UNIVERSITÄT BIELEFELD

„Digitale Selbstverteidigung“ für Forschende

Woche der Forschungskompetenz
05.03.2024

Michael Sundermeyer
Informationssicherheitsbeauftragter
Universität Bielefeld

UNIVERSITÄT BIELEFELD

Royale Sicherheit von Informationen…

UNIVERSITÄT BIELEFELD

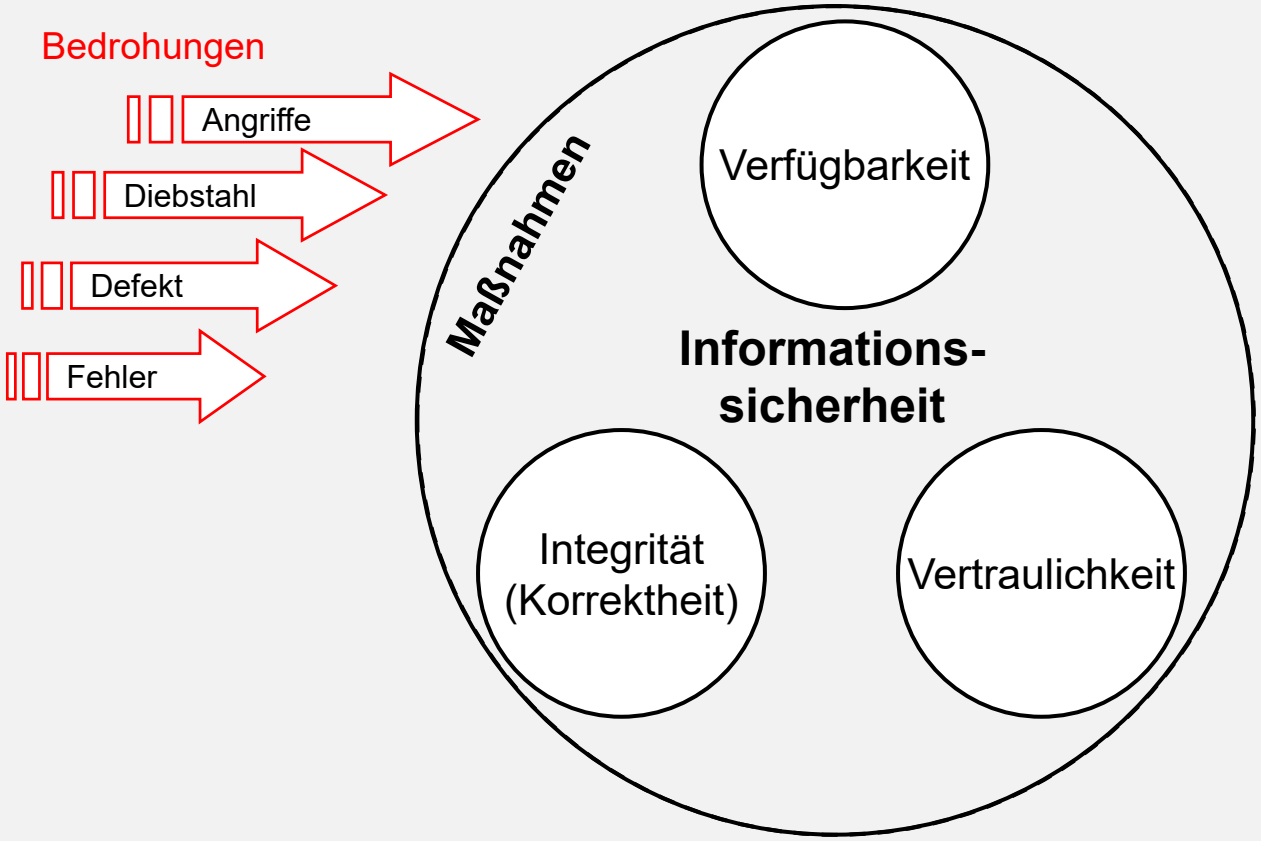
Worum geht’s bei Informationssicherheit?

Forschungskontext

- Ziel: Wertvolle Daten angemessen zu schützen
- Was schützen? Forschungsdaten, Personaldaten, Gesundheitsdaten, Finanzdaten, etc.
- Wovor schützen? Verlust (Zerstörung), Manipulation und unbefugter Einsichtnahme

UNIVERSITÄT BIELEFELD

Ziele der Informationssicherheit



UNIVERSITÄT BIELEFELD

Informationssicherheit & Datenschutz

Informationssicherheit

- Die Informationssicherheit hat das Ziel alle Daten angemessen zu schützen (unabhängig davon, ob ein Personenbezug besteht oder nicht)
- Die Informationssicherheit schützt die **Interessen der Organisation**

Datenschutz

- Der Datenschutz hat das Ziel Daten, die personenbezogen sind d.h. einer natürlichen Person zugeordnet werden können zu schützen
- Der Datenschutz schützt die (gesetzlich geregelten) **Betroffenenrechte**

UNIVERSITÄT BIELEFELD

Informationssicherheit an der Universität

UNIVERSITÄT BIELEFELD

Die Uni ist doch sicher, oder?

- Ich bin kein IT-Profi. Da kann ich nicht viel zur Informationssicherheit beitragen…
- **Die wichtigste Firewall sitzt „vor dem Rechner“** – jede*r Einzelne trägt durch sicheres Verhalten zur Sicherheit der gesamten Universität bei!
- UND: Alle sind für die Sicherheit in ihrem Arbeitsbereich mit verantwortlich („**Siehst Du was, sag was!**“)

UNIVERSITÄT BIELEFELD

Das ist tatsächlich passiert (Auszug)

- Gezielter Angriff auf Mitarbeiter, Löschung von Daten
- Gehackter Server der Uni Bielefeld greift die FU Berlin an
- Verschlüsselungs-Trojaner verschlüsselt ca. 10.000 Dateien
- Bewerbungsunterlagen stehen ungeschützt im Netz
- Buchhaltung erhält gefälschten E-Mails im Namen des Rektors
- Erpressungsversuch mit angeblicher Sicherheitslücke
- 200 Gigabyte Daten von gehackten Forschungsserver kopiert
- 800 Euro Schaden für Mitarbeiter durch Geschenkkarten-Betrug
- Phishing und gehackte E-Mail Konten in allen Bereichen

UNIVERSITÄT BIELEFELD

Gute Presse, schlechte Presse…

Ransomware: Daten von Uni Duisburg-Essen im Darknet, Uni Innsbruck attackiert

Die Daten aus dem Cyber-Angriff auf die Uni Duisburg-Essen wurden im Darknet veröffentlicht. Derweil hat die Uni Innsbruck eine Attacke am Wochenende abgewehrt.

Lesezeit: 2 Min. In Pocket speichern 147

Cyberangriff: TU Berlin rechnet mit monatelangen IT-Einschränkungen

Es wird noch einige Zeit dauern, bis die zentralen IT-Systeme der TU Berlin nach der Ransomware-Attacke wieder laufen. Auch das SAP-Kernsystem ist betroffen.

Lesezeit: 1 Min. In Pocket speichern 296

320 GByte interne Daten von Fraunhofer-Institut im Darknet

Nach einem Ransomware-Angriff werden die erbeuteten Daten für 2 Millionen US-Dollar auf der Darknetplattform Industrial Spy zum Kauf angeboten.

in Pocket speichern merken 5. Mai 2022, 11:09 Uhr, Moritz Tremmel/dpa

Online-Probleme an der Uni

Die Bielefelder Uni hat aktuell große Rechner-Probleme. Ausgerechnet zum Semesterstart ist seit gestern u.a. das kommentierte Vorlesungs-verzeichnis EKW nicht mehr online abrufbar. Das Verzeichnis ist für die Studenten unverzichtbar, weil sie darin u.a. einsehen können, wo ihre nächsten Vorlesungen und Seminare stattfinden.
Uni-Sprecher Ingo Lohuis kann zurzeit noch nicht sagen, wo genau das Problem liegt. Die Uni hat mittlerweile auch externe Computerexperten hinzugezogen, um den Fehler zu finden.

UNIVERSITÄT BIELEFELD

Regelungen zur Informationssicherheit

UNIVERSITÄT BIELEFELD

Regelungen zur Informationssicherheit

Leitlinie
Ziele, Rollen und Umsetzung des Sicherheitsprozesses

Basisschutzregelungen
Regelungen für Beschäftigte, Führungskräfte & IT-Personal

Richtlinien
Detail-Regelungen u.a. für Cloud-Speicher, Telearbeit etc.

Allgemein

Konkret

- Sicherer Arbeitsplatz
- Datenablage und Dienste
- E-Mail Nutzung
- Passwörter
- Vorgehen bei Vorfällen


UNIVERSITÄT BIELEFELD

SICHERE DATEN: DAS MÜSSEN SIE TUN

Sichere Passwörter

- Mindestlänge 12 Zeichen, Buchstaben, Zahlen und Sonderzeichen verwenden
- Passwörter je nach Verwendungsbereich variieren
- Passwörter geheim halten
- Passwortsätze oder „Passwort Manager“ nutzen!

