



Nicht anbeißen! Wie Sie Online-Ködern entkommen.

ZAWiW Akademie Woche – AG 09

Lukas Pietzschmann und Janek Schoffit
Institut für Verteilte Systeme, Universität Ulm

22. September 2025

1. Intro



Lukas Pietzschmann

 Schutz öffentlicher Daten
 Institut für Verteilte Systeme



Janek Schoffit

 Netzwerk-Sicherheit
 Institut für Verteilte Systeme



- In Deutschland wurden letztes Jahr mindestens 37,5 Millionen Phishing Angriffe versucht
- Und 2,6 Millionen Mails mit schädlichen Anhängen versendet
- In Unternehmen sind bis zu 47% der Mails böswillig
- Betrüger im Internet werden immer raffinierter
 - ▶ Vor allem seit der Verbreitung von KI-Tools
- Es existieren spezielle Tools um echte Webseiten zu kopieren
 - ▶ Diese greifen dann Daten ab und senden diese an die Betrüger



Z1 Sensibilisierung

Welche Gefahren gibt es überhaupt?

Z2 Erkennung

Wie erkenne ich betrügerische Inhalte?

Z3 Umgang

Wie reagiere ich richtig auf solche Inhalte?

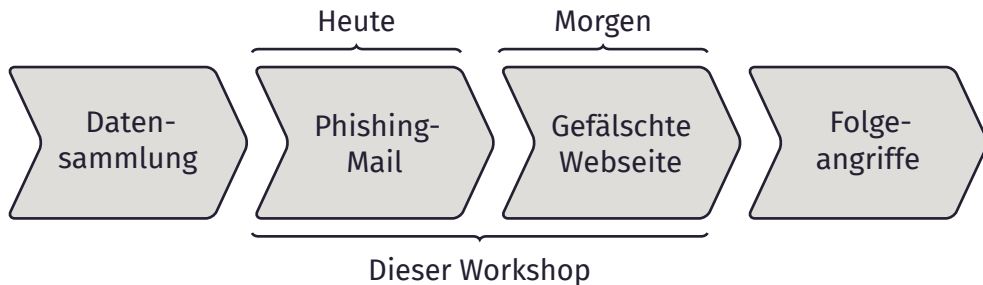
~~Z4 Expertise~~

~~Wie funktionieren solche
Angriffe technisch?~~

~~Z5 Details~~

~~Welche technischen Details
stecken dahinter?~~







Phishing Mails

Was das mit fischen zu tun hat und wie man sie erkennt

Lukas Pietzschmann

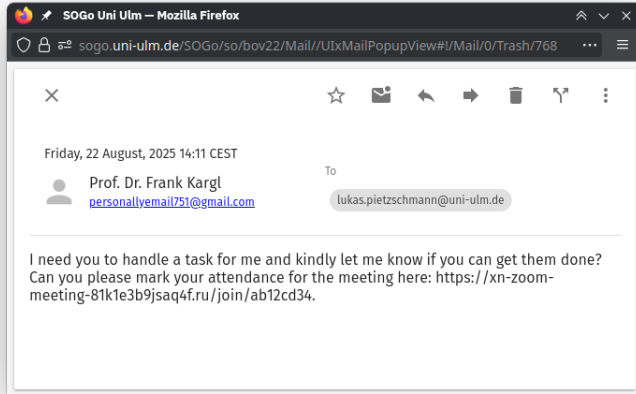
Institut für Verteilte Systeme, Universität Ulm

22. September 2025

2. Phishing Mails

WAS HAT DAS MIT FISCHEN ZU TUN?

- ▶ Angreifer *fischen* im Internet nach Daten
- Fishing zielt nicht auf eine einzelne Person ab
 - ▶ Das wäre Spear-Phishing
 - ▶ Phishing-Mails sind also Massenmails
- Das Ziel ist meistens
 - Login-Daten zu stehlen,
 - Kreditkarteninformationen zu erhalten oder
 - Schadsoftware zu verbreiten



TAKEAWAY #1

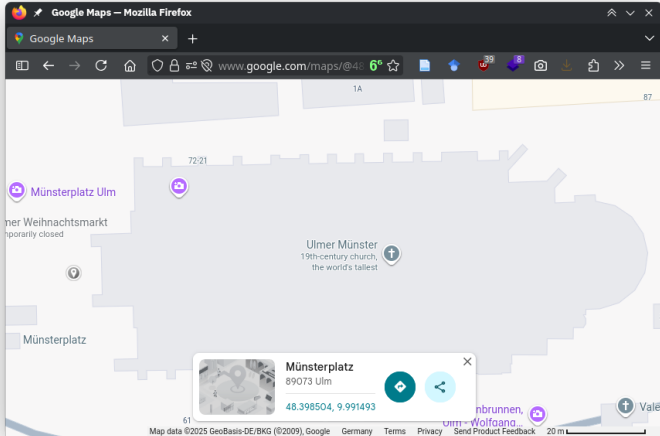
Der Name des Absenders ist leicht zu fälschen!

