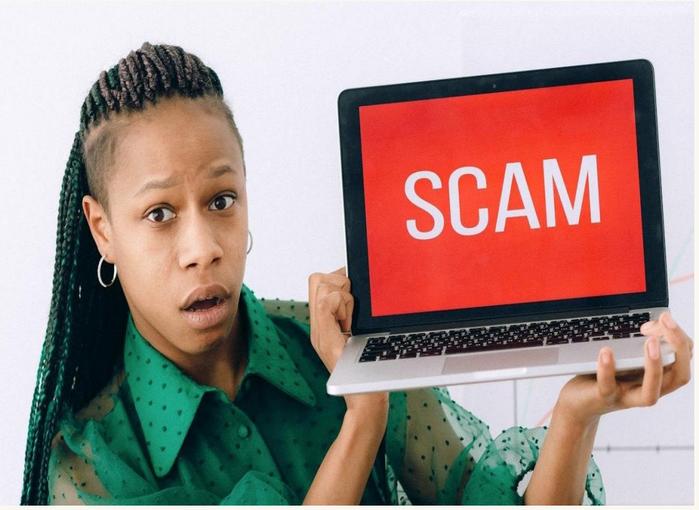
WORKSHOP · 90 MIN · DIGITALTAG 2026

Digitale Sicherheit *für alle.*

Klicken mit Bedacht, nicht in Panik. Ein Workshop für eine einfache und sichere Internetnutzung — keine Vorkenntnisse nötig.



„Sicheres Klicken beginnt mit einer 3-Sekunden-Pause."

HEUTE GEHT ES **NICHT** UM

Hackerfilme.

Es geht um **drei einfache Gewohnheiten**, die sofort helfen.

Erkennen

verdächtige E-Mails, SMS, Anrufe und QR-Codes.

Stopp

nicht voreilig klicken — kurz innehalten und prüfen.

Schützen

Konten, Passwörter, Geräte und Daten absichern.

Faustregel: erst denken, dann klicken.

VOM KÖDER ZUM SICHERHEITSPLAN

Ein 90-minütiges Praxistraining.

© Humour mod hacking.dk

1

Betrugstricks

Die Psychologie hinter jedem Betrug verstehen.

2

Phishing & Co.

Mail-, SMS-, Sprach- und QR-Varianten erkennen.

3

Passwörter & 2FA

Konten und Geräte absichern.

4

Live-Tools

Echte Sicherheits-Tools gemeinsam ausprobieren.

5

Dein Plan

Ein Notfallplan und ein persönlicher nächster Schritt.

Keine Sorge — niemand wird live gehackt. Nur wachgerüttelt.

AUFWÄRMEN

Hat dich das Internet schon einmal reingelegt?

Hand hoch, wer eine davon kennt.

„Ihr Paket konnte nicht zugestellt werden."

ECHT? UNSICHER? BETRUG?

„Ihr Konto wird heute gesperrt."

ECHT? UNSICHER? BETRUG?

„Sie haben gewonnen! Geben Sie nur Ihre Daten ein."

ECHT? UNSICHER? BETRUG?

