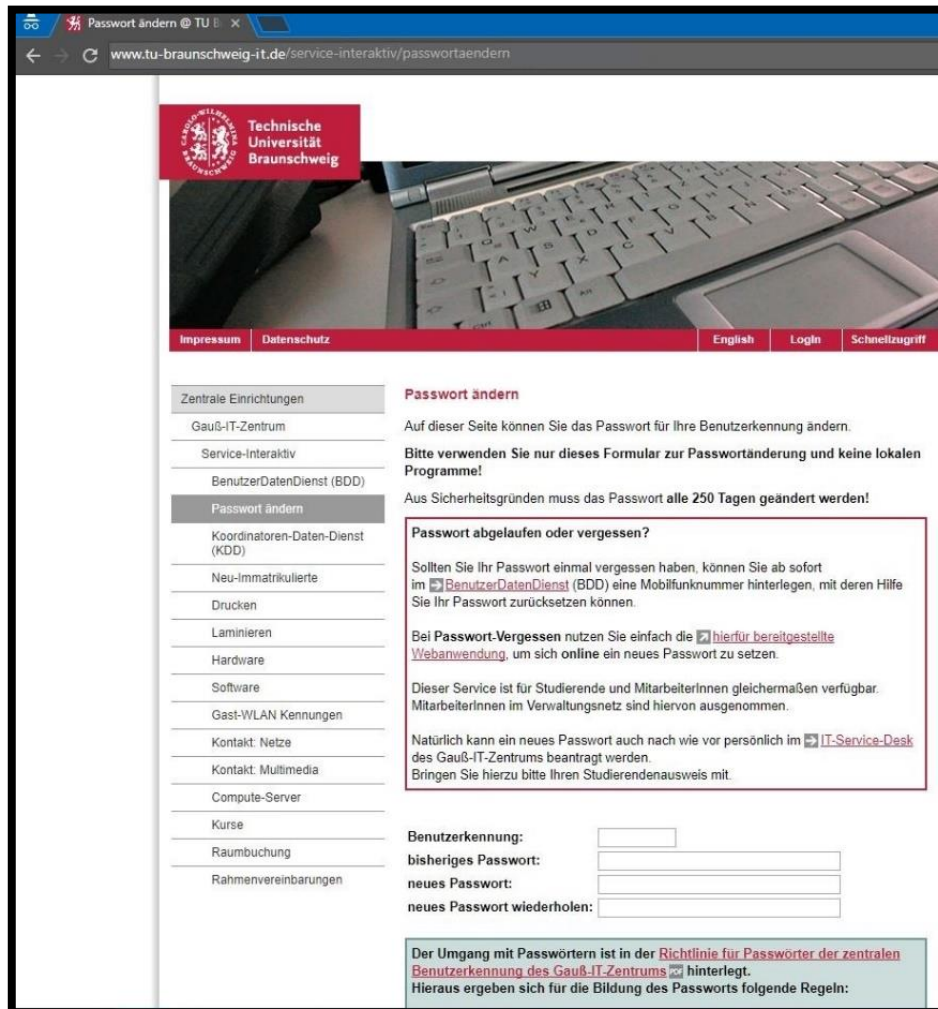


Bild: 11



Was ist Phishing?

Vorgehen des Angreifers

Angriffstypen

Schutzmaßnahmen

Link Manipulation
erkennen

Phishing-Mail

Phishing-Website

Passwort ändern @ TU B

www.tu-braunschweig-it.de/service-interaktiv/passwortaendern



Was ist Phishing?