Kanzler <lukas@uni-ulm.de> wird oft nur als „Kanzler“ angezeigt. Die tatsächliche E-Mail-Adresse bleibt versteckt.

TAKEAWAY #2

Klicken Sie nicht blind auf Links!

Achten Sie genau darauf ob der Link „komische“ Zeichen enthält, oder ob die Domain dem entspricht, was Sie erwarten.





- Gleiches gilt auch für das Internet
 - ▶ Jede Website hat eine ~~Koordinate~~ IP-Adresse
- Diese ist genauso schwer zu merken
 - ▶ Deshalb gibt es Domains
- Auch eine Domain besteht auch aus mehreren Teilen
 - ▶ Top-Level-Domain > Domain > Subdomain

akademie.zawiw.de

↑ ↑ ↙
Subdomain Domain Top-Level-Domain

xn-zoom-meeting-81k1e3b9jsaq4f.ru

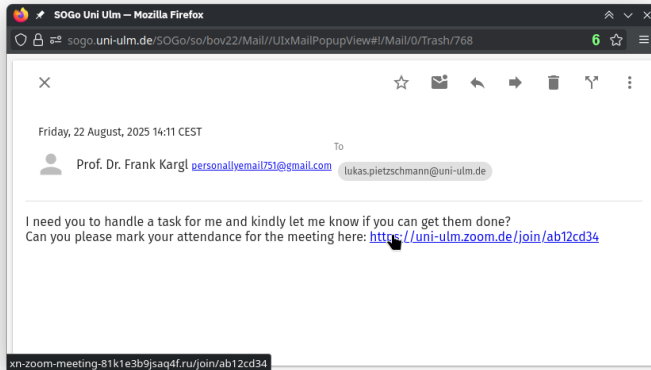
↑ ↗
Domain Top-Level-Domain

TAKEAWAY #3

Links können zwar ähnlich zu einer seriösen Seite aussehen, aber bei genauerem Hinsehen unterscheiden sie sich doch.

- `ing.de.ru` statt `ing.de`
- `volksbankulm.de` statt `volksbank-ulm.de`
- `arnazon.de` statt `amazon.de`

Schauen Sie genau hin! ▶ <https://dnstwister.report>



TAKEAWAY #4

Der Linktext kann den eigentlichen Link verstecken.

Oft wird der Linktext genutzt um den Link besser in den Text einzubetten („klicken Sie [hier](#)“). Er kann aber genauso das eigentliche Ziel verschleiern.

Achten Sie genau darauf, ob der Linktext und der tatsächliche Link übereinstimmen.

FUNKTIONIERT DAS IMMER?

- Auf mobilen Geräten funktioniert das meistens nicht
- Oft nutzen auch vertrauenswürdige Seiten Tools, die den Link modifizieren. Z.b. um (1) Klicks zu zählen oder (2) um zu verfolgen, von wo der Klick kam, ...
- Und was genau soll ich jetzt machen?
 - ▶ Gar nichts!
 - ▶ Wenn Sie unsicher sind, gehen Sie lieber direkt auf die Seite, anstatt auf den Link zu klicken.
 - ▶ <https://www.youtube.com/watch?v=gSQgbCo6PAg>

GENUG TECHNISCHES FÜRS ERSTE



- Wie werden Sie angesprochen?
- Werden Sie überhaupt mit Namen angesprochen?
- Passt die Anrede zum Kontext?
 - ▶ Z.B. „Sehr geehrter Lukas“ klingt komisch — Warum fehlt der Nachname?
 - ▶ Oder „Hallo Kunde“ — Warum nicht mit Namen?
 - ▶ Oder „Lieber Freund“ — Kennen Sie die Person?



Konto Verifizieren

Hallo, geehrter Abonnent!

Wir benötigen Ihre Mithilfe, um Ihr Paypal-Konto wieder neu in Gang zu bringen. Bis diese Erneuerung, die Verbindung zu Ihrem PayPal-Konto limitiert ist.

Wo kann man dieses Problem finden?

Kurzlich haben wir erfahren, dass eine potenziell nicht gesetzmäßige Benutzung der Kreditkarte von diesem PayPal-Konto stattfand. Zu Ihrem Schutz haben wir den Zugang zu Ihrem PayPal-Konto begrenzt.

