Von der Zielscheibe zum Schutzschild

Cybersicherheit im Bildungsalltag

Katja Zierleyn und Marie Menke

Bundesamt
für Sicherheit in der
Informationstechnik

Bild: © AdobeStock/Nirut

Cybercrime in den Schlagzeilen

IT-Sicherheitsvorfall: Varta stoppt Produktion

Der Batteriehersteller Varta AG hat nach einem Cybervorfall die IT-Systeme sowie seine Produktion heruntergefahren.



Varta steht für Vertrieb, Aufladung, Reparatur transportabler Akkumulatoren.
(Bild: Skorzewiak/Shutterstock.com)

13.02.2024, 20:58 Uhr Lesezeit: 2 Min. | Security

Von Dirk Knop

Chinesische Cyberkriminelle hatten jahrelang Zugriff auf Chiphersteller NXP

Die in China verortete Cybergang Chimera soll zwischen 2017 und 2020 Zugang zu NXP-Netzwerken gehabt und vor allem Chipdesigns in die Finger bekommen haben.

Alert!

IT-Management-Plattform SolarWinds über mehrere Wege angreifbar

Die SolarWinds-Entwickler haben mehrere Sicherheitslücken in ihrer Software geschlossen. Angreifer können etwa für Abstürze sorgen.

Cyberkriminalität

Immer mehr Lösegeldattacken

Vor allem Mittelständler sind häufig unzureichend gegen Angriffe mit Erpressungssoftware geschützt. Cyberversicherungen werden teuer.

Susanne Schier Frankfurt, Baden-Baden

Der Markt für US-Staatsanleihen ist der größte und wichtigste der Welt. Und doch gelang es Hackern am vergangenen Donnerstag, dieses riesige Geschäft durcheinanderzubringen. Der US-Ableger der chinesischen Großbank ICBC meldete eine sogenannte Ransomware-Attacke: werden die Preise tendenziell weiter steigen, da auch die Schäden aktuell wieder zunehmen", prognostizierte Hasse.

Die Juristin ist bereits seit mehr als 20 Jahren bei Munich Re tätig und seit 2019 unter anderem für das Cybergeschäft in Europa und Lateinamerika verantwortlich. Im deutschen Markt ist ein gutes Dutzend größerer Erstversicherer im Cy-

Russische Angreifer klauen Quellcode von Microsoft

Seit Monaten greifen staatlich geförderte Cyberkriminelle die Systeme von Microsoft an. Das dauert auch jetzt noch an, dabei konnten Daten entwendet werden.



Datenleck: AT&T setzt die Passwörter von Millionen von Kunden zurück

Nachdem Kontodaten von etwa 73 Millionen aktuellen und ehemaligen AT&T-Kontoinhabern im Dark Web aufgetaucht sind, wird das Unternehmen aktiv.

US-Regierungsbehörden: IT seit Jahren durch chinesische Angreifer unterwandert

Sicherheitsbehörden in den USA schlagen Alarm – Volt Typhoon ist bereits vor Jahren in kritische US-Infrastrukturen eingedrungen. Ursprung der Attacken: China.

Cybercrime: KI-generierte Malware in freier Wildbahn gesichtet

Sicherheitsexperten von HP weisen auf einen beunruhigenden Trend hin: Kriminelle nutzen verstärkt generative KI zur Entwicklung von Malware.

Londoner Kliniken: Cyberkriminelle veröffentlichen Daten

Infolge eines Cyberangriff auf einen Pathologiedienstleister sind Londoner Kliniken im Notbetrieb. Jetzt haben die Cyberkriminellen Daten veröffentlicht.

Cyber-Angreifer erbeuten E-Mails aus Microsofts Cybersicherheitsabteilung

Die kriminelle Gruppe Midnight Blizzard hat sich Zugang zu E-Mails von Microsoft-Mitarbeitern verschafft. Sie wollte wohl wissen, was Microsoft über sie weiß.

Kritische Infrastruktur

Mehr Cyberangriffe auf deutsche Seehäfen

Stand: 05.09.2024 08:56 Uhr

Deutsche Seehäfen waren zuletzt immer häufiger von Cyberangriffen betroffen. Besonders seit Beginn des russischen Angriffskrieges hat die Zahl der Cyberattacken zugenommen.

CYBERANGRIFF

Iranische Hacker greifen laut FBI in US-Wahlkampf ein

Malware: Cyberkriminelle verteilen Malware über Videos auf Youtube

Teils auf verifizierten Youtube-Kanälen werden Spiele-Cracks versprochen. In Wirklichkeit jedoch wird Malware geliefert.

Updates unmöglich: Niederlande müssen Ampeln wegen Sicherheitslücke austauschen

Per Funk können Angreifer die Ampeln aus der Ferne umschalten und somit den Straßenverkehr stören. Der Austausch wird Jahre in Anspruch nehmen.