Vorgehen des Angreifers

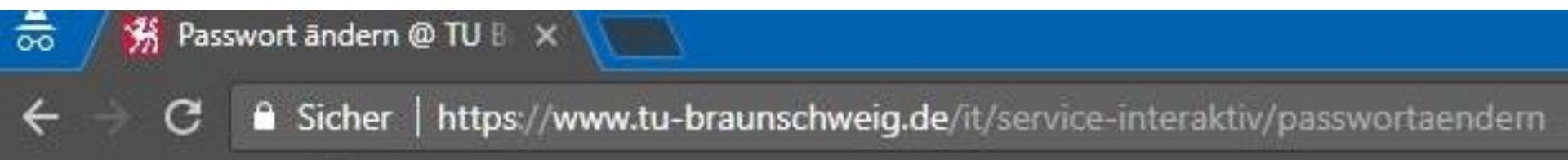
Angriffstypen

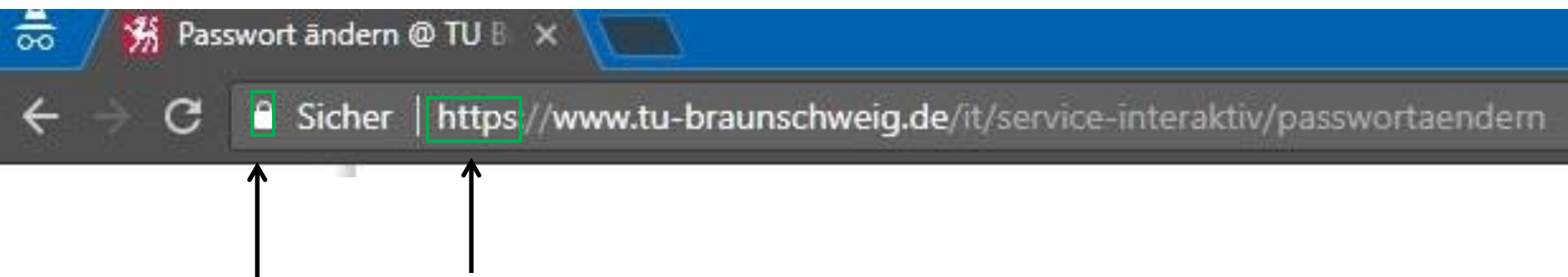
Schutzmaßnahmen

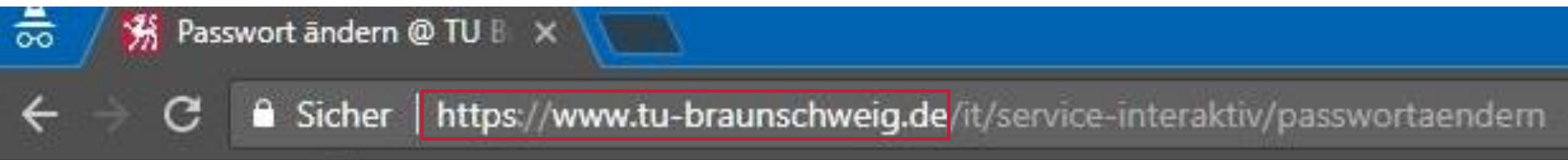
Link Manipulation
erkennen

Phishing-Mail

Phishing-Website







Passwort ändern @ TU ! x
www.tu-braunschweig-it.de/service-interaktiv/passwortaendern

Technische Universität Braunschweig

Impressum Datenschutz English Login Schnellzugriff Schnellsuche

Zentrale Einrichtungen

- Gauß-IT-Zentrum
- Service-Interaktiv
- BenutzerDatenDienst (BDD)
- Passwort ändern**
- KoordinatorInnen-Daten-Dienst (KDD)
- Neu-Immatrikulierte
- Drucken
- Laminieren
- Hardware
- Software
- Gast-WLAN Kennungen
- Kontakt: Netze
- Kontakt: Multimedia
- Compute-Server
- Kurse
- Raumbuchung
- Rahmenvereinbarungen

Passwort ändern

Auf dieser Seite können Sie das Passwort für Ihre Benutzerkennung ändern.
Bitte verwenden Sie nur dieses Formular zur Passwortänderung und keine lokalen Programme!

Aus Sicherheitsgründen muss das Passwort **alle 250 Tagen geändert werden!**

Passwort abgelaufen oder vergessen?

Sollten Sie Ihr Passwort einmal vergessen haben, können Sie ab sofort im [BenutzerDatenDienst](#) (BDD) eine Mobilfunknummer hinterlegen, mit deren Hilfe Sie Ihr Passwort zurücksetzen können.

Bei **Passwort-Vergessen** nutzen Sie einfach die [hierfür bereitgestellte Webanwendung](#), um sich online ein neues Passwort zu setzen.

Dieser Service ist für Studierende und MitarbeiterInnen gleichermaßen verfügbar. MitarbeiterInnen im Verwaltungsnetz sind hiervon ausgenommen.

Natürlich kann ein neues Passwort auch nach wie vor persönlich im [IT-Service-Desk](#) des Gauß-IT-Zentrums beantragt werden. Bringen Sie hierzu bitte Ihren Studierendenausweis mit.

Benutzerkennung:

bisheriges Passwort:

neues Passwort:

neues Passwort wiederholen:

Der Umgang mit Passwörtern ist in der [Richtlinie für Passwörter der zentralen Benutzerkennung des Gauß-IT-Zentrums](#) hinterlegt. Hieraus ergeben sich für die Bildung des Passworts folgende Regeln:

Zentrale Einrichtungen

Gauß-IT-Zentrum

Service-Interaktiv

BenutzerDatenDienst (BDD)

Passwort ändern

Koordinatoren-Daten-Dienst
(KDD)

Neu-Immatrikulierte

Drucken

Laminieren

Hardware

Software

Gast-WLAN Kennungen

Kontakt: Netze

Kontakt: Multimedia

Compute-Server

Kurse

Raumbuchung

Rahmenvereinbarungen

Passwort ändern

Auf dieser Seite können Sie das Passwort für Ihre Benutzerkennung ändern.

