

Image by Epic Top 10 Site

Cybercrime: Verbrechen im und gegen das Netz

Das Dezernat LPP 222 Cybercrime

Hauptaufgaben

- „Computerkriminalität“
(herausragende Fälle, hoher Schaden, neue/unbekannte Tatbegehungsweise, besonderer Sachverstand)
- Zentralstelle Cybercrime für das Saarland
(Ansprechpartner für die Polizeidienststellen im Land und das BKA)
- ZAC – Zentrale Ansprechstelle Cybercrime
(für Wirtschaftsunternehmen)

Cybercrime im engeren Sinne

Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten

Cybercrime im weiteren Sinne

Straftaten, die mittels Informationstechnik begangen werden

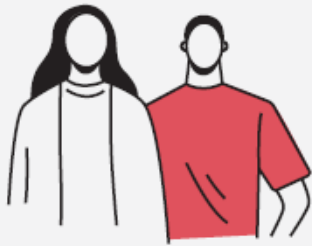
Was genau versteht man eigentlich unter Cybercrime?

Bild: Freepik.com

Die Lage der IT-Sicherheit in Deutschland 2022

Top 3-Bedrohungen je Zielgruppe

Gesellschaft



Identitätsdiebstahl
Sextortion
Fake-Shops im Internet

Wirtschaft



Ransomware
Schwachstellen, offene oder
falsch konfigurierte Online-Server
IT-Supply-Chain: Abhängigkeiten
und Sicherheit

Staat und Verwaltung



Ransomware
APT
Schwachstellen, offene oder
falsch konfigurierte Online-Server

Quelle: Die Lage der IT-Sicherheit in Deutschland, BSI

Ausspähen von Daten



**Wie gelangen Kriminelle an unsere Daten
und was fangen sie damit an?**

Phishing – Das Angeln nach Daten



Unter Phishing (Kunstwort aus **password** und **fishing**) versteht man den Versuch, mittels gefälschter Webseiten, E-Mails, Social Engineering, usw. an Daten des Opfers zu gelangen.

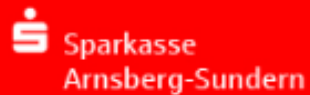
Phishing - Ein Beispiel

The image displays three overlapping screenshots illustrating a phishing attack targeting Sparkasse Arnsberg-Sundern customers.

Top Screenshot (Email): A phishing email from "Sparkasse informiert" with the address "<suporte@rebootonline.com.br>". The email header includes "An" and "Dr". The main body features the Sparkasse logo and the text "Erweiterung der Online-Banking Funktionalität". Below this, it states "Sehr geehrte Nutzer" and mentions "um die Anwendung unsere Updates getätigt". It then says "Zur Freischaltung der n schnellstmöglich in Ihre Dies können Sie einfach". A red button labeled "Jetzt Anmelden" is visible, followed by "Vielen Dank für Ihre Koo".

Middle Screenshot (Fake Website): A browser window showing a fake Sparkasse website. The address bar indicates a malicious URL: "Schädlich | homelogsapk.com/SSA0216OG". The page features the Sparkasse logo and a navigation bar with "Service-Center", "Online-Banking", "Produkte & Angebote", "Firmenkunden", and "Immobilien". A central message box titled "S-CERT Verfahren Sicherheitsumstellung" states: "Bitte melden Sie Ihr Konto bis zum 11.11.2021 für das neue S-CERT Sicherheitssystem an, der Grund dafür sind die sicherheitsrelevanten Systemupdates." Below this, it says "Bitte wählen Sie Ihre Sparkasse" and provides a field for "BLZ oder Ort".

Bottom Screenshot (Fake Website): Another browser window showing a fake Sparkasse website. The address bar indicates a malicious URL: "Schädlich | homelogsapk.com/sicher-einloggen". The page features the Sparkasse logo and a navigation bar with "Service-Center", "Online-Banking", "Produkte & Angebote", "Firmenkunden", and "Immobilien". The main heading is "Online-Banking: Login". Below this, it says "Ihre Zugangsdaten" and provides fields for "Anmeldename oder Legitimations-ID:" (filled with "Max Mustermann") and "PIN:" (filled with "*****"). A red button labeled "Anmelden" is visible. At the bottom, it says "Mit dem Absenden Ihrer Anmeldedaten bestätigen Sie, dass Sie unsere Sicherheitshinweise zur Kenntnis genommen haben." and includes links for "Impressum", "AGB", "Datenschutz", and "Sicherheitshinweise".