Ausgangssituation

Angespannte Lage

- BSI-Lagebild: „angespannt bis kritisch“
- Professionalisierte Tätergruppen, teils staatlich unterstützt
- Missbrauch von KI zur Automatisierung von Angriffen
- Zunehmend gezielte und glaubwürdige Täuschungen
- Verbraucherinnen und Verbraucher oft überfordert mit Schutzmaßnahmen
- BSI empfiehlt: Updates, Backups, Sensibilisierung, Informationsangebote



Schadprogramm-Varianten: Durchschnittlich 309.000 neue pro Tag

Schwachstellen in Softwareprodukten: Täglich 78 neue

DDoS-Angriffe: Über dem Mittel Verdopplung des Anteils der bandbreitenstarke Angriffe

Phishing-URLs und -IPs: Täglich 1.000 neue

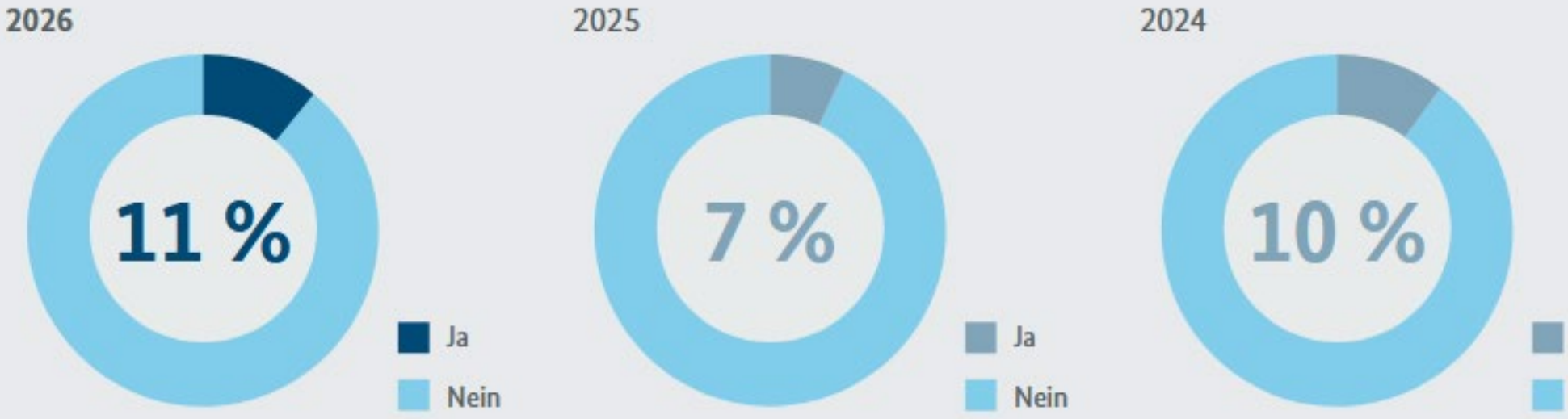
Cybercrime-as-a-Service

Schadprogramm „auf Bestellung“

- Finanziell motivierte Angriffe werden von einer ganzen Schattenwirtschaft aus kriminellen Dienstleistungen rund um den Cyberangriff begleitet.
- Diese wird auch als Cybercrime-as-a-Service (CCaaS, Cyberstraftat als Dienstleistung) bezeichnet.
- Ransomware-, Phishing- und DDoS-as-a-Service
- Professionalisierung des Cybercrime-Ökosystems
- Einstiegshürden für Täter sinken
- Global agierende Täter, schwer zu verfolgen
- Industrialisierung verschärft Bedrohungslage

