

„Digitale Selbstverteidi- gung“ für Forschende / Lehrende

PEP-Angebot
22.06.2022

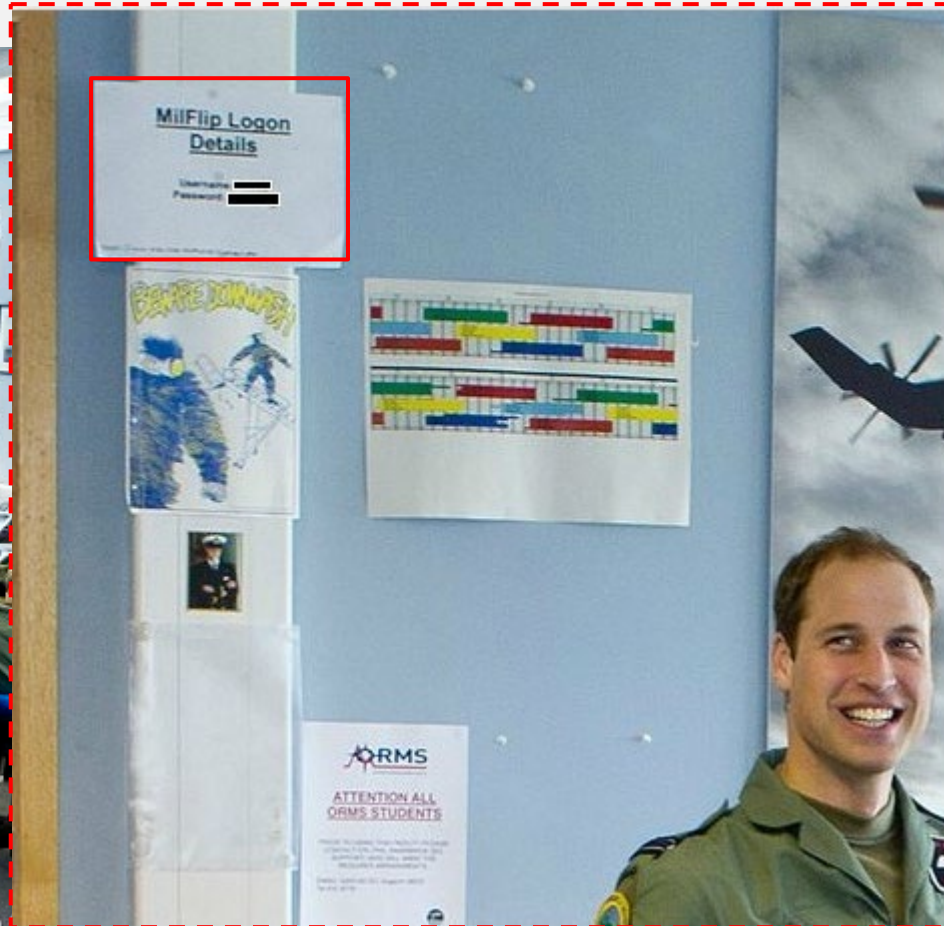
Michael Sundermeyer
Informationssicherheitsbeauftragter
Universität Bielefeld



Fragen im Vorfeld

- Tools zur sicheren Datenübermittlung an Dritte
- Verschlüsselungs-Tools für unterschiedliche Plattformen betrachten
- Einstellungen am Computer bzw. in Software um Daten bestmöglich zu schützen
- Sichere Alternativen zu „gängigen Programmen“

Royale Sicherheit von Informationen...



©Crown Copyright, 2012
www.dukeandduchessofcambridge.org

Worum geht's bei Informationssicherheit?

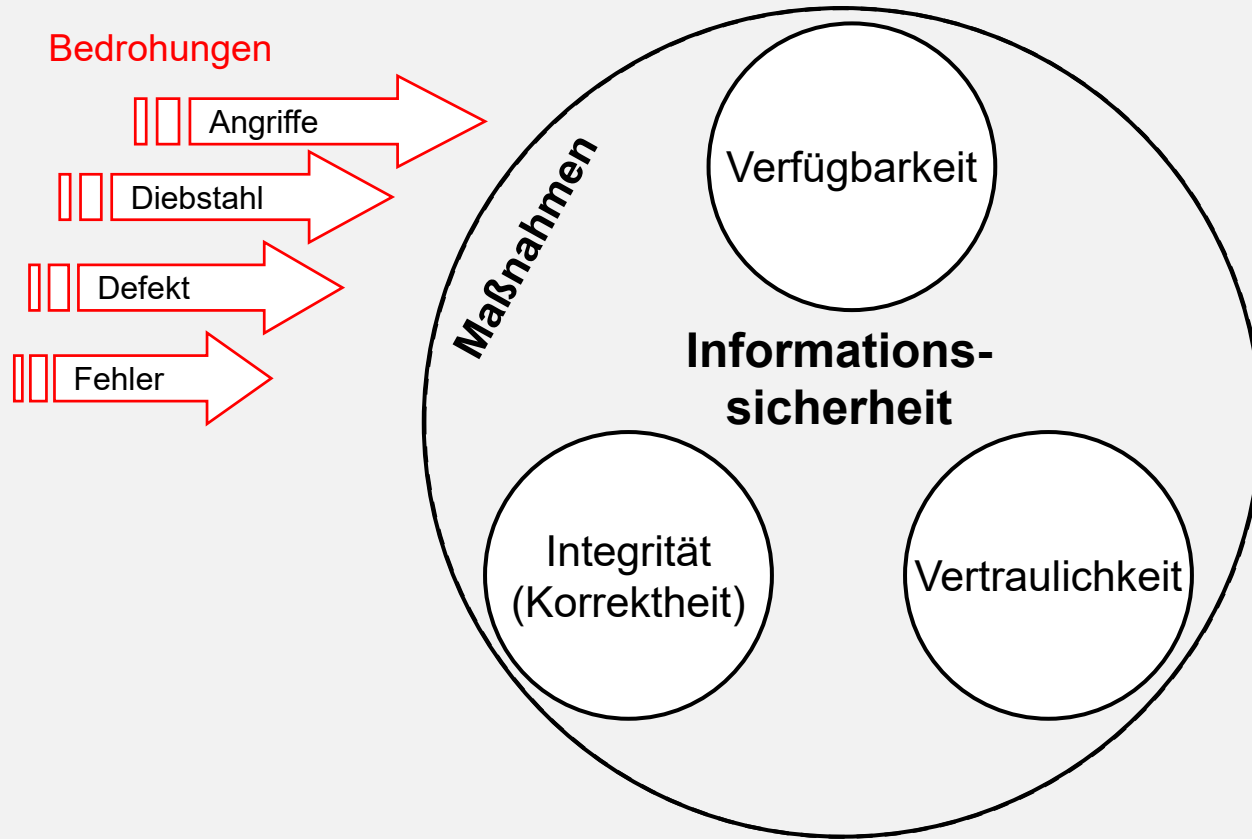
An der Universität

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

Privat

- Ziel: Meine wichtigen privaten Daten angemessen zu schützen
- Was schützen? App-Daten, Fotos, Kontakte, Verträge, Bewegungsdaten etc.
- Wovor schützen? Zerstörung, Manipulation und unbefugter Einsichtnahme