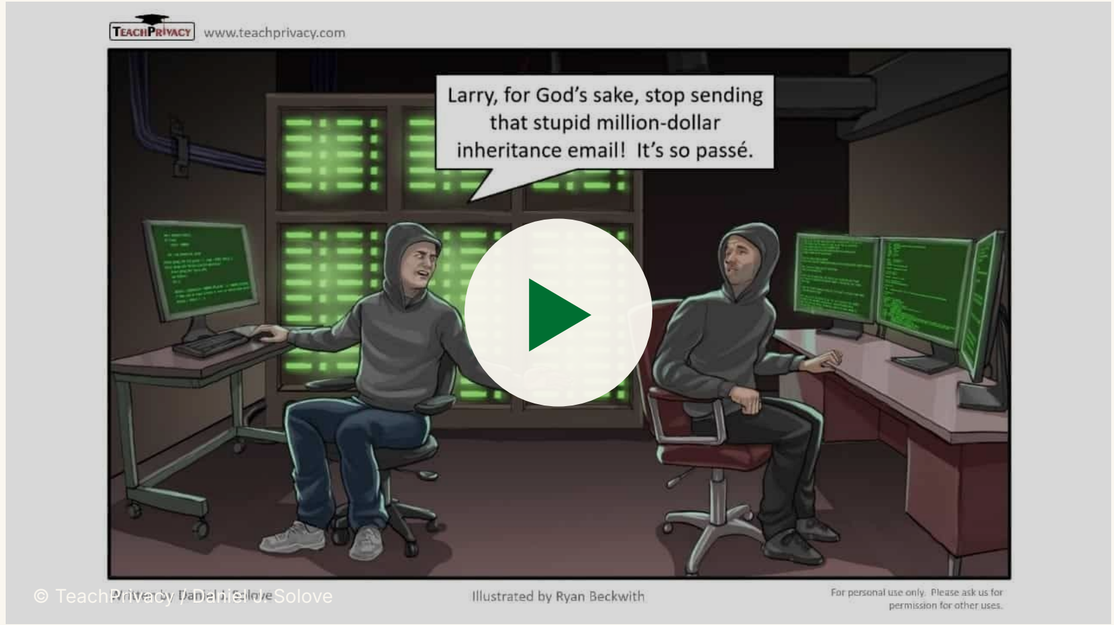
Heute trainieren wir den kurzen Sicherheitsmoment vor dem Klick.

VIDEO

2 MINUTEN LACHEN

Erst lachen wir. Dann schauen wir auf die Methode.

▶ „Phishing Attack" ansehen



Kurze Auswertung — 3 Fragen

- → Was war lustig?
- → Was war gefährlich?
- → Welchen Trick hat der Angreifer benutzt?

Humor hilft. Klicken bleibt freiwillig.

PHISHING IST KEIN TECHNIK-PROBLEM

Es ist ein *menschlicher Trick* im digitalen Kostüm.

Angst
„Ihr Konto wird gesperrt."

⏰ **Dringlichkeit**
„Nur heute!"

Neugier
„Schau dir dieses Foto von dir an."

Autorität
„Wir sind von der Bank / Polizei / IT."

Hilfsbereitschaft
„Ich brauche dringend deine Hilfe."

Gier
„Sie haben gewonnen!"

Wenn die Nachricht auf deine Gefühle zielt — drück Pause.

GLEICHER BETRUG, ANDERE BÜHNE

Spam · Phishing · Smishing Vishing · Quishing.

Spam
Massennachrichten mit Links oder Anhängen.

Phishing
Gefälschte Mails oder Seiten, die Zugangsdaten stehlen.

Smishing
Phishing per SMS oder Messenger.

Vishing
Betrug per Anruf oder Sprachnachricht.

Quishing
QR-Codes, die auf gefälschte Seiten führen.

Mini-Spiel: Beispiele den Begriffen zuordnen — laut, ohne Scham.

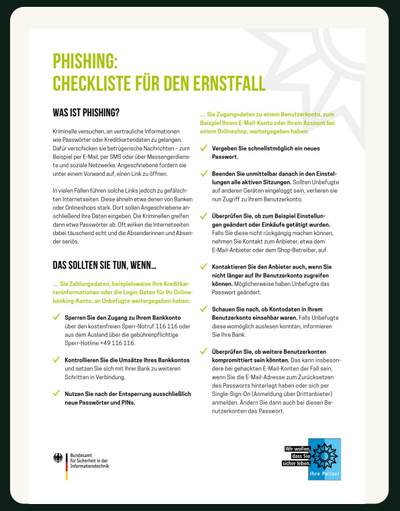
KURZ ANSCHAUEN

5 Methoden gegen Phishing- Mails.

1. **Absender** genau prüfen.
2. **Druck und Drohungen** erkennen.
3. **Links** vor dem Klick prüfen.
4. **Anhänge** nur öffnen, wenn erwartet.
5. Im Zweifel über einen **zweiten Kanal** nachfragen.

Wenn eine Mail dich mehr stresst als Montag ohne Kaffee – erst prüfen.

3 *Sekunden.*



PHISHING:
CHECKLISTE FÜR DEN ERNSTFALL

WAS IST PHISHING?

