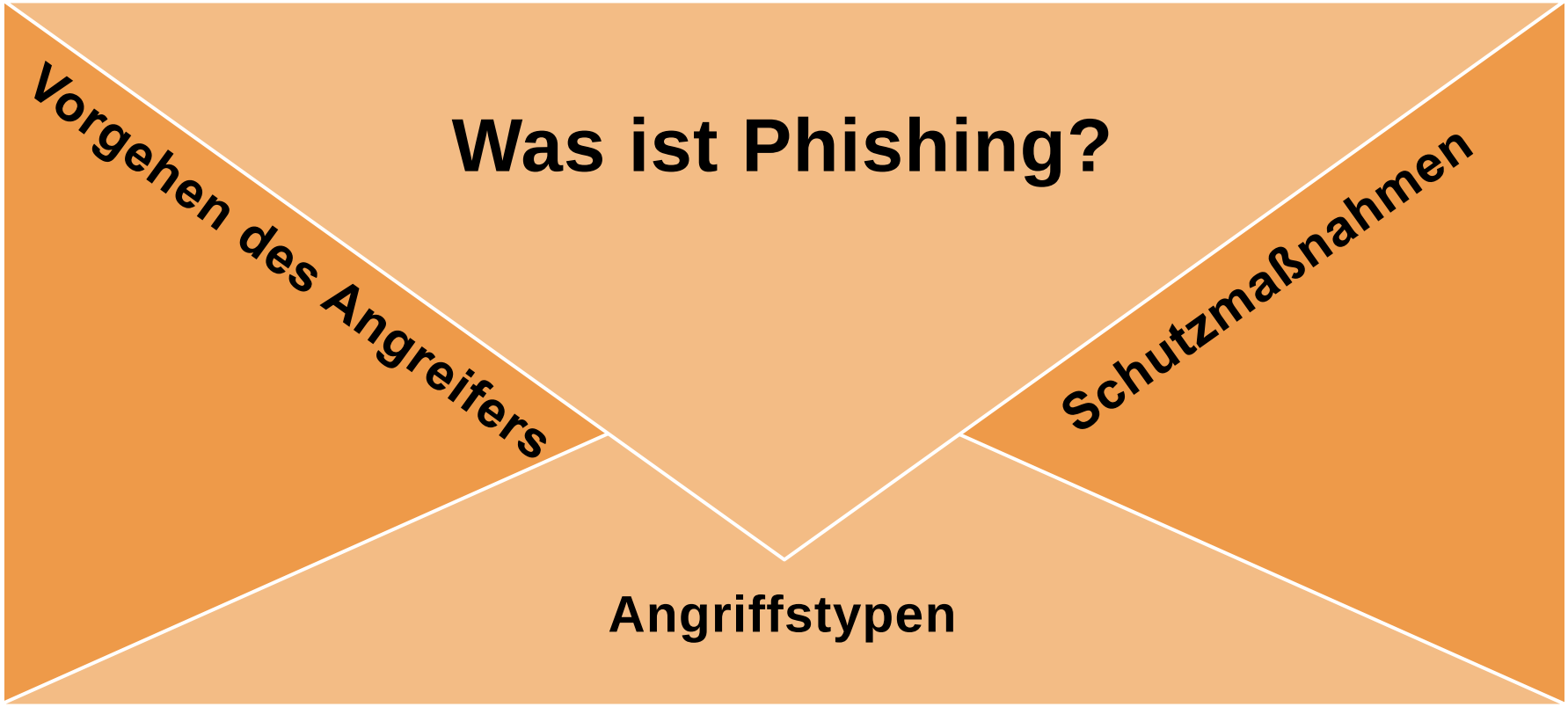
Technische Universität Braunschweig

Gauß-IT-Zentrum

Anti-Phishing

Christian Kühn und Yasin Piri, 23.11.2017

Agenda


Was ist Phishing?
Vorgehen des Angreifers
Schutzmaßnahmen
Angriffstypen

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

Bild: 1

- Bankdaten

Bild: 2

- Bankdaten

Bild: 2

- Benutzerkonten mit den dazugehörigen Passwörter

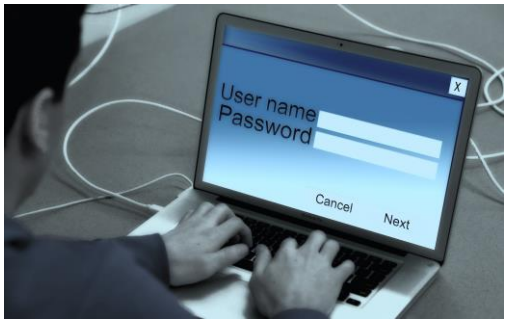


Bild: 3

- Bankdaten

Bild: 2

- Benutzerkonten mit den dazugehörigen Passwörter

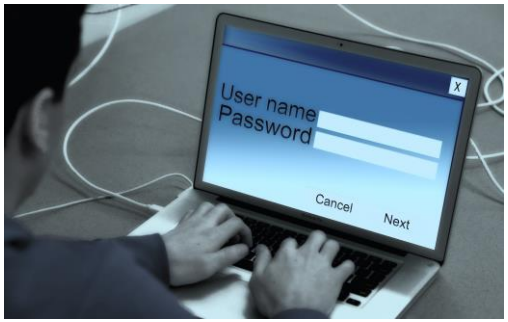


