

# Unsichere Webseiten erkennen

Michael Schwarz | CISPA | 16. September 2023





# Wer bin ich?



---

Fokus auf Seitenkanal Angriffe

 @misc0110

 michael.schwarz@cispa.de

**Michael Schwarz**

Faculty @ CISPA

**Sicher?**

**Vertrauenswürdig?**

---



# Sicher? Vertrauenswürdig?

Internet-Filiale - Sparka

sparkasse-saarbruecken.de...

Sparkasse Saarbrücken Anmelden

### Die neue Sparkassen-Card (Debitkarte)

Ein echtes Multitalent.

Schalten Sie Ihre Sparkassen-Card (Debitkarte) jetzt bei 3-D Secure frei und genießen Sie sicheres Online-Shopping, weltweites Bezahlen und direkte Abbuchung.

[Mehr erfahren](#)

Neue Telefonnummern  
Online-Kredit beantragen  
DebitBank Depot online eröffnen  
Sparkassendepot online eröffnen  
Bausparangebot berechnen  
Vorteilswelt

#### Neues Online-Banking

Besser. Neuer. Übersichtlicher.

Das neue Online-Banking ist da. Erleben Sie mehr Übersicht und neue Funktionen. Damit Sie Ihre Finanzen noch besser im Griff haben.

[Mehr erfahren](#)

#### Sparkassen-KontoSchutz

Flexibel ist einfach.

Mit dem Sparkassen-KontoSchutz für Ihr Girokonto.

[Mehr erfahren](#)

#### Ihre Grüne Kreditkarte

Einfach nachhaltig

Möchten Sie sich gemeinsam mit uns nachhaltig engagieren?

[Mehr erfahren](#)

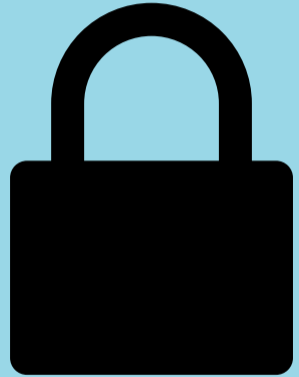


# Sicher? Vertrauenswürdig?





# Was bedeutet das Schloss?





# Was es bedeutet



Schloss

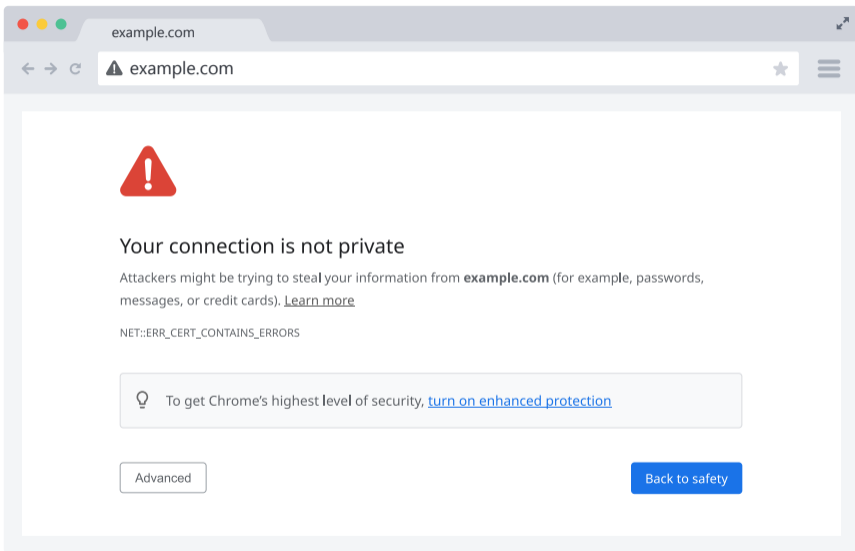
=



Abhörer



# Abhörsicherheit ist Standard







# Was es NICHT bedeutet



Schloss



Vertrauen



# Jeder kann ein Zertifikat bekommen



Let's Encrypt

[Dokumentation](#)

[Hilfe bekommen](#)

[Spenden](#)

[Über uns](#)

[Sprachen](#)