Was kann man nun machen?

infolge dieser argwönischen Tätigkeiten auf Ihrem Konto bitten wir Sie, sich als legitimer Kartenhalter zu bestätigen. Dann können Sie Ihren PayPal Konto wie vor nutzen.

Viel Spaß beim Kaufen mit sicheren Kosten wünscht Ihnen PayPal

So verifizieren Sie Ihr PayPal Konto in nur wenigen Schritten:

1

Loggen Sie sich auf in Ihr Konto ein.

2

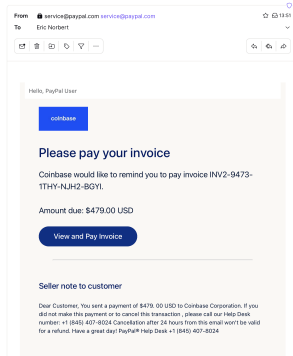
Folgen Sie den Anweisungen

3

Wählen Sie Ihr Bankkonto

[Zur PayPal-Seite](#)

Invoice from PayPal



- Oft werden Emotionen ausgenutzt um Sie zum Handeln zu bewegen
 - Angst
 - Neugier
 - Folgsamkeit
 - Hilfsbereitschaft
- Achten Sie außerdem auf folgende Dinge:
 - Versprechen von Belohnungen
 - Grammatik- und Rechtschreibfehler
 - Vertrauensaufbau und Empathie

Rechnung fehlgeschlagen - Konto gesperrt

NETFLIX

Hi [REDACTED]

Wir haben Probleme mit Ihren aktuellen Rechnungsinformationen. Wir werden es erneut versuchen, aber in der Zwischenzeit möchten Sie möglicherweise Ihre MASTERCARD in Ihren Zahlungsdetails aktualisieren.

JETZT KONTO AKTUALISIEREN

Wir sind hier, um Ihnen zu helfen, wenn Sie es brauchen. Besuche den Hilfezentrum für mehr info oder kontaktiere uns.

Deine Freunde bei Netflix

zu



Blockierter Verbindungsversuch

Hi [REDACTED]

Jemand hat gerade mit Ihrem Passwort versucht, sich von einer Nicht-Google-Anwendung aus bei Ihrem Konto anzumelden. Wir haben diese Person blockiert, aber wir raten Ihnen zu überprüfen, was passiert ist. Überprüfen Sie Ihre Kontobewegungen, um sicherzustellen, dass keine anderen Personen Zugriff auf Ihr Konto haben.

[Meine Kontoaktivität anzeigen \(link\)](#)

zu

Steuerrückerstattungsprogramm: Ihr Rabattbetrag

Hallo [REDACTED]

Aufgrund der jüngsten Eskalation hat die Regierung dringende Schritte unternommen, um COVID-19 als meldepflichtige Krankheit gesetzlich aufzulisten.

Als Vorsichtsmaßnahme hat die britische Regierung mit der National Insurance und dem National Health Service (NHS) zusammengearbeitet, um in ihrem Aktionsplan ein neues Steuerrückerstattungsprogramm für den Umgang mit COVID-19 einzurichten.

Sie haben jetzt Anspruch auf eine Steuerrückerstattung in Höhe von 213,64 [REDACTED]

Erhalten Sie Ihre Rückerstattung

zu

Hallo zusammen,

Hiermit möchten wir Sie über unsere neue Unternehmensrichtlinie in Bezug auf Urlaubsanspruch, Bezahlung und Krankengeld informieren, die ab dem nächsten Monat in Kraft tritt. Die in diesem Dokument beschriebenen Änderungen betreffen reguläre Vollzeit-, Teilzeit- und leistungsberechtigte Zeitarbeitskräfte. Daher ist es zwingend erforderlich, dass alle Mitarbeiter diese neue Richtlinie so schnell wie möglich zur Kenntnis nehmen.

Bitte [klicken](#) Sie entweder [hier](#) oder auf den untenstehenden Link, um das überarbeitete Urlaubs- und Krankengelddokument anzuzeigen.

Vielen Dank,

Das HR-Team

Richtlinie anzeigen

zu

Microsoft-Konto**Passwort abgelaufen**

Ihr Host-Administrator hat Ihr Passwort für Ihre E-Mail so festgelegt, dass es jeden Monat abläuft.

Dies ist eine Funktion zum Schutz Ihres Profils. Daher ist es zwingend erforderlich, dass Sie Ihr Passwort erneuern, um Probleme mit Ihrer E-Mail zu vermeiden.