Bild: 3

- Namen (Freunde, Familie, Arbeitskollegen)
- Telefonnummer


Bild: 4

- Daten verkaufen

Bild: 6

- Daten verkaufen
- Vermögensschäden

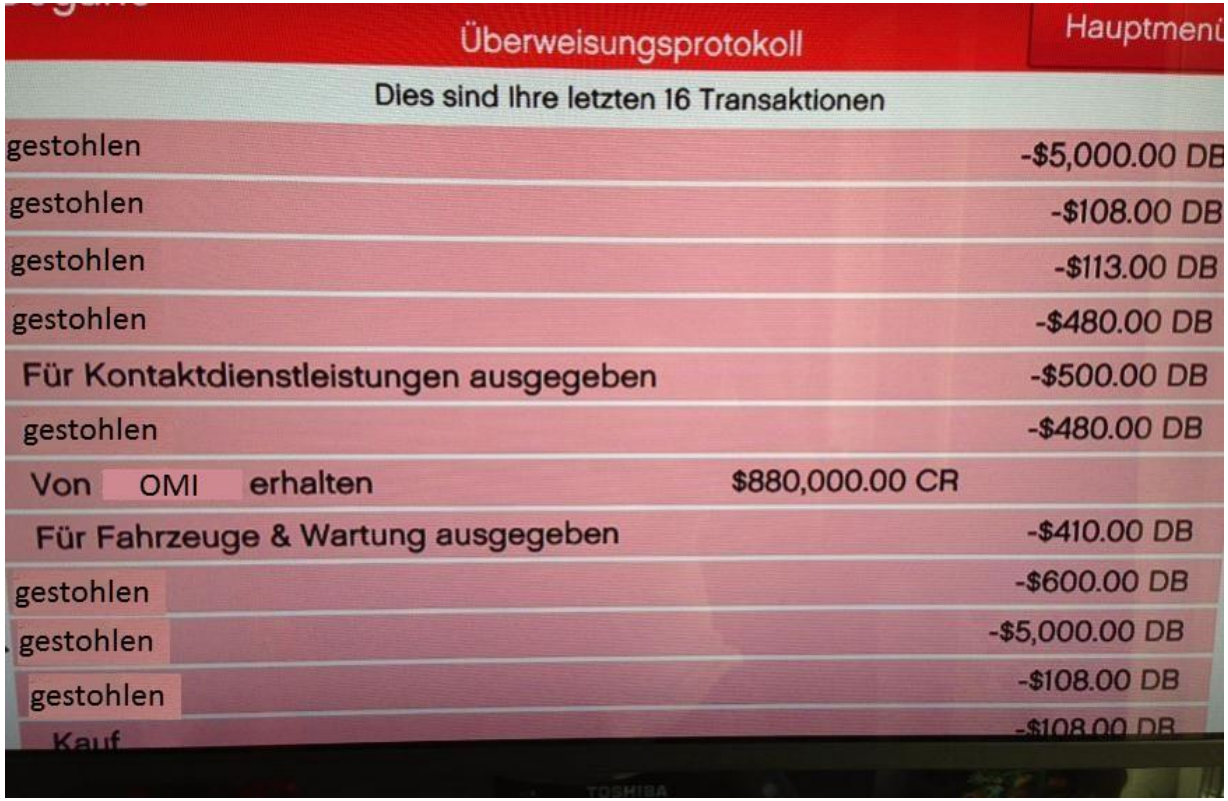


Bild: 7

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

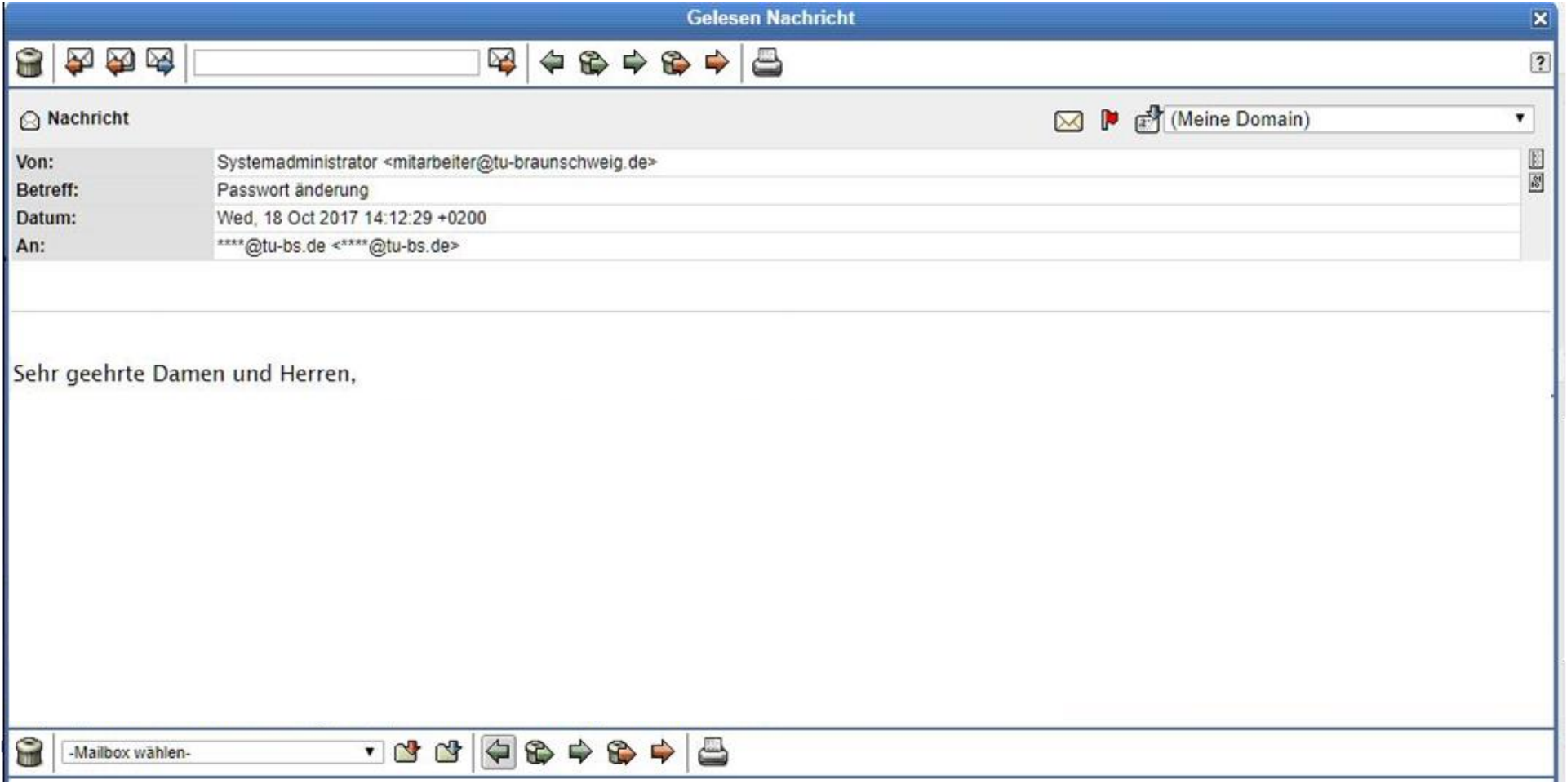

Gelesen Nachricht
Nachricht
(Meine Domain)
Von: Systemadministrator <mitarbeiter@tu-braunschweig.de>
Betreff: Passwort änderung
Datum: Wed, 18 Oct 2017 14:12:29 +0200
An: ****@tu-bs.de <****@tu-bs.de>
Sehr geehrte Damen und Herren,
-Mailbox wählen-