ISRG celebrates 10 years of helping build a brighter Internet →

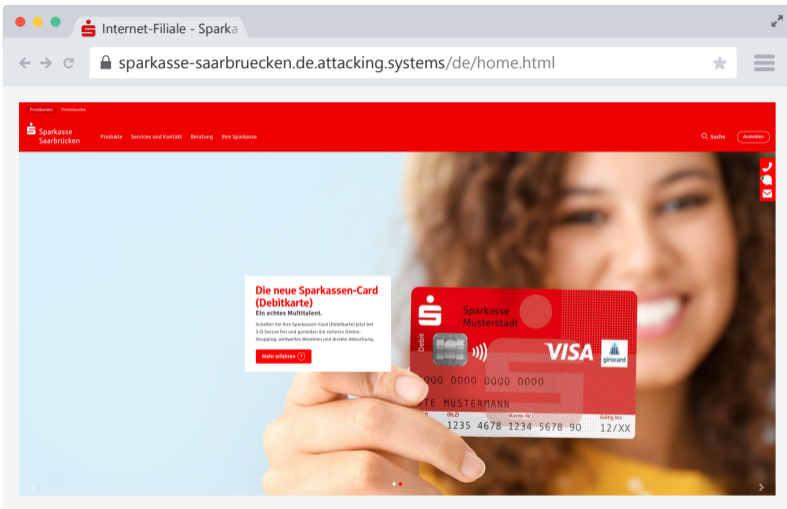
## Über Let's Encrypt

Let's Encrypt ist eine freie, automatisierte und offene Zertifizierungsstelle (CA) und läuft für die Öffentlichkeit. Der Dienst wird zur Verfügung gestellt von [Internet Security Research Group \(ISRG\)](#).

Wir geben Menschen die digitalen Zertifikate, die sie zur Aktivierung von HTTPS (SSL/TLS) auf ihrer Webseite benötigen, kostenlos und in der benutzerfreundlichsten Variante, die uns möglich ist. Wir machen das, um ein noch sicheres Web zu erstellen, das die Privatsphäre akzeptiert.



# Gesamte Adresse ist Wichtig





# Gesamte Adresse ist Wichtig

Internet-Filiale - Sparkasse

sparkasse-saarbruecken.de.attacking.systems/de/home.html

Internet-Filiale - Sparkasse

sparkasse-saarbruecken.de/de/home.html

Produkte | Sparkassen

Sparkasse Saarbrücken

Produkte Services und Kontakt Beratung Ihre Sparkasse

Suche Anmelden

**Die neue Sparkassen-Card (Debitkarte)**  
Ein echtes Multitalent.  
Schicken Sie Ihre Sparkassen-Card (Debitkarte) jetzt bei 3-D Secure frei und genießen Sie sicheres Online-Shopping, weltweites Bezahlen und direkte Abbuchung.

Mehr erfahren

Debit Sparkasse Musterstadt

VISA girocard

0000 0000 0000 0000

TE MUSTERMANN

1235 4678 1234 5678 90 12/XX

An illustration on a light blue background. On the left, a hand in a blue suit sleeve holds a silver key. To the right of the hand is a white rectangular sign with a dark blue border. The sign contains the text 'Das Schloss ist wichtig, aber nicht ausreichend.' in black and blue font.

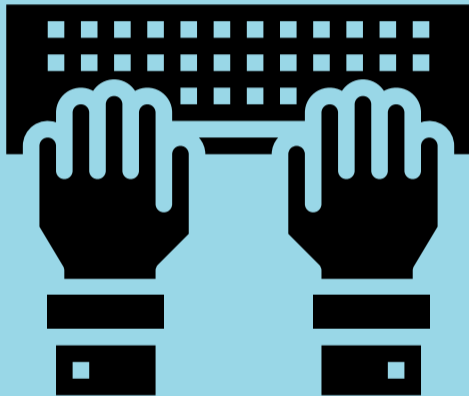
Das **Schloss** ist wichtig, aber  
**nicht ausreichend.**