[Erneuern](#)

Vielen Dank,

Microsoft-Sicherheitsabteilung

- Ergibt der Anhang in diesem Kontext Sinn?
 - ▶ Z.B. eine Rechnung von einem Onlineshop
- Welche Dateiendung hat der Anhang?
 - ▶ Vorsicht bei ausführbaren Dateien (.exe, .bat, .cmd, ...)

TAKEAWAY #5

Phishing-Mails versuchen oft Emotionen auszunutzen um Sie zum Handeln zu bewegen!

Lassen Sie sich nicht hetzten! Nehmen Sie sich Zeit um die Mail zu überprüfen.

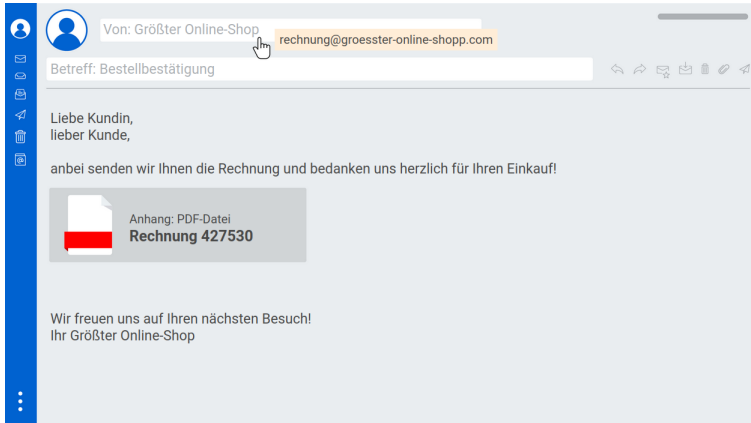
- Nichts anklicken, oder antworten!
- Email löschen oder in den Spam-Ordner verschieben
- E-Mail Anbieter oder Firma kontaktieren

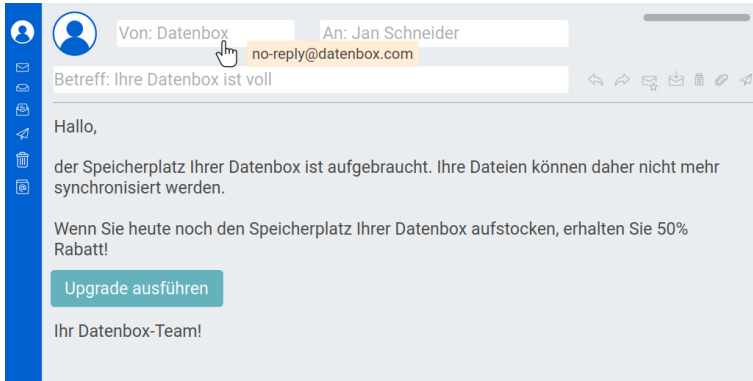


3. Quizz

3.1

AUFGABE 1





3.3

AUFGABE 3

Hanna Müller

8:30 AM

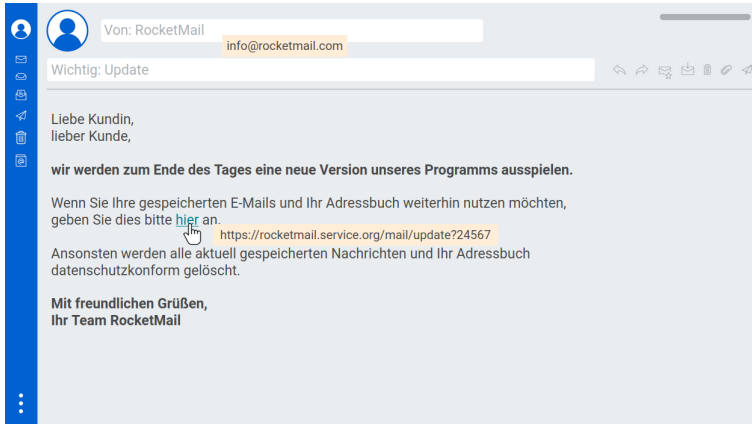
Sie haben eine freigegebene Datei von Hanna Müller erhalten