Bild: 11

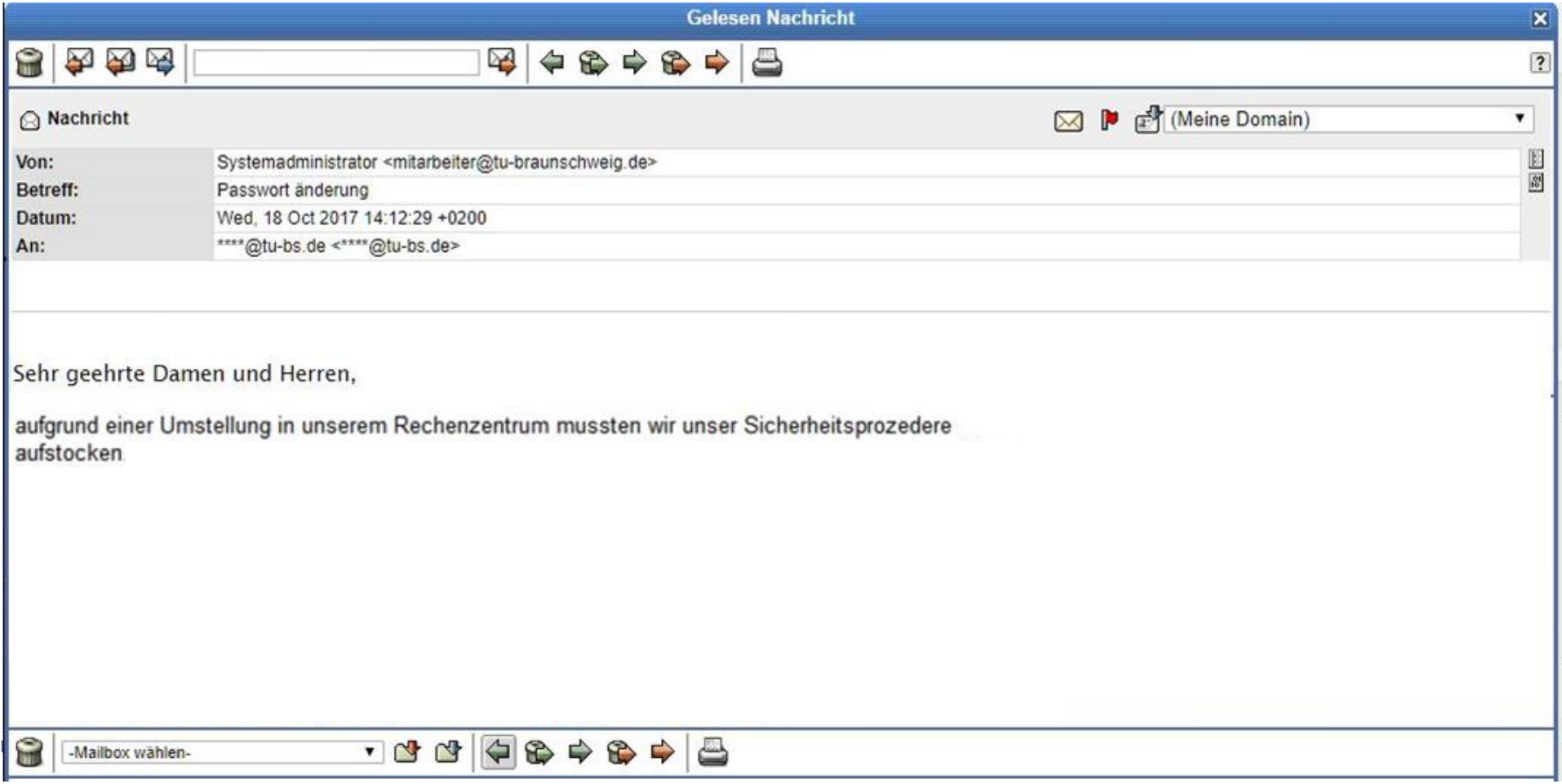

Gelesen Nachricht
Nachricht
(Meine Domain)
Von: Systemadministrator <mitarbeiter@tu-braunschweig.de>
Betreff: Passwort änderung
Datum: Wed, 18 Oct 2017 14:12:29 +0200
An: ****@tu-bs.de <****@tu-bs.de>
Sehr geehrte Damen und Herren,
aufgrund einer Umstellung in unserem Rechenzentrum mussten wir unser Sicherheitsprozedere aufstocken
-Mailbox wählen-

Bild: 11

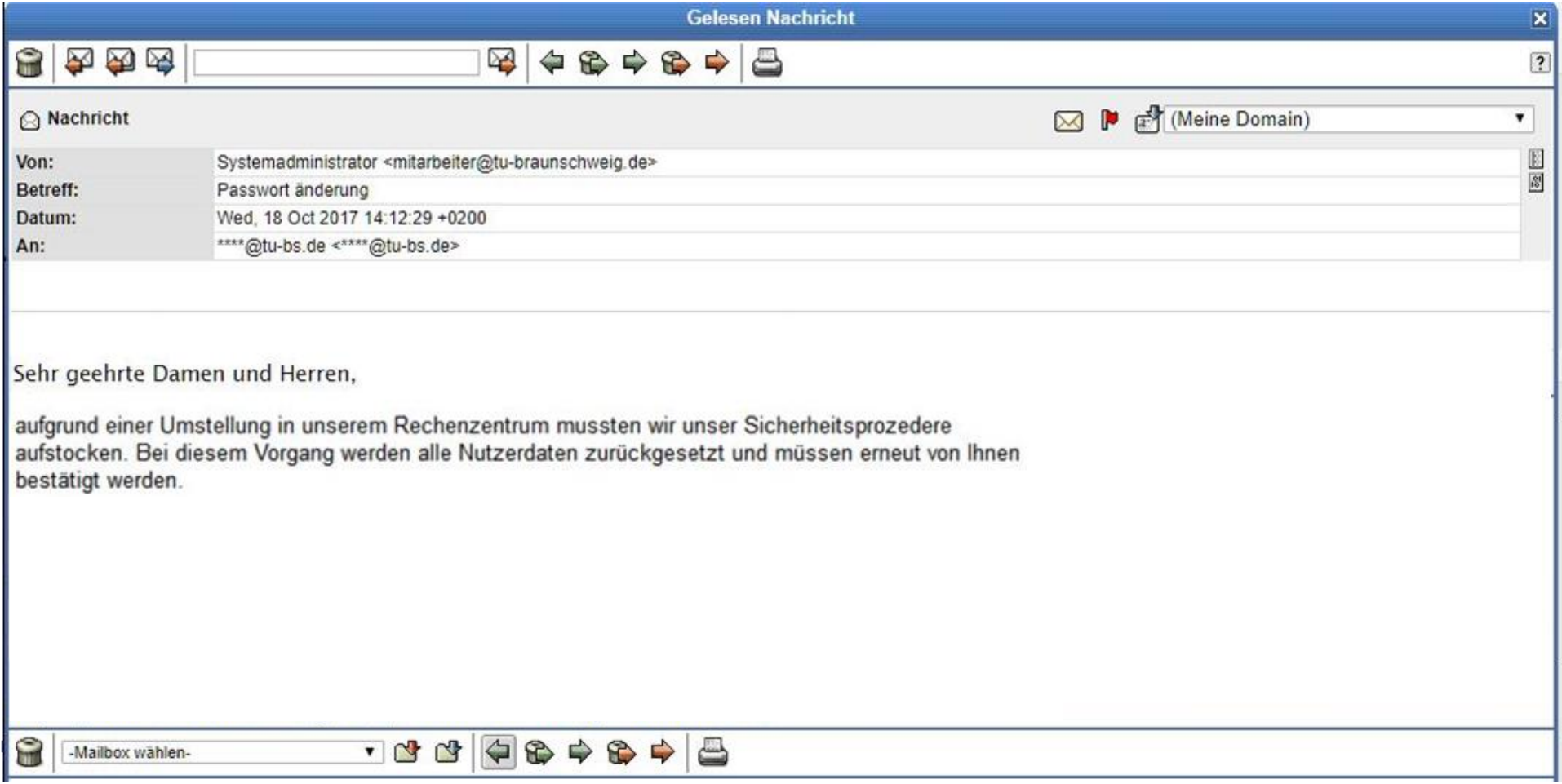

Gelesen Nachricht
Nachricht
(Meine Domain)
Von: Systemadministrator <mitarbeiter@tu-braunschweig.de>
Betreff: Passwort änderung
Datum: Wed, 18 Oct 2017 14:12:29 +0200
An: ****@tu-bs.de <****@tu-bs.de>
Sehr geehrte Damen und Herren,
aufgrund einer Umstellung in unserem Rechenzentrum mussten wir unser Sicherheitsprozedere aufstocken. Bei diesem Vorgang werden alle Nutzerdaten zurückgesetzt und müssen erneut von Ihnen bestätigt werden.
-Mailbox wählen-