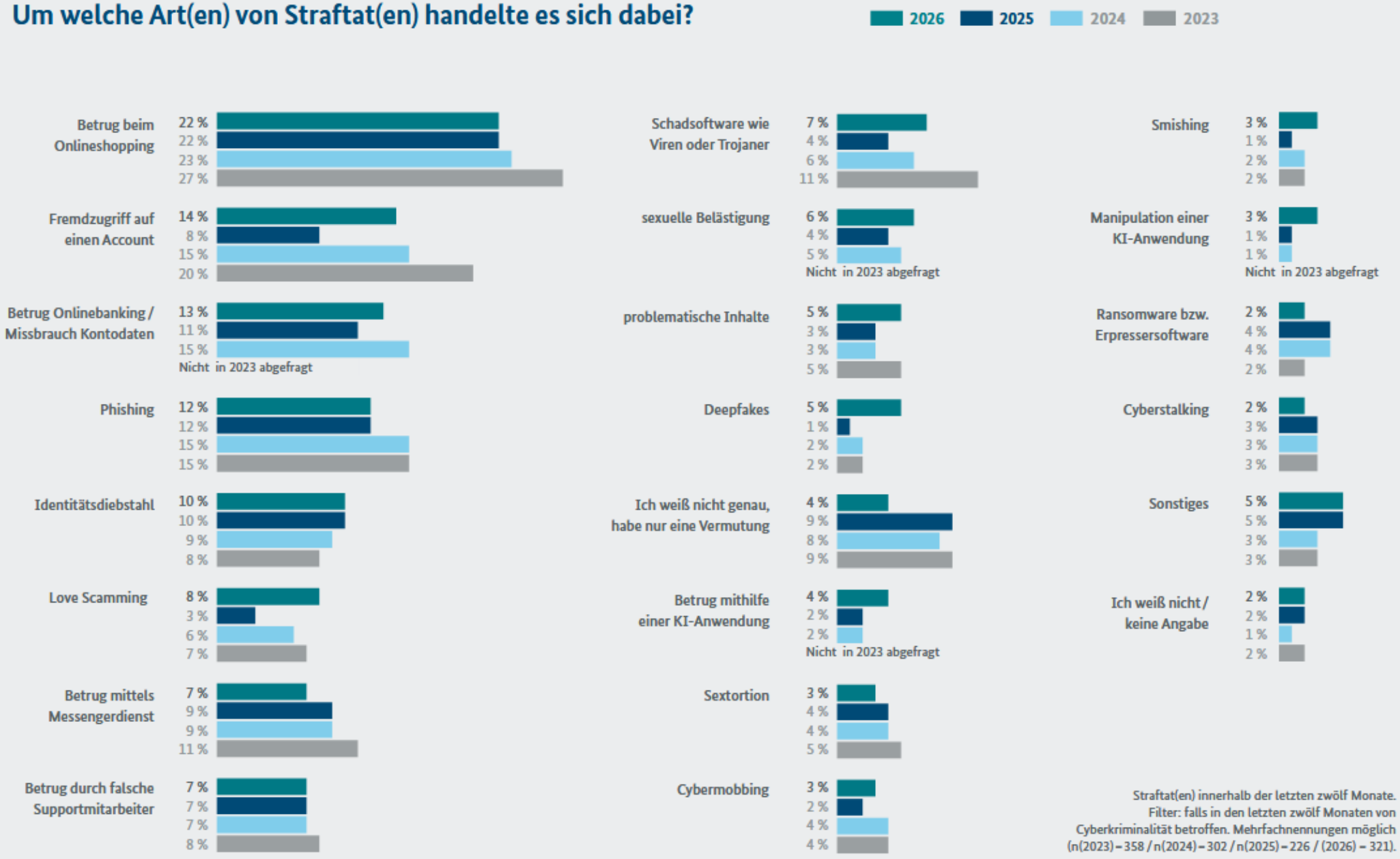


Waren Sie in den letzten zwölf Monaten von Kriminalität im Internet betroffen?



Betroffenheit von Cyberkriminalität letzte zwölf Monate (n(2023) = 3.012 / n(2024) = 3.047 / n(2025) = 3.061 / n(2026) = 3.060).

Sie haben angegeben, in den vergangenen zwölf Monaten Opfer von Cyberkriminalität gewesen zu sein. Um welche Art(en) von Straftat(en) handelte es sich dabei?



Straftat(en) innerhalb der letzten zwölf Monate.
Filter: falls in den letzten zwölf Monaten von Cyberkriminalität betroffen. Mehrfachnennungen möglich (n(2023) = 358 / n(2024) = 302 / n(2025) = 226 / (2026) = 321).

Bundesamt
für Sicherheit in der
Informationstechnik

Das BSI ist die **Cybersicherheitsbehörde des Bundes** und Gestalter einer sicheren Digitalisierung in Deutschland. Unser Ziel ist der sichere Einsatz von Informations- und Kommunikationstechnik in Staat, Wirtschaft und Gesellschaft.

Gründung

01. Januar 1991



Unsere Stakeholder

Staat

Wirtschaft

Gesellschaft

Wissenschaft

Prävention

Detektion

Reaktion

- Übernahme technischer Schutzmaßnahmen
- Nationales IT-Lagezentrum
- Technische Unterstützung und Dienstleistungen
- CERT-Bund und MIRTs
- Beratung und Service-Center
- Kooperation
- Allianz für Cybersicherheit
- UP KRITIS
- Begleitung in der Aus- und Fortbildung
- Technische Richtlinien
- Zertifizierung
- IT-Sicherheitskennzeichen