Kriminelle versuchen, an vertrauliche Informationen wie Passwörter oder Kreditkartendaten zu gelangen. Dafür verschicken sie betrügerische Nachrichten – zum Beispiel per E-Mail, per SMS oder über Messengerdienste und soziale Netzwerke. Angeschriebene fordern sie unter einem Vorwand auf, einen Link zu öffnen.

In vielen Fällen führen solche Links jedoch zu gefälschten Internetseiten. Diese ähneln etwa denen von Banken oder Onlineshops stark. Dort sollen Angeschriebene anschließend ihre Daten eingeben. Die Kriminellen greifen dann etwa Passwörter ab. Oft wirken die Internetseiten dabei täuschend echt und die Absenderinnen und Absender seriös.

DAS SOLLTEN SIE TUN, WENN…

… Sie Zahlungsdaten, beispielsweise Ihre Kreditkarteninformationen oder die Login-Daten für Ihr Onlinebanking-Konto, an Unbefugte weitergegeben haben:

- **Sperren Sie den Zugang zu Ihrem Bankkonto** über den kostenfreien Sperr-Notruf 116 116 oder aus dem Ausland über die gebührenpflichtige Sperr-Hotline +49 116 116.
- **Kontrollieren Sie die Umsätze Ihres Bankkontos** und setzen Sie sich mit Ihrer Bank zu weiteren Schritten in Verbindung.
- **Nutzen Sie nach der Entsperrung ausschließlich neue Passwörter und PINs.**

… Sie Zugangsdaten zu einem Benutzerkonto, zum Beispiel Ihrem E-Mail-Konto oder Ihrem Account bei einem Onlineshop, weitergegeben haben:

- **Vergeben Sie schnellstmöglich ein neues Passwort.**
- **Beenden Sie unmittelbar danach in den Einstellungen alle aktiven Sitzungen.** Sollten Unbefugte auf anderen Geräten eingeloggt sein, verlieren sie nun Zugriff zu Ihrem Benutzerkonto.
- **Überprüfen Sie, ob zum Beispiel Einstellungen geändert oder Einkäufe getätigt wurden.** Falls Sie diese nicht rückgängig machen können, nehmen Sie Kontakt zum Anbieter, etwa dem E-Mail-Anbieter oder dem Shop-Betreiber, auf.
- **Kontaktieren Sie den Anbieter auch, wenn Sie nicht länger auf Ihr Benutzerkonto zugreifen können.** Möglicherweise haben Unbefugte das Passwort geändert.
- **Schauen Sie nach, ob Kontodaten in Ihrem Benutzerkonto einsehbar waren.** Falls Unbefugte diese womöglich auslesen konnten, informieren Sie Ihre Bank.
- **Überprüfen Sie, ob weitere Benutzerkonten kompromittiert sein könnten.** Das kann insbesondere bei gehackten E-Mail-Konten der Fall sein, wenn Sie die E-Mail-Adresse zum Zurücksetzen des Passworts hinterlegt haben oder sich per Single-Sign-On (Anmeldung über Drittanbieter) anmelden. Ändern Sie dann auch bei diesen Benutzerkonten das Passwort.

Bundesamt für Sicherheit in der Informationstechnik

Wir helfen Ihnen sicher zu sein.

DER 3-SEKUNDEN-CHECK

Drei Fragen, bevor der Finger schneller ist als das Hirn.

1. **Kenne** ich den Absender?
2. Ergibt der Inhalt **überhaupt Sinn?**
3. Habe ich Link, Anhang oder Anfrage **erwartet?**

Bei Zweifel: nicht antworten – Nummer oder Website selbst nachschlagen.

ÜBUNG

Eine Phishing-Mail zerlegen.

From: Sparkasse Security <>
Subject: **LETZTE WARNUNG: Ihr Konto wird heute gesperrt!**

Sehr geehrte Kundin, sehr geehrter Kunde, wir haben ungewöhnliche Aktivitäten festgestellt. Bitte **bestätigen Sie sofort Ihre Zugangsdaten:**

http://sparkasse-login-check.net Anhang: Invoice.pdf.exe

⚠ **Absender-Domain** wirkt komisch — nicht die echte Sparkasse.

⚠ **Druck** — „LETZTE WARNUNG".

⚠ **Link** passt nicht zur echten Bank.

⚠ **.pdf.exe** — eine getarnte ausführbare Datei.