Was tun wenn doch etwas passiert

- EDV-Betreuung und Vorgesetzte informieren (PEVZ hilft weiter)
- Betroffenes Gerät nicht ausschalten, nach Möglichkeit vom Datennetz bzw. Internet trennen

uni-bielefeld.de/informationssicherheit

Stand: November 2019

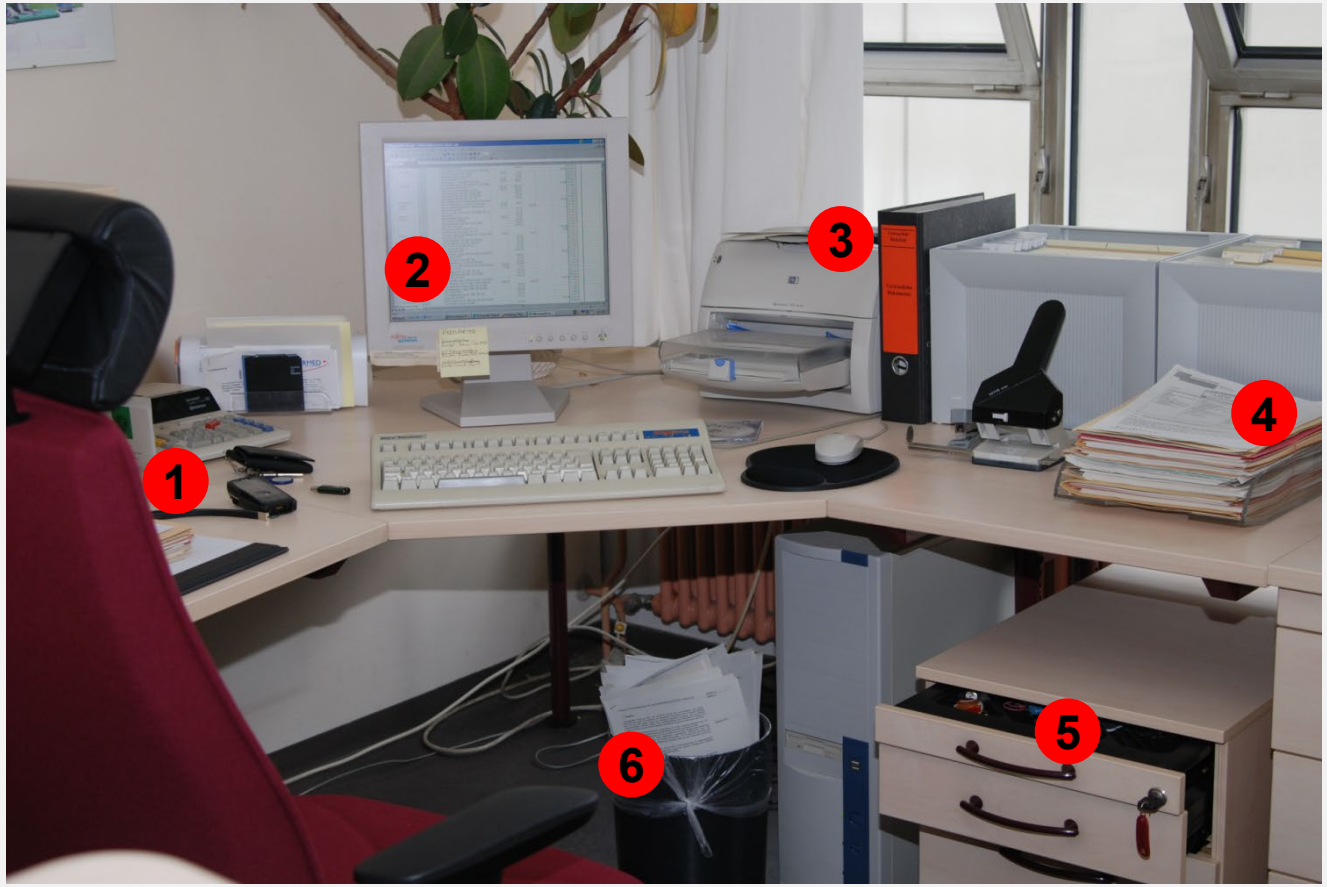
Alle Regelungen sind auf der Webseite der Informationssicherheit abrufbar

UNIVERSITÄT BIELEFELD

Sicherer Arbeitsplatz

UNIVERSITÄT BIELEFELD

Sicherer Arbeitsplatz?



- Typischer Büro-Arbeitsplatz aus der Verwaltung
- Die Tür des Büro steht offen, es ist keine Person im Büro

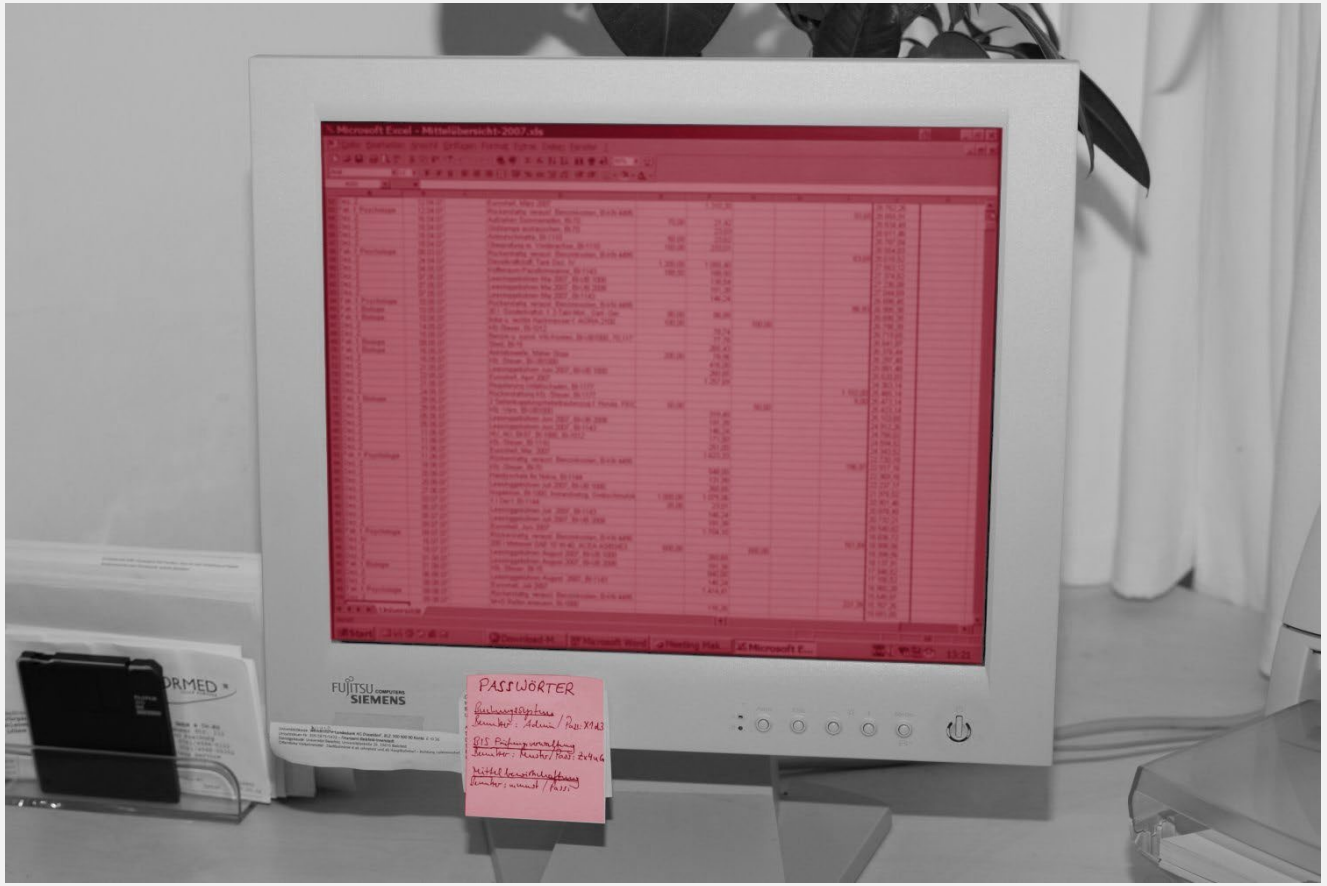
UNIVERSITÄT BIELEFELD

„Persönliche“ dienstliche Gegenstände

- Datenträger wie z.B. USB-Sticks fassen viele Daten und gehen schnell verloren
- (Elektronische) Schlüssel gestatten Zutritt zu verschlossenen Bereichen wo weitere Daten liegen könnten
- Smartphones sind leichte Beute und enthalten ebenfalls Daten z. B. in WhatsApp, E-Mails etc.