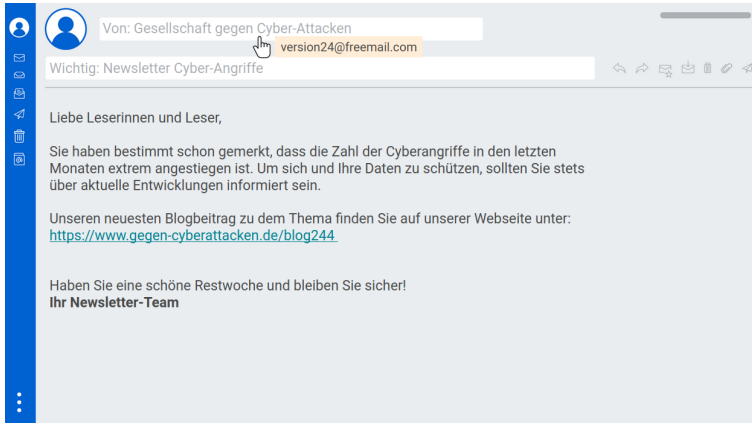
Datei ansehen:

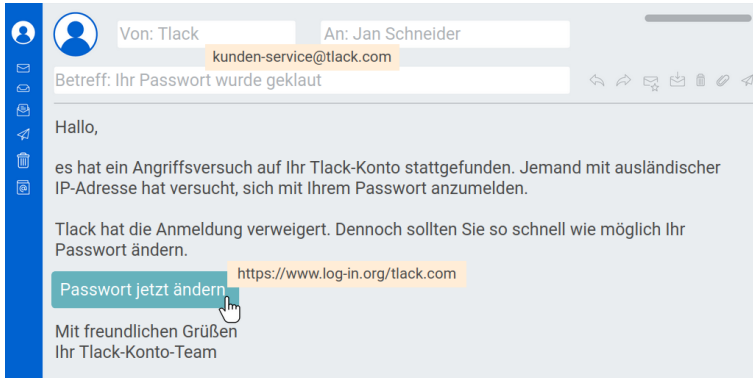
https://1drv.ms/w/s!AuLd0cPQLpfDdGITQTZ_LsY9oFQ?e=Rp65vU

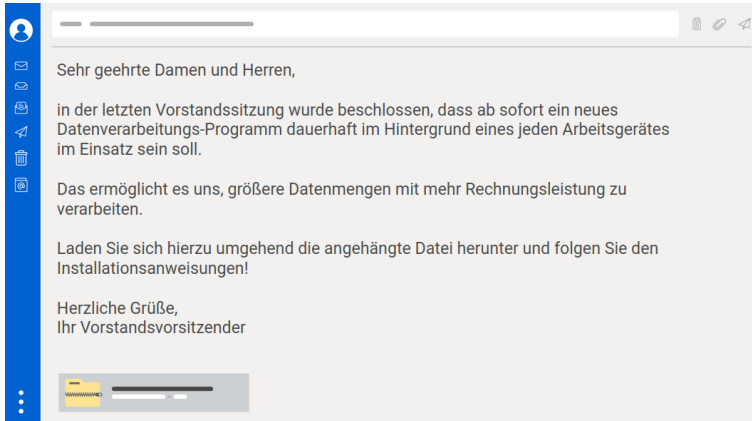
Vielen Dank
Hanna Müller











Lukas Pietzschmann

Ulm, 22. September 2025

lukas.pietzschmann@uni-ulm.de



Gefälschte Webseiten

Wieso diese so echt aussehen und wie man sie trotzdem erkennt

Janek Schoffit

Institut für Verteilte Systeme, Universität Ulm

23. September 2025

4. Intro

WAS IST EIGENTLICH EINE GEFÄLSCHTE WEBSITE?

Gefälschte Webseiten sind illegitime Internetseiten, die dazu da sind, betrügerische, böswillige Angriffe durchzuführen.

Kaspersky

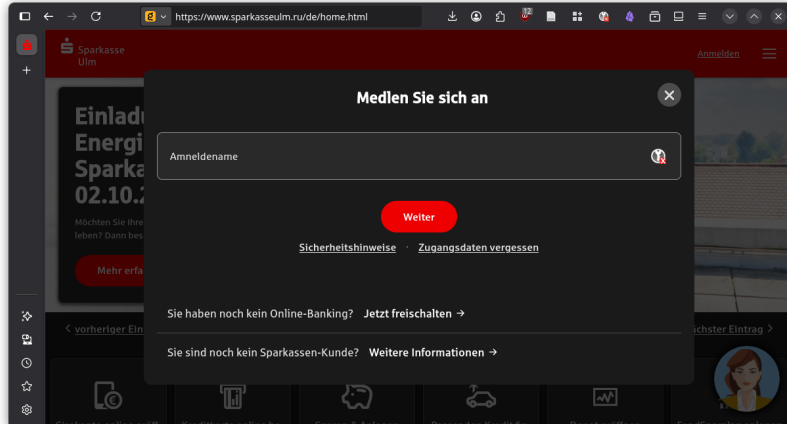
Angreifer nutzen folgende Funktionsweise:

Köder Nutzer werden auf betrügerische Website gelockt (durch Links, Mails, ...)