⚠ Fragt direkt nach **Passwort / PIN**.

Diese Mail trägt einen falschen Schnurrbart.

LIVE-ÜBUNG

Google Phishing Quiz.

Gemeinsam üben — ohne echte Zugangsdaten.

phishingquiz.withgoogle.com

Trainer-Tipp: Teilnehmende erst in Kleingruppen abstimmen lassen, dann gemeinsam auflösen.

→ 3–5 Beispiele gemeinsam durchgehen

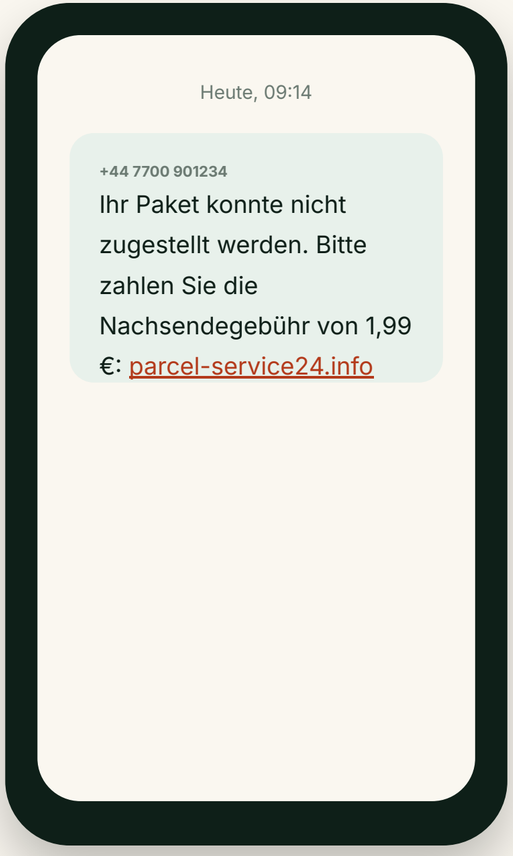
→ Nach jedem: Was wirkte verdächtig?

→ Was wirkte überzeugend echt?

→ Welche Regel hätte geholfen?

SMISHING

Das Paket, das nie ankam.



- ✗ Nicht direkt auf den Link tippen.
- ✓ App oder Website des Versanddienstes selbst öffnen.
- ✗ Niemals Kartendaten über einen SMS-Link eingeben.
- ✓ Nachricht löschen — oder melden.

Ein Paket kann warten. Dein Konto sollte nicht müssen.

VISHING

Wenn das Telefon Theater spielt.

HÄUFIGE GESPRÄCHSEINSTIEGE

- *„Wir rufen von Ihrer Bank an."*
- *„Ich bin vom Microsoft-Support."*
- *„Bitte bestätigen Sie den Code in Ihrer App."*
- *„Lassen Sie mich kurz auf Ihren Computer zugreifen."*

DEINE SICHERE STANDARD-ANTWORT

„Danke. Ich rufe selbst über die offizielle Nummer zurück."

Dann auflegen. Nummer auf der offiziellen Bankkarte oder Website nachschlagen — nicht die vom Anrufer genannte.

Microsoft ruft nicht an, weil dein Drucker traurig ist.

NEUE RISIKEN · 2026

KI-Stimmen & Deepfakes.

Auch wenn es *klingt* wie jemand Bekanntes, kannst du trotzdem nachprüfen.

Stimmen und Videos können nachgeahmt werden.

Schockanrufe nutzen Angst und Zeitdruck aus.

Geld oder Daten? Über einen zweiten Kanal prüfen.

Familien-**Codewort** vereinbaren.

MINI-ÜBUNG

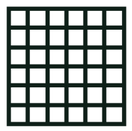
Was wäre ein gutes Codewort — das nicht auf Instagram steht?

Take 30 Sekunden. Whisper it to your partner / friend / family — never type it on a public channel.

QUISHING

QR-Codes sind Überraschungstüten.

Den Link siehst du erst nach dem Scannen — genau das nutzen Betrüger aus.



„Parkgebühr hier zahlen."