Ziele der Informationssicherheit



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

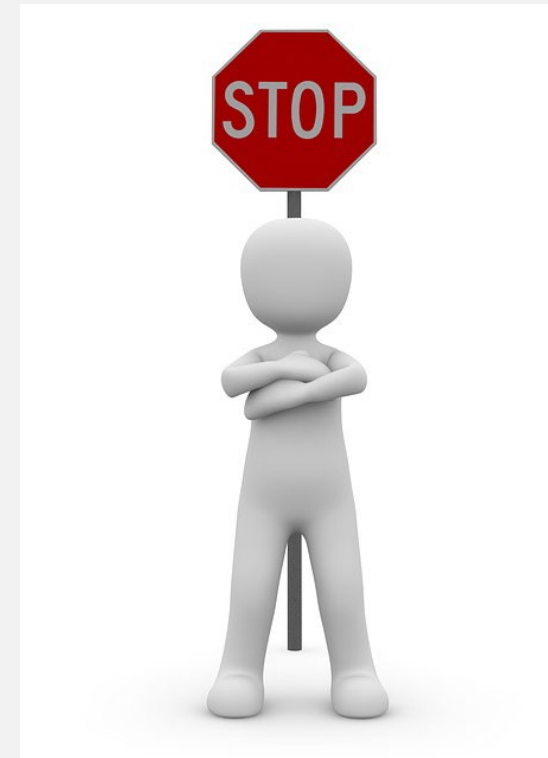
- Der Datenschutz hat das Ziel Daten, die personenbezogen sind d.h. einer natürlichen Person zugeordnet werden können zu schützen
- Der Datenschutz schützt die (gesetzlich geregelten) **Betroffenenrechte**

Informationssicherheit an der Universität



Die Uni ist doch sicher, oder?

- **Die wichtigste Firewall sitzt „vor dem Rechner“** – jede*r Einzelne trägt durch sicheres Verhalten zur Sicherheit der gesamten Universität bei!



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



Gute Presse, schlechte Presse...

Cyberangriff auf Berliner Hochschule

Datenklau an der HTW

Bei einer Attacke verschlüsselten Unbekannte Server der Hochschule. Die betroffenen Systeme wurden vorsorglich abgeschaltet. VON LARENA KLÖCKNER



03.05.2022, 16:41 Uhr

derStandard.at > Web > Netzpolitik > IT-Security

Noten, Budgetinfos: Massiver Datendiebstahl an Uni Graz

7. Jänner 2016, 17:09

Fast 50 GB Informationen sollen von Insider entwendet worden sein – Uni: Keine persönlichen Daten gestohlen

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.

5. Mai 2022, 11:09 Uhr, Moritz Tremmel/dpa

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



Online-Probleme an der Uni



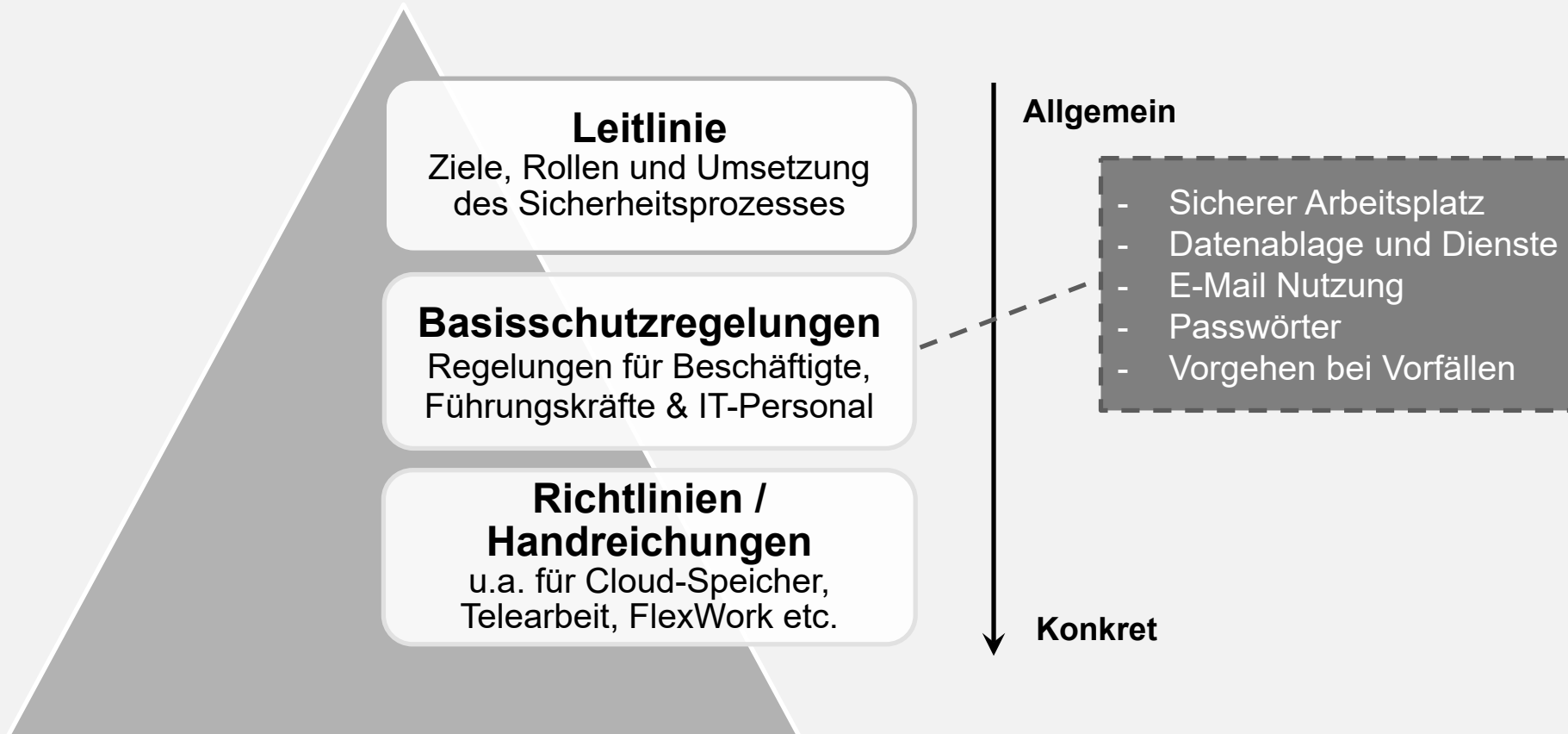
Die Bielefelder Uni hat aktuell große Rechner-Probleme. Ausgerechnet zum Semesterstart ist seit gestern u.a. das kommentierte Vorlesungs-verzeichnis EKW nicht mehr online abrufbar. Das Verzeichnis ist für die Studenten unverzichtbar, weil sie darin u.a. einsehen können, wo ihre nächsten Vorlesungen und 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.