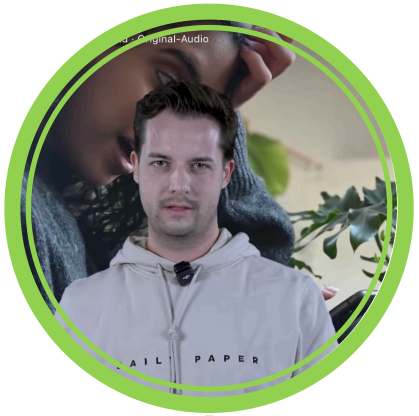
Bundesministerium
des Innern

Bundesamt für Sicherheit
in der Informationstechnik

Angebote des Verbraucherschutzes im BSI











Online

Alles aus einer Hand

Webseite & Newsletter

Die zentrale Anlaufstelle mit Lösungen für alle digitalen Herausforderungen

Print

Cyber zum Anfassen

Wegweiser & Anleitungen

Unsere Produkte bleiben im Kopf und erleichtern den digitalen Alltag

Social Media

Direkte Ansprache

Instagram & Co.

IT-Sicherheit niedrigschwellig erklärt – etwa in kurzen Instagram-Reels

Multimedia

Nicht nur für die Ohren

Podcast & Videoserien

Leicht verdaulich, klug und unterhaltsam – auf allen Streaming-Plattformen

Vor Ort

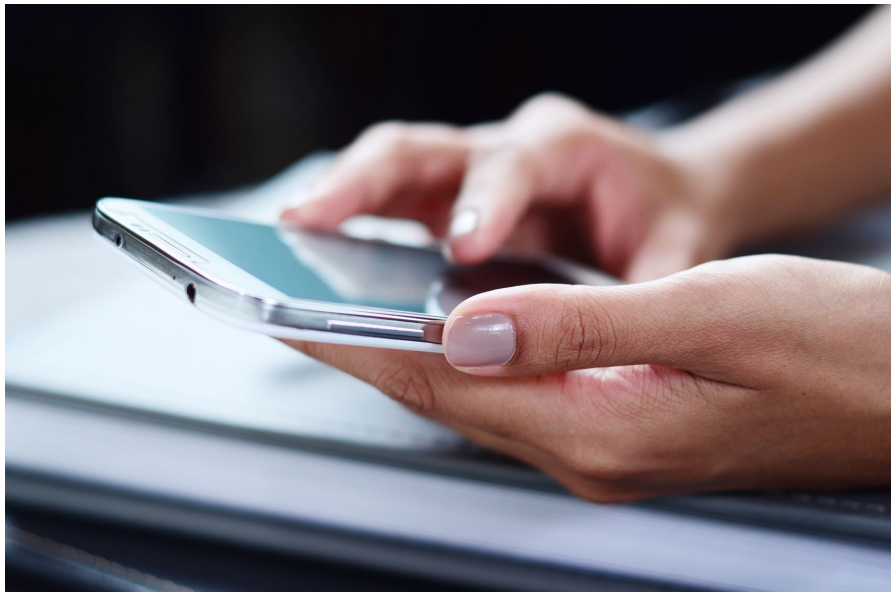
Vor Ort für euch

IFA, Gamescom & Co.

Vorträge und Messeauftritte für den direkten Dialog mit unseren Zielgruppen

Cybersicherheit im Bildungsalltag

Besonderheiten im Bildungswesen



- Cybersicherheit ist **lebenslanges Lernen**: Technik entwickelt sich weiter, Angriffsszenarien und Schutzmaßnahmen ebenso. Daher stellt das BSI verschiedene Materialien für Dozentinnen und Dozenten bereit.
- Der **Alltag im Bildungswesen** und insb. in der Erwachsenenbildung unterscheidet sich von dem Arbeitsalltag in anderen Organisationen.
  - Breiter Einsatz privater Geräte erschwert sowohl das Absichern entsprechender Infrastruktur als auch die Vermittlung
  - Große Heterogenität bezüglich digitaler Kompetenzen, beruflicher und persönlicher Kontexte sowie der individuellen Risikowahrnehmung
- Dozentinnen und Dozenten haben eine besondere **Vorbildfunktion**: Cybersicherheit findet im Alltag immer statt – und nicht nur dann, wenn explizit Cybersicherheit vermittelt werden soll.