Erweiterung der Online Banking Funktionalitäten

Sehr geehrte Nutzer des Onlinebankings

um die Anwendung unseres Online Bankings zu vereinfachen wurden
Updates getätigt

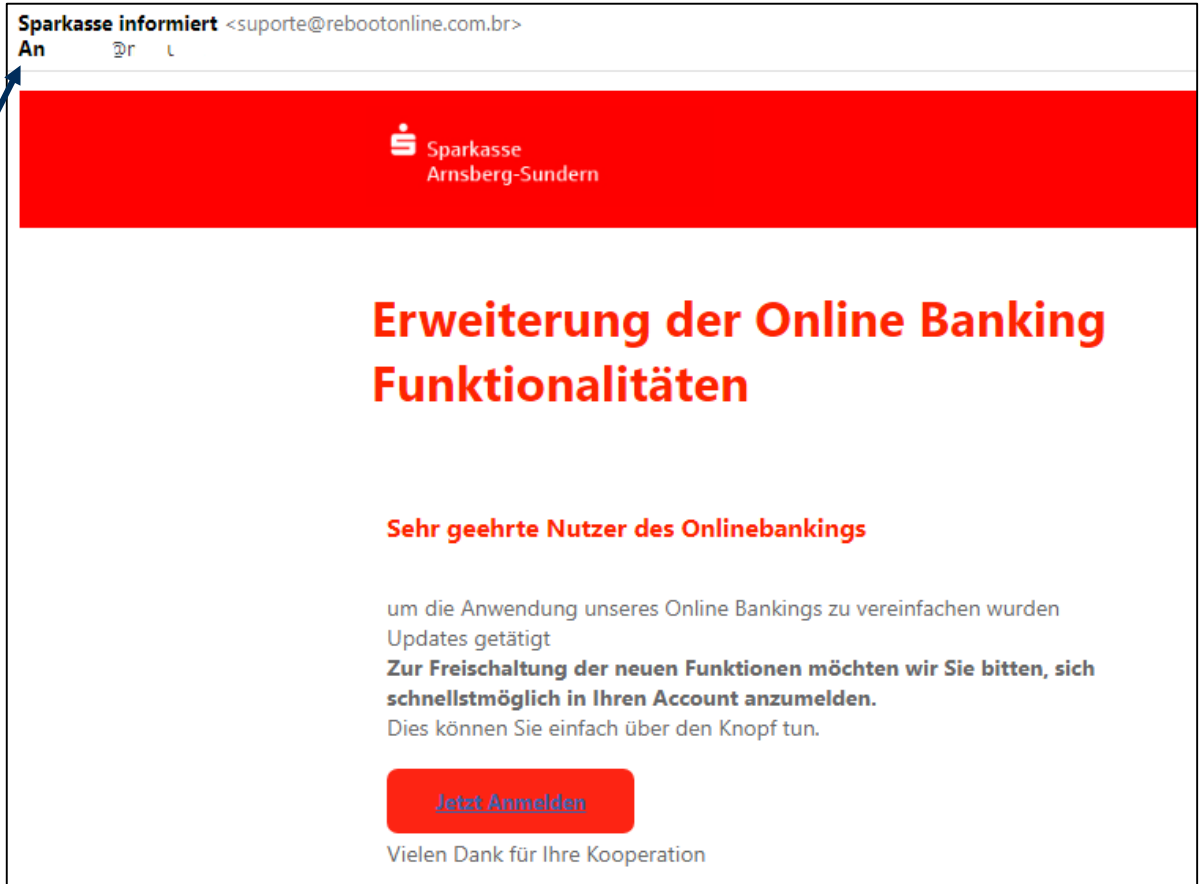
**Zur Freischaltung der neuen Funktionen möchten wir Sie bitten, sich
schnellstmöglich in Ihren Account anzumelden.**

Dies können Sie einfach über den Knopf tun.

[Jetzt Anmelden](#)

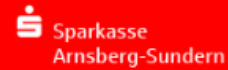
Vielen Dank für Ihre Kooperation





Sparkasse informiert <suporte@rebootonline.com.br>
An @r L

ACHTUNG: Absender ist nicht die Sparkasse !!!



Erweiterung der Online Banking Funktionalitäten

Sehr geehrte Nutzer des Onlinebankings

um die Anwendung unseres Online Bankings zu vereinfachen wurden
Updates getätigt

**Zur Freischaltung der neuen Funktionen möchten wir Sie bitten, sich
schnellstmöglich in Ihren Account anzumelden.**

Dies können Sie einfach über den Knopf tun.

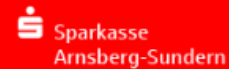
[Jetzt Anmelden](#)

Vielen Dank für Ihre Kooperation



Bin ich Kunde bei dieser Sparkasse ?





Erweiterung der Online Banking Funktionalitäten

Sehr geehrte Nutzer des Onlinebankings

um die Anwendung unseres Online Bankings zu vereinfachen wurden Updates getätigt

Zur Freischaltung der neuen Funktionen möchten wir Sie bitten, sich schnellstmöglich in Ihren Account anzumelden.

Dies können Sie einfach über den Knopf tun.

[Jetzt Anmelden](#)

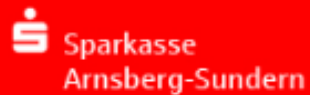
Vielen Dank für Ihre Kooperation

Sehr geehrte Nutzer des Onlinebankings

um die Anwendung unseres Online Bankings zu vereinfachen wurden

Verdächtig: Persönliche Anrede fehlt !





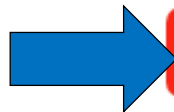
Erweiterung der Online Banking Funktionalitäten

Sehr geehrte Nutzer des Onlinebankings

um die Anwendung unseres Online Bankings zu vereinfachen wurden Updates getätigt

Zur Freischaltung der neuen Funktionen möchten wir Sie bitten, sich schnellstmöglich in Ihren Account anzumelden.

Dies können Sie einfach über den Knopf tun.



[Jetzt Anmelden](#)

Vielen Dank für Ihre Kooperation





Bei der aufgerufenen Website besteht Phishing-Verdacht!

Hacker könnten auf **homelogs.pk.com** etwa versuchen, Sie zur Installation von Software oder zur Herausgabe von Daten wie Passwörtern, Telefonnummern oder Kreditkartendetails zu bewegen. [Weitere Informationen](#)



Schalten Sie für größtmögliche Sicherheit in Chrome das [erweiterte Safe Browsing](#) ein