Regelungen zur Informationssicherheit



Regelungen zur Informationssicherheit

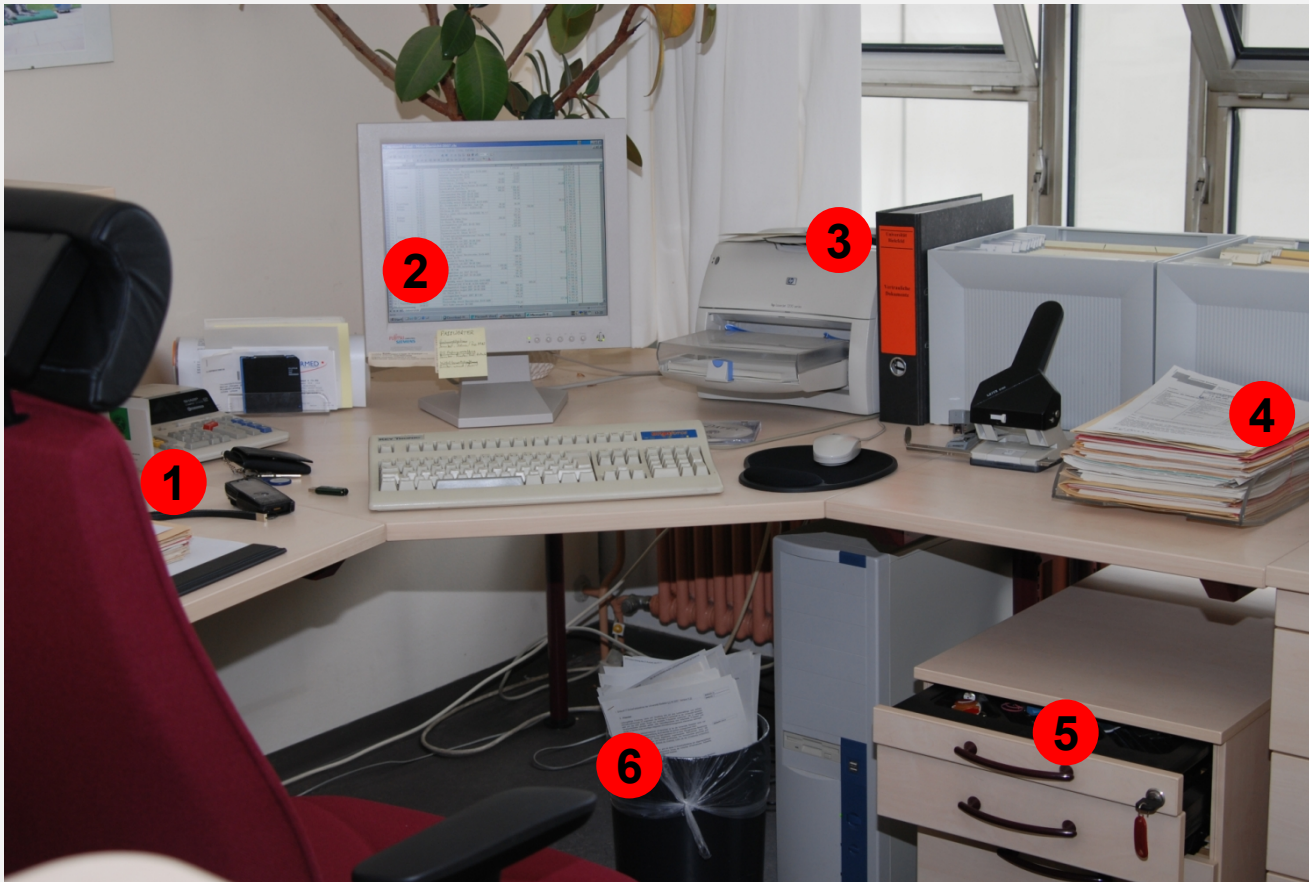


Alle Regelungen sind auf der Webseite der Stabsstelle Informationssicherheit abrufbar

Sicherer Arbeitsplatz



Sicherer Arbeitsplatz?



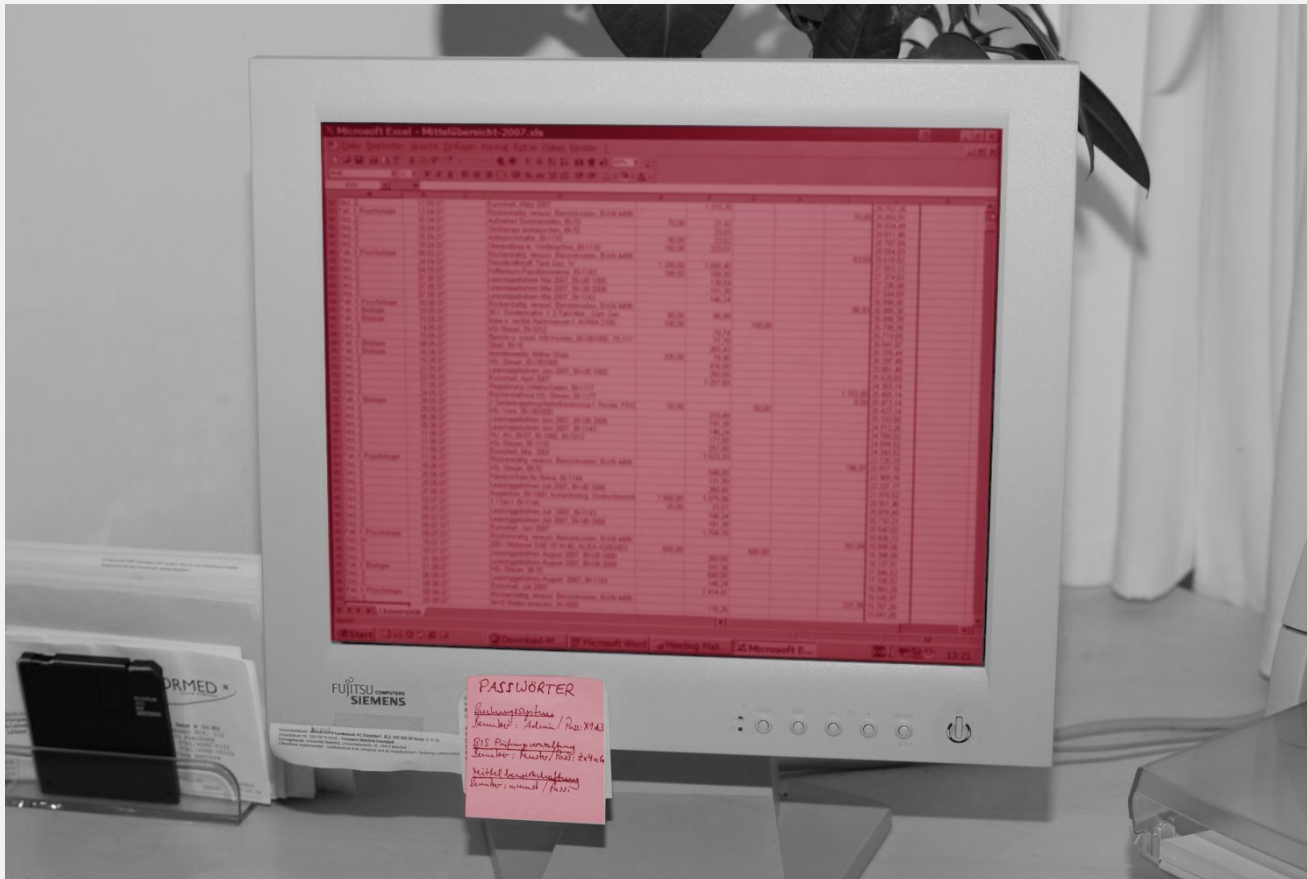
- Typischer Büro-Arbeitsplatz aus der Verwaltung
- Die Tür des Büro steht offen, es ist keine Person im Büro