- Gefälschte QR-Aufkleber auf Parkautomaten und Ladesäulen.
- Gefälschte Briefe, angeblich von deiner Bank.
- QR-Codes in E-Mails wirken wie Links — gleiches Risiko.
- ✓ **URL-Vorschau** vor dem Öffnen — die meisten Handys zeigen sie an.

Nicht jeder QR-Code will dein Freund sein.

FAKE NEWS

Quelle schlägt *Bauchgefühl.*

JmS
Journalismus macht Schule

CHECKLISTE: FALSCHNACHRICHTEN ERKENNEN
Gerüchte, Übertreibungen, Propaganda, Desinformation

• Fakten hinterfragen

→ In welchem Kontext sind die Infos noch im Internet zu finden?

→ Wer wird zitiert? Handelt es sich um eine*n glaubwürdigen Expert*in?

→ Wer könnte ein Interesse daran haben, derartige Informationen zu verbreiten?

• Quelle prüfen

→ Wie seriös erscheinen weitere Artikel der vermeintlichen Fake News Seite? Was wird noch so veröffentlicht?

→ Datum einer Meldung ansehen und die Überschrift in eine Suchmaschine eingeben

→ URL kontrollieren: Falschmeldungen erscheinen häufig im Design bekannter Medienmarken. Oftmals unterscheidet sich die URL nur durch einen Zusatz wie einen Bindestrich oder eine Endung wie .net vom Original.

→ Kommt die Meldung aus einem sozialen Netzwerk? Wie lange gibt es den Twitter / Facebook-Account bereits? Wie viele Freunde oder Follower hat er? Wer sind die Follower / Freunde? Hat der Account einen blauen Verifizierungshaken?

Checkliste: Journalismus macht Schule

URL
Quelle und vollständige URL prüfen.

Datum
Datum und Kontext prüfen — ist es alt?

Autor
Autor und Impressum suchen.

Vergleichen
Mit seriösen Medien abgleichen.

Bilder
Fotos & Videos rückwärts suchen.

Wenn eine Nachricht dich nur wütend macht — erst recherchieren.

MINI-SPIEL

Echt, unklar oder falsch?

A Fall

„Neues Bußgeld ab morgen – Quelle: unbekannter Blog."

Was fehlt? Quelle, Datum, offizielle Mitteilung.

B Fall

Ein Foto „aus Darmstadt" – aber Kennzeichen und Schilder passen nicht.

Was prüfen? Bilderrückwärtssuche, Ort, Kontext.

C Fall

„Ein Experte sagt..." – aber kein Name, kein Institut, kein Link.

Was prüfen? Wer genau? Gibt es Fachquellen?

Regel: nicht teilen, bevor du es einordnen kannst.

PASSWÖRTER

Der Haustürschlüssel des Internets.

- ✔ Ein individuelles Passwort **pro Konto**.
- ✔ Lang schlägt clever — nutze eine **Passphrase**.
- ✘ Keine Namen, Geburtstage, Tastaturmuster.
- ✘ In keinem Wörterbuch. Nie wiederverwendet.
- ✔ **Mehrfaktor-Authentifizierung** aktivieren.