Bild: 11

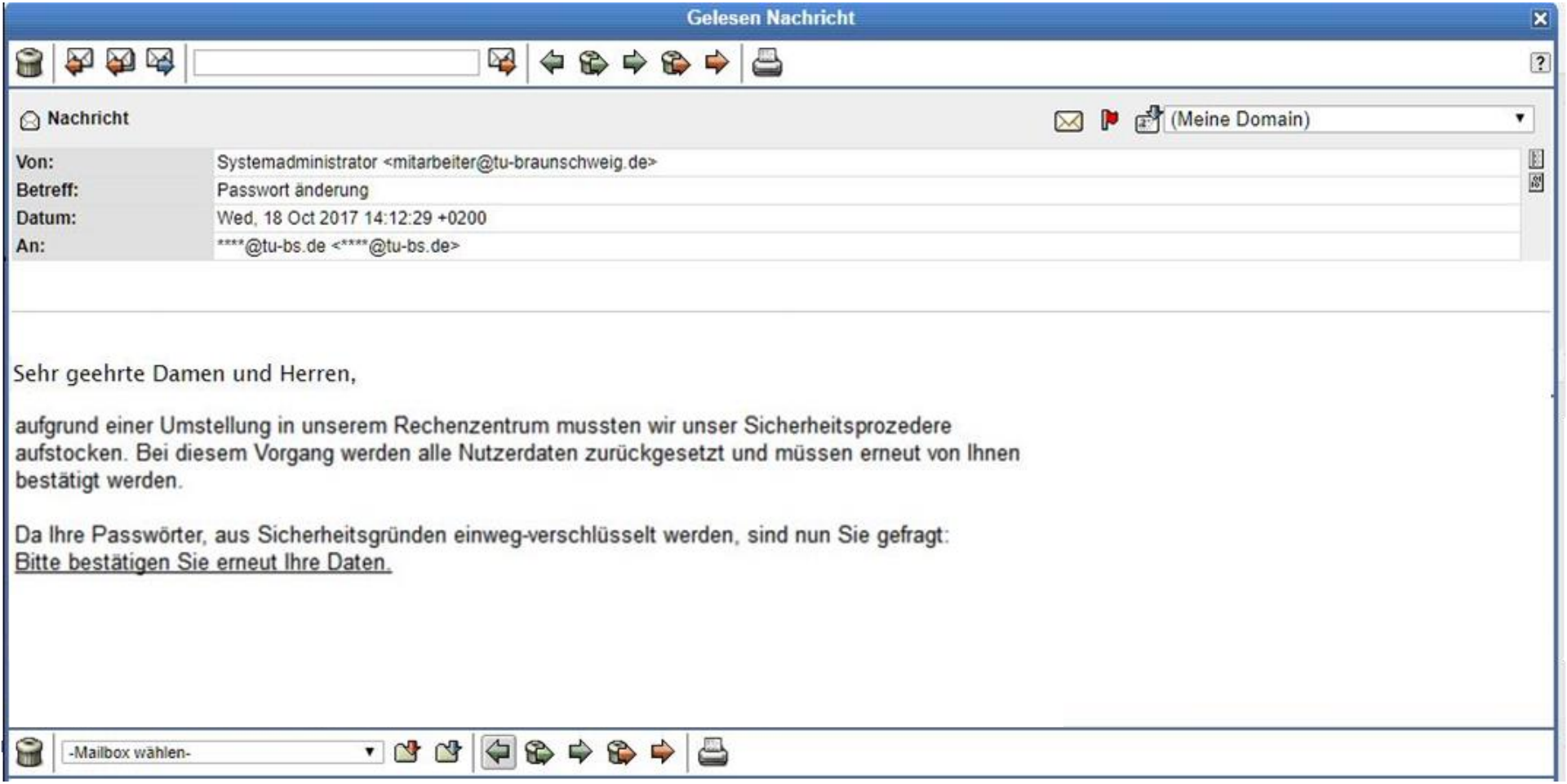

Gelesen Nachricht
Nachricht
(Meine Domain)
Von: Systemadministrator <mitarbeiter@tu-braunschweig.de>
Betreff: Passwort änderung
Datum: Wed, 18 Oct 2017 14:12:29 +0200
An: ****@tu-bs.de <****@tu-bs.de>
Sehr geehrte Damen und Herren,
aufgrund einer Umstellung in unserem Rechenzentrum mussten wir unser Sicherheitsprozedere aufstocken. Bei diesem Vorgang werden alle Nutzerdaten zurückgesetzt und müssen erneut von Ihnen bestätigt werden.
Da Ihre Passwörter, aus Sicherheitsgründen einweg-verschlüsselt werden, sind nun Sie gefragt:
Bitte bestätigen Sie erneut Ihre Daten.
-Mailbox wählen-

Bild: 11

Gelesen Nachricht

Nachricht

(Meine Domain)

Von:	Systemadministrator <mitarbeiter@tu-braunschweig.de>
Betreff:	Passwort änderung
Datum:	Wed, 18 Oct 2017 14:12:29 +0200
An:	****@tu-bs.de <****@tu-bs.de>

Sehr geehrte Damen und Herren,

aufgrund einer Umstellung in unserem Rechenzentrum mussten wir unser Sicherheitsprozedere aufstocken. Bei diesem Vorgang werden alle Nutzerdaten zurückgesetzt und müssen erneut von Ihnen bestätigt werden.

Da Ihre Passwörter, aus Sicherheitsgründen einweg-verschlüsselt werden, sind nun Sie gefragt:
Bitte bestätigen Sie erneut Ihre Daten.

Die nächsten Schritte werden Ihnen auf der Seite mitgeteilt. Bitten geben Sie alle Daten vollständig ein.

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

-Mailbox wählen-

Bild: 11

Gelesen Nachricht

Nachricht

(Meine Domain)

Von:	Systemadministrator <mitarbeiter@tu-braunschweig.de>
Betreff:	Passwort änderung
Datum:	Wed, 18 Oct 2017 14:12:29 +0200
An:	****@tu-bs.de <****@tu-bs.de>

Sehr geehrte Damen und Herren,

aufgrund einer Umstellung in unserem Rechenzentrum mussten wir unser Sicherheitsprozedere aufstocken. Bei diesem Vorgang werden alle Nutzerdaten zurückgesetzt und müssen erneut von Ihnen bestätigt werden.