„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.

„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

Freie Informationen I



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

Freie Informationen II



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

Freie Informationen III



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

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

Sichere IT-Geräte



Basisschutz

- 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 (App Store, Webseite der Hersteller) installieren (Risiko Sicherheitslücken, Trojaner)
 - Unnötige Software deinstallieren / löschen
 - Regelmäßig Datensicherungen (Backup) erstellen

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)

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 mehr benötigte deinstallieren
- Geräte ohne Updates möglichst austauschen, nicht mehr für kritische Funktionen nutzen (z. B. Onlinebanking)

„Sichere“ Dienste / Anbieter



IT im Wandel

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

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.
 - des BSI (Bundesamt für Sicherheit in der Informationstechnik) oder
 - auf Basis der internationalen Norm ISO 27001 (vgl. ISO 9001)
- Aber: Gute Zertifizierungen sind aufwändig und teuer, viele kleine Anbieter haben (noch) keine

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?

Sicherer Umgang mit Daten



Datenspeicherung

Risiko: IT-Gerät, Datenträger (Festplatte, USB Stick) gehen kaputt, ohne Datensicherung (Backup) sind Daten verloren

Maßnahmen:

- An der Uni: Dienstliche Daten immer auf Netzlaufwerken speichern (automatisches Backup!)
- Unterwegs: Kopie der Daten auf „Sciebo“ ablegen (www.sciebo.de - sichere Campuscloud mit bis zu 500 GB kostenlosem Speicher) – Einschränkungen beachten
- Keine dienstliche Daten bei externen Cloud-Anbietern wie Dropbox, Onedrive etc. speichern (vgl. Regelungen zur Informationssicherheit der Universität)

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 von Sciebo löschen, wenn diese nicht mehr benötigt werden

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

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.

Sicher am Netz / im Internet



Wlan-Router

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

Dienste im Universitätsnetz

- Im Homeoffice oder auf Dienstreise: Bei der Nutzung von Uni-Diensten immer eine VPN-Verbindung verwenden, auch wenn diese technisch nicht immer 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 hängen nicht „nackt“ im Internet

Sicherer Browser

- Auf dem aktuellen Stand halten (Updates automatisch installieren)
- Datensparsame „Google“-Suche nutzen (Duckduckgo, Startpage)
- Plugins für 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)

„Anonym“ im Netz

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

E-Mail-Sicherheit



E-Mail-Sicherheit

- Versand von Uni-E-Mail an Uni-E-Mail (@uni-bielefeld.de): Daten verlassen Uni-Server nicht
- Versand an externe E-Mail Adressen: Daten verlassen die Universität, Vertraulichkeit bei Übermittlung oft nur auf Postkartenniveau (jeder „Zusteller“ kann den Inhalt sehen)
- Externer Versand vertraulicher Informationen: S/MIME-Zertifikat oder andere Verschlüsselungsmechanismen nutzen

- Wichtiger Hinweis: Eine permanente, automatische Weiterleitung von dienstlichen E-Mails an externe Anbieter ist nicht gestattet

S/MIME-Zertifikat

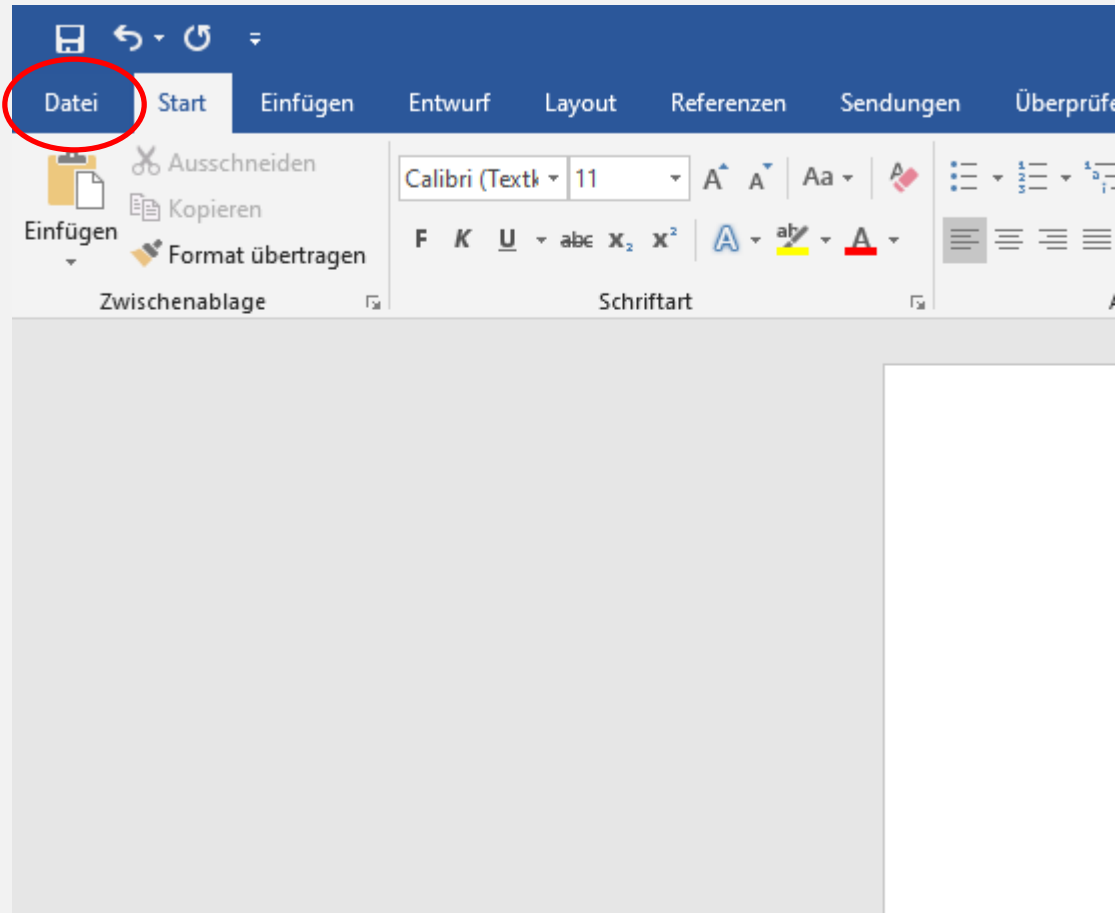
- Zertifikat unterstützt digitales unterschreiben („signieren“) UND verschlüsseln von E-Mails
- Sog. „Public-Private-Key-Verfahren“ – die Gegenseite muss ebenfalls über ein Zertifikat verfügen
- Zertifikat kann über das DFN beim BITS beantragt werden



Verschlüsselung von Daten



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).