Bitte verwenden Sie nur dieses Formular zur Passwortänderung und keine lokalen Programme!

Aus Sicherheitsgründen muss das Passwort **alle 250 Tagen geändert werden!**

Passwort abgelaufen oder vergessen?

Sollten Sie Ihr Passwort einmal vergessen haben, können Sie ab sofort im [BenutzerDatenDienst \(BDD\)](#) eine Mobilfunknummer hinterlegen, mit deren Hilfe Sie Ihr Passwort zurücksetzen können.

Bei **Passwort-Vergessen** nutzen Sie einfach die [hierfür bereitgestellte Webanwendung](#), um sich **online** ein neues Passwort zu setzen.

Dieser Service ist für Studierende und MitarbeiterInnen gleichermaßen verfügbar. MitarbeiterInnen im Verwaltungsnetz sind hiervon ausgenommen.

Natürlich kann ein neues Passwort auch nach wie vor persönlich im [IT-Service-Desk](#) des Gauß-IT-Zentrums beantragt werden. Bringen Sie hierzu bitte Ihren Studierendenausweis mit.

Benutzerkennung: bisheriges Passwort: neues Passwort: neues Passwort wiederholen:

Der Umgang mit Passwörtern ist in der [Richtlinie für Passwörter der zentralen Benutzerkennung des Gauß-IT-Zentrums](#) [PDF](#) hinterlegt.

Hieraus ergeben sich für die Bildung des Passworts folgende Regeln:

- Firefox Add-on zum Schutz von Passwörtern, Zahlungsdaten und weiteren sensiblen Daten
<https://secuso.aifb.kit.edu/PassSecPlus.php> (Chrome / Firefox)

- Firefox Add-on zum Schutz von Passwörtern, Zahlungsdaten und weiteren sensiblen Daten
 - <https://secuso.aifb.kit.edu/PassSecPlus.php> (Chrome / Firefox)
- HTTPS mit Extended Validation Zertifikat



- Firefox Add-on zum Schutz von Passwörtern, Zahlungsdaten und weiteren sensiblen Daten
 - <https://secuso.aifb.kit.edu/PassSecPlus.php> (Chrome / Firefox)

- HTTPS mit Extended Validation Zertifikat



- HTTPS ohne Extended Validation Zertifikat




Sie besuchen eine Seite des Betreibers: **g o o g l e . c o m**.
Überprüfen Sie diese Angabe, bevor Sie hier Daten eingeben.

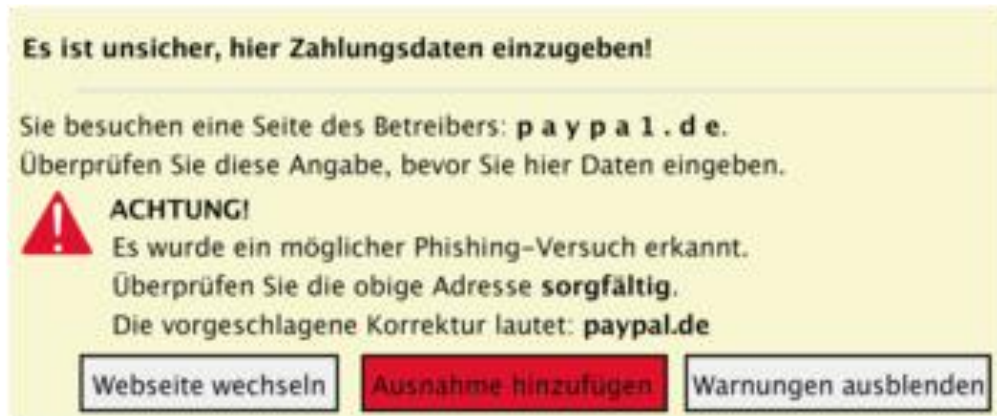
Ich habe die Angabe geprüft

Okay, verstanden

- <https://secuso.aifb.kit.edu/PassSecPlus.php> (Chrome / Firefox)
- Kein HTTPS



- <https://secuso.aifb.kit.edu/PassSecPlus.php> (Chrome / Firefox)
- Kein HTTPS 
- Prüfen der Domain durch Suchmaschinen und Web of Trust



- <https://secuso.aifb.kit.edu/PassSecPlus.php> (Chrome / Firefox)

- Kein HTTPS

Passwort



- Prüfen der Domain durch Suchmaschinen und Web of Trust

Es ist unsicher, hier Zahlungsdaten einzugeben!