Da Ihre Passwörter, aus Sicherheitsgründen einweg-verschlüsselt werden, sind nun Sie gefragt:
Bitte bestätigen Sie erneut Ihre Daten.

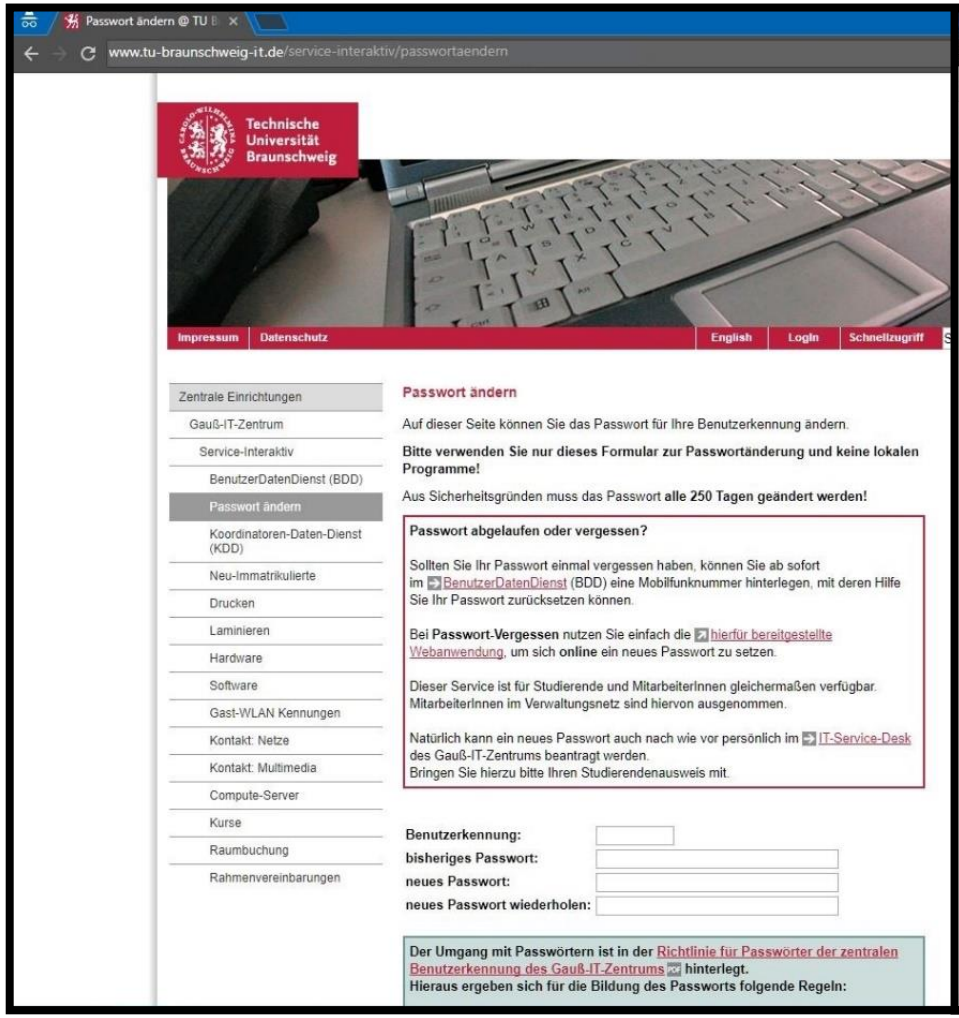
Die nächsten Schritte werden Ihnen auf der Seite mitgeteilt. Bitten geben Sie alle Daten vollständig ein.

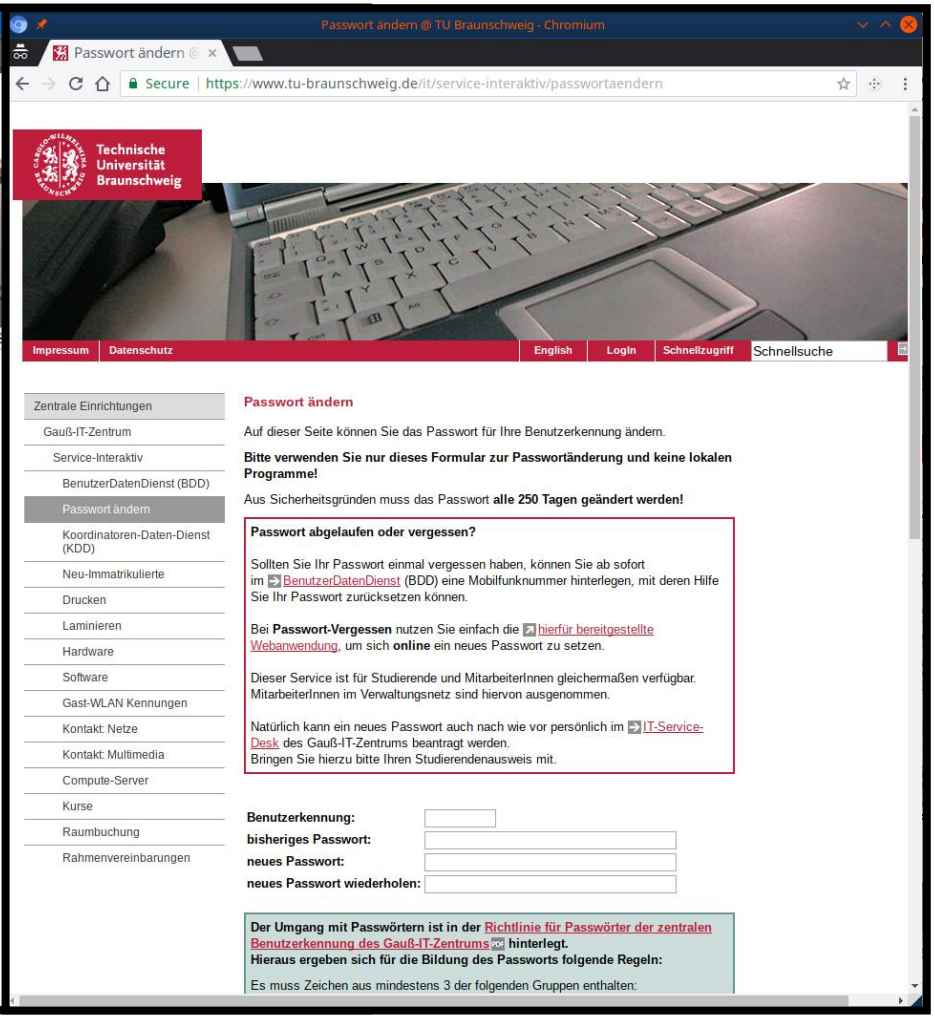
https://www.tu-braunschweig.de/it/service-interaktiv/passwortaendern