UNIVERSITÄT BIELEFELD

„Offener“ Bildschirm



- Bildschirm ist nicht gesperrt, Fremde haben ungehindert Zugriff auf alle Daten
- Einblick in vertrauliche Daten (Stichwort: Einblickwinkel) ist möglich
- Passwörter für verschiedene Dienste hängen am Monitor

UNIVERSITÄT BIELEFELD

Freie Informationen I

- Ordner mit vertraulichen Dokumenten frei zugänglich
- Ausdrucke z. B. mit vertraulichen Daten bleiben im Drucker liegen

UNIVERSITÄT BIELEFELD

Freie Informationen II

- Frei einsehbare Informationen liegen auf dem Schreibtisch (Stichwort: „Clean Desk Policy“)

UNIVERSITÄT BIELEFELD

Freie Informationen III

- Vertrauliche Dokumente finden sich oft im normalen Papiermüll wieder
- Frei zugänglicher Aktenschrank mit Dokumenten, Schlüsseln etc. bergen Risiken

UNIVERSITÄT BIELEFELD

Sichere Flexwork

- Verarbeitete Informationen an Arbeitsort anpassen
- Einblickwinkel bedenken, Geräte bei Nichtgebrauch sperren
- Unterlagen sicher transportieren und verwahren
- Verwendung von privaten IT-Geräten nicht gestattet (Verwaltung)
- Alle Flexwork-Regelungen hier

UNIVERSITÄT BIELEFELD

Sichere IT-Geräte

UNIVERSITÄT BIELEFELD

Basisschutz (für alle IT-Geräte)

- Updates schnell installieren, am besten automatisch - Stand regelmäßig prüfen
- Anti-Malwareschutz nutzen, Geräte regelmäßig scannen
- Firewall verwenden
- Nur notwendige Software aus vertrauenswürdigen Quellen installieren (App Store, Webseite der Hersteller)
- Unnötige Software deinstallieren / löschen
- Regelmäßig Datensicherungen (Backup) erstellen

UNIVERSITÄT BIELEFELD

Windows

- Automatische Updates einschalten
- Anti-Virenschutz (MS Defender oder Sophos kostenlos vom BITS)
- Firewall (Windows-Firewall reicht im allgemeinen)
- App „Windows-Sicherheit“ regelmäßig konsultieren
- Windows Datensparsam konfigurieren z. B. mit „ShutUp10++“ bzw. Verbraucherzentrale
- Tipp: Von Hause aus ist Linux deutlich Datensparsamer (für Einsteiger z. B. Ubuntu oder Linux Mint)

UNIVERSITÄT BIELEFELD

Smartphone / Tablets

- Android oder iOS haben unterschiedliche Sicherheitskonzepte
  - iOS erhält von Apple ca. 7 Jahre Sicherheitsupdates
  - Android-Updates hängen stark vom Hersteller ab (z. B. Samsung bis zu 5 Jahre)
- Jede neue Betriebssystem-Version macht die Geräte wieder etwas sicherer
- Apps regelmäßig aktualisieren, nicht benötigte deinstallieren
- Geräte ohne Updates möglichst austauschen, nicht mehr für kritische Funktionen nutzen (z. B. Onlinebanking)

UNIVERSITÄT BIELEFELD

„Sichere“ Dienste / Anbieter

UNIVERSITÄT BIELEFELD

IT im Wandel

- In den letzten 10 Jahren tiefgreifender Wandel, wie IT-Angebote zur Verfügung gestellt wird
- Entwicklung von neuen, spannenden und hilfreichen Angeboten verläuft immer schneller
- Viele Angebote nur noch als „Software-as-a-Service“ aus „der Cloud“
- Daten liegen auf „someone elses Computer“, viele Nutzende teilen sich das Angebot („public Cloud“)
- Lokale IT steht vor der Herausforderung der Entwicklung zu folgen
- Eigene Maßnahmen zum Schutz der Daten greifen nur bedingt, muss mich auf Anbieter „verlassen“?

UNIVERSITÄT BIELEFELD

Vertrauen ist gut…

- Anbieter werben mit „höchsten Sicherheitsstandards“, „geprüfter TüV-Sicherheit“, „DSGVO-Konformität“ und vielen technischen Schlagworten, die beeindrucken können
- Marketing-Aussagen lassen sich selbst von IT-Fachleuten nur schwer verifizieren, für normale Nutzende ist es noch schwieriger
- Lösungsansatz: Unabhängige Sicherheitszertifizierungen z. B.
  - auf Basis der internationalen Norm ISO 27001 (vgl. ISO 9001)
  - des BSI (Bundesamt für Sicherheit in der Informationstechnik) oder
- Aber: Gute Zertifizierungen sind aufwändig und teuer, viele kleine Anbieter haben (noch) keine

UNIVERSITÄT BIELEFELD

Was tun?

- So geplant wie möglich vorgehen
  - Welches Ziel habe ich, was brauche ich dafür? (Anforderung-/Bedarfsanalyse)
  - Welche Daten verarbeite ich?
    - Wie „kritisch“ oder „sensibel“ sind diese? (Sicherheit / Schutzbedarf der Daten beachten)
    - Handelt es sich um personenbezogene Daten (DSGVO / Datenschutz beachten)
  - Kann mich meine EDV-Betreuung unterstützen, bietet das BITS vielleicht etwas an?
  - Was haben externe Anbieter im Angebot (Marktsichtung)
  - Sind die Angebote für meine Anforderungen / die Art der Daten geeignet?
  - Hat die Universität ggf. bereits einen Vertrag mit dem Anbieter?

UNIVERSITÄT BIELEFELD

Sicherer Umgang mit Daten

UNIVERSITÄT BIELEFELD

Sichere Datenspeicherung

- Als **ersten Speicherort** grundsätzlich immer die **Netzlaufwerke** nutzen (automatisches Backup!)
- Zusätzlich kann **Sciebo** genutzt werden (Campuscloud, bis zu 500 GB kostenloser Speicher).

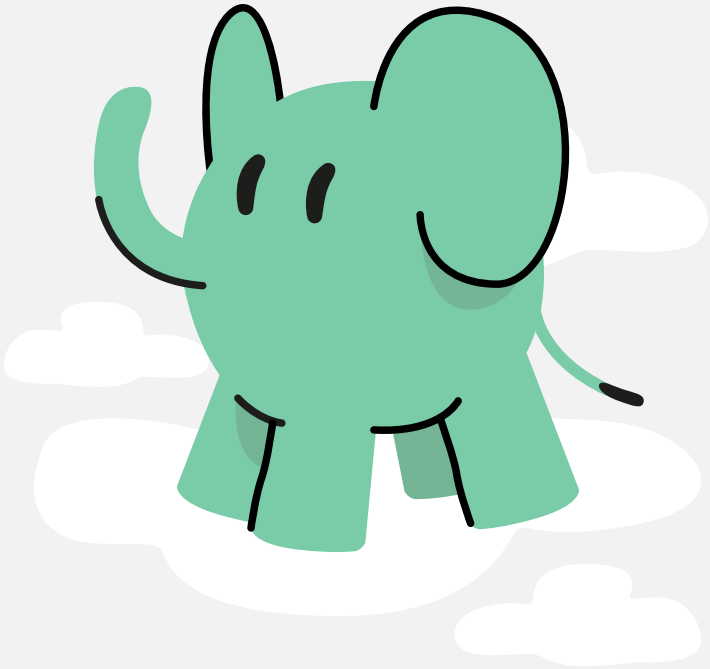
  Aber: Kein echtes Backup, dass von Nutzern verwendet werden kann

  Daten mit hoher Vertraulichkeit müssen verschlüsselt werden (Cloud-Regelungen)
- Nutzung von externen Cloud-Anbietern (z. B. Dropbox, Onedrive, iCloud) mit welchen die Uni keinen Vertrag abgeschlossen hat ist **nicht gestattet** (Regelungen zur Informationssicherheit)
- Externe Festplatten, USB-Sticks etc. sind grundsätzlich nicht für eine (Langzeit)Speicherung von Daten geeignet

UNIVERSITÄT BIELEFELD

Daten (ver)teilen

- Daten auf „Sciebo“ ablegen – wenn diese sensibel sind, dann Daten vorher verschlüsseln (Tools siehe folgende Folien)
- Sciebo-Link erstellen und per E-Mail verteilen
- Alternativ unterstützt Sciebo auch Gast-Accounts (voller Funktionsumfang)
- Daten auf Sciebo löschen, wenn diese nicht mehr benötigt werden



UNIVERSITÄT BIELEFELD

Daten auf Dienstreisen

Risiko: Unbefugte Kenntnisnahme von Informationen durch Dritte z. B. durch mitlesen, mithören oder kopieren von Informationen

Maßnahmen:

- Informationen sicher Transportieren: Digital verschlüsseln, analog in geschlossenen Behältnissen. IT-Geräte nicht unbeaufsichtigt liegen lassen (z. B. im Zug)
- Öffentlicher Raum (ÖPNV, Café etc.): Mithören von Gesprächen oder mitlesen von Dokumenten („shoulder surfing“) bedenken. Vertrauliche Informationen nur in geeigneter Umgebung bearbeiten
- Dienstreise ins Ausland (CN, RU, USA etc.): Nur „saubere“ IT-Geräte bzw. notwendiges Datenset mitnehmen. IT-Geräte können beim Grenzübertritt durchsucht und ausgelesen werden

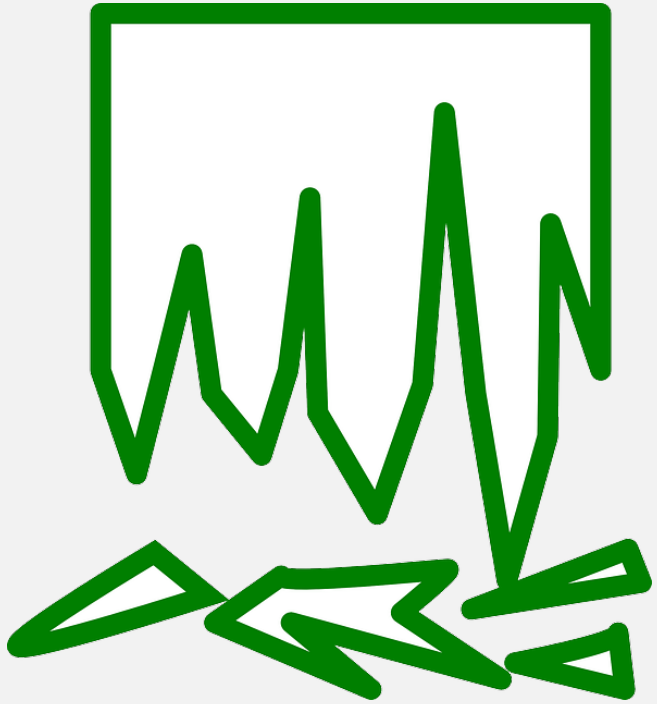
UNIVERSITÄT BIELEFELD

Daten vernichten

Risiko: Unbefugte Kenntnisnahme von Informationen durch Dritte („dumpster diving“)

Maßnahmen:

- Vertrauliche Informationen auf Papier: Schredder mit ausreichender Sicherheitsstufe verwenden (professionelle Aktenvernichtung wird auch zentral angeboten)
- Vertrauliche Informationen auf Datenträgern: In der BITS-Beratung (Raum V0-215) stehen entsprechende Sicherheitstonnen zur Entsorgung von IT-Geräte bzw. Datenträger bereit. Diese werden von einem Unternehmen professionell geschreddert.