# Typosquatting

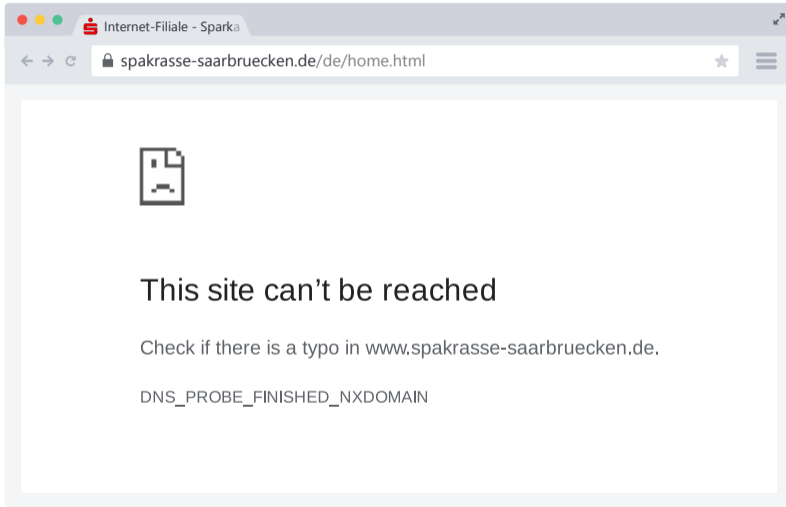
---



# Schon einmal **vretippt?**



# Vertippen passiert





# Vertippen passiert

The screenshot shows a web browser window with the address bar containing "sparkasse-saarbruecken.de/de/home.html". The website header is red and features the Sparkasse Saarbrücken logo, navigation links for "Produkte", "Services und Kontakt", "Beratung", and "Für Sparkasse", a search bar, and a "Anmelden" button. The main content area features a large image of a smiling woman holding a red Sparkasse debit card. A white callout box is overlaid on the image, containing the following text:

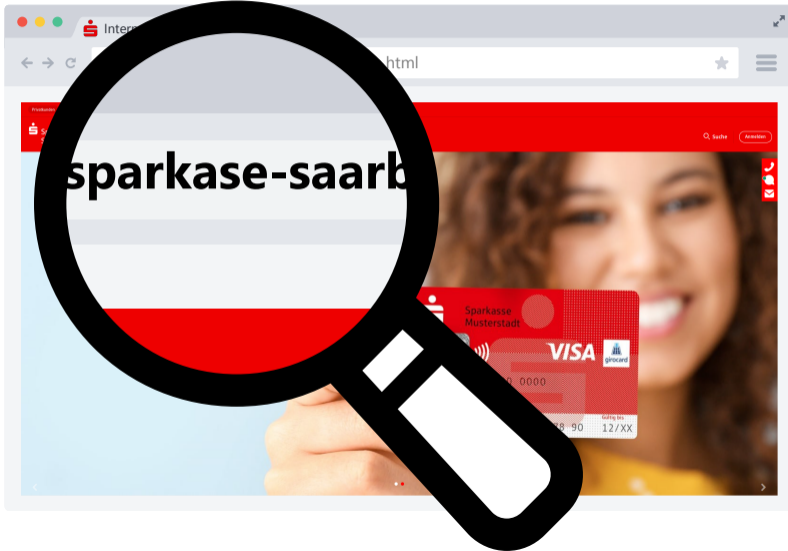
**Die neue Sparkassen-Card (Debitkarte)**  
Ein echtes Multitalent.  
Schließen Sie Ihre Sparkassen-Card (Debitkarte) jetzt bei 3-D Secure End und genießen Sie sicheres Online-Shopping, weltweites Bezahlen und direkte Abbuchung.

[Mehr erfahren](#)

The card itself is red and displays the Sparkasse logo, "Sparkasse Musterstadt", "Debit", "VISA", and "girocard" logos. The card number is "0000 0000 0000 0000", the name is "MUSTERMANN", and the expiration date is "12/XX".



# Vertippen passiert





# Homographische Angriffe

The screenshot shows a browser window with the URL 'coinex.com/'. The website header includes the CoinEx logo and navigation links for Fiat, Märkte, Spot, Futures, Finanzen, Aktion, and Mehr. A 'regulieren' button is visible in the top right. The main content area features the heading 'Globale Kryptowährungsbörse' and a registration form with an input field for 'E-Mail-Adresse' and a 'Jetzt registrieren' button. Below this, there is a grid of five cryptocurrency price cards:

Symbol	Price (USD)	Change (%)
BLAT/USD	0.065080	-1.43%
XMR/USD	143.93	-1.29%
ADA/USD	0.2606	-0.68%
PEPE/USD	0.000008241	-0.84%
XRP/USD	0.5155	-0.63%

Below the price cards are three promotional banners: 'Warnung vor Phishing-Betrug Bewahre Passwörter sicher auf', 'CoinEx-Spot-Ranking' (offering 5,000 USD), and '3 Monate Ohne Vorbehalt' (offering 10% registration bonus). A news snippet below reads 'CoinEx hat die Belohnungen des XNA Airdrops verteilt!'. At the bottom, there is a 'Markt Trend' section with a search bar and a table of market data:

Coin-Typ	Letzter Preis(USD)	24h %Veränderung	Wert(USD)	Markt
BTC Bitcoin	25,950.41	-0.28%	505.40B	

A 'Hilfe' button is located in the bottom right corner of the page.