-Mailbox wählen-

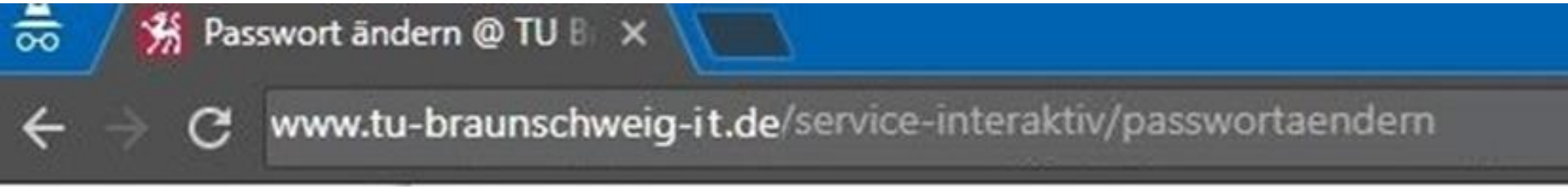
http://www.tu-braunschweig-it.de/service-interaktiv/passwortaendern

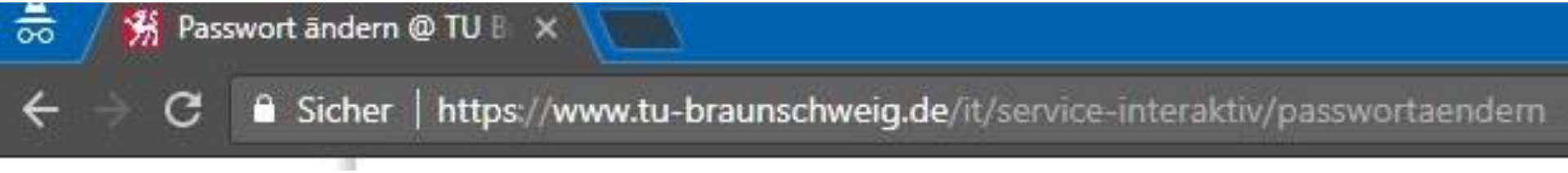
Bild: 11


Passwort ändern @ TU B
www.tu-braunschweig-it.de/service-interaktiv/passwortaendern
Technische Universität Braunschweig
Impressum
Datenschutz
English
Login
Schnellzugriff
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 hinterlegt.
Hieraus ergeben sich für die Bildung des Passworts folgende Regeln:

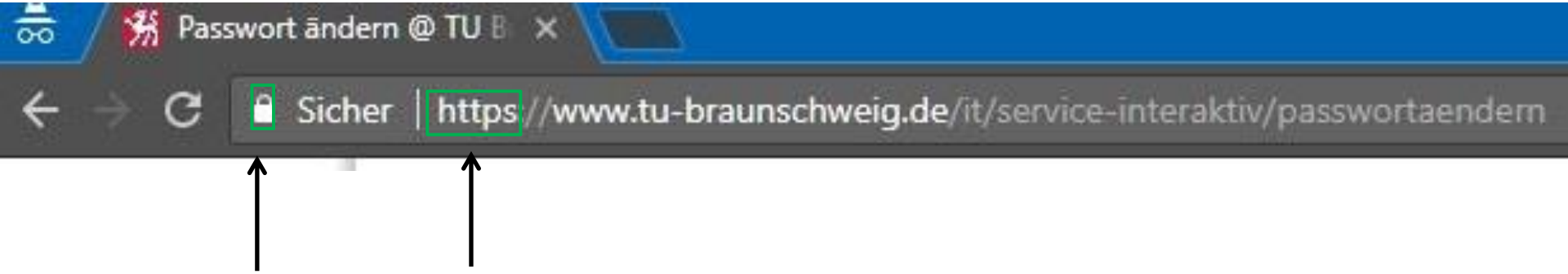

Passwort ändern @ TU Braunschweig - Chromium
Passwort ändern
Secure
https://www.tu-braunschweig.de/it/service-interaktiv/passwortaendern
Technische Universität Braunschweig
Impressum
Datenschutz
English
Login
Schnellzugriff
Schnellsuche
Zentrale Einrichtungen
Gauß-IT-Zentrum
Service-Interaktiv
BenutzerDatenDienst (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 hinterlegt.
Hieraus ergeben sich für die Bildung des Passworts folgende Regeln:
Es muss Zeichen aus mindestens 3 der folgenden Gruppen enthalten:

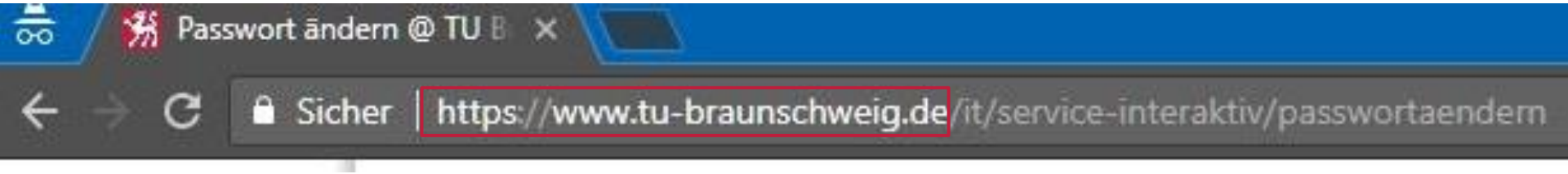

Passwort ändern @ TU B
www.tu-braunschweig-it.de/service-interaktiv/passwortaendern

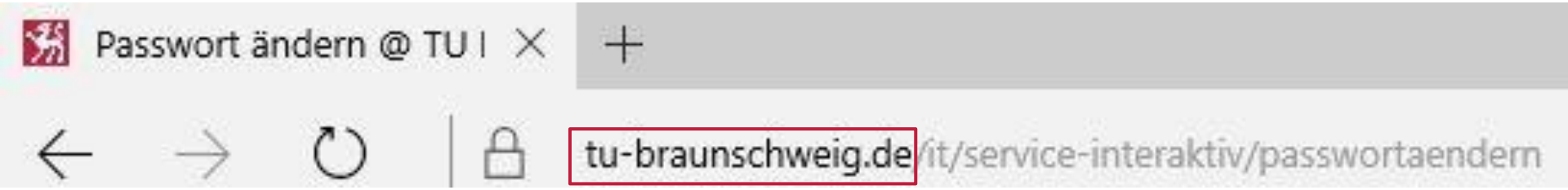

Passwort ändern @ TU B
www.tu-braunschweig-it.de/service-interaktiv/passwortaendern