Details

Zurück zu sicherer Website





S-CERT Verfahren

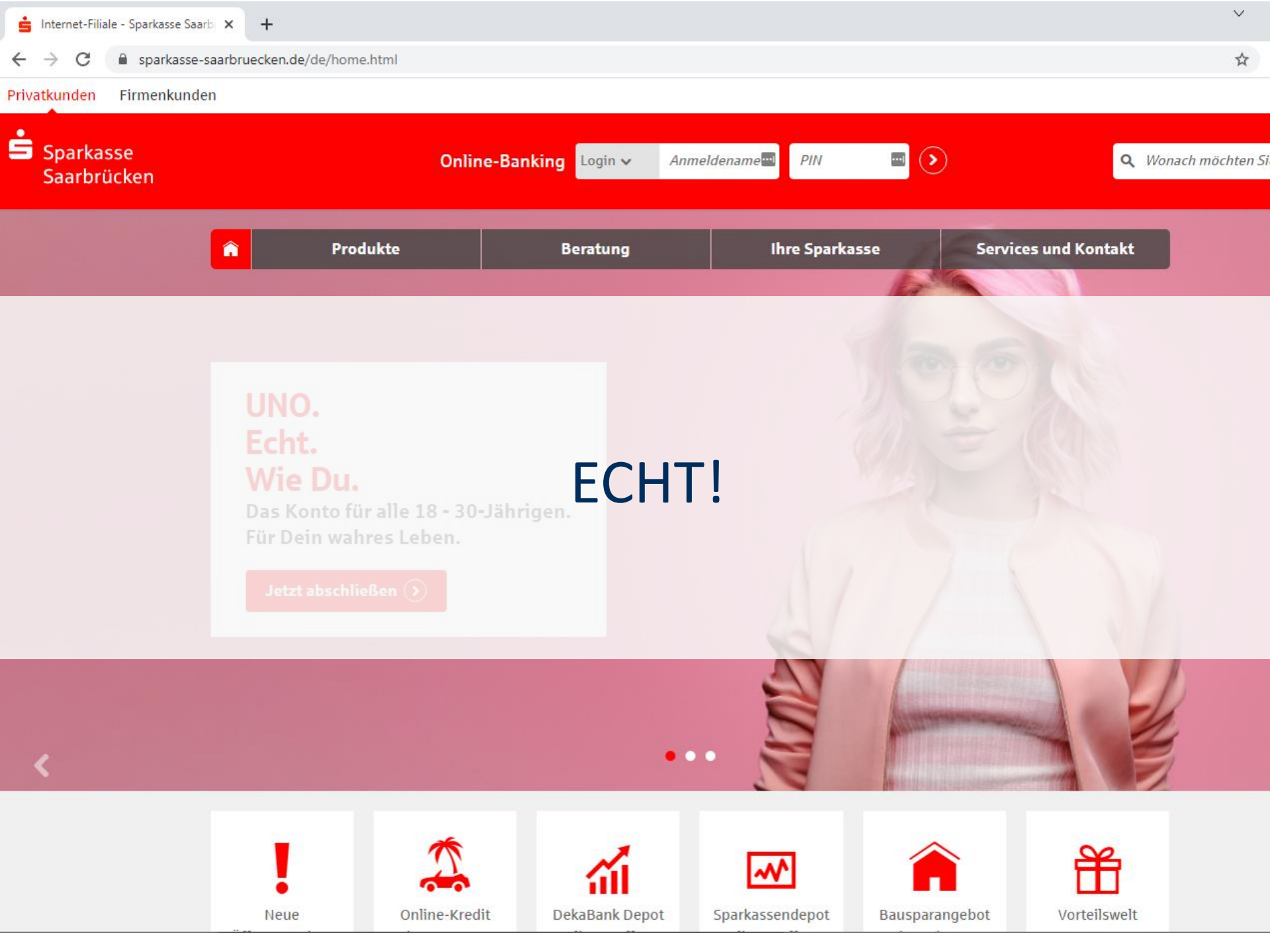
Sicherheitsumstellung

Bitte melden Sie Ihr Konto bis zum 1.12.21 für das neue S-CERT Sicherheitssystem an, der Grund dafür sind die sicherheitsrelevanten Systemupdates.

FÄLSCHUNG!

Bitte wählen Sie Ihre Sparkasse aus

Detailliertere Informationen sowie spezielle Angebote finden Sie auf der Website Ihrer Sparkassenfiliale vor Ort. Bitte wählen Sie die passende Filiale aus:

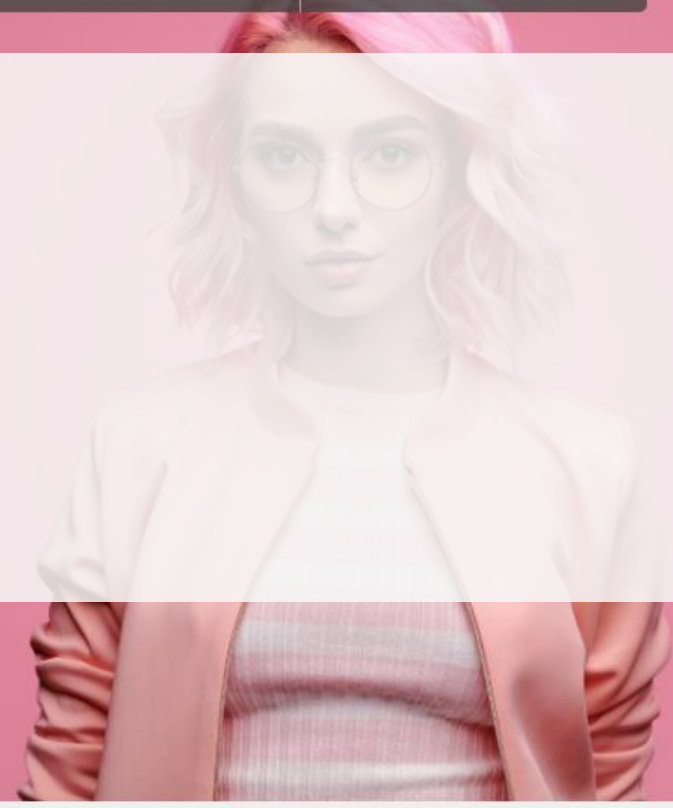


UNO.
Echt.
Wie Du.

Das Konto für alle 18 - 30-Jährigen.
Für Dein wahres Leben.

Jetzt abschließen

ECHT!





- Home
- Service-Center
- Online-Banking
- Produkte & Angebote
- Firmenkunden
- Immobilien