# Homographische Angriffe

The screenshot shows a browser window with the URL 'coinex.com/'. The website header includes the CoinEx logo and navigation links for Fiat, Märkte, Spot, Futures, Finanzen, Aktion, and Mehr. A 'regulieren' button is visible in the top right. The main content area features the heading 'Globale Kryptowährungsbörse' and a registration form with an input field for 'E-Mail-Adresse' and a 'Jetzt registrieren' button. Below this, there are five market price cards for various cryptocurrencies: BLAT/USD, XMR/USD, ADA/USD, PEPE/USD, and XRP/USD. A carousel of promotional banners follows, including one about phishing warnings and another about a 'CoinEx-Spot-Ranking' with a 5,000 USD reward. At the bottom, there is a 'Markt Trend' section with a search bar and a table of market data.

Coin-Typ	Letzter Preis(USD)	24h %Veränderung	Wert(USD)	Markt
BTC Bitcoin	25,950.41	-0.28%	505.40B	



## Ein genauer Blick



**Echte Webseite**



## Ein genauer Blick



**Echte Webseite**

Lateinische Zeichen



## Ein genauer Blick



**Echte Webseite**  
Lateinische Zeichen



**Falsche Webseite**



## Ein genauer Blick



**Echte Webseite**  
Lateinische Zeichen



**Falsche Webseite**  
Kyrillische Zeichen



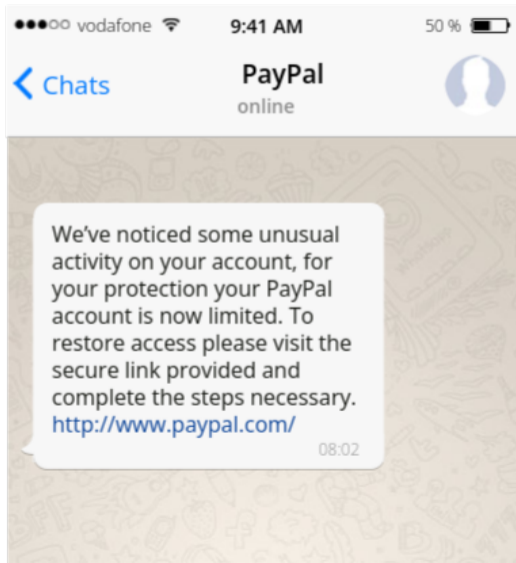


# Verschiedene Alphabete

Latein	Kyrillisch	Griechisch	Hebräisch
a	а	α	
c	с		
e	е	ε	
o	о		ו
p	р	ρ	
x	х	χ	
y	у	Υ	
i	и	ι	י
n	н	η	נ



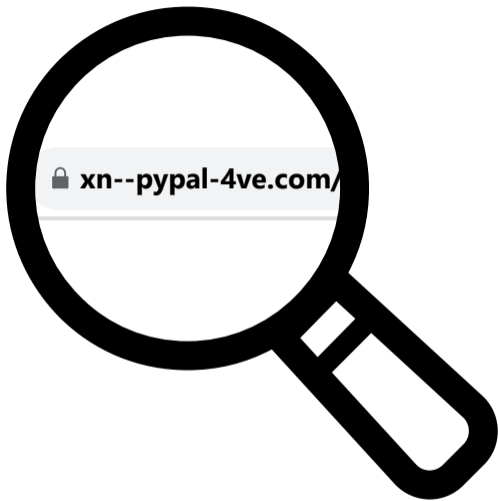
# Homographische Angriffe: Links

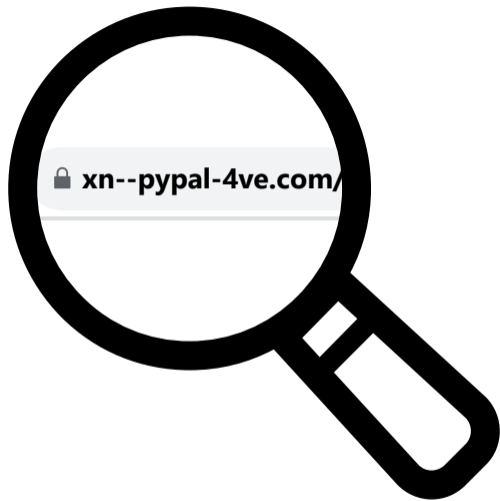


An illustration of a hand in a blue suit sleeve holding a silver key. The key is positioned to the left of a white rectangular sign with a dark blue border. The sign contains text in German. The background is a solid light blue color.