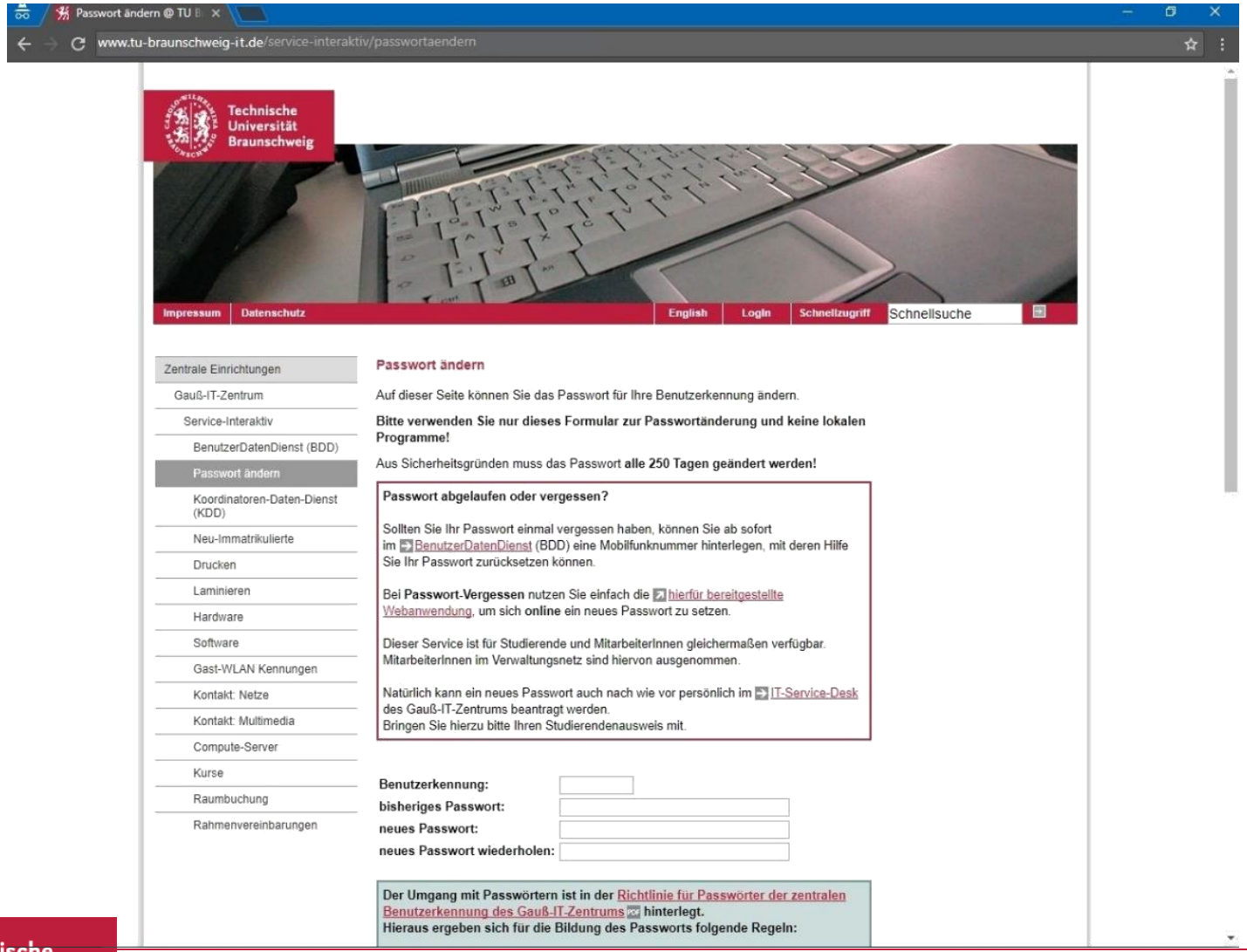

Passwort ändern @ TU B
Sicher
https://www.tu-braunschweig.de/it/service-interaktiv/passwortaendern


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


Passwort ändern @ TU B
Sicher
https://www.tu-braunschweig.de/it/service-interaktiv/passwortaendern


Passwort ändern @ TU B
Sicher
https://www.tu-braunschweig.de/it/service-interaktiv/passwortaendern


Passwort ändern @ TU I
tu-braunschweig.de/it/service-interaktiv/passwortaendern


Passwort ändern @ TU B
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
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 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 hinterlegt.
Hieraus ergeben sich für die Bildung des Passworts folgende Regeln:

PassSec+

- Firefox Add-on zum Schutz von Passwörtern, Zahlungsdaten und weiteren sensiblen Daten

PassSec+

- Firefox Add-on zum Schutz von Passwörtern, Zahlungsdaten und weiteren sensiblen Daten

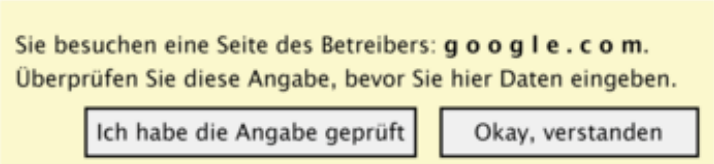
- HTTPS mit Extended Validation Zertifikat

PassSec+

- Firefox Add-on zum Schutz von Passwörtern, Zahlungsdaten und weiteren sensiblen Daten

- HTTPS mit Extended Validation Zertifikat

- HTTPS ohne Extended Validation Zertifikat



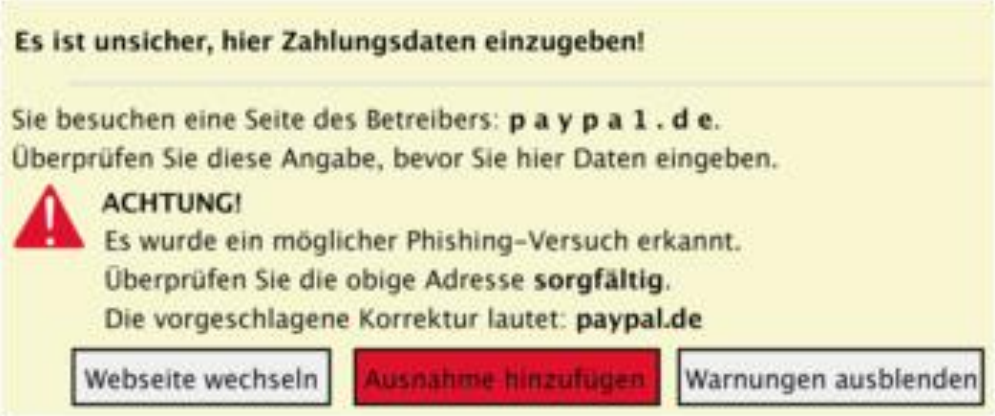
PassSec+

- Kein HTTPS

PassSec+

- Kein HTTPS

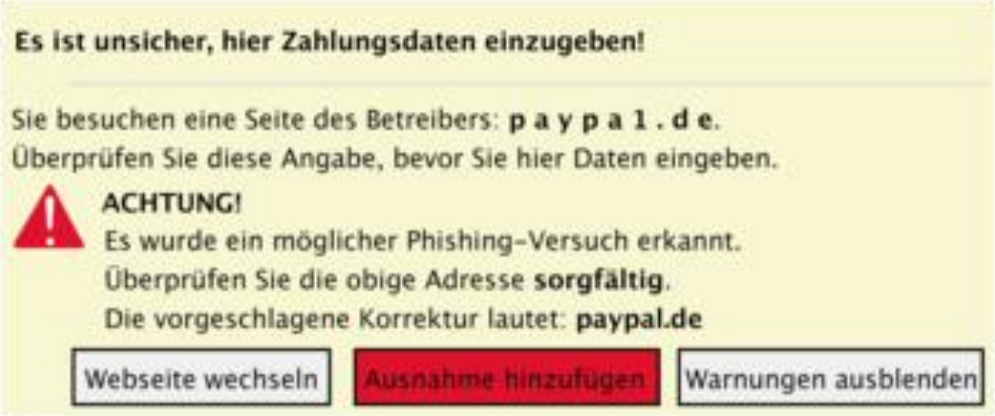
- Prüfen der Domain durch Suchmaschinen und Web of Trust



PassSec+

- Kein HTTPS

- Prüfen der Domain durch Suchmaschinen und Web of Trust



- zusätzliche Cookie Einstellungen

TORPEDO

- Thunderbird Add-On zum besseren Erkennen von Phishing Mails

TORPEDO

- Thunderbird Add-On zum besseren Erkennen von Phishing Mails

- 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.