Einzelne Office Dateien verschlüsseln

The screenshot shows the 'Informationen' ribbon in Microsoft Office. On the left, a blue sidebar contains navigation icons and labels: 'Informationen', 'Neu', 'Öffnen', 'Speichern', 'Speichern unter', 'Als Adobe PDF speichern', 'Verlauf', 'Drucken', 'Freigeben', and 'Exportieren'. The main area displays the 'Informationen' ribbon with the 'Dokument schützen' button highlighted by a red box. A dropdown menu is open, showing several options: 'Immer schreibgeschützt öffnen', 'Mit Kennwort verschlüsseln' (highlighted by a red box), 'Bearbeitung einschränken', and 'Zugriff einschränken'. Each option includes a brief description of its function.

Informationen

Dokument schützen

Steuern Sie, welche Arten von Änderungen andere vornehmen können.

Immer schreibgeschützt öffnen
Verhindern Sie versehentliche Änderungen, indem Sie Leser bitten, der Bearbeitung ausdrücklich zuzustimmen.

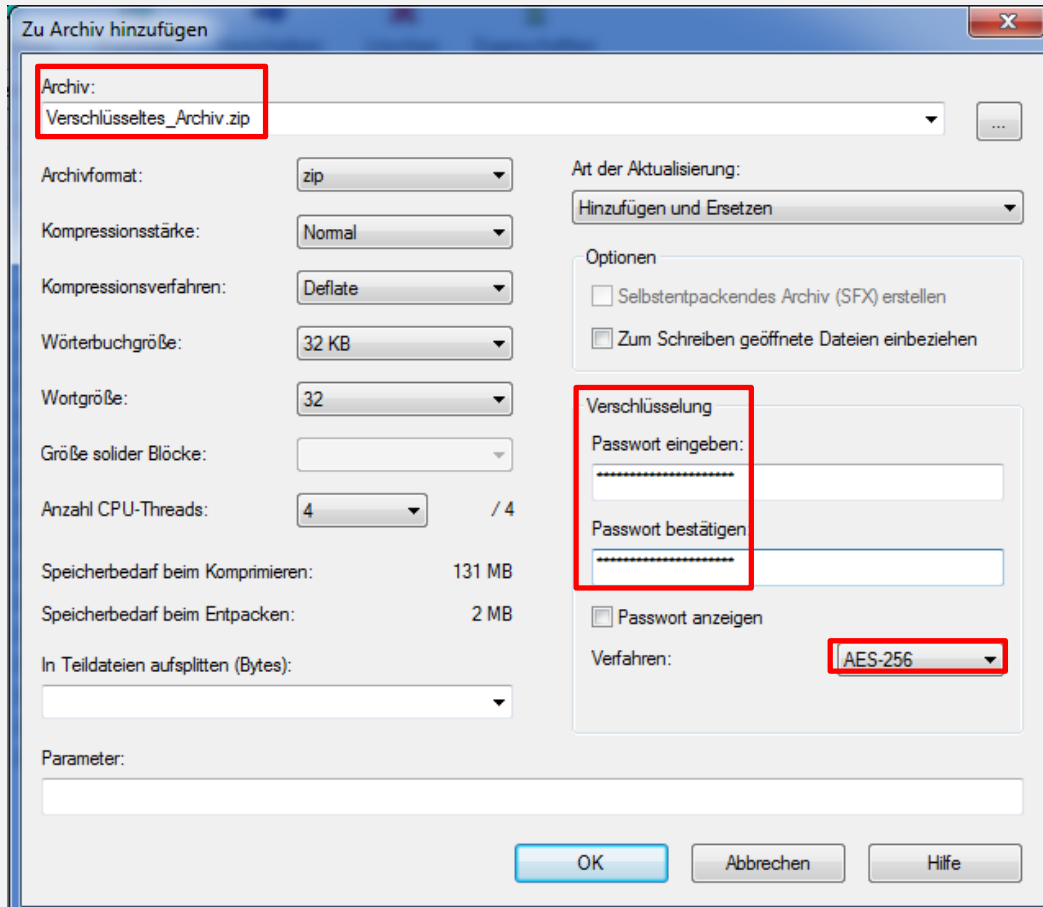
Mit Kennwort verschlüsseln
Dieses Dokument mit einem Kennwort schützen.

Bearbeitung einschränken
Die Arten von Änderungen steuern, die von anderen vorgenommen werden können.

Zugriff einschränken
Personen Zugriff erteilen, Bearbeitungs-, Kopier- oder Druckberechtigung jedoch entfernen.

- 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).

Mehrere Dateien einfach verschlüsseln



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

Noch mehr Komfort: Boxcryptor



- Einfache, transparente Verschlüsselung von Verzeichnissen z. B. auf Netzlaufwerken, Sciebo oder von anderem „Cloud-Speicher“
- Unterstützt unkompliziertes Arbeiten mit mehreren Personen (Gruppen)
- Unterstützt Notfallwiederherstellung bei einem Passwortverlust

Verschlüsselung – das ist zu beachten

- Verschlüsselung löst viele Fragen – birgt aber auch Risiken. Es empfiehlt sich, diese mit Augenmaß und nur dann einzusetzen, wenn notwendig
- Die Sicherheit von Verschlüsselung steht und fällt mit dem verwendeten „Schlüssel“ – z. B. einem ausreichend starken Passwort
- Wichtig: Den Schlüssel sicher hinterlegen – ohne Schlüssel sind die Daten verloren

Phishing & Social Engineering



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



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.