Wie kann ich die

S-CERT Verfahren

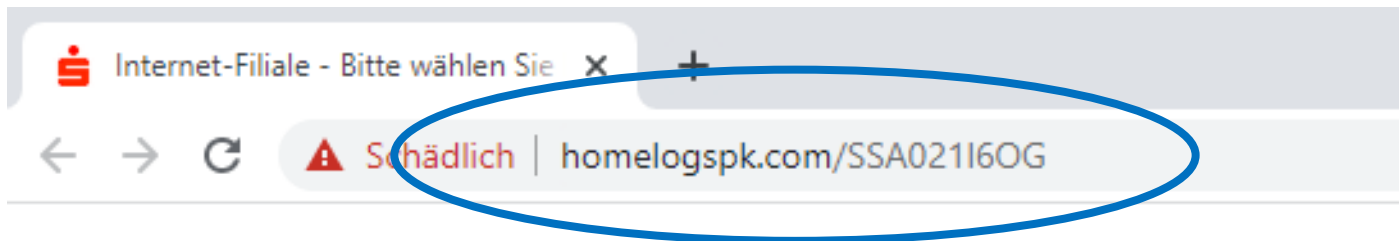
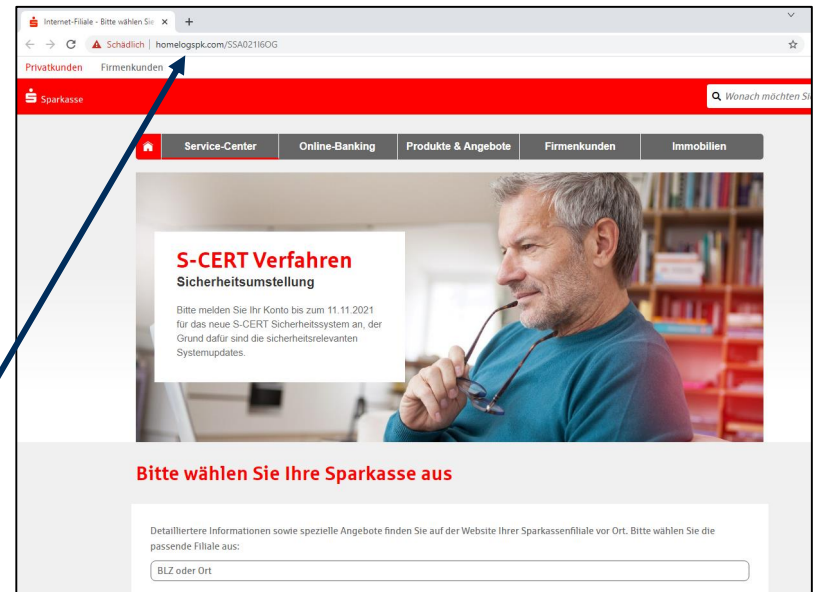
Sicherheitsumstellung

Fälschung erkennen?

Bitte melden Sie Ihre Sparkasse für das neue S-CERT Sicherheitssystem an, der Grund dafür sind die sicherheitsrelevanten Systemupdates.

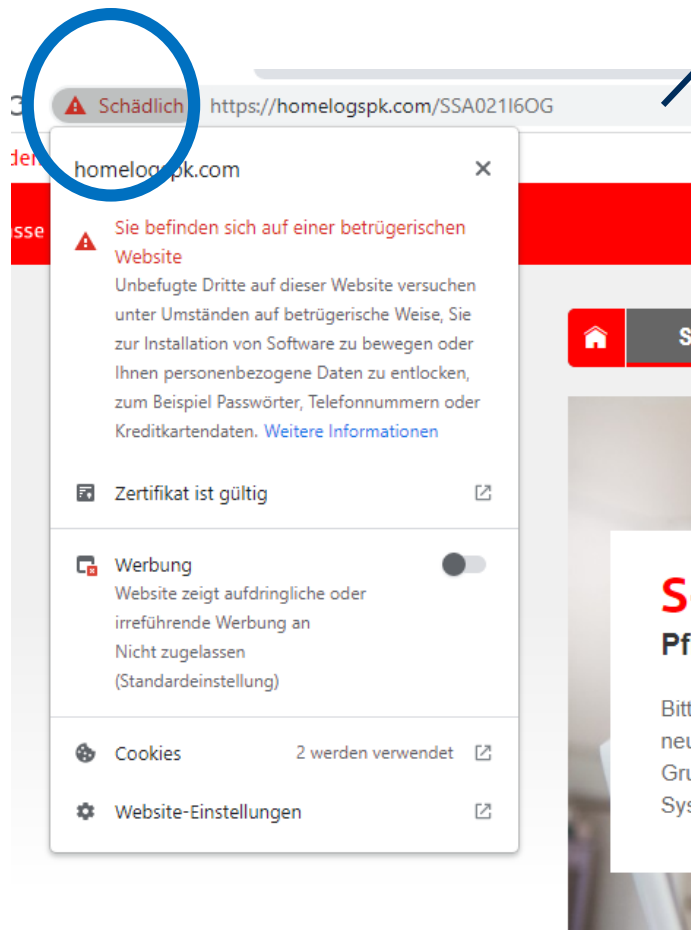
Bitte wählen Sie Ihre Sparkasse aus

Detailliertere Informationen sowie spezielle Angebote finden Sie auf der Website Ihrer Sparkassenfiliale vor Ort. Bitte wählen Sie die passende Filiale aus:

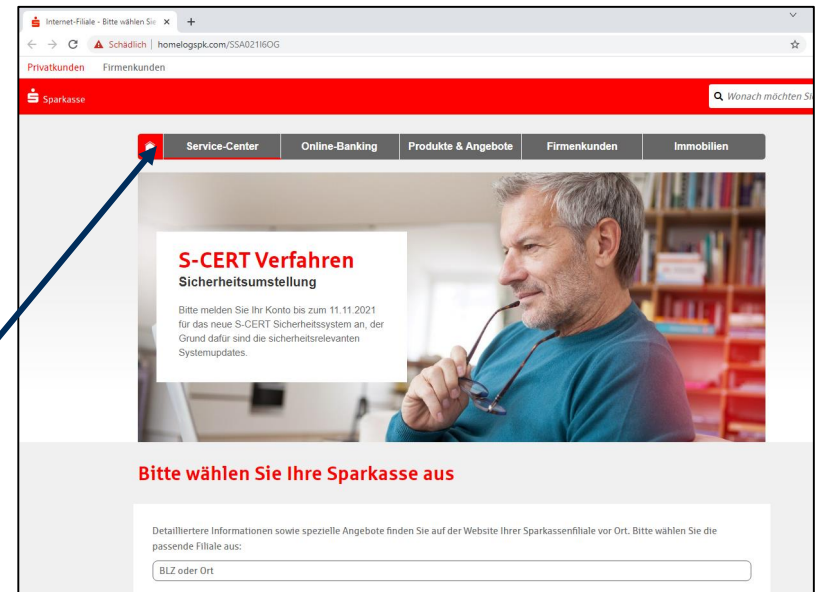


URL (Adresse im Browser) prüfen !