AUFMARSCH SCHLECHTER PASSWÖRTER

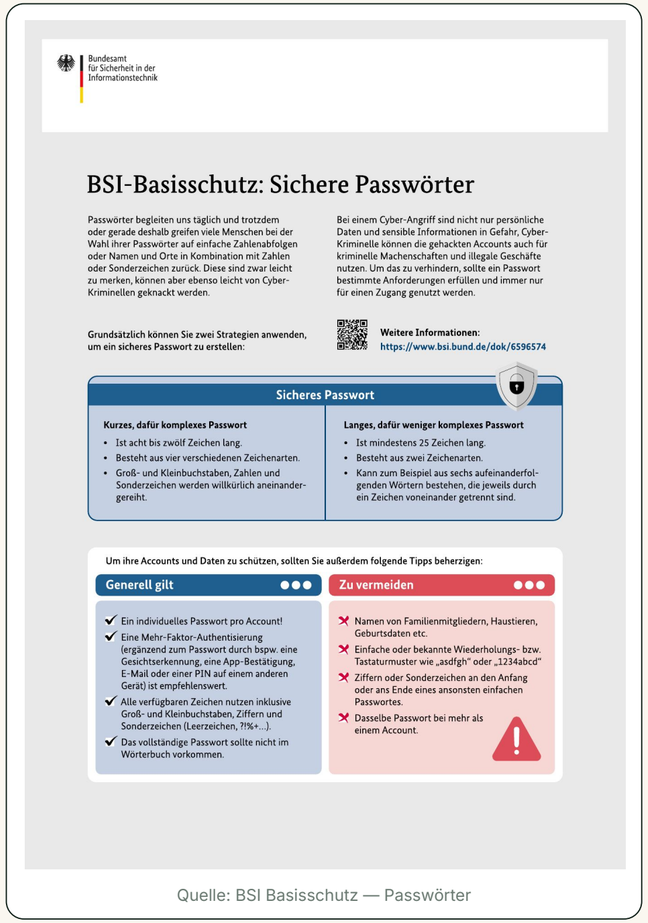
~~123456~~

~~password~~

~~Sommer2026!~~

~~Berlin123~~

„123456 ist kein Passwort. Es ist eine Fußmatte mit der Aufschrift: Bitte eintreten."



Bundesamt für Sicherheit in der Informationstechnik

BSI-Basisschutz: Sichere Passwörter

Passwörter begleiten uns täglich und trotzdem oder gerade deshalb greifen viele Menschen bei der Wahl ihrer Passwörter auf einfache Zahlenabfolgen oder Namen und Orte in Kombination mit Zahlen oder Sonderzeichen zurück. Diese sind zwar leicht zu merken, können aber ebenso leicht von Cyber-Kriminellen geknackt werden.

Bei einem Cyber-Angriff sind nicht nur persönliche Daten und sensible Informationen in Gefahr, Cyber-Kriminelle können die gehackten Accounts auch für kriminelle Machenschaften und illegale Geschäfte nutzen. Um das zu verhindern, sollte ein Passwort bestimmte Anforderungen erfüllen und immer nur für einen Zugang genutzt werden.

Grundsätzlich können Sie zwei Strategien anwenden, um ein sicheres Passwort zu erstellen:

Weitere Informationen:
https://www.bsi.bund.de/dok/6596574

Sicheres Passwort

Kurzes, dafür komplexes Passwort
- Ist acht bis zwölf Zeichen lang.
- Besteht aus vier verschiedenen Zeichenarten.
- Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen werden willkürlich aneinandergereiht.

Langes, dafür weniger komplexes Passwort
- Ist mindestens 25 Zeichen lang.
- Besteht aus zwei Zeichenarten.
- Kann zum Beispiel aus sechs aufeinanderfolgenden Wörtern bestehen, die jeweils durch ein Zeichen voneinander getrennt sind.

Um ihre Accounts und Daten zu schützen, sollten Sie außerdem folgende Tipps beherzigen:

Generell gilt
- ✓ Ein individuelles Passwort pro Account!
- ✓ Eine Mehr-Faktor-Authentisierung (ergänzend zum Passwort durch bspw. eine Gesichtserkennung, eine App-Bestätigung, E-Mail oder einer PIN auf einem anderen Gerät) ist empfehlenswert.
- ✓ Alle verfügbaren Zeichen nutzen inklusive Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ?!%+...).
- ✓ Das vollständige Passwort sollte nicht im Wörterbuch vorkommen.

Zu vermeiden
- ✘ Namen von Familienmitgliedern, Haustieren, Geburtsdaten etc.
- ✘ Einfache oder bekannte Wiederholungs- bzw. Tastaturmuster wie „asdfgh" oder „1234abcd"
- ✘ Ziffern oder Sonderzeichen an den Anfang oder ans Ende eines ansonsten einfachen Passwortes.
- ✘ Dasselbe Passwort bei mehr als einem Account.

Quelle: BSI Basisschutz — Passwörter

Quelle: BSI Basisschutz – starke Passwörter.

ÜBUNG

Baue deine eigene Passphrase.

1

Denke dir einen Satz aus.

„Meine Tante trinkt jeden Morgen zwei Kaffees!"

2

Wörter kombinieren.

Meine-Tante-trinkt-2-Kaffees-jeden-Morgen!

3

Pro Konto anpassen.

Nicht überall dieselbe Passphrase. Pro Dienst einen Teil variieren.