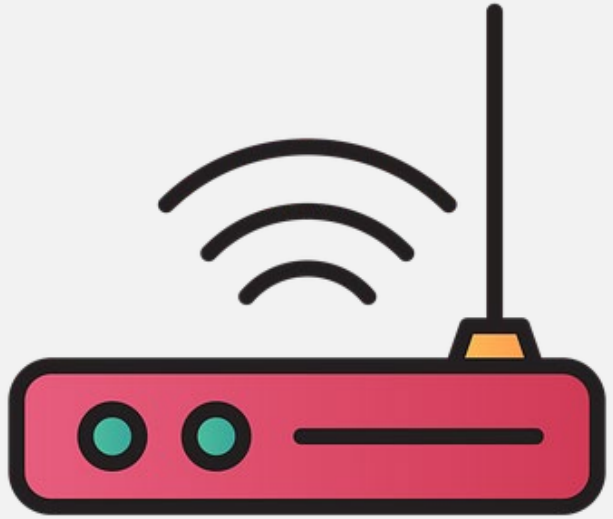
UNIVERSITÄT BIELEFELD

Sicher am Netz / im Internet

UNIVERSITÄT BIELEFELD

Wlan-Router

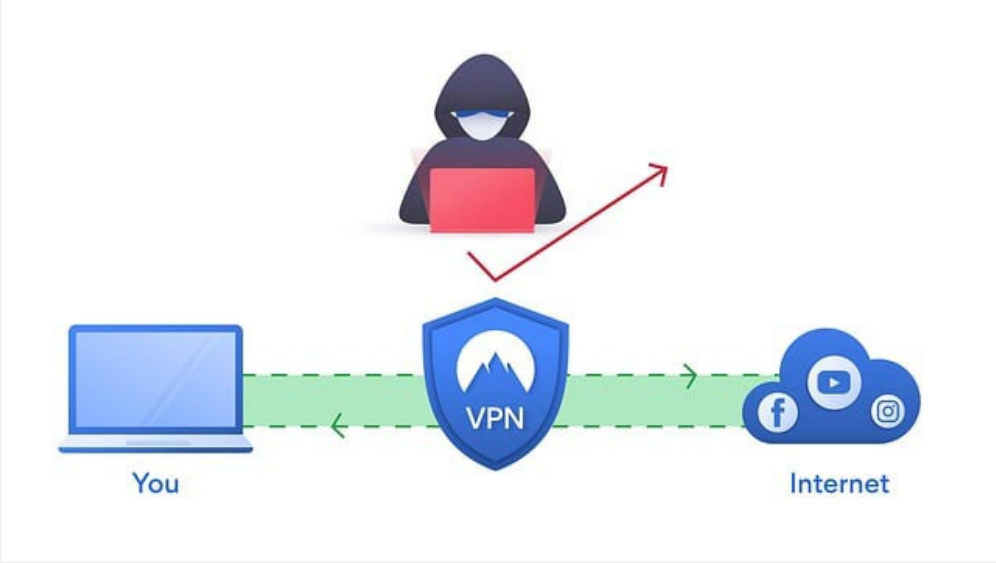
- SSID-Bezeichnung ändern (Hinweise auf Router-Modell)
- Mindestens WPA2 mit starkem Passwort verwenden (20-30 Zeichen, Worte verketten)
- Abweichendes, starkes Passwort für Admin-Zugang (Konfiguration Router Einstellungen) verwenden
- Automatische (Firmware-)Updates aktivieren, Router austauschen, die keine Updates mehr bekommen
- Gastnetz einrichten (z. B. auch für IoT / Smart-Home Geräte)
- WPS-Funktion nur bei Bedarf aktivieren



UNIVERSITÄT BIELEFELD

Dienste im Universitätsnetz

- Im Homeoffice oder auf Dienstreise: Bei der Nutzung von Uni-Diensten immer eine VPN-Verbindung verwenden, auch wenn diese technisch nicht zwingend notwendig ist (z. B. E-Mail, Sciebo etc.)
- VPN bietet zusätzliche Sicherheit gegen ungewolltes mitlesen und verändern von Daten
- IT-Geräte befinden sich hinter der Uni-Firewall und sind damit nicht „nackt“ im Internet



UNIVERSITÄT BIELEFELD

Sicherer Browser

- Auf dem aktuellen Stand halten (Updates automatisch installieren)
- Datensparsame Suche nutzen (Duckduckgo, Startpage)
- Plugins für mehr Sicherheit / Datensparsamkeit: z .B. NoScript, uBlock Origin, HTTPS everywhere, Privacy Badger (Disclaimer: Plugins können zu Funktions- und Komforteinbußen führen ;-))
- Grundsätzlich Plugins sparsam nutzen (erheben ebenfalls Daten, Negativ-Beispiele WoT, Ghostery), regelmäßig Bestand prüfen und nicht benötigte löschen
- Berechtigungen von Websites prüfen (meist unter „Datenschutz und Sicherheit“)
- Passwörter (besser) nicht im Browser speichern (wenn, dann nur mit gutem Masterkennwort)

UNIVERSITÄT BIELEFELD

„Anonym“ im Netz

- Echte Anonymität nur sehr schwer herstellbar
- „Privates Fenster“ im Browser ist nicht zur Anonymisierung geeignet
- VPN-Dienst verhindert, das eigene IP-Adresse öffentlich sichtbar ist
- Browser für TOR-Netzwerk („Darknet“) gewährleistet deutlich höhere Anonymität (auch hier nicht 100%)
- Weiterführende Informationen: https://www.bleib-virenfrei.de/it-sicherheit/schutz-der-privatsphaere/

UNIVERSITÄT BIELEFELD

Sichere E-Mail Nutzung

UNIVERSITÄT BIELEFELD

E-Mail Sicherheit – alles auf einer Postkarte?

- Versand an Uni-E-Mail Adressen (@uni-bielefeld.de): Gut geschützt, Daten verlassen Netz der Uni nicht
- Versand an externe E-Mail Adressen (z. B. an @web.de): Schutz auf **Postkartenniveau** (jeder „Zusteller“ kann den Inhalt sehen)
- Versand von vertraulichen Informationen: Verschlüsselung nutzen (siehe nächste Folien)

- **Wichtiger Hinweis**: Eine permanente, automatische Weiterleitung von dienstlichen E-Mails an externe Anbieter (web.de, gmail.com etc.) ist nicht gestattet

UNIVERSITÄT BIELEFELD

E-Mail Verschlüsselung mit „Zertifikat“

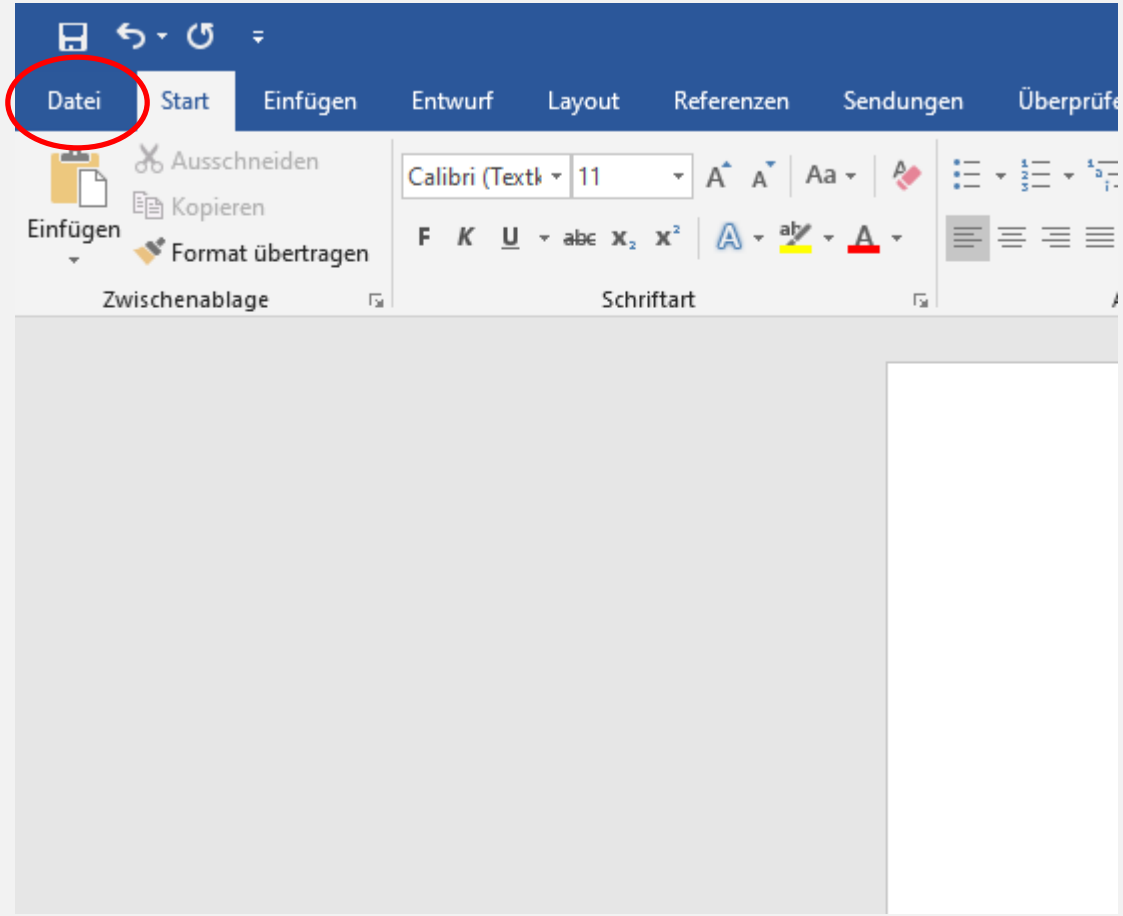
- S/MIME-Zertifikat (digitales Schlüsselpaar) unterstützt digitales **unterschreiben** („signieren“) UND **verschlüsseln** von E-Mails
- Sog. „Public-Private-Key-Verfahren“ – die empfangende Seite muss zur Entschlüsselung ebenfalls über ein S/MIME-Zertifikat verfügen
- Zertifikat kann beim BITS beantragt werden
- Zertifikat wird im E-Mail Programm hinterlegt und kann bei Bedarf zur Verschlüsselung der gesamten E-Mail verwendet werden (Inhalt und Anhang)