Phishing – jetzt kennt ***** 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,

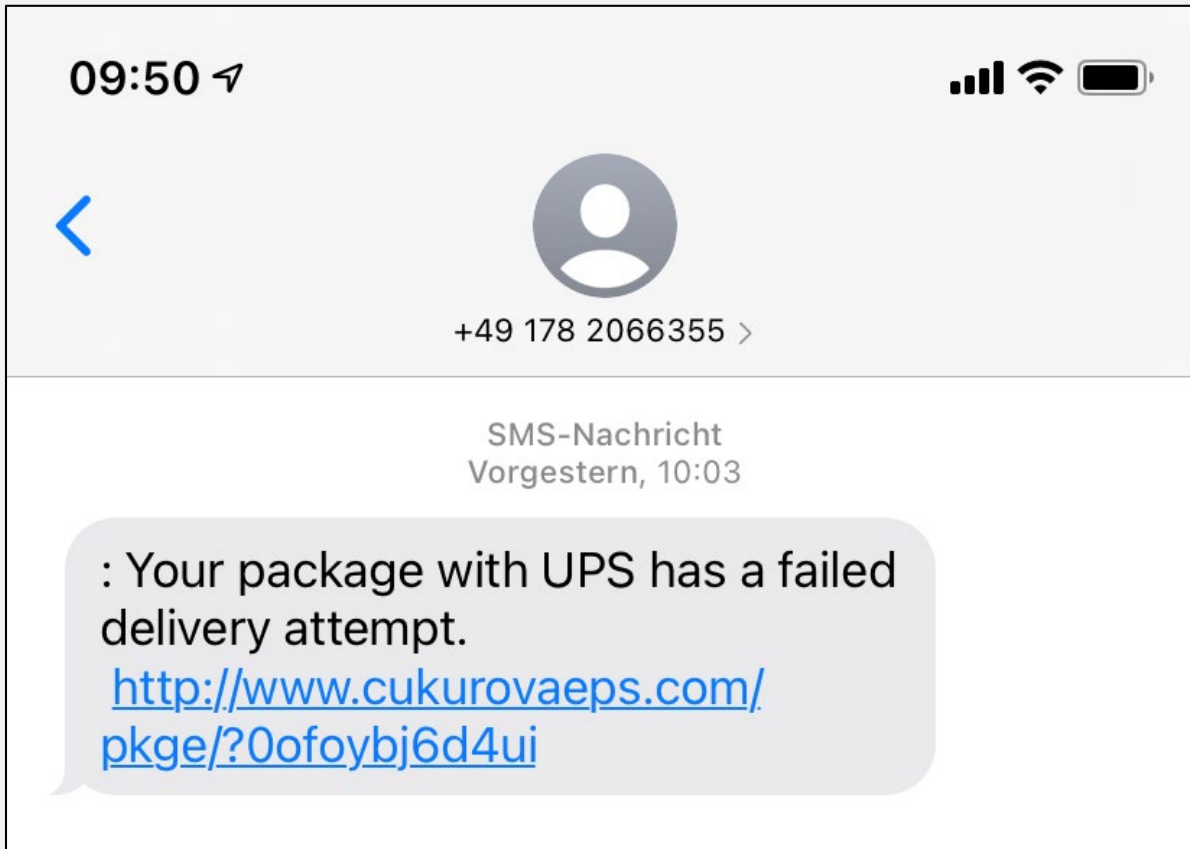
Wir empfehlen Ihnen, Ihr Konto zu <http://www.creachile.org/includes/domit/bielefeld.htm> vermeiden.

Ein Klick auf den unten stehenden Link **Klicken, um Link zu folgen**

<https://webmail.uni-bielefeld.de/uwc/auth>

Danke.
Universität Bielefeld.

Smishing – Passworte per SMS angeln



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

Phishing stoppen

- Absenderadresse prüfen (aber Achtung: Kann sehr einfach gefälscht werden!)
- Plausibilität der Inhalte prüfen: Ist der Inhalt überhaupt relevant? Erwarte ich z. B. einen Anhang? (Anleitung [hier](#)). 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 Meister*innen: <https://nophish-quiz.secuso.org/>

Social engineering

- Angreifende Person manipuliert auf zwischenmenschlicher Ebene
- Situationen oft per Telefon oder in direktem Kontakt
- Vergleichbare „Dynamik“ wie Phishing, durch (versteckte) Manipulation zu unsicheren bzw. unsachgemäßen Handlungen zu verleiten
 - Anderen „helfen“ wollen („mein Baby schreit gerade und ich bin total gestresst und hilflos“)
 - Sich geschmeichelt fühlen („mir wurde gesagt sie sind die beste Mitarbeiterin und richtige Person für mein Anliegen“)
 - Sich unter Druck fühlen („hier spricht die vorgesetzte Person“ bzw. „das ist dringend und wichtig“ !!)



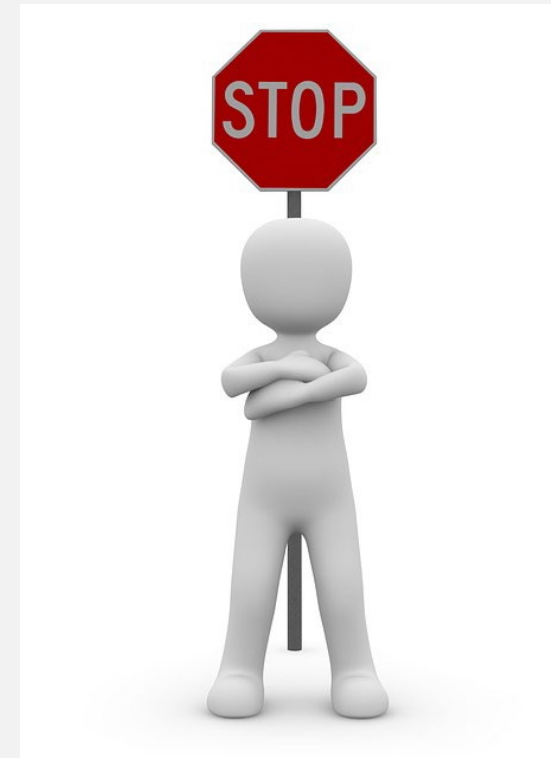
Beispiel: So „einfach“ geht social engineering



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

Social engineering stoppen

- Gesunde Skepsis als Grundhaltung
- Innere Plausibilitäts-Checkliste erstellen (macht das Sinn?)
- Auf Bauchgefühl vertrauen (da stimmt doch was nicht)
 - Dynamik unterbrechen („ist gerade schlecht, kann ich sie zurückrufen“)
 - Identität des Kontakts prüfen (Internet, sich über Telefonzentrale verbinden lassen)
 - Sich rückversichern (Rückfrage bei angeblicher Einrichtung, Firma)
 - Wichtig: Ereignisse weitergeben!



Was tun wenn **doch** etwas passiert

Umgehend die EDV-Betreuung informieren

- Zentralverwaltung: Service Desk (-6000)
- Fakultäten und Einrichtungen: EDV-Kontakt im PEVZ

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

VERHALTEN BEI IT-NOTFÄLLEN

 **Ruhe bewahren & IT-Notfall melden**
Lieber einmal mehr als einmal zu wenig anrufen!

 IT-Notfallrufnummer:
0521/106-6000

 Wer meldet?

 Welches IT-System ist betroffen?

 Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

 Wann ist das Ereignis eingetreten?

 Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen	Beobachtungen dokumentieren	Maßnahmen nur nach Anweisung einleiten
--	-----------------------------	--

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Passwörter



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.)

Drei Schritte zum sicheren Passwort

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

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

Drei Schritte zum sicheren Passwort

2. Anfangsbuchstaben sammeln

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

Drei Schritte zum sicheren Passwort

2. Anfangsbuchstaben sammeln

MkPivbBuMzs

Drei Schritte zum sicheren Passwort

3. Zahlen und Sonderzeichen sammeln

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

Drei Schritte zum sicheren Passwort

3. Zahlen und Sonderzeichen sammeln

MkP1vbBuMz\$!

Drei Schritte zum sicheren Passwort

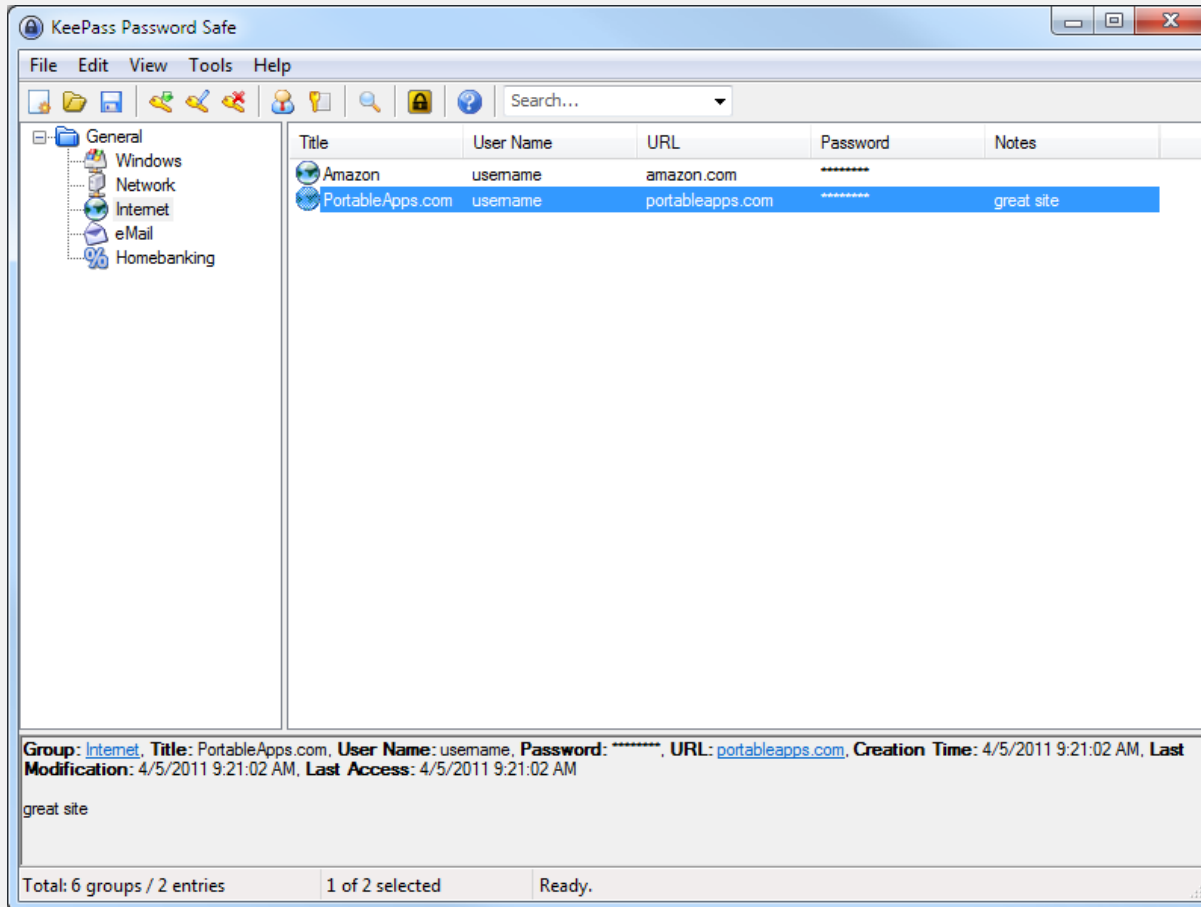
Ergebnis: Leicht zu erinnerndes und sicheres Passwort

MkP1vbBuMz\$!

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

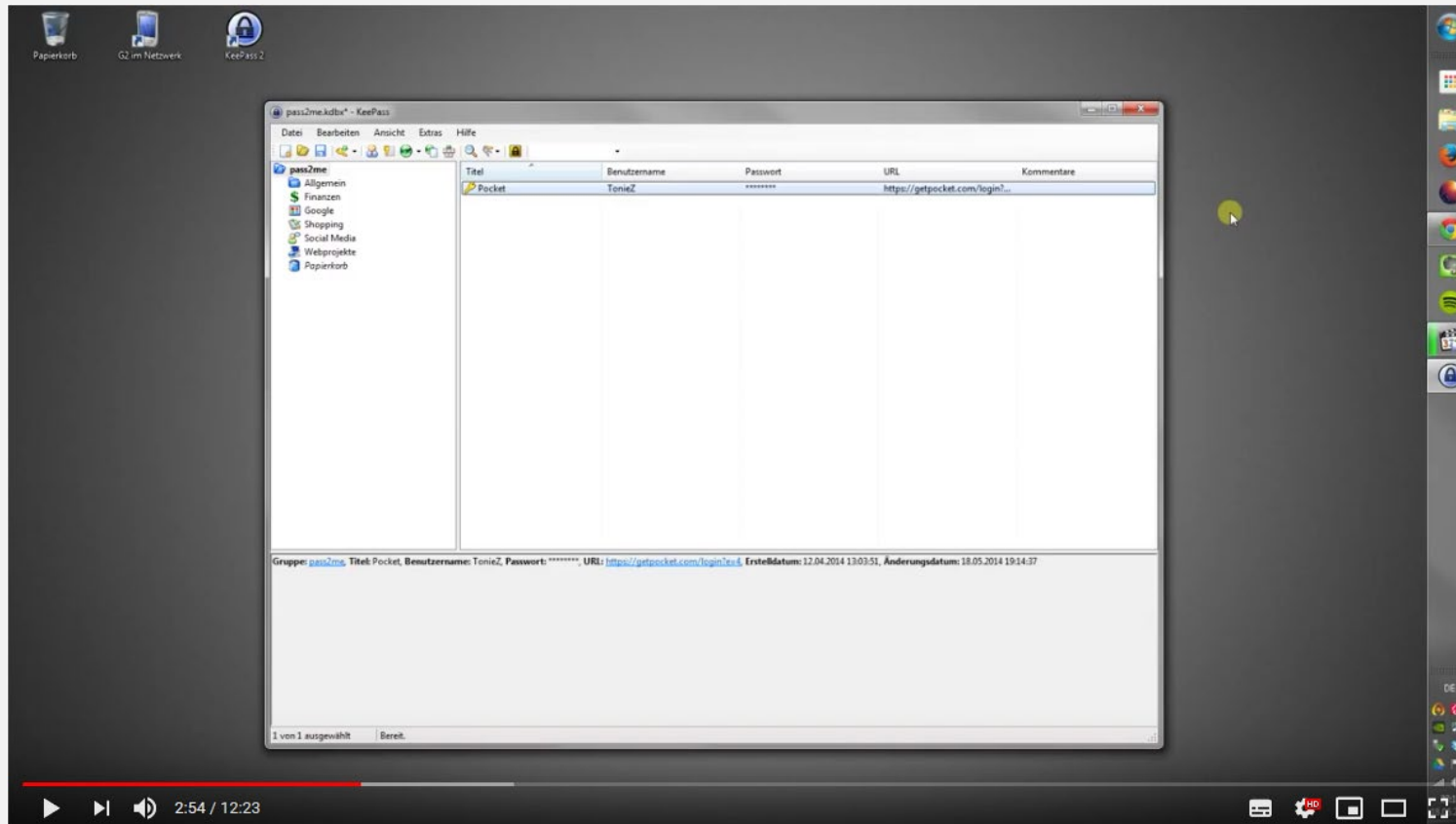
Noch besser: Passwort Manager / Tresor nutzen!