Sie besuchen eine Seite des Betreibers: **p a y p a 1 . d e**.
Überprüfen Sie diese Angabe, bevor Sie hier Daten eingeben.



ACHTUNG!

Es wurde ein möglicher Phishing-Versuch erkannt.
Überprüfen Sie die obige Adresse **sorgfältig**.
Die vorgeschlagene Korrektur lautet: **paypal.de**

Webseite wechseln

Ausnahme hinzufügen

Warnungen ausblenden

- zusätzliche Cookie Einstellungen



- Thunderbird Add-On zum besseren Erkennen von Phishing Mails
<https://secuso.aifb.kit.edu/TORPEDO.php> (Thunderbird / Chrome / Firefox)

- Thunderbird Add-On zum besseren Erkennen von Phishing Mails
<https://secuso.aifb.kit.edu/TORPEDO.php> (Thunderbird / Chrome / Firefox)

- Sicherer Link

https://de.wikipedia.org/wiki/Technische_Universit%C3%A4t_Darmstadt

<https://de.wikipedia.org>
/wiki/Technische_Universität_Darmstadt

Die Domain (hervorgehobener Bereich) wurde von den Entwicklern von TORPEDO als wenig riskant eingestuft.



[Mehr Informationen zu diesem Spezialfall und zur Durchführung der Überprüfung](#)

- Thunderbird Add-On zum besseren Erkennen von Phishing Mails
<https://secuso.aifb.kit.edu/TORPEDO.php> (Thunderbird / Chrome / Firefox)

- Riskanter Link

<http://www.echo-online.de/lokales/darmstadt/index.htm>

[http://www. echo-online.de
/lokales/darmstadt/index.htm](http://www.echo-online.de/lokales/darmstadt/index.htm)

Die Domain (hervorgehobener Bereich) der URL ist TORPEDO nicht bekannt und kann daher nicht automatisch beurteilt werden.



Überprüfen Sie die Domain gründlich und entscheiden dann, ob dieser vertraut werden kann. Nur wenn diese vertrauenswürdig ist, klicken Sie auf den Link, ansonsten löschen Sie diese E-Mail.



Mehr Informationen zur Durchführung der Überprüfung

Link ist deaktiviert, damit Sie die Domain in Ruhe prüfen.
Verbleibende Zeit: 02 Sekunde(n)

- Thunderbird Add-On zum besseren Erkennen von Phishing Mails
<https://secuso.aifb.kit.edu/TORPEDO.php> (Thunderbird / Chrome / Firefox)

- Vertrauter Link

<https://www.darmstadt.de/leben-in-darmstadt/arbeit-beruf/>

<https://www.darmstadt.de/leben-in-darmstadt/arbeit-beruf/>

Die Domain (hervorgehobener Bereich) wurde von Ihnen als wenig riskant eingestuft (entweder manuell oder weil Sie früher auf einen entsprechenden Link geklickt haben).



Mehr Informationen zu den "wenig riskant" eingestuften Domains

- Weitere Tools und Informationen:
 - **SECUSO für den Bürger / für KMU** <https://secuso.aifb.kit.edu/642.php>
 - **NoPhish** <https://secuso.aifb.kit.edu/NoPhish.php>
 - **NoPhish Video (5 Minuten)** <https://www.youtube.com/watch?v=XesIAkZluwY>
 - **NoPhish Quiz** <https://secuso.org/quiz-betr-nachrichten>
 - **SECUSO Passwort-Quiz:** <https://secuso.org/quiz-passwortsicherheit>
 - **Privacy Friendly Apps für Android:** <https://secuso.aifb.kit.edu/105.php>



Immer die Ruhe bewahren!

WWW.DASDEMOT.DE

- Passwort ändern

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

Benutzerkennung:	<input type="text"/>
bisheriges Passwort:	<input type="password"/>
neues Passwort:	<input type="password"/>
neues Passwort wiederholen:	<input type="password"/>

Der Umgang mit Passwörtern ist in der [Richtlinie für Passwörter der zentralen Benutzerkennung des Gauß-IT-Zentrums](#) pdf hinterlegt.

Bild: 20

- Passwort ändern
- Unternehmen kontaktieren

0531/391-**55555**



Bild: 21

- Passwort ändern
- Unternehmen kontaktieren
0531/391-55555
- Vorfall melden



Bild: 22

- Passwort ändern
- Unternehmen kontaktieren
0531/391-**55555**
- Vorfall melden
- Vom Unternehmen beraten lassen



Bild: 23

- Passwort ändern
- Unternehmen kontaktieren
0531/391-5555
- Vorfall melden
- Vom Unternehmen beraten lassen
- Konto sperren
116 116



Bild: 24



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