Das **Schloss** steht nur für  
**Abhörsicherheit.**

Es muss nicht die richtige  
**Webseite sein!**






Spezielle Anzeige bei **mehreren** Alphabeten



## Browser Hinweise

✕

**Did you mean google.com?**

Attackers sometimes mimic sites by making hard-to-see changes to the web address.

[Learn more](#)

Yes, continue



Google Safe Browsing



Google Safe Browsing







# Google Safe Browsing: bmbf.de

The screenshot shows a web browser window with the address bar containing the URL `https://transparencyreport.google.com/safe-browsing/search?url=https:%2F%2...`. The page title is "Google Transparency Report" and the active tab is "Site status". The main heading is "Safe Browsing site status". Below the heading is a paragraph explaining Google's Safe Browsing technology. A search box labeled "Check site status" contains the URL `https://www.st-ingbert.de`. The search results show a green checkmark and the text "No unsafe content found".

Google Transparency Report

Overview Site status

## Safe Browsing site status

Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can search to see whether a website is currently dangerous to visit.

Check site status

`https://www.st-ingbert.de` 🔍

Current status

✔ No unsafe content found

# VirusTotal: goggle.com

The screenshot shows the VirusTotal interface for a URL analysis. The browser address bar displays the URL: `virustotal.com/gui/url/dbaaccead676025a3a07e8f138053b6fd5ed231c07b132...`. The main content area shows the URL `http://www.google.com/` with a Community Score of 10/90. A warning indicates that 10 security vendors flagged this URL as malicious. The analysis status is 200, and the last analysis date is 14 hours ago. The 'DETECTION' tab is active, showing a table of security vendors' analysis results.

10 security vendors flagged this URL as malicious

Reanalyze Search Graph API

Status: 200 | Last Analysis Date: 14 hours ago

Community Score: 10 / 90

DETECTION | DETAILS | LINKS | COMMUNITY 23 +

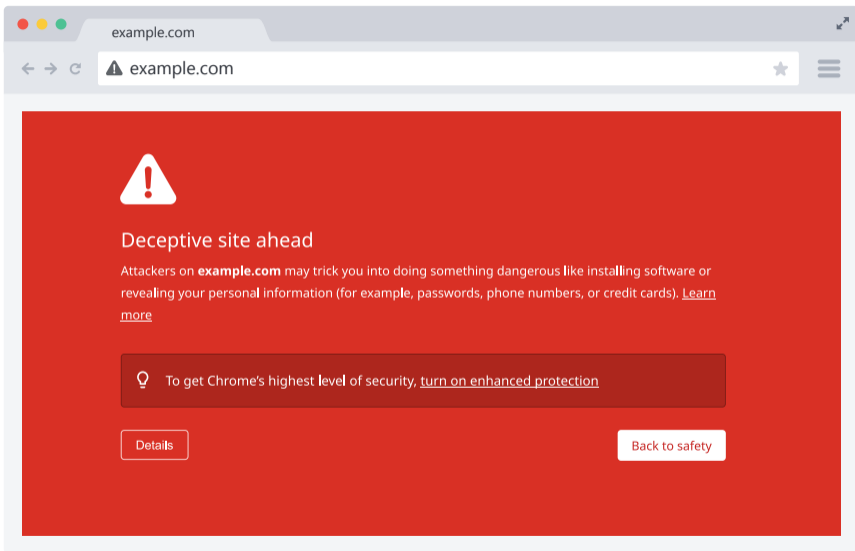
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.


Security vendors' analysis Do you want to automate checks?