Wichtig: dieses Beispiel nie 1:1 übernehmen — eigenes bauen.

LIVE-TOOL

Warum „Sommer2026!" nicht clever ist.

cyberwordlists.com

Angreifer testen die beliebtesten Passwörter zuerst. Schau, was auf der Liste steht.

STARK ODER SCHWACH?

`Berlin123`	SCHWACH
`Summer2026!`	SCHWACH
`Morgen-Kaffee-Wolke-74!`	STARK

Wichtig: niemals echte Passwörter in Websites oder Folien eingeben.

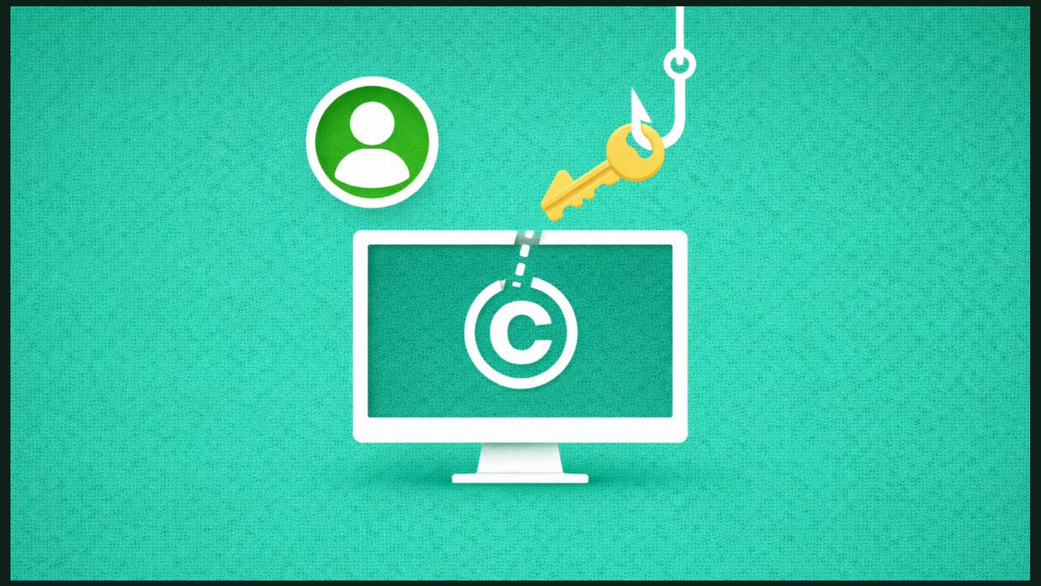
Starke Passwörter wirken auf Menschen langweilig und auf Bots unmöglich.

LIVE-TOOL

Have I Been Pwned?

Datenlecks prüfen — freiwillig und nur mit einer Test-Adresse.

';--have i been pwned?



haveibeenpwned.com →

- → Nur mit einer **Test-Adresse** demonstrieren.
- → Wenn gefunden: **Passwort ändern**, nicht wiederverwenden.
- → **2FA** für wichtige Konten aktivieren.
- → Für **Leak-Benachrichtigungen** anmelden.

„Pwned" heißt nicht Panik. Es heißt: handeln.

2FA & PASSKEYS

Passwort *plus* Sicherheitsgurt.

Zweiter Faktor: App-Code, Smartphone-Bestätigung oder Sicherheits schlüssel.

Passkeys: modern, passwortlos — nutzen, wenn verfügbar.

⚠ Niemals eine 2FA-Abfrage bestätigen, die du **nicht selbst ausgelöst hast** .

Backup-Codes sicher aufbewahren.

2FA ist ein Türsteher – dein Passwort allein steht nicht auf der Liste.

Die meisten Kontoübernahmen scheitern genau hier.

LIVE-TOOL

VirusTotal: Türsteher für Links & Dateien.

virustotal.com

Live-Demo: URL-Tab → ein harmloses Beispiel prüfen → Ergebnis besprechen.

- → URLs, Dateien, Domains, IPs prüfen.
- → Urteile mehrerer Scanner vergleichen.
- ⚠ „Grün" heißt nicht 100 % sicher.
- ⚠ Niemals private oder vertrauliche Dateien hochladen.