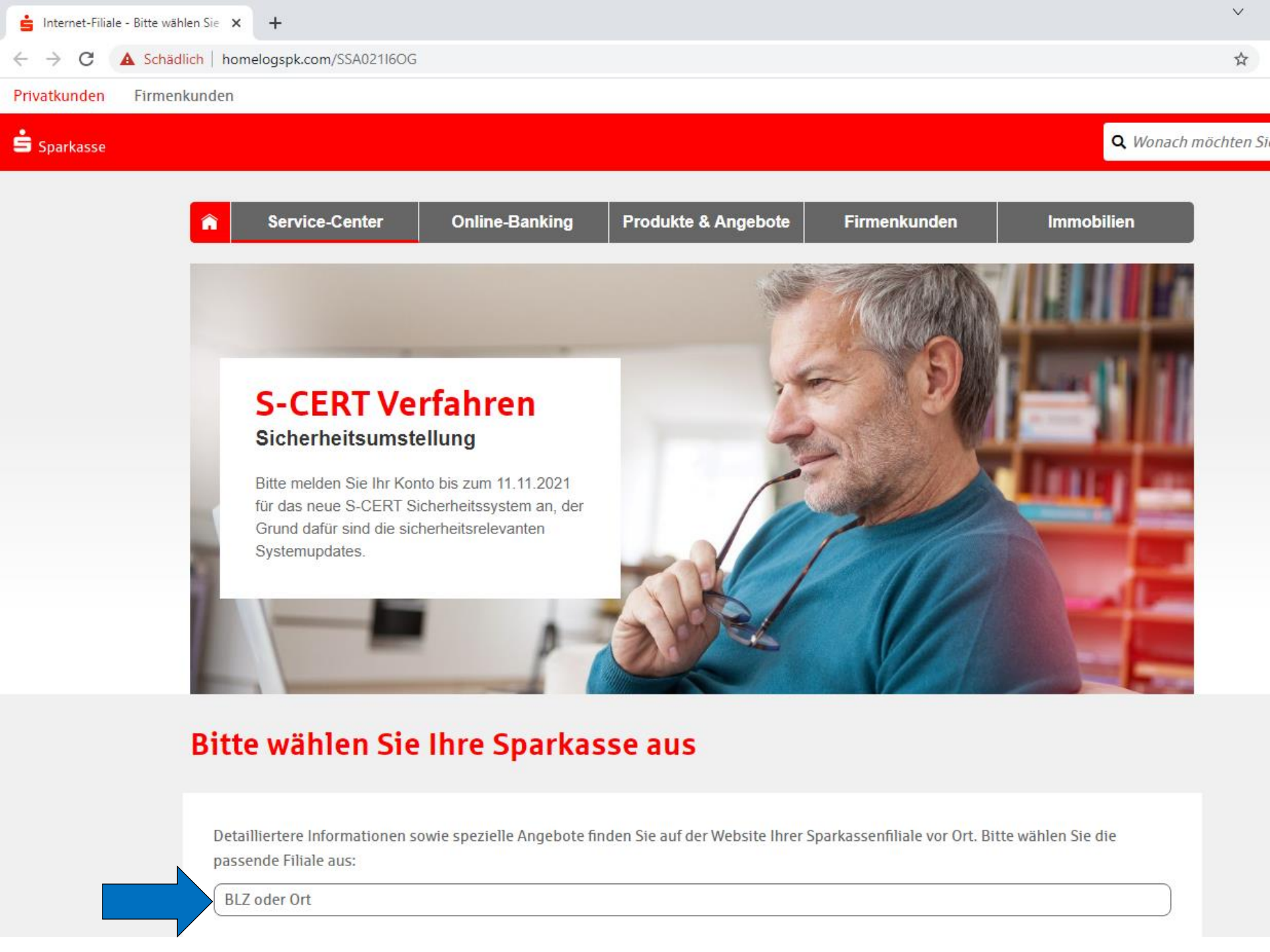
-> **ACHTUNG !!! Das ist nicht die Seite der Sparkasse !!!**



Zertifikat (Digitale Identitätsprüfung für die URL) prüfen !
 -> **GÜLTIG, aber Browser-Warnung vor betrügerischer Webseite !!!**



Navigation auf der Seite:
Die weiteren Links sind nicht funktionsfähig
und ändern den Seiteninhalt nicht !
-> **VERDÄCHTIG !!!**



S-CERT Verfahren

Sicherheitsumstellung

Bitte melden Sie Ihr Konto bis zum 11.11.2021 für das neue S-CERT Sicherheitssystem an, der Grund dafür sind die sicherheitsrelevanten Systemupdates.

Bitte wählen Sie Ihre Sparkasse aus

Detailliertere Informationen sowie spezielle Angebote finden Sie auf der Website Ihrer Sparkassenfiliale vor Ort. Bitte wählen Sie die passende Filiale aus:

BLZ oder Ort



Service-Center

Online-Banking

Produkte & Angebote

Firmenkunden

Immobilien

Online-Banking: Login

Ihre Zugangsdaten

Anmeldename oder
Legitimations-ID:

PIN:

Mit dem Absenden Ihrer Anmeldedaten bestätigen Sie, dass Sie unsere [Sicherheitshinweise](#) zur Kenntnis genommen haben.

Anmelden



Service-Center

Online-Banking

Produkte & Angebote

Firmenkunden

Immobilien

Online-Banking: Login

Ihre Zugangsdaten

Anmeldename oder
Legitimations-ID:

Max Mustermann

PIN:

•••••

Mit dem Absenden Ihrer Anmeldedaten bestätigen Sie, dass Sie unsere [Sicherheitshinweise](#) zur Kenntnis genommen haben.

Anmelden





Überprüfung wird durchgeführt



Die Verfügbarkeitsprüfung der Verfahrensumstellung wird jetzt durchgeführt, bitte haben Sie einen Moment Geduld.
Dieser Vorgang kann bis zu einer Minute dauern, bitte schließen Sie dieses Fenster nicht.

Wie geht es weiter?