Agenda

- Online-Betrug
- Schadsoftware
- Accountschutz
- Kleiner Exkurs: KI
- Wichtigste Präventionsmaßnahmen

Bild: © AdobeStock/Liudmyla

01. Online-Betrug



Bild: © AdobeStock/Azazul

Betrugsmaschen im Internet

- **häufigste Straftat** im Internet
- **Am weitesten verbreitete Formen**: Betrug beim Onlineshopping sowie Phishing
- **Mögliche Ziele** von Online-Betrug:
  - Herausgabe von persönlichen Daten (z. B. Passwort oder Postadresse)
  - Geldzahlungen oder anderweitige Bereicherung, etwa durch Verkauf gefälschter Produkte
  - Einschleusen von Schadsoftware, die dann weitere Ziele verfolgt
- **Einfallswege**, auf denen Opfer kontaktiert werden:
  - Phishing-E-Mails als Klassiker
  - Smishing – Betrug per SMS
  - Aber auch: via QR-Code, am Telefon, über SEO-Poisoning oder Captchas



Oft genutzte Narrative

Zeitdruck

„Zahlen Sie innerhalb von 24 Stunden“

Vertrauen

„Papa, ich hatte einen Unfall und brauche dringend Geld“

Autorität

„Polizei, wir bitten um Ihre Mithilfe“

Glück

„Helfen Sie mir, mein Vermögen von 10 Mio. € außer Landes zu bringen“

Routine

„Sie müssen Ihr Konto verifizieren“

Drohungen

„Wir veröffentlichen das, wenn Sie nicht zahlen“
„Das geht sonst raus an alle Ihre Kontakte“

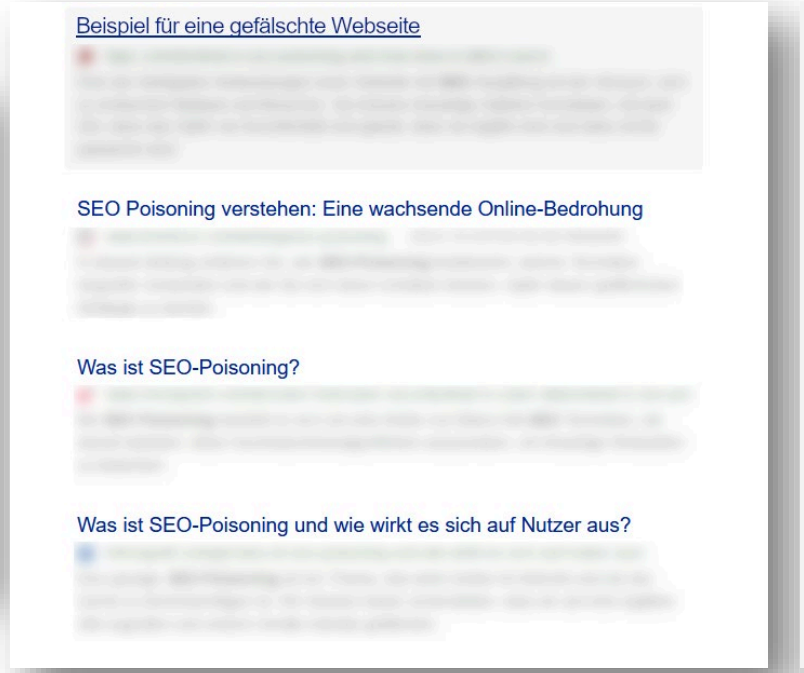
Neugierde

„In der angehängten Liste erfahren Sie, ob Sie für den Fronteinsatz eingezogen werden“

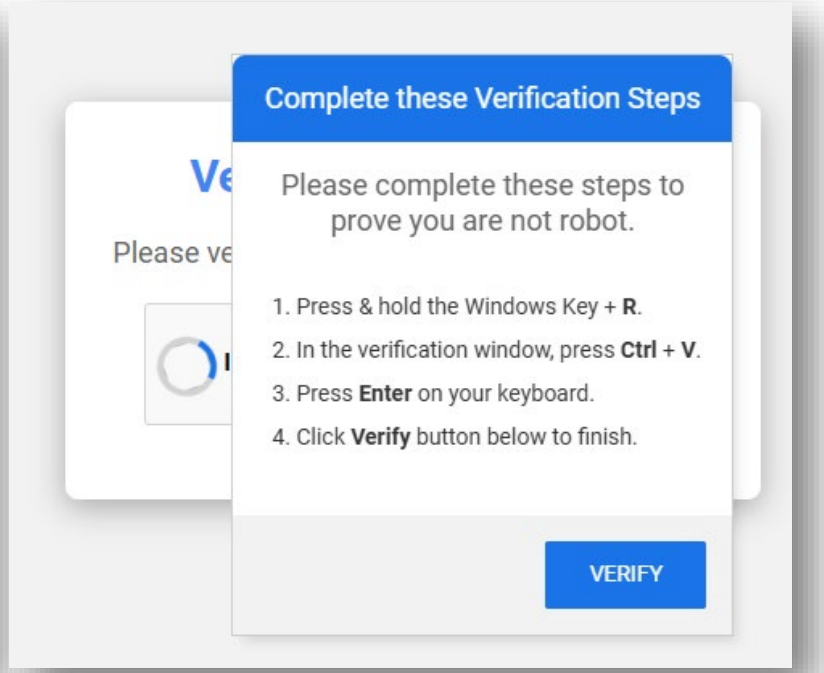
Betrugsmaschen im Internet



„Quishing“ (via QR-Code“)



SEO-Poisoning (via Suchmaschinen-Platzierung)



Fake-Captcha

02. Schadprogramme



Bild: © AdobeStock/Azazul

Schadprogramme

Was hat das mit mir zu tun?