GERÄTE-GRUNDLAGEN

Langweilig, aber es *funktioniert wirklich.*

Updates installieren
Handys, Laptops, Browser, Router.

Antivirus aktivieren
Windows Defender reicht für die meisten.

Bildschirmsperre nutzen
PIN, Fingerabdruck oder Gesicht.

Nur offizielle Stores
App Store / Play Store / Hersteller-Seiten.

Backups machen
Fotos, Dokumente — Cloud oder externe Festplatte.

Aufgeräumter Schreibtisch
keine Passwörter auf Haftnotizen.

Updates sind Gemüse für deinen Laptop. Ungeliebt. Gesund.

WENN ES PASSIERT

Ich habe geklickt. Was nun?

1
Sofort das Passwort ändern.

2
Alle aktiven Sitzungen abmelden.

3
Konto & Einstellungen prüfen.

4
Bank informieren · Sperr-Hotline 116 116.

5
Anbieter, Organisation oder Polizei kontaktieren.

Nicht zahlen. Nicht schämen. Melden hilft auch anderen.

SPIEL

Betrüger-Bingo.

Klick jedes Feld, das du erkennst. Drei in einer Reihe → ab in den Müll, nicht klicken.

Dringlichkeit — „jetzt handeln!"	Konto wird gesperrt	Unbekannter Link	Rechtschreibfehler
Komische Absender-Adresse	„Du hast gewonnen!"-Versprechen	Zahlungsaufforderung	Zufälliger QR-Code
Unerwarteter Anhang	Fragt nach Passwort	Gibt sich als deine Bank aus	Gibt sich als Paketdienst aus

Hier heißt „Bingo": nicht klicken.

DEIN PERSÖNLICHER SICHERHEITSPLAN

Drei kleine Schritte schlagen einen perfekten Plan.

HEUTE

Ein wichtiges Passwort ändern — oder einen Passwort-Manager einrichten.

DIESE WOCHE

2FA für E-Mail, Bank und Social Media aktivieren.

AB JETZT

Der 3-Sekunden-Check — before every link, file, or QR code.

Abschlussfrage: welche eine Regel nimmst du heute mit nach Hause?

D1g1tal für alle

DIGITALE SICHERHEIT FOR EVERYONE

Vielen Dank für Ihre Aufmerksamkeit

DIGITALE SICHERHEIT FOR EVERYONE

Klicken mit Bedacht, *nicht in Panik.*

ANMELDUNG

Bitte schicke eine kurze E-Mail mit Vorname, Nachname und E-Mail-Adresse.

contact@januam.com

KONTAKT

Tel: **+49 (0) 176 76642122**

Web: januam.org

Kursseite: januam.org/product/digital-fur-alle

Nicht jeder Link verdient deine Aufmerksamkeit. Manche verdienen nur den Müll.

ALLE WORKSHOP-LINKS AUF EINEN BLICK

Tools & Videos.

HUMOR-VIDEO
Phishing Attack →

VIDEO
5 Methoden gegen Phishing →

QUIZ
Google / Jigsaw Phishing Quiz →

DATENLECK
Have I Been Pwned →

PASSWORTLISTEN
Häufige Passwörter →

LINK-CHECK
VirusTotal →

Erinnerung: niemals echte Passwörter oder vertrauliche Dateien in Demo-Tools eingeben.

QUELLEN & MATERIALIEN

Grundlage der Inhalte.

REFERENZMATERIALIEN

- BSI / Polizei Phishing-Checkliste
- BSI Basisschutz — starke Passwörter
- Checkliste zur Erkennung von Fake News
- Übersicht Spam, Phishing, Smishing, Vishing, Quishing
- BSI-Leitfaden — Inhalte für Cyber-Security-Awareness-Schulungen

TOOLS & BILDNACHWEISE

- VirusTotal docs: docs.virustotal.com
- Have I Been Pwned: haveibeenpwned.com
- Google / Jigsaw Phishing Quiz
- Bilder: TeachPrivacy, Humour Against Hacking, Phil Johnson (Medium), Bitdefender, THE Campus, The Cyber Signal

Diese Folien sind ein Awareness-Workshop für Nicht-Experten. Für Rechtsberatung, Forensik oder technische Incident Response bitte Fachleute hinzuziehen.