Falle Nutzer werden dazu verleitet, sensible Daten einzugeben (Login, Kreditkarte, ...)

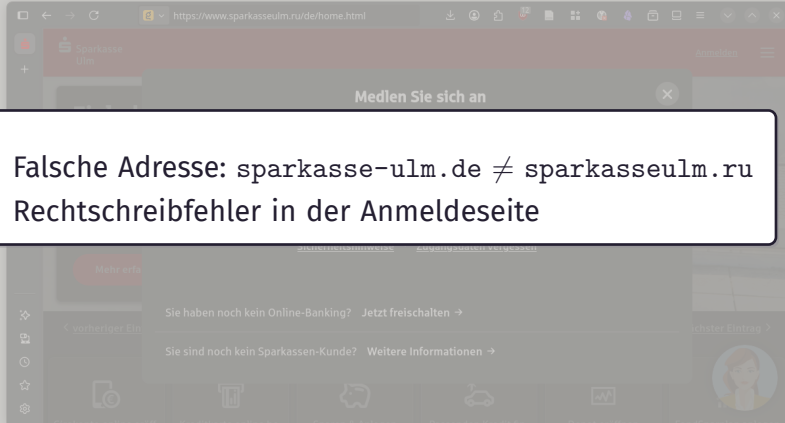
Missbrauch Angreifer nutzen sensible Informationen aus (Identitätsdiebstahl, Finanzbetrug, ...)

QUIZ: IST DIESE WEBSITE ECHT?



QUIZ: IST DIESE WEBSITE ECHT?

- Falsche Adresse: sparkasse-ulm.de $\neq$ sparkasseulm.ru
- Rechtschreibfehler in der Anmeldeseite



5. Indikatoren

www.uni-ulm.de

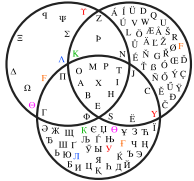
Subdomain Domain Top-Level-Domain

Subdomain

Domain

Top-Level-Domain

WAS IST EINE FAKE-DOMAIN?



- Fake-Domain zeigt auf eine bösartige Webseite
- Einzelne Buchstaben können aus einem anderen Alphabet sein

www.uni-ulm.de

www.uni-ulm.de

► <https://www.irongeek.com/homoglyph-attack-generator.php>

Seit ca. 2010 möglich durch Einführung von IDN (Internationalized Domain Names)

- Dadurch sind nahezu alle Arten von Zeichen in Domains möglich
- Bspw. auch Emoji Domains (außer , **TM**, )



¹Internationalizing Domain Names in Applications

WAS BEDEUTET DAS FÜR UNS?

- Nicht blind auf jeden Link klicken
- Im Browser auf den dahinterliegenden Link achten
- Wenn Domain xn-- enthält vorsichtiger sein

WEITERE INDIKATOREN FÜR EINE FAKE-DOMAIN

Leicht veränderte Domain:

- - durch _ ersetzt
- Buchstaben Ähnlichkeit: $l \leftrightarrow I$, $m \leftrightarrow n$, $O \leftrightarrow 0$
- Buchstabnedreher
- Falsche Top-Level-Domain (bspw. .com statt .de)
- Fehlende/Hinzugefügte Trennzeichen

Beispiel:

`www.volksbank-ulm-biberach.de` ▶ `www.volksbankulm-biberach.de`

Weitere Beispiele: `https://dnstwister.report/`

5.5 WEITERE INDIKATOREN FÜR EINE FAKE-DOMAIN

Leicht veränderte Domain:

- - durch _ ersetzt

Bei wichtigen Seiten (bspw. Online-Banking) besonders auf die Schreibweise der Adresse/Domain achten und am besten einprägen.

Beispiel:

`www.volksbank-ulm-biberach.de` ▶ `www.volksbankulm-biberach.de`

Weitere Beispiele: <https://dnstwister.report/>



`https://volksbankulm-biberach.de/login`

**Bitte keine echten Login-Daten
eingeben!**

QUIZ: DOMAINS

Bei welchen dieser Beispiele handelt es sich vermutlich um Fake-Domains?

1. `google.google.com`
2. `mail.google.com`
3. `www.google.com.de`
4. `www.photos.goog-le.com`

QUIZ: DOMAINS

Bei welchen dieser Beispiele handelt es sich vermutlich um Fake-Domains?

1. `www.sparkasse-uIm.de`
2. `login.volksbank-ulm-bieberach.de`
3. `www.sparkasse-ulm.de`
4. `login.volksbank-ulm-biberach.do`

WIE IST EIN LINK AUFGEBAUT?