UNIVERSITÄT BIELEFELD

Verschlüsselung von Daten

UNIVERSITÄT BIELEFELD

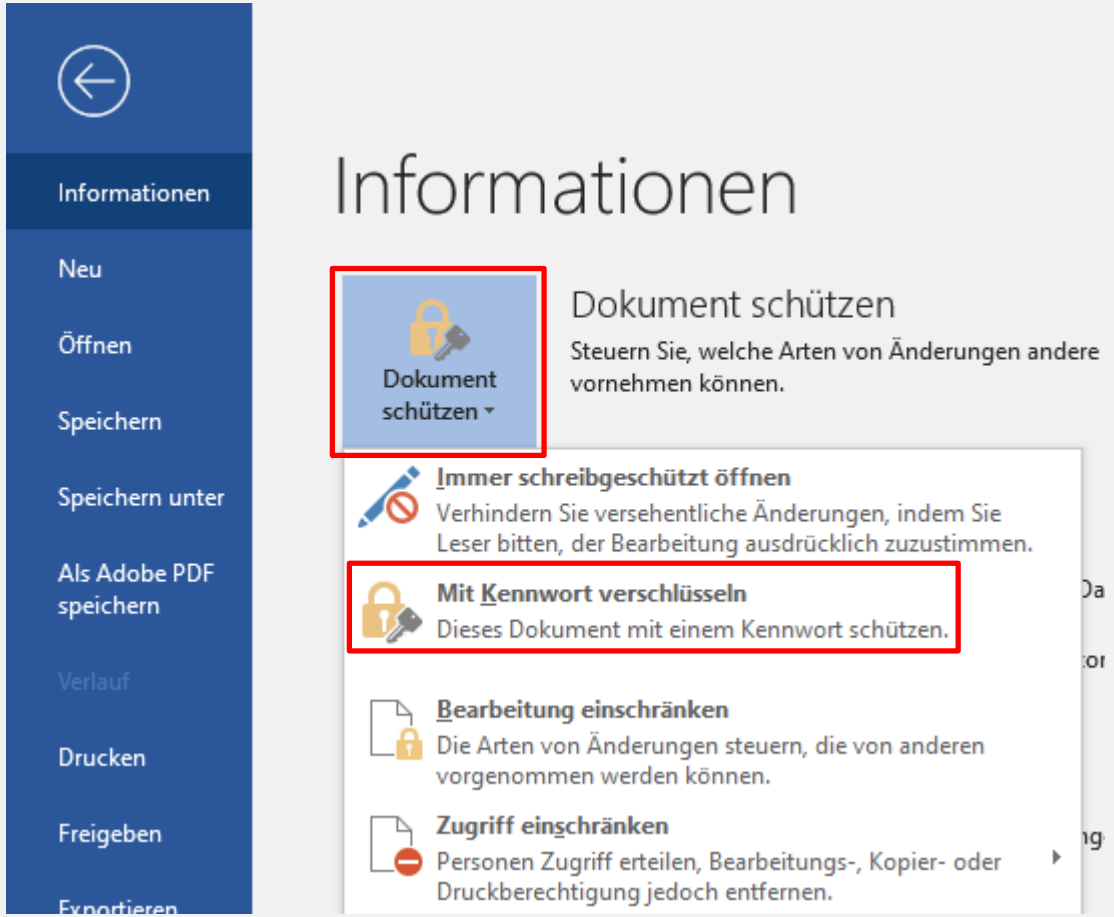
Einzelne Office Dateien verschlüsseln



- Einfache Verschlüsselung von einzelnen Microsoft-Office-Dateien z. B. um diese per E-Mail zu versenden
- Wichtig: Ausschließlich aktuelle Office-Formate verwenden (z. B. .docx).

UNIVERSITÄT BIELEFELD

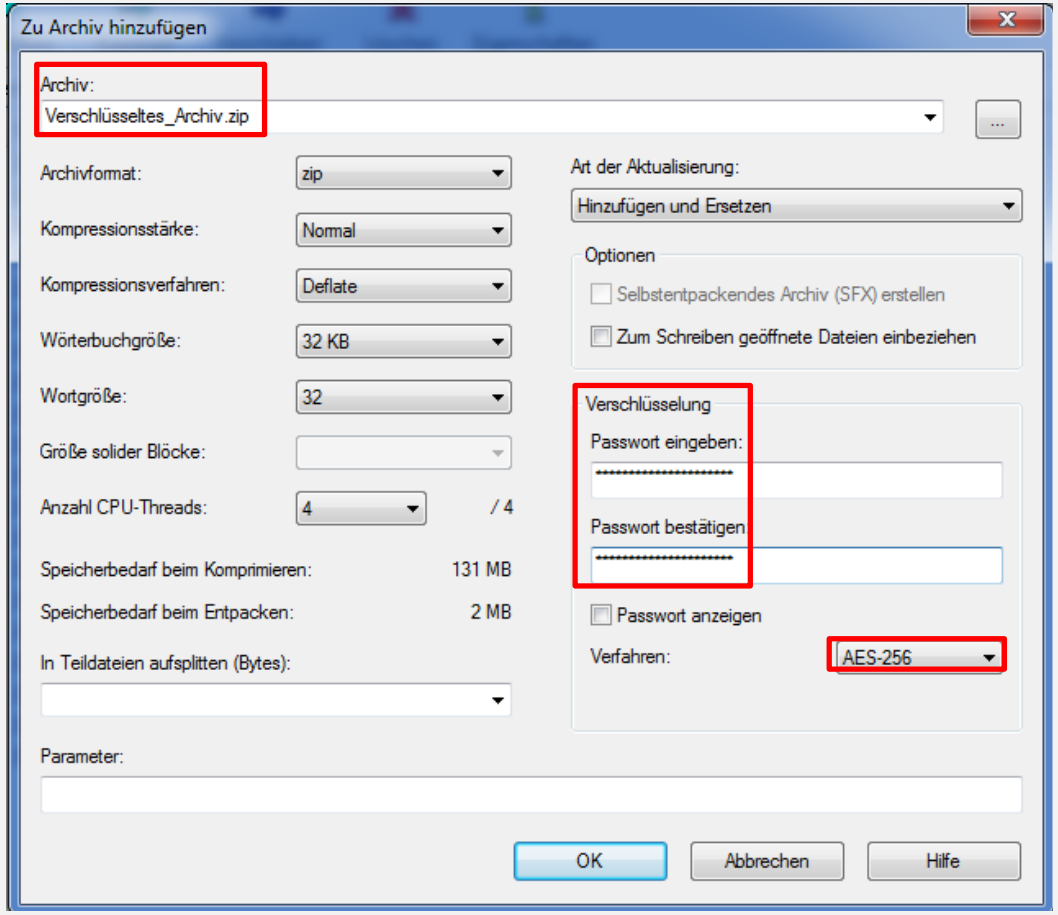
Einzelne Office Dateien verschlüsseln



- Einfache Verschlüsselung von einzelnen Microsoft-Office-Dateien z. B. um diese per E-Mail zu versenden
- Wichtig: Ausschließlich aktuelle Office-Formate verwenden (z. B. .docx).

UNIVERSITÄT BIELEFELD

Mehrere Dateien einfach verschlüsseln



- Einfache Verschlüsselung von mehreren Dateien durch Erstellung von verschlüsselten Archiven
- Webseite: https://www.7-zip.de/

UNIVERSITÄT BIELEFELD

Verschlüsselung – das ist zu beachten

- Verschlüsselung hat viele **Vorteile** – birgt aber auch **Risiken**. Müssen abgewogen und Verschlüsselung mit Augenmaß eingesetzt werden.
- Sicherheit der Verschlüsselung hängt von der Qualität des Schlüssels - u.a. einem ausreichend starken Passwort - ab
- Wichtig: Den Schlüssel sicher hinterlegen – **ohne Schlüssel sind die Daten verloren**

UNIVERSITÄT BIELEFELD

Akute Bedrohung: Phishing

UNIVERSITÄT BIELEFELD

Phishing – da fällt doch keiner drauf rein!