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!

KeePass – einfach erklärt



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

Zusammenfassung



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 / Vorgesetzte*r)
- Auf dem aktuellen Stand bleiben mit Hinweisen und Fortbildungen
- Gehirn zusammen mit dem Computer einschalten und lieber einmal zu viel fragen...

Ansprechpersonen



Ansprechpersonen

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

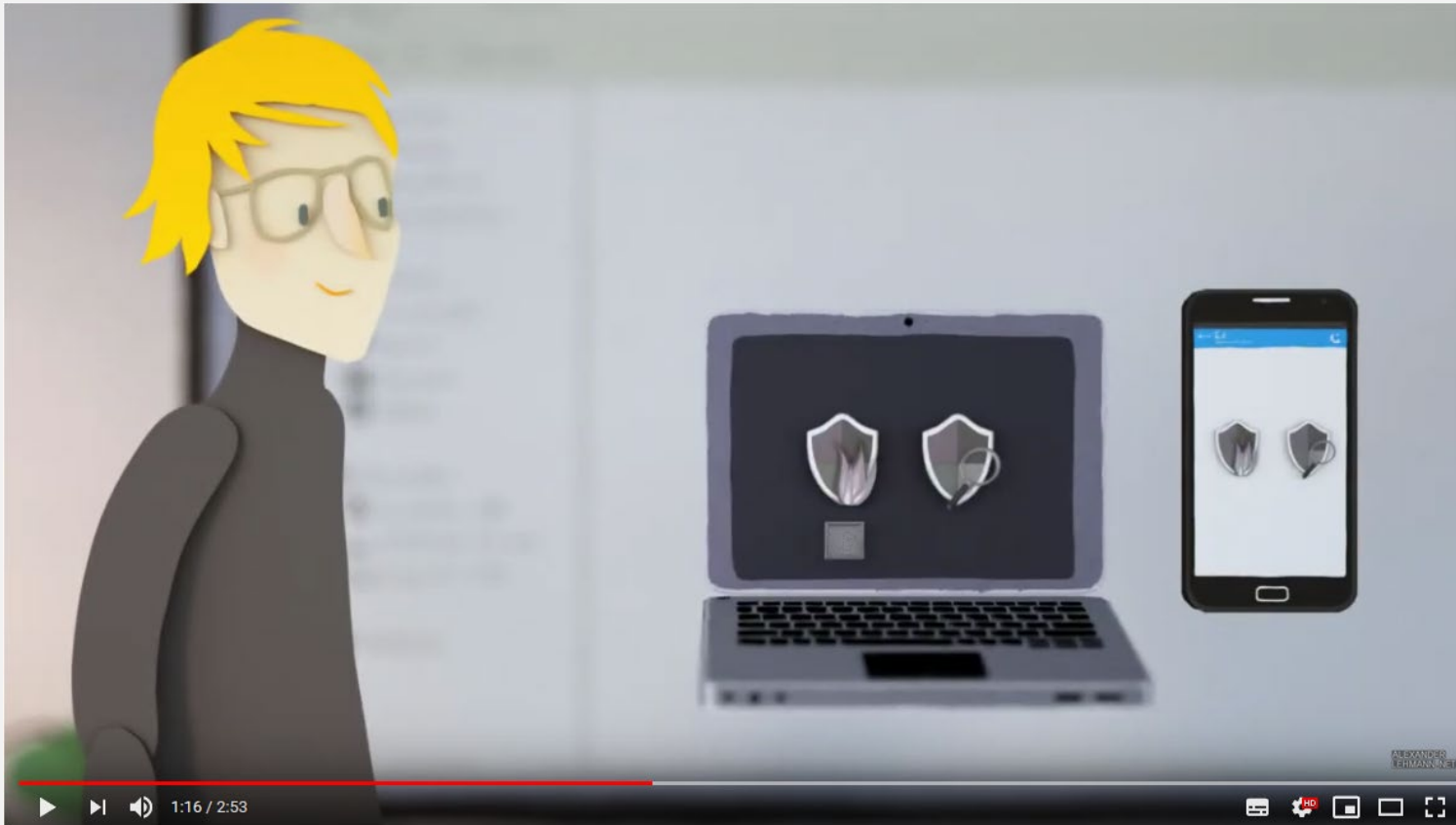
Private Selbstverteidigung



Private Selbstverteidigung kompakt

- Antivirus-Software installieren (vom Hersteller des Betriebssystems oder kostenlos beim BITS)
 - Smartphone (v.a. Android): z. B. Sophos Intercept X installieren (Grundversion kostenlos)
- Firewall scharf schalten (vom Hersteller des Betriebssystems)
- Betriebssystem und Software/Apps immer auf dem aktuellen Stand halten
- Browser gegen Tracking und Angriffe absichern (NoScript, uOrigin etc.)
- Regelmäßig Backups machen (z. B. externe Festplatte oder Cloudspeicher kaufen)
- Regelmäßig prüfen, ob die Maßnahmen aktiv sind und noch „funktionieren“
- Über Bedrohungen informiert bleiben (z. B. mit www.bsi-fuer-buerger.de)
- Gehirn vor dem Rechner einschalten hilft auch privat... ;-)

Maßnahmen für Datensicherheit



<https://www.youtube.com/watch?v=XMPg7IFcmnU>

**Vielen Dank für
Eure Aufmerksamkeit.**

Fragen?



Kontakt

Michael Sundermeyer

Raum: Q0-150 | Durchwahl: 3032

michael.sundermeyer@uni-bielefeld.de / informationssicherheit@uni-bielefeld.de

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

Twitter: @unibi_itsec