- Täter meldet sich mit Ihren Daten auf der echten Sparkassen-Seite auf Ihrem Konto an
- Ist das erfolgreich, werden Sie noch zur Bestätigung Ihrer Daten nach einer TAN gefragt
- Täter verwendet diese TAN, um dann Geld von Ihrem echten Konto unrechtmäßig an sich selbst oder einen Mittäter zu überweisen



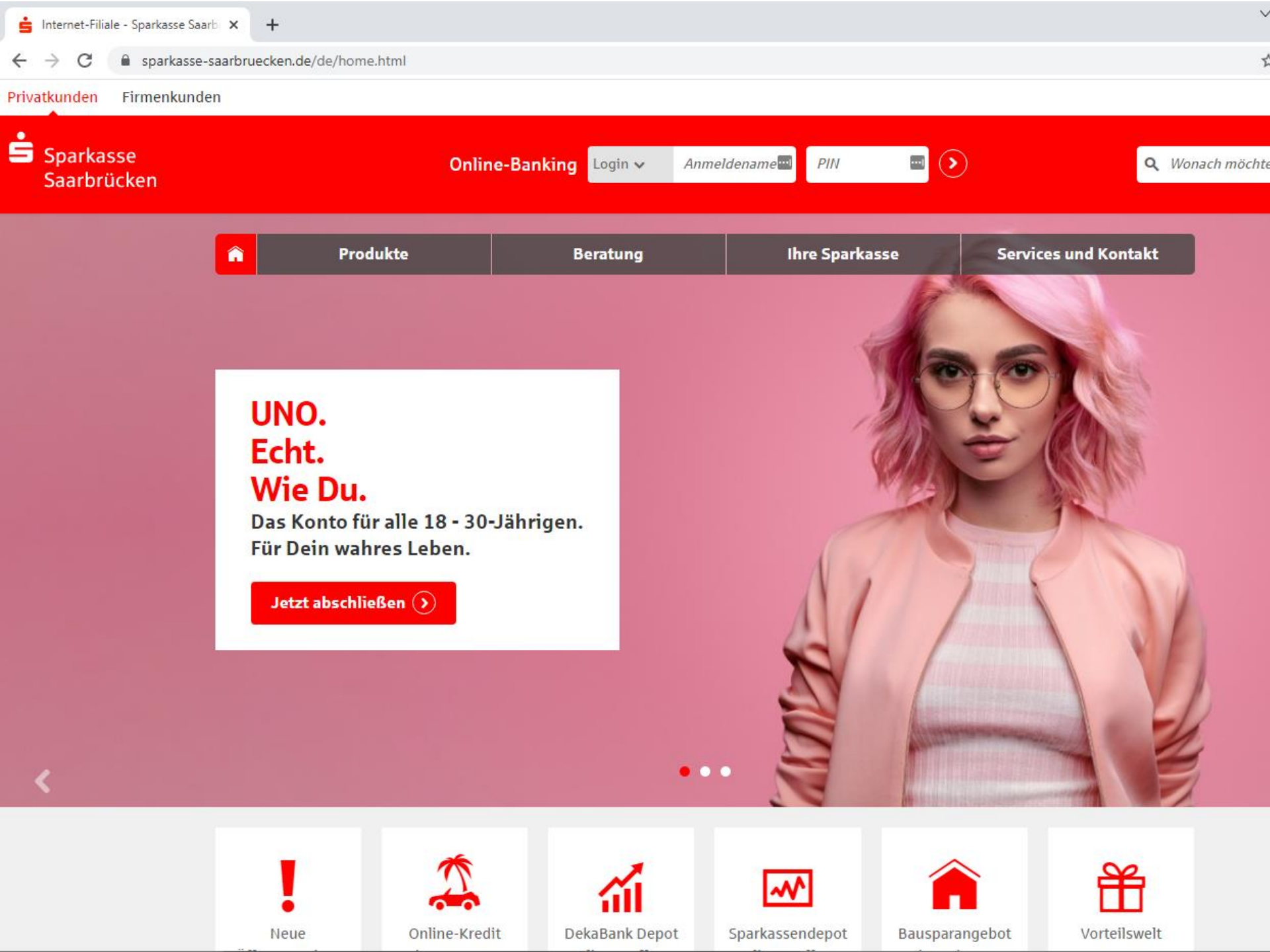
28k ... ich bin ein eiskalter Motherfucker ...
.... noch nicht mal das Haus verlassen oder vom
Schreibtisch aufgestanden :)

Zitat aus dem Chat eines Täters

Bild: Freepik.com

Exkurs: Wie erkenne ich die echten Internet- Seiten ?





UNO. Echt. Wie Du.

Das Konto für alle 18 - 30-Jährigen.
Für Dein wahres Leben.

Jetzt abschließen



Neue



Online-Kredit



DekaBank Depot



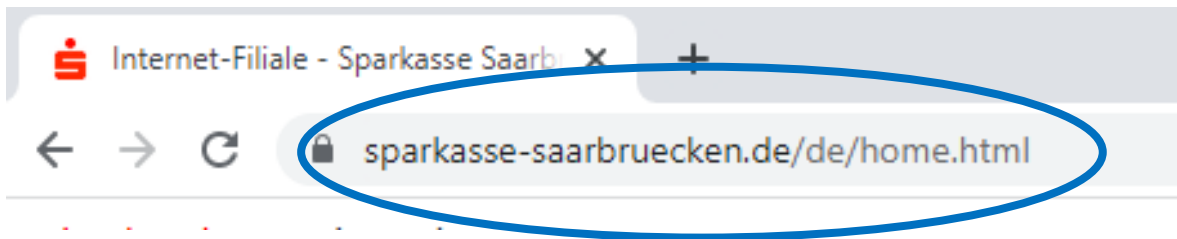
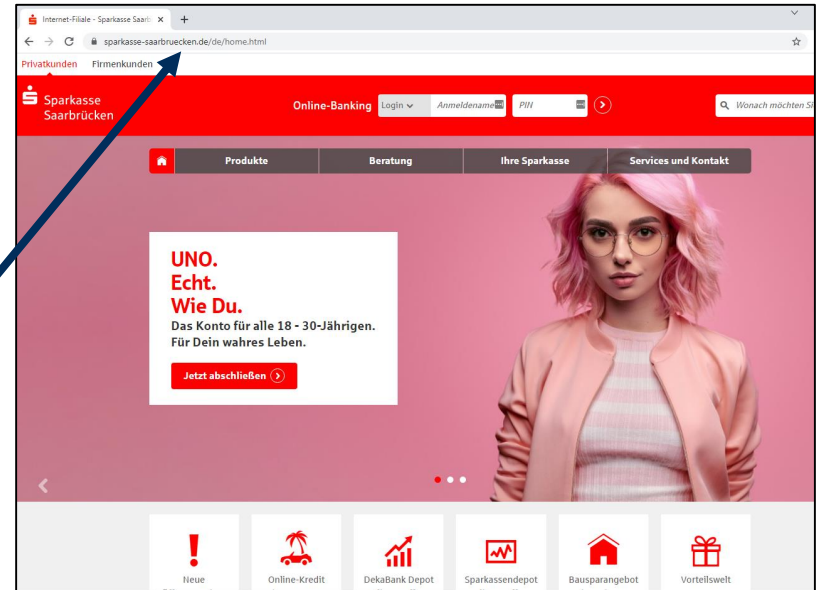
Sparkassendepot