E-Mails, die ein legitimes Anliegen vorgaukeln

- Gefälschte Absender (irgendwas@uni-bielefeld.de)
- Namen von Beschäftigten (PEVZ!) oder Uni-Logos
- Links die angeblich auf die Uni-Webseite führen

Angreifer arbeiten oft mit „Angst und Schrecken“:

- Ihr E-Mail Postfach ist voll
- Es gibt ein kritisches Update
- Wer nichts tut, hat keinen Zugriff mehr

UNIVERSITÄT BIELEFELD

Phishing – sag mal bitte Dein Passwort…

Von: UniversitätBielefeld Universität© [customerservice.dept@uni-bielefeld.de]
An: miriam.giesguth@gmx.de
Cc:
Betreff: Sie haben 1 ungelesene Nachricht !!!

Universität Bielefeld

Lieber Student/Mitarbeiter,

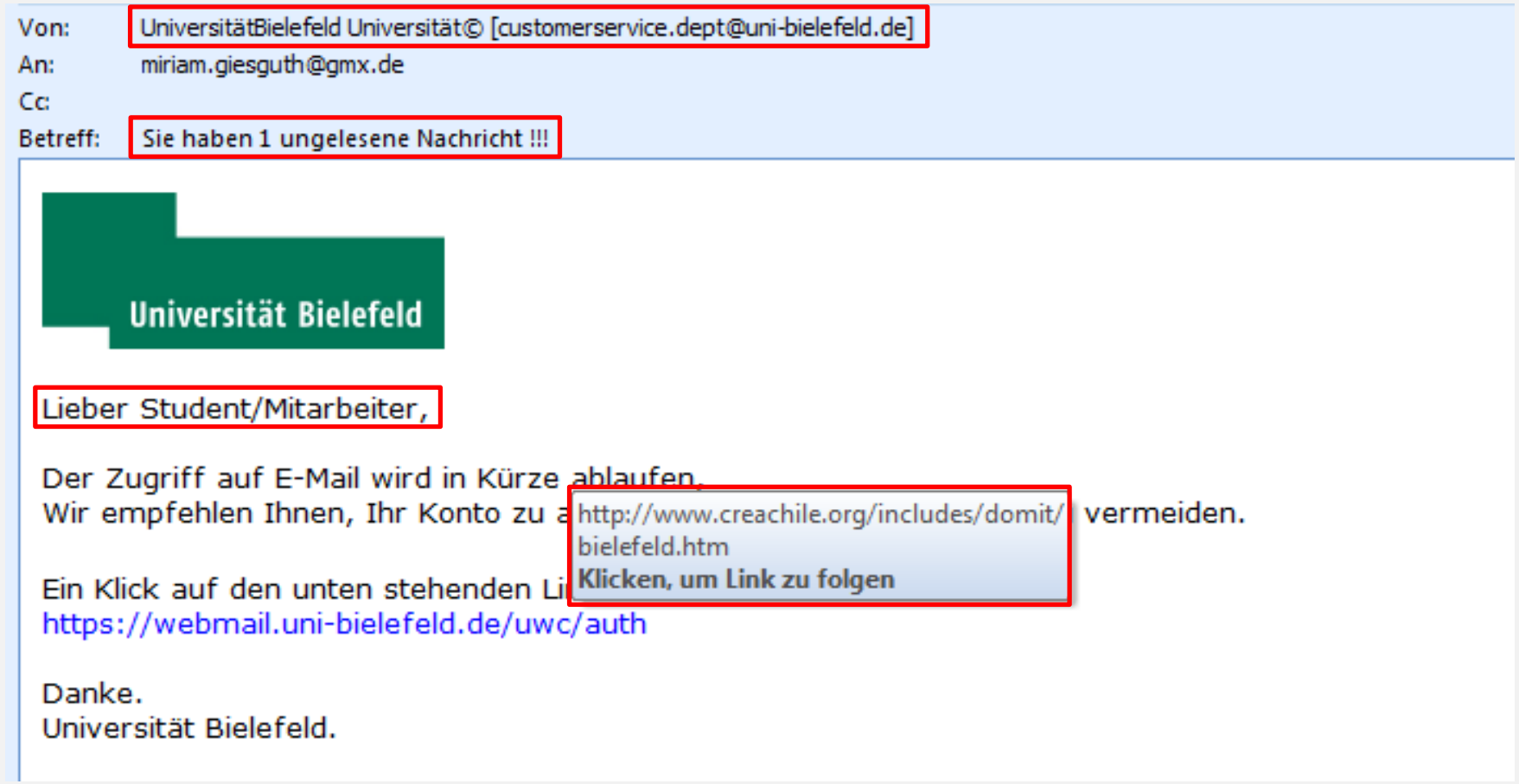
Der Zugriff auf E-Mail wird in Kürze ablaufen,
Wir empfehlen Ihnen, Ihr Konto zu aktualisieren, um die Aussetzung zu vermeiden.

Ein Klick auf den unten stehenden Link um Ihr Konto zu aktualisieren.
https://webmail.uni-bielefeld.de/uwc/auth

Danke.
Universität Bielefeld.

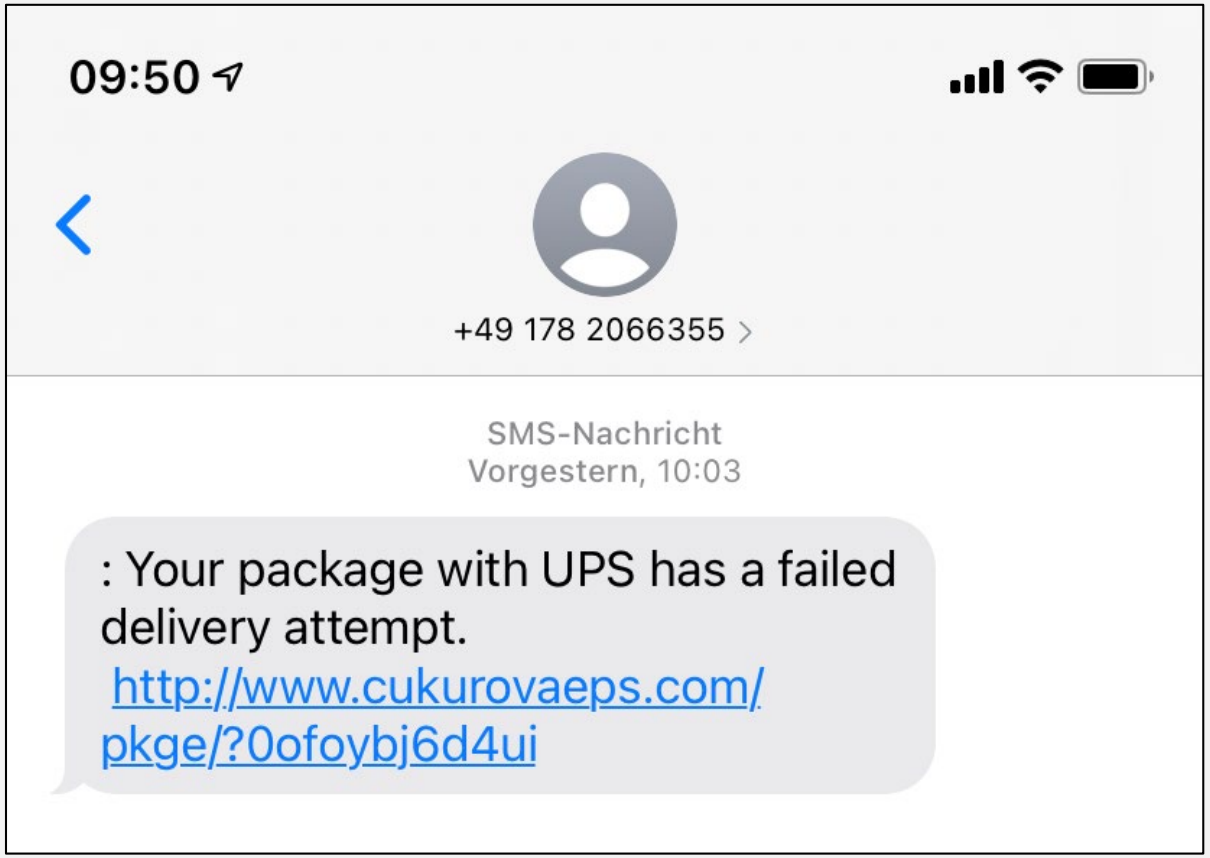
UNIVERSITÄT BIELEFELD

Phishing – jetzt kennt ****** Dein Passwort…



UNIVERSITÄT BIELEFELD

Smishing – Passworte per SMS angeln

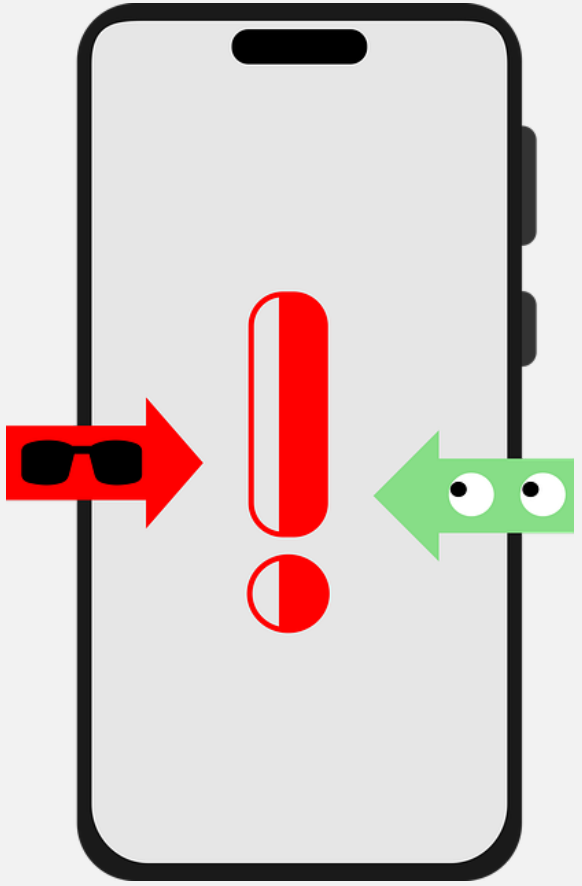


- Phishing per SMS oder andere Messenger (WhatsAppp, Signal, Telegram, Threema)
- Gleiche manipulative „Tricks“ wie bei Phishing