- Computerprogramme, die schädliche Operationen ausführen, Sammelbegriff für bösartige Software (engl. Malware)
- **Ziel:** Systeme infizieren, Daten ausspähen oder beschädigen; mitunter auch Erpressung
- **Typen:** Viren, Würmer, Trojaner, Spyware, Ransomware
- **Mögliche Folgen:**
  - Datenverlust oder -verschlüsselung
  - Identitäts- oder Kontodaten-Diebstahl
  - Manipulation oder Sabotage von Systemen



Wie fange ich mir Schadprogramme generell ein?

E-Mail-Anhänge



Social Engineering



infizierte Webseite



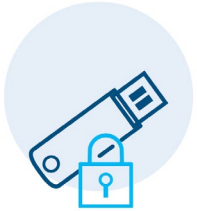
SEO-Poisoning



infizierte Software



USB-Stick



Schadprogramme

Wie kann ich mich schützen?

- Regelmäßige Updates (Betriebssystem, Apps, Router)
- Virenschutz und Firewall aktiv halten
- Vorsicht bei Anhängen und Links – auch von bekannten Kontakten
- Nur offizielle Quellen für Downloads und Apps nutzen
- Regelmäßige Backups auf externen Datenträgern
- Starke Passwörter, Zwei-Faktor-Authentisierung oder, wo möglich, Passkey



03. Accountschutz



Bild: © AdobeStock/Azazul

Wie verwalte ich meine Passwörter sicher?

Passwort-Manager

- Verwahren von Passwörtern und Benutzernamen
- Nur ein Masterpasswort notwendig
- Unterstützung bei der Passwortvergabe
- Warnung vor gefährlichen Websites und möglichen Phishing-Attacken
- Synchronisieren möglich

Tipp: Entscheidungshilfe auf der BSI-Website

E-Mail bis Social Media: Für welche Konten brauchen Sie einen Passwort-Manager?

Browser-basiert oder eigenständig: Welches Programm passt am besten zu Ihren Online-Gewohnheiten?

Cloud oder Festplatte: Wo werden Ihre Daten gesichert?

Sensible Daten: Benötigen Sie einen zweiten Faktor zur Authentisierung?

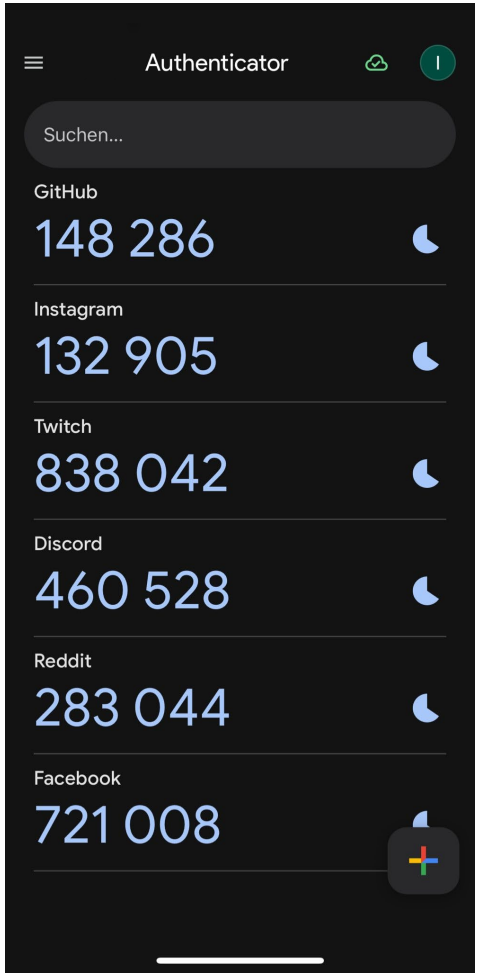
Komplexe Kombinationen: Haben Sie ein sicheres Masterpasswort?

Zwei Faktor-Authentisierung

Mehr Sicherheit für Online-Konten

- Bedeutet: Neben Ihrem Passwort geben Sie beispielsweise noch eine PIN ein, die Sie per SMS auf Ihr Handy bekommen.
- Beide Faktoren sollten aus unterschiedlichen Kategorien stammen, z.B. Wissen (Passwort) und Besitz (TAN-Generator) oder Biometrie (Fingerabdruck)
- Gelangt Ihr Passwort in falsche Hände, sind Ihre sensiblen Daten dennoch geschützt.