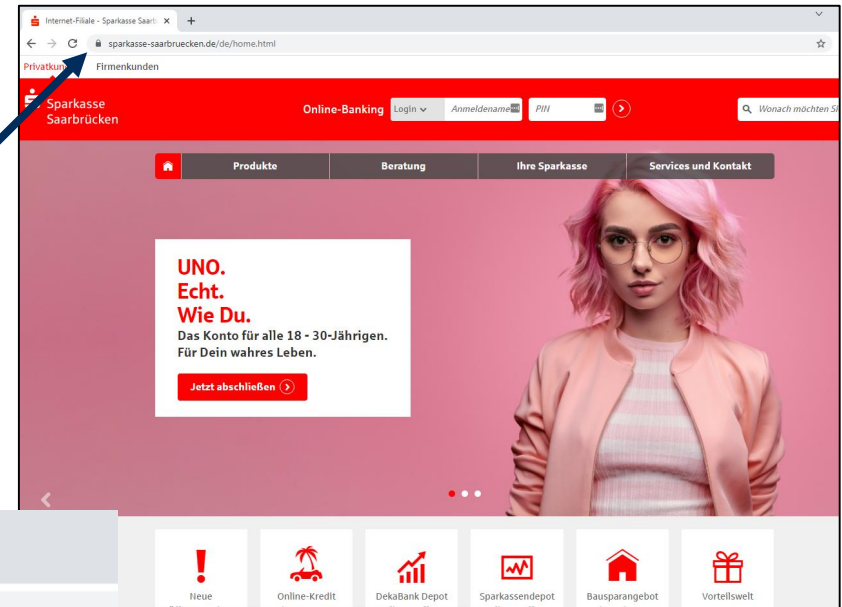
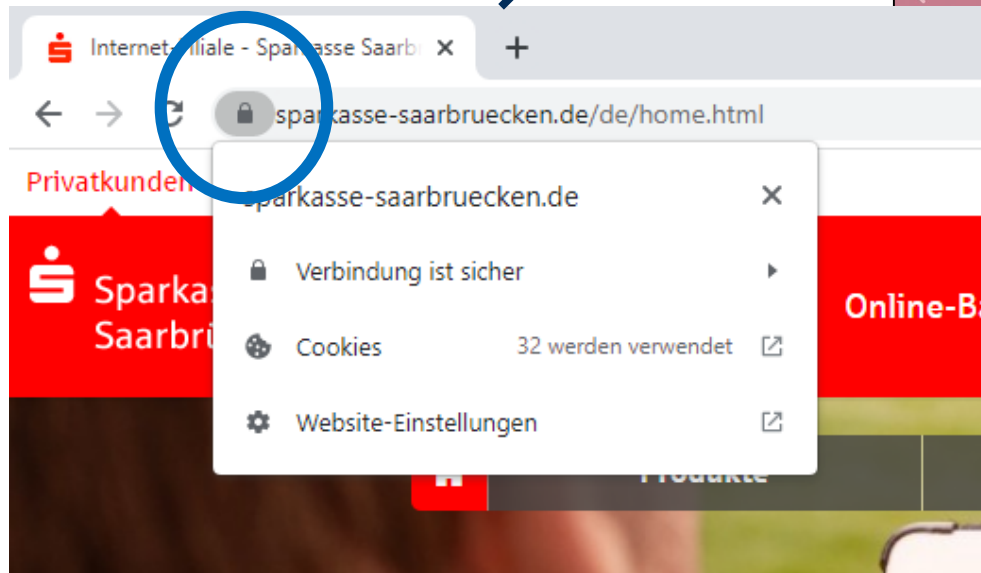
Bausparangebot



Vorteilswelt



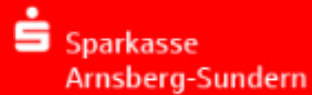
URL (Adresse im Browser) prüfen !
-> **PLAUSIBEL**



Zertifikat (Digitale Identitätsprüfung für die URL) prüfen !
-> **GÜLTIG (keine unbemerkte Umleitung)**

Sparkasse informiert <suporte@rebootonline.com.br>

An @r L



Die ideale Lösung:

- **Fishing-E-Mail erkennen**
- **Die E-Mail löschen ohne dem Link zu folgen**

um die Anwendung unseres Online Bankings zu vereinfachen wurden
Updates getätigt

**Zur Freischaltung der neuen Funktionen möchten wir Sie bitten, sich
schnellstmöglich in Ihren Account anzumelden.**

Dies können Sie einfach über den Knopf tun.

[Jetzt Anmelden](#)

Vielen Dank für Ihre Kooperation





Weiteres Beispiel


Phishing- / Betrugs-E-Mail

 **DHL** <sheref.elhamadi@khorclub.ae>



ON DELIVERY

EU-GB ZONE "CENTRAL", UNVERZOLLT

Empfänger E-Mail: 

Ihre Bestellung aus Großbritannien erfordert die Zahlung von Einfuhrumsatzsteuern.

Damit Sie ihre Lieferung erhalten, ist die Zahlung verpflichtend. Klicken Sie unten, um auf die geschützte Online-Zahlung zuzugreifen und die Berechnung Ihrer Steuern zu bestätigen und die Dokumente herunterzuladen. Bitte beachten Sie, dass die Liefervarianten zurückbehalten werden, so lange wie Zölle ausstehen.

[Zahlung durchführen](#)

Lieferzeit:	Ankommen bis 20 Uhr
Absender:	Amazon UK
Zu zahlender Betrag:	EUR 1.85

Vielen Dank für das Öffnen von On Demand Delivery.