UNIVERSITÄT BIELEFELD

Phishing stoppen

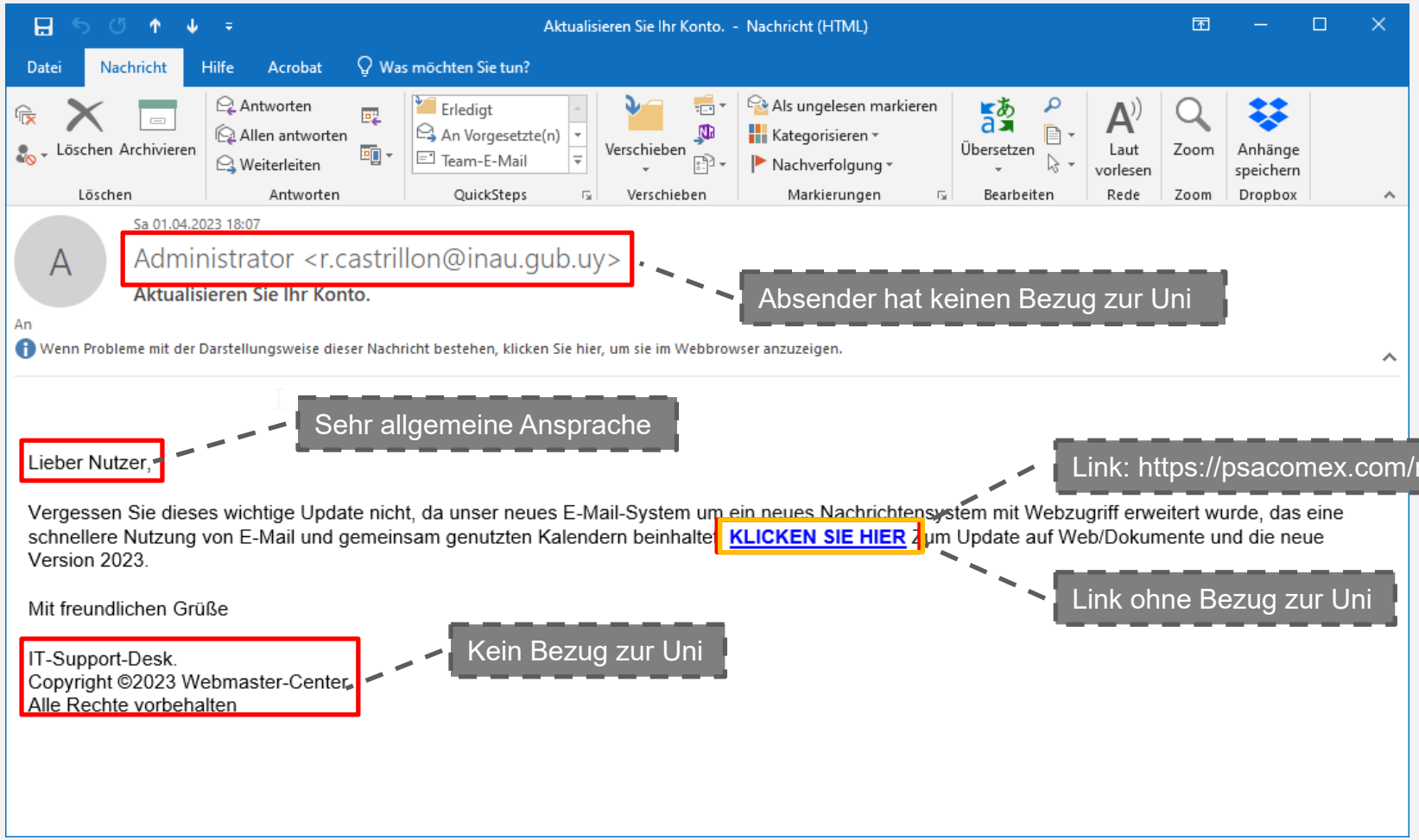
- Absenderadresse von E-Mail prüfen (kann sehr einfach gefälscht werden)
- Plausibilität der Inhalte Prüfen (Anleitung hier): Ist die E-Mail überhaupt relevant? Erwarte ich einen Anhang? Weitere Möglichkeit: Telefonisch beim vermeintlichen Absender nachfragen
- Links vor dem Öffnen prüfen (Mauszeiger länger auf dem Link stehen lassen)
- Phishing-Mails löschen, ggf. Service Desk des BITS informieren (servicedesk@uni-bielefeld.de)



- Übung macht die Meister*in: https://nophish-quiz.secuso.org/

UNIVERSITÄT BIELEFELD

Phishing-Beispiel zum üben



UNIVERSITÄT BIELEFELD

Beispiel: So „einfach“ geht social engineering

https://www.youtube.com/watch?v=fHhNWAKw0bY

UNIVERSITÄT BIELEFELD

Was tun wenn doch etwas passieren sollte?

UNIVERSITÄT BIELEFELD

Quiz: Was tun wenn doch etwas passiert?

a) Ich arbeite weiter und hoffe, dass sich das Problem von selber erledigt

b) Ich arbeite mit einem anderen, nicht betroffenen IT-System weiter

c) Ich versuche das Problem selber zu lösen – ist ja schließlich MEIN Problem

d) Ich frage Kolleg*innen, die sich damit besser auskennen

e) Ich stelle die Arbeit am betroffenen System ein und trenne es vom Netzwerk

f) Ich informiere meine vorgesetzte Person

g) Ich rufe meine EDV-Betreuung an

h) Ich rufe das BITS an

Spoiler: Es gibt mehr als nur eine richtige Antwort :-)

UNIVERSITÄT BIELEFELD

DAS tun, wenn doch etwas passiert!

a) Ich stelle die Arbeit am betroffenen System ein und trenne es vom Netzwerk (Kabel raus, Wlan aus)

b) Ich rufe das BITS an (-6000) (kann nie schaden)

c) Ich rufe meine EDV-Betreuung an (bei Fakultäten und Einrichtungen meistens richtig)

d) Ich informiere meine vorgesetzte Person

UNIVERSITÄT BIELEFELD

DAS tun, wenn doch etwas passiert!

Inhalt der Meldung

- Wer ruft an?
- Was ist passiert bzw. was wurde beobachtet?
- Wann ist es passiert (Datum, Uhrzeit)?
- Wo ist es passiert (Ort)?

Für Rückfragen erreichbar bleiben

UNIVERSITÄT BIELEFELD

Passwörter

UNIVERSITÄT BIELEFELD

Passwörter sicher gestalten – und nutzen

Aufbau

- Mindestlänge 12 Zeichen (je länger desto besser)
- Buchstaben, Zahlen und Sonderzeichen mischen
- Keine Tastatur-Muster, keine bekannten Wörter (Wörterbuchangriffe)

Verwendung

- Niemals weitergeben oder „teilen“
- Anderer Dienst = anderes Passwort
- Wenn notieren dann so hinterlegen wie viel Bargeld oder die PIN der Bankkarte – am besten einen Passwort Manager/Safe nutzen (KeePass, Lastpass, RoboForm etc.)

UNIVERSITÄT BIELEFELD

Drei Schritte zum sicheren Passwort

1. Passwort-Merk-Satz bilden / finden. Beispielsweise:

Mein komplexes Passwort ist vor bösen Buben und Mädels ziemlich sicher!

UNIVERSITÄT BIELEFELD

Drei Schritte zum sicheren Passwort

2. Anfangsbuchstaben sammeln

Mein komplexes Passwort ist vor bösen Buben und Mädels ziemlich sicher!

UNIVERSITÄT BIELEFELD

Drei Schritte zum sicheren Passwort

2. Anfangsbuchstaben sammeln

MkPivbBuMzs

UNIVERSITÄT BIELEFELD

Drei Schritte zum sicheren Passwort

3. Zahlen und Sonderzeichen sammeln

Mein komplexes Passwort 1st vor bösen Buben und Mädels ziemlich $icher!

UNIVERSITÄT BIELEFELD

Drei Schritte zum sicheren Passwort

3. Zahlen und Sonderzeichen sammeln

MkP1vbBuMz$!