Avira	Phishing	CyRadar	Malicious
Dr.Web	Malicious	Fortinet	Phishing
Kaspersky	Phishing	Lionic	Malicious
Seclookup	Malicious	Sucuri SiteCheck	Malicious
VIPRE	Malicious	Webroot	Malicious
ESET	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean	AlertVault	Clean

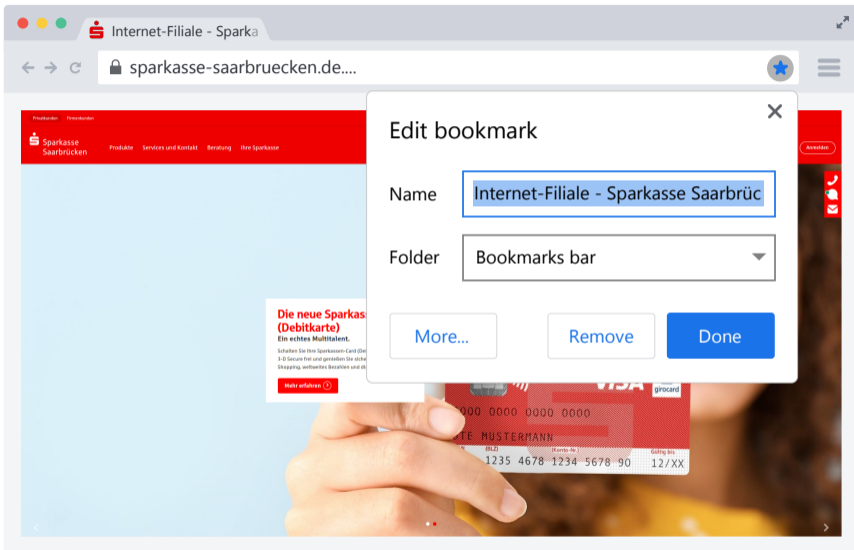


# Browser Warnungen





**Warnungen vom Browser  
nicht ignorieren!  
Besser einmal zu oft  
kontrollieren.**



The screenshot shows a web browser window with the address bar displaying "sparkasse-saarbruecken.de...". The page content is partially obscured by a white "Edit bookmark" dialog box. The dialog box has a title bar with a close button (X) and contains the following fields:

- Name:** A text input field containing "Internet-Filiale - Sparkasse Saarbrüc".
- Folder:** A dropdown menu currently set to "Bookmarks bar".

At the bottom of the dialog box, there are three buttons: "More...", "Remove", and "Done".

In the background, the website header for "Sparkasse Saarbrücken" is visible, along with a promotional banner for "Die neue Sparkas (Debitkarte) Ein echtes Multitalent." and a hand holding a Visa girocard.



# Passwort Manager

The screenshot shows a web browser window with the address bar displaying "sparkasse-saarbruecken.de/de/home.html". The page header is red with the Sparkasse Saarbrücken logo and "Anmelden" link. The main content area is titled "Melden Sie sich an" and contains a login form. The form has a text input for "Anmeldename: 12345678" with a link "Eingabe ändern" and a password input for "Passwort/PIN" with an "Anzeigen" toggle. A green notification bar shows "Ihr Gerät" with a checkmark and "12345678". A password manager popup is open over the password field, showing "Manage passwords..." and "Anmelden" buttons. At the bottom, there are links for "Sicherheitshinweise" and "Zugangsdaten vergessen?".

Internet-Filiale - Sparka

sparkasse-saarbruecken.de/de/home.html

Sparkasse Saarbrücken [Anmelden](#)

### Melden Sie sich an

Anmeldename: 12345678 [Eingabe ändern](#)

Passwort/PIN [Anzeigen](#)

Ihr Gerät 12345678 [Anmelden](#)

[Manage passwords...](#) [Anmelden](#)

[Sicherheitshinweise](#) · [Zugangsdaten vergessen?](#)

Sie haben noch kein Online-Banking? [Jetzt freischalten](#) →

Sie sind noch kein Sparkassen-Kunde? [Weitere Informationen](#) →

An illustration of a hand in a blue suit sleeve holding a grey tablet. The tablet screen is white with a dark blue border and contains the text 'Browserfunktionen verwenden für mehr Sicherheit.' in black and blue. The background is a solid light blue.

**Browserfunktionen  
verwenden für mehr  
Sicherheit.**



- Kriminelle werden immer kreativer
- Schutz von Browsern ist nicht perfekt
- Bestehende Funktionen nutzen für mehr Sicherheit
- Mitdenken ist trotzdem extrem wichtig



# Unsichere Webseiten erkennen

Michael Schwarz | CISPA | 16. September 2023