In Fachsprache sagen wir dazu *URL* (Uniform Resource Locator)

https:// uni-ulm.de /in/vs.html
Protokoll Domain Pfad

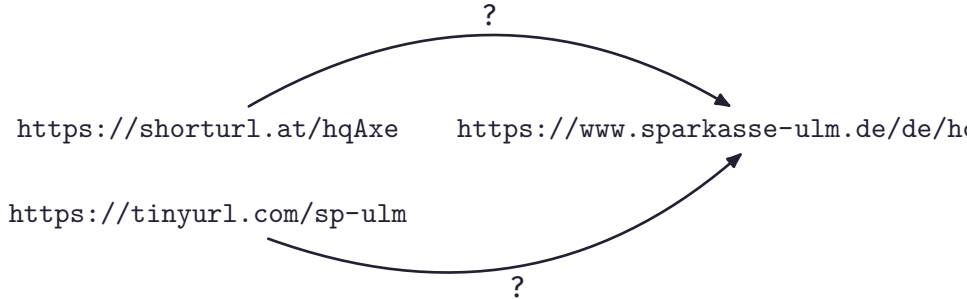
- Auf verdächtige Pfade achten
- Im Browser über Links hovern und URL betrachten
- Links auf Websites können die URL verschleiern
- Intransparente URL-Shortener vermeiden

QUIZ: URLs

Bei welchen dieser Beispiele handelt es sich vermutlich um gefälschte Adressen?

- `https://uni-ulm.de/payment/form.php`
- `https://uni-ulm.de/in/vs`
- `https://uni-ulm.de/c2NhbS13ZWJzaXRlCg`
- `https://ulm.de/0/2016/ulm-fur-einsteiger/paypal.html`

Bieten eine möglichst kurze URL an, die auf eine längere URL weiterleitet.



Bekannte URL-Shortener:

- `bit.ly`
 - `tinyurl.com`
 - `t.co` (Twitter)
 - `shorturl.at`
 - `is.gd`
- Diese Art von Links möglichst vermeiden!

- Bei falscher Domain kann man sich sicher sein, dass mit der Website etwas nicht stimmen kann
- URL im Auge behalten, um verdächtige/fehlende Zeichen zu erkennen
- URL-Shortener leiten auf unvorhersehbare URLs weiter

6. Fake-Website am Inhalt erkennen

FEHLENDES IMPRESSUM

- Jede Website benötigt ein Impressum
 - ▶ (Ausnahme: rein private Seiten)
- Bei Shops und Websites mit Loginbereich zusätzlich auf die Datenschutzerklärung achten

Falls Impressum nicht direkt auffindbar:

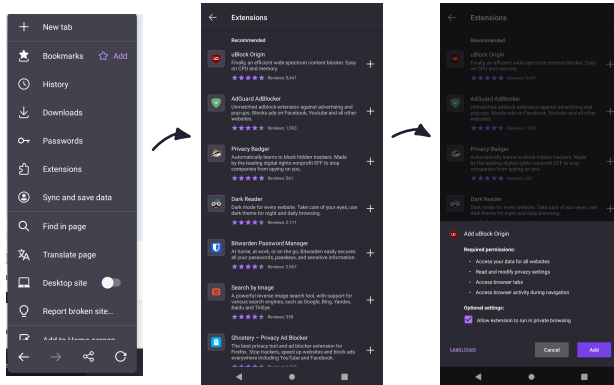
- Im Footer (ganz unten) der Seite
- In der Seitenleiste
- `/impressum` oder `imprint` oder `/about` am Ende der URL

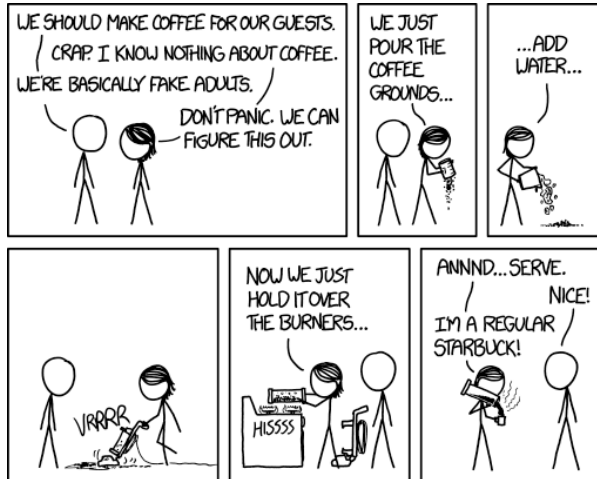
- Weiterleitungen auf andere Seiten (Domain im Auge behalten)
 - ▶ `uulm.de` → `uni-ulm.de`
- Rechtschreibung und Layout
- Plausibilität der Inhalte
- Zahlungs- und Datennachfrage