UNIVERSITÄT BIELEFELD

Drei Schritte zum sicheren Passwort

Ergebnis: Leicht zu erinnerndes und sicheres Passwort

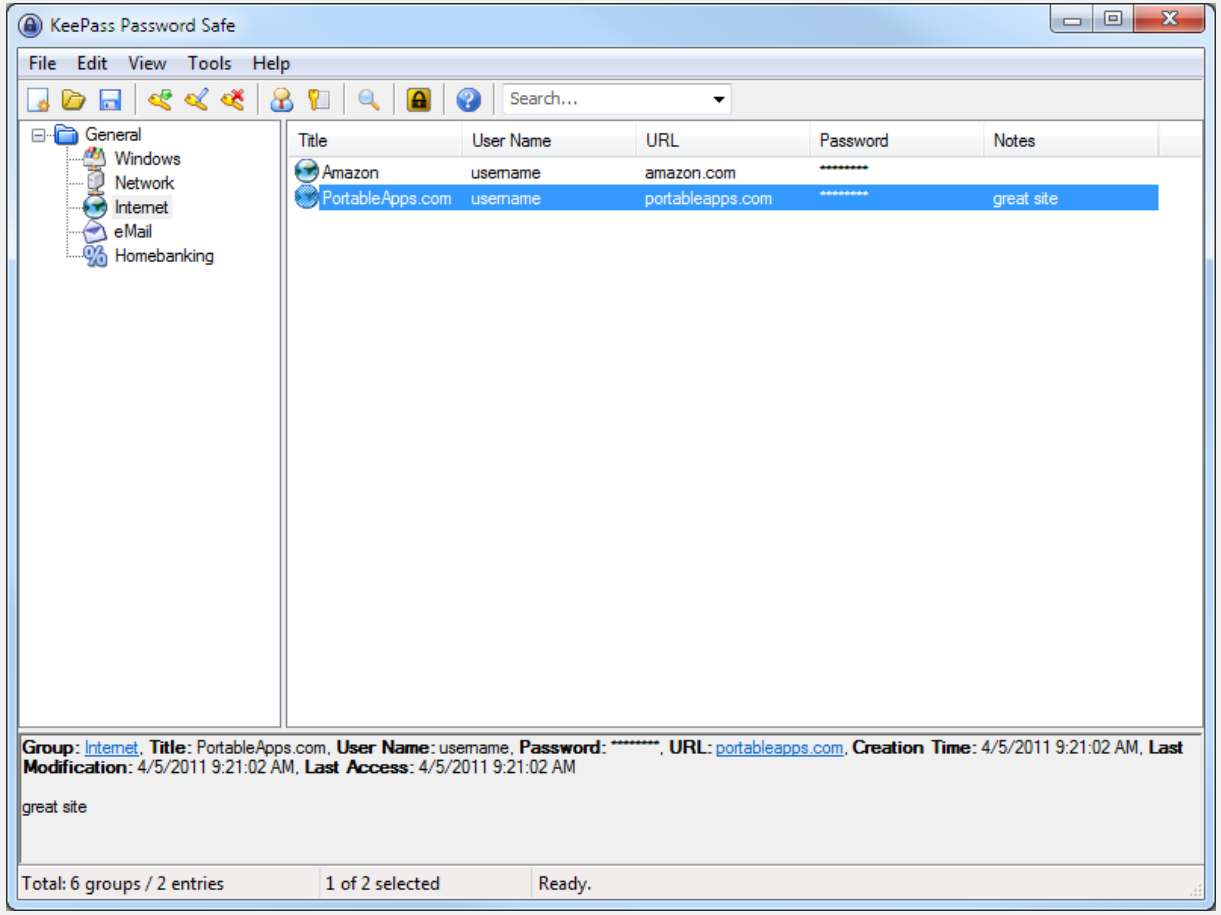
MkP1vbBuMz$!

Merkhilfe aufschreiben ist möglich: Böse Buben = Uni E-Mail Zugang

Noch besser: Passwort Manager / Tresor nutzen!

UNIVERSITÄT BIELEFELD

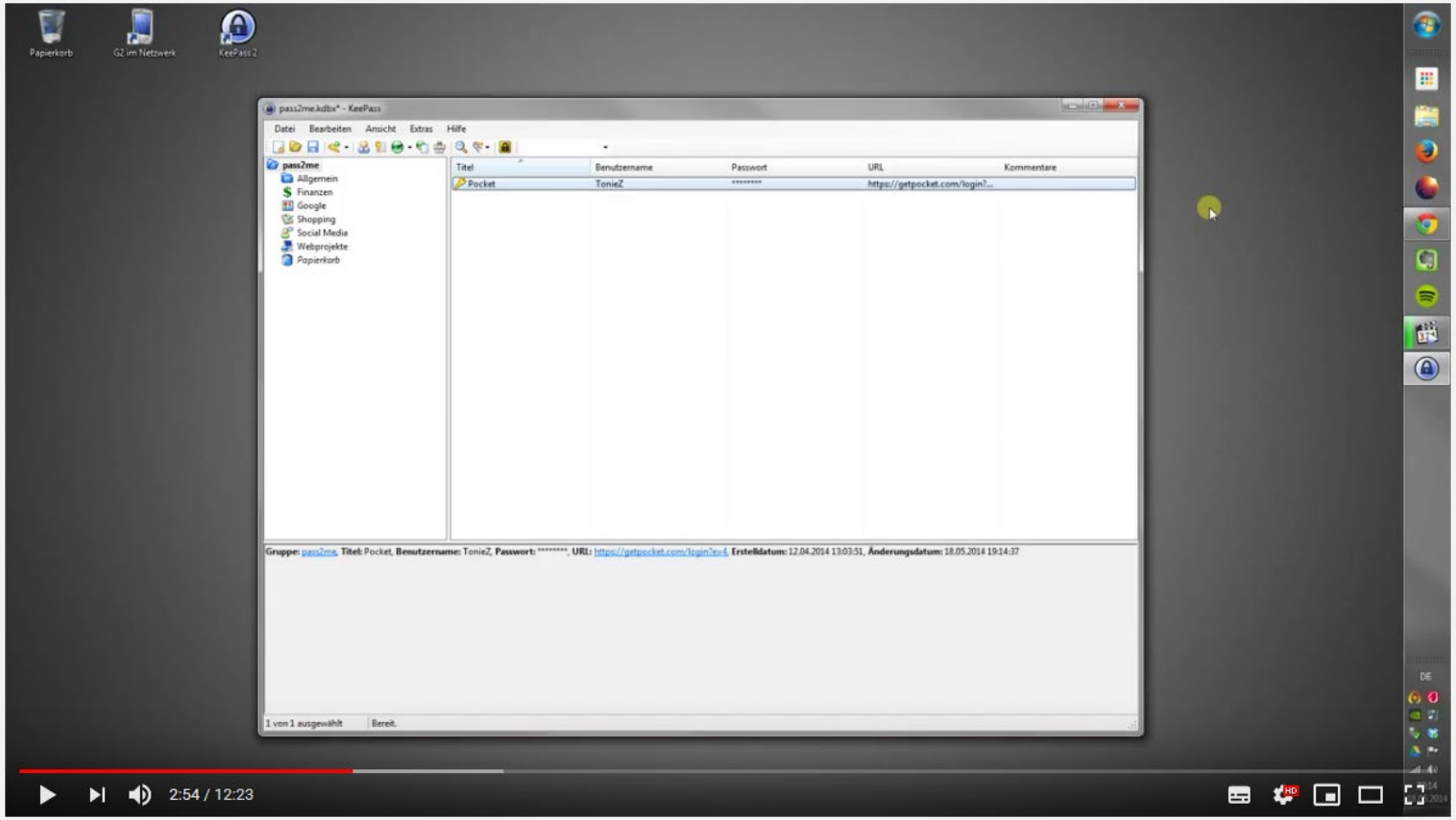
Passwort-Tresor: Sichere Merkhilfe



- Ein Passwort für alle Zugänge
- Viele gute, teilweise kostenlose Angebote: KeePass (XC), Roboform, 1Password, Password Safe etc.
- Von der Uni wird KeePass empfohlen (kostenlos, Open Source)
- Passwort Manager im Browser sollten (wenn überhaupt) ebenfalls nur mit einem guten Masterpasswort genutzt werden!

UNIVERSITÄT BIELEFELD

KeePass – einfach erklärt



https://www.youtube.com/watch?v=gJNLZJ2i7SA

UNIVERSITÄT BIELEFELD

Zusammenfassung

UNIVERSITÄT BIELEFELD

Das kann jeder*r dienstlich tun

- Aufmerksam & informiert bleiben, Daten, Türen und Computer „abschließen“
- Nichts vertrauliches oder wertvolles frei herumliegen lassen („Clean Desk Policy“)
- Für dienstlich Daten Uni-Dienste Nutzen (z. B. Netzlaufwerke, Sciebo, Teamchat etc.)
- Gute Passwörter verwenden (Passwortmanager) und diese nie teilen/weitergeben
- E-Mails mit Vorsicht genießen (Absender, Inhalt, Links, Anhänge vor dem öffnen prüfen)
- Auf permanente E-Mail Weiterleitung zu externen Anbietern (Google, web.de etc.) verzichten
- Merkwürdiges Verhalten des Rechners/Sicherheitsvorfälle melden (EDV-Betreuung / Vorgesetze*r)
- Auf dem aktuellen Stand bleiben mit Hinweisen und Fortbildungen
- Gehirn zusammen mit dem Computer einschalten und lieber einmal zu viel fragen…

UNIVERSITÄT BIELEFELD

Ansprechpersonen

UNIVERSITÄT BIELEFELD

Kontakt

Stabsstelle Informationssicherheit

Michael Sundermeyer / Roman Elenbogen

Raum: T6/T7-235 | Durchwahl: 3032 / 3187

informationssicherheit@uni-bielefeld.de

Webseite: http://www.uni-bielefeld.de/informationssicherheit

UNIVERSITÄT BIELEFELD

Weitere Ansprechpersonen

- Behördliche Datenschutzbeauftragte (→ PEVZ)
- Datenschutz- und Informationssicherheitskoordinator*innen (DISK) (→ PEVZ)
- EDV-Betreuungen (→ PEVZ)
- BITS Service Desk / BITS Hotline (→ PEVZ)

UNIVERSITÄT BIELEFELD

Vielen Dank für Eure Aufmerksamkeit.

Fragen?