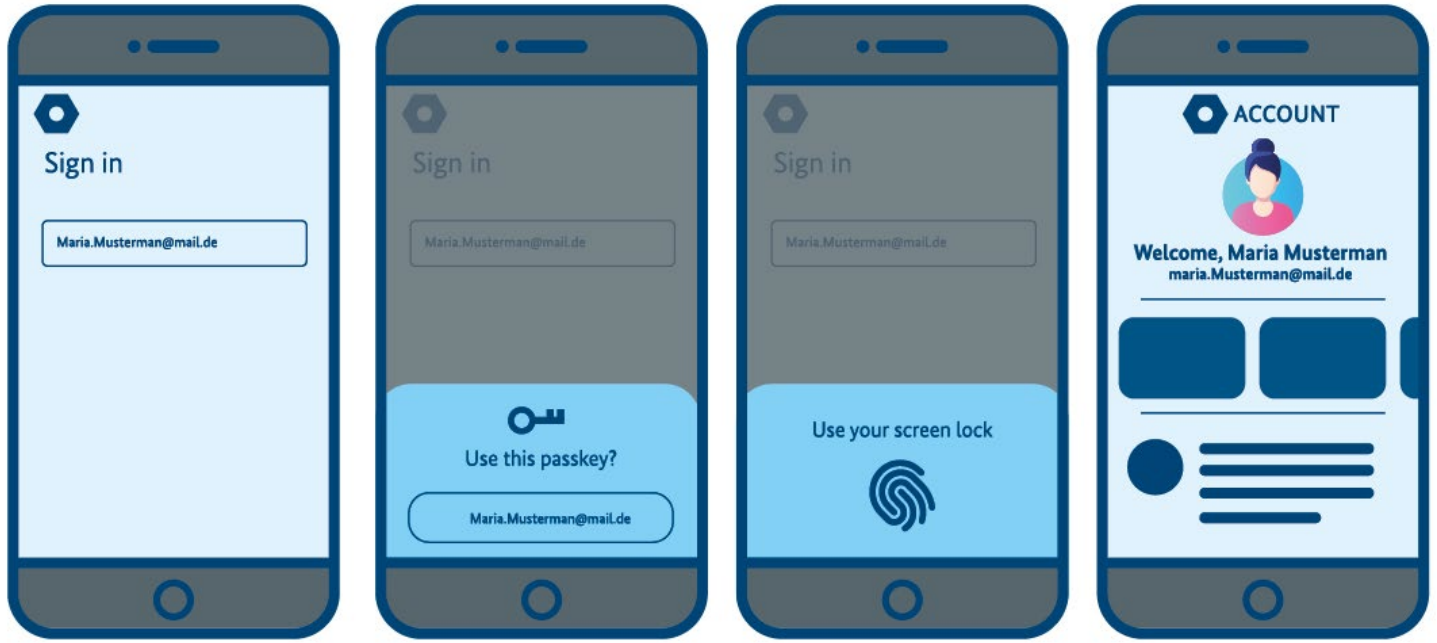
Tipp: Videos auf dem YouTube-Kanal des BSI.



Passkey

Mehr Sicherheit für Online-Konten

- Ersetzt Passwörter gänzlich und enthalt schon eine Zwei-Faktor-Authentisierung
- Kryptografisches Verfahren, bei dem – stark vereinfacht gesagt – ein öffentlicher und ein privater Schlüssel aufeinandertreffen müssen
- Einmal eingerichtet sehr leicht zu nutzen



Tipp: Infoseite auf der BSI-Website

04. Kleiner Exkurs: Künstliche Intelligenz



Bild: © AdobeStock/Azazul

1 Überlegen Sie, ob eine KI-Anwendung für Ihren Zweck geeignet ist.

2 Gehen Sie sparsam mit personenbezogenen und vertraulichen Daten um.

3 Klicken Sie nur auf einen Link, wenn Sie die Anwendung explizit um einen Link gebeten haben.

4 Beziehen Sie KI-Anwendungen nur aus seriösen Quellen.

5 Formulieren Sie Ihre Eingaben mit Bedacht und möglichst spezifisch.

6 Lassen Sie sich nicht täuschen: Vorsicht vor Betrugsmaschen.

7 Sorgen Sie für einen grundlegenden Schutz Ihrer Geräte, Anwendungen und Konten.

8 Bleiben Sie wachsam – und informiert.

Zusatztipps für Fortgeschrittene:

9 Behalten Sie im Hinterkopf: Eine KI-Anwendung ist abhängig von ihren Trainingsdaten.

10 Informieren Sie sich in den Datenschutzerklärungen und AGB z. B. über die Rechte, die der Hersteller sich einräumt.

11 Prüfen Sie Plugins und Zusatzangebote von Drittanbietern vor der Nutzung.



05. Wichtigste Präventionsmaßnahmen

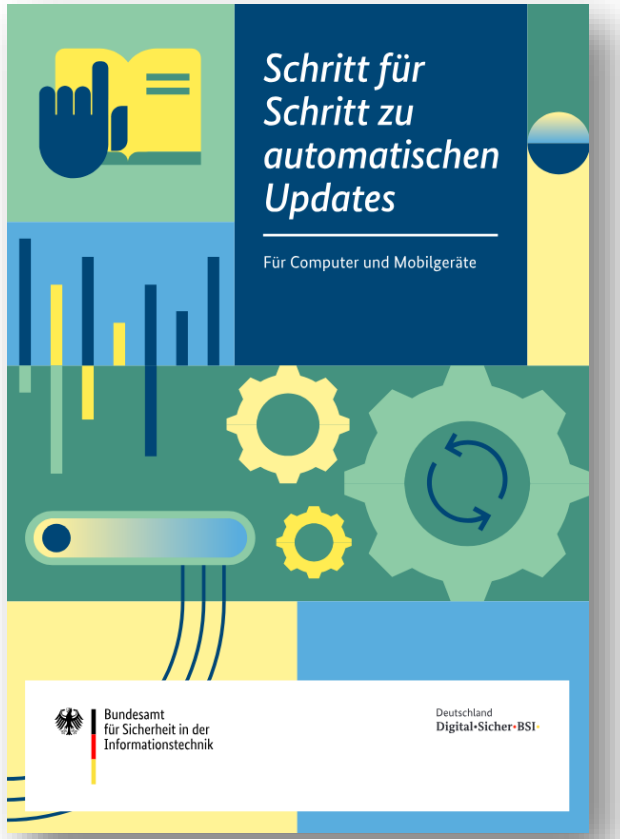


Bild: © AdobeStock/Azazul

Schutzmaßnahmen und Prävention

Prüfen Sie, ob Sie für alle Geräte und Anwendungen automatische Updates aktiviert haben!

- **Warum wichtig:**
  - Schließen Sicherheitslücken
  - Schutz vor Schadsoftware und Angriffen
- **Empfehlungen:**
  - Regelmäßige Aktualisierung von Betriebssystem, Apps und Software
  - Automatische Updates nutzen, wenn möglich
  - Auch Router, IoT- und Smart-Home-Geräte einbeziehen



Schutzmaßnahmen und Prävention

Erstellen Sie eine Liste Ihrer Benutzerkonten und prüfen Sie, ob diese ausreichend abgesichert sind!

- Starke Passwörter verwenden
- Passwortmanager einrichten
- Zwei-Faktor-Authentisierung (2FA) aktivieren
- Wo möglich, auf Passkeys umsteigen



Grafik: Quelle: Bundesregierung/Tybussek

Schutzmaßnahmen und Prävention

Legen Sie regelmäßig eine Datensicherung an!

- **Warum wichtig:**
  - Schutz vor Ransomware und Datenverlust
  - Wiederherstellung nach Geräteausfall
- **Empfehlungen:**
  - Regelmäßig Backups erstellen
  - Unterschiedliche Optionen: automatisierte vs. manuelle Datensicherung, lokale Datenträger
  - Daten verschlüsseln
  - Speicherung an getrennten Orten (z.B. externes Laufwerk und Cloud)



Schutzmaßnahmen und Prävention

Prüfen Sie, ob Virenschutz und Firewall aktiviert sind!

- **Virenschutzprogramme:**
  - Schutz vor Schadsoftware
  - Regelmäßige Updates erforderlich
- **Firewall:**
  - Überwacht und kontrolliert den Datenverkehr
  - Blockiert unerwünschte Verbindungen (BSI)
- **Empfehlung des BSI:**
  - Nutzung integrierter Sicherheitsfunktionen
  - Bei Bedarf zusätzliche Sicherheitssoftware installieren



Schutzmaßnahmen und Prävention

Bleiben Sie wachsam!

- **Phishing:**
  - Täuschende E-Mails oder Webseiten
  - Ziel: Herausfinden von Passwörtern oder persönlichen Daten (BSI)
- **Social Engineering:**
  - Manipulation durch Vertrauen oder Dringlichkeit
  - Ziel: Nutzer zu unvorsichtigen Handlungen bewegen
- **Empfehlung:**
  - Vorsicht bei unerwarteten Nachrichten oder Anrufen
  - Keine sensiblen Informationen preisgeben
  - Offizielle Kanäle für Rückfragen nutzen

Vielen Dank für Ihre Aufmerksamkeit!

Gibt es Fragen?

Referat K 13
Informationsvermittlung und Verbrauchersensibilisierung

referat-k13@bsi.bund.de
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us:

Bild: © AdobeStock/Nirut