Steht für eine sichere Verbindung zwischen dem Computer und der Website

- `http://` unverschlüsselte Variante
- Unverschlüsselte Verbindungen können abgehört und manipuliert werden
- Kein `https://`
- ▶ wird durch aktuelle Browser (meistens) verhindert

- HTTPS-only Modus aktivieren
 - ▶ Testen mit `neverssl.com`
- Ad-Blocker: uBlock Origin
 - ▶ blockt Werbedomains, viele Tracker und bekannte Phishing Websites
 - ▶ Vorteile: Websites sehen schöner aus, weniger Akkuverbrauch
 - ▶ Bonus: Auch in Firefox für Android installierbar





7. Passwort Sicherheit

Formel zur Berechnung der Anzahl möglicher Kombinationen:

$$\text{Kombinationen} = \text{Anzahl Zeichen}^{\text{Passwort Länge}}$$

Bank PIN: (Zeichen: 0–9, Länge: 4)

$$10000 = 10^4$$

Angenommen ein Computer testet 2 Milliarden Kombination pro Sekunde

$$\frac{10000}{2.000.000.000} = 0,000005s$$

Einfaches Passwort: Passwort12345

(Zeichen: a-zA-Z0-9 $\rightarrow 26 + 26 + 10 = 62$, Länge: 13)

$$62^{13} \approx 2.000285393 \cdot 10^{23}$$

Angenommen ein Computer testet 2 Milliarden Kombination pro Sekunde

$$\frac{2.000285393 \cdot 10^{23}}{2.000.000.000} \approx 1.000142696 \cdot 10^{14} \text{s} \approx 3171431 \text{ Jahre}$$

► Sicheres Passwort gefunden. Oder?!

Formel zur Berechnung der Anzahl möglicher Kombinationen: Beispiel
2: Einfaches Passwort: `Password12345`



Frei verfügbare Listen:

<https://github.com/danielmiessler/SecLists>

- E-Mail und Passwort Kombinationen aus Datenlecks
- Häufig genutzte Passwörter enthalten
- Große Datenmengen können schnell durchsucht werden

WAS MACHT EIN GUTES PASSWORT AUS?

- Einfach zu merken
- Schwierig zu erraten
- Nicht in Passwort Listen enthalten
- Für jeden Account ein anderes Passwort verwenden
- Regelmäßig ändern (besonders bei Verdacht auf Datenleck)

WIE KANN MAN SICH PASSWÖRTER MERKEN?

Sätze bilden:

- Beispiel: "100EuroScheineSindGrün!"(23 Zeichen)
- **Vorteile:** Länge, Nicht in Passwort Listen, Einfach zu merken
- **Nachteile:** Viel zu tippen

Anfangsbuchstaben eines Satzes:

- Beispiel: "100 Euro Scheine sind Grün! Das Gras auch."→
"100ESsG!DGa"(11 Zeichen)
- **Vorteile:** Weniger zu tippen, Nicht in Passwort Listen, Eselsbrücke
- **Nachteile:** Viel Denkarbeit um das Passwort zu rekonstruieren

SPEICHERMETHODEN FÜR PASSWÖRTER

Passwörter auf Papier notieren:

- **Vorteile:** Simpel, Kein Computer nötig
- **Nachteile:** Handschrift lesbar?, Nicht immer dabei, Bei Verlust sind alle Passwörter weg, Klartext

Passwort Manager:

- **Vorteile:** Einfach zu bedienen, Verschlüsselt, Automatisches Ausfüllen, Synchronisation über Geräte
- **Nachteile:** Initiale Einrichtung, Sicherheit abhängig vom Master Passwort, Software Bugs

PASSKEYS: ALTERNATIVEN ZU PASSWÖRTERN

Authentifizierung ohne Passwort

- Biometrische Verfahren: Fingerabdruck, Gesichtserkennung, Iris-Scan
- FIDO2/WebAuthn: Hardware Token (z.B. Yubikey)
- 2-Faktor-Authentifizierung (2FA): z.B. TOTP Apps (Google Authenticator, Authy)

8. Diskussionsrunde

HABEN SIE FRAGEN?



<https://cloudstore.uni-ulm.de/s/fb4MG8Kk5sbbWjk>

Janek Schoffit

Ulm, 23. September 2025

janek.schoffit@uni-ulm.de