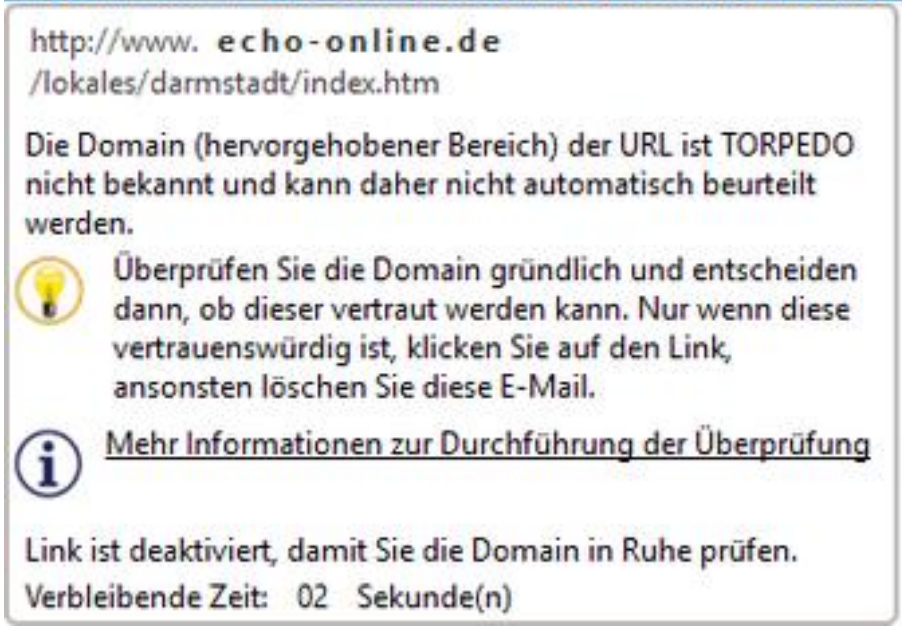
Mehr Informationen zu diesem Spezialfall und zur Durchführung der Überprüfung

TORPEDO

- Thunderbird Add-On zum besseren Erkennen von Phishing Mails

- Riskanter Link

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



TORPEDO

- Thunderbird Add-On zum besseren Erkennen von Phishing Mails

- 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


Immer die Ruhe bewahren!
WWW.DASDEMOT.DE

- Passwort ändern

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.

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

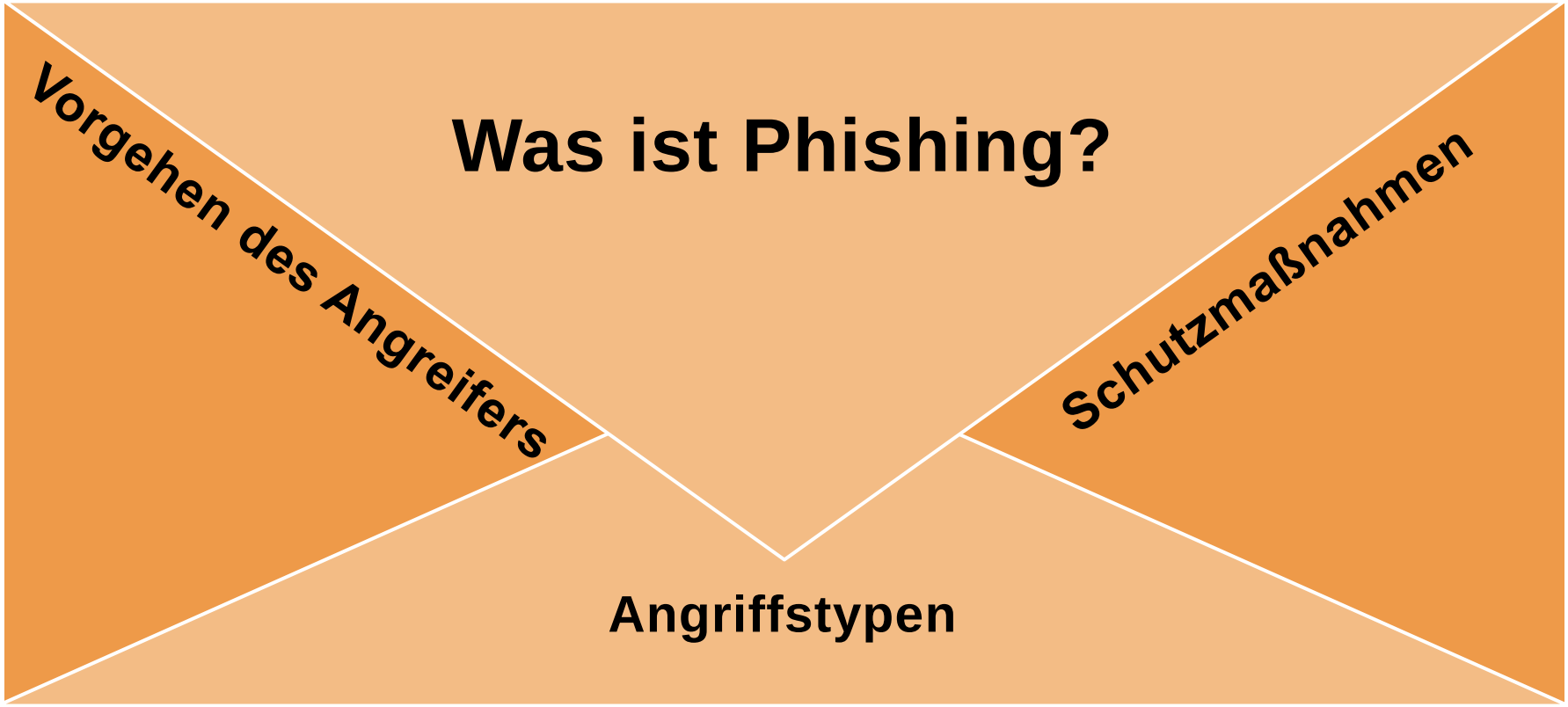
- Passwort ändern
- Unternehmen kontaktieren

  0531/391-**55555**
- Vorfall melden
- Vom Unternehmen beraten lassen
- Konto sperren

  116 116

Bild: 24

Was haben wir gelernt?



Technische Universität Braunschweig

Anti-Phishing

Yasin Piri und Christian Kühn, 24.11.2017