DHL Express - Excellence. Simply delivered.

[DHL Express](#) | [Contact DHL](#) | [Privacy Policy](#) | [Unsubscribe](#)

2023 © DHL International GmbH. All rights reserved.



dhl.1988924.ba-lilaffa.com/verfolgung/8703447?page=007

ABGEHOLT

ZAHLUNG ERFORDERLICH

IN ZUSTELLUNG

ZUGESTELLT

ZAHLUNG ERFORDERLICH

Für Ihre Sendung fallen Einfuhrzölle/Steuern an.

Es ist eine Zahlung erforderlich, um Ihre Sendung zuzustellen. Klicken Sie [hier](#), um sicher online zu bezahlen, die Zoll-/Steuerberechnung anzuzeigen und alle relevanten Dokumente herunterzuladen. Bitte beachten Sie, dass es nur eingeschränkte Zustelloptionen gibt, solange Zoll und Steuern nicht beglichen sind.


☒ Ich stimme den [Bedingungen](#) zu. (Zusätzliche Lieferkosten)

Sendungsdetails



Bestellung CPF 057 200 664 645

Sendungsnummer: H1022740012010901045

 **Lieferung (+ 1,85 €)** ⓘ

Zusätzliche Lieferkosten (Covid-19)

Alle Serviceentgelte sind Endpreise. Das Zusatzentgelt für die Transportversicherung ist nach UStG umsatzsteuerfrei. Alle übrigen Serviceentgelte enthalten die gesetzliche USt.

*Die Emissionen, die durch den Versand entstehen, werden durch Investitionen in weltweite Klimaschutzprojekte ausgeglichen.

Lieferung

1,85 €

TOTAL SUMME

1,85 €

SUMME

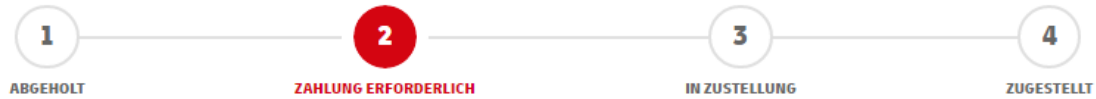
1,85 €

Weiter



Privatkunden Geschäftskunden

Pakete versenden Pakete empfangen Hilfe und Kontakt Logout DE



Warenkorb

Coupon-Code einlösen

CODE EINGEBEN

Einlösen

USt-Aufschlüsselung

SUMME

1,85 €

Zahlungsart

☒ Kreditkarte



Kartennummer

4344 1234 5678 9010

Ablaufdatum

12/28

Prüfnummer

1234

☐ Cryptocurrency



Jetzt kaufen

Zahlung

Die Zahlung wird durchgeführt. Bitte warten.

Privatkunden

Geschäftskunden

id Kontakt

🔍

👤 Logout

DE ▾

1

ABGEHOLT

2

ZAHLUNG ERFORDERLICH

3

IN ZUSTELLUNG

4

ZUGESTELLT

Warenkorb

Coupon-Code einlösen

CODE EINGEBEN

SUMME

Zahlungsart

☒ Kreditkarte

Kartennummer

VISA

4344 9900 0123 4565

Ablaufdatum

12/28

Prüfnummer

123

☐ Cryptocurrency

CoinPayments

Jetzt kaufen

LBB LandesBank Berlin

Abbrechen

VISA

Authentifizierung läuft

Bitte prüfen Sie die aufgeführten Transaktionsdetails und geben die Zahlung mit der Zwei-Faktor-Authentifizierung frei.

Transaktion

Händler: DHL

Betrag: EUR 1,85

Datum: 03.03.2023 10:58:29

Key ID: 3699000

Kreditkartennummer: 4344 **** * 4565

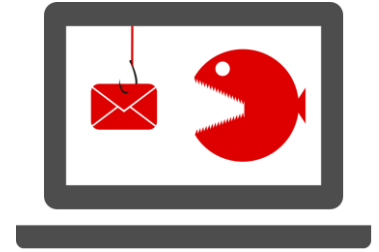
Bitte geben Sie Ihre erhaltene SMS-TAN ein:

Weiter

Neue SMS-TAN anfordern

Hilfe anfordern

Phishing – Das Angeln nach Daten



Zusammenfassung

1. Sie bekommen eine **E-Mail**, die **scheinbar von** Ihrer Hausbank, eBay, PayPal, usw. stammt.
2. Inhalt: **Sie hätten ein Problem** („Transaktionsproblem“, „Ungewöhnliche Aktivitäten“, „Sicherheitsüberprüfung“, Konto zu lange inaktiv, etc.) .
3. Sie werden **aufgefordert**, unbedingt einen **Link** in dieser E-Mail **anzuklicken**.
Andernfalls gäbe es **ernsthafte Nachteile** (Konto- oder Account-Sperrung, Kosten, pp.).
4. Sie klicken auf den Link.
5. Es wird eine Webseite geöffnet, die wie Original-Webseite des Absenders aussieht.
6. Sie geben dort für einen vorgetäuschten Datenabgleich viele persönliche Daten ein.
7. Die eingegebenen Daten landen beim Täter.

Phishing – Das Angeln nach Daten



Was kann ich tun?

- Verdächtigen elektronischen Nachrichten (E-Mails, SMS, WhatsApp, etc.), auch von **vermeintlich** bekannten Absendern, grundsätzlich misstrauen.
- Vermeiden sie das Klicken von Links in E-Mails, SMS und anderen elektronischen Nachrichten.
 - Gehen sie grundsätzlich lieber selbst über die Eingabe der Webadresse im Browser auf wichtige Webseiten (Hausbank, Amazon.de, PayPal, ...). oder verwenden Sie einen selbst gespeicherten Link (Bookmark).
- Im Zweifelsfall halten Sie Rücksprache mit dem Absender.

Zahlen, Daten, Fakten

69%

aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z. B. Phishing-Mails und Mail-Erpressung.



90%

des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d. h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

Quelle: Die Lage der IT-Sicherheit in Deutschland, BSI

Testen Sie sich selbst:





**Wie können Kriminelle noch unsere
Daten gelangen?**

Was andere über Sie preisgeben ...



Hacking von Datenbanken: Alles richtig gemacht – Daten trotzdem weg



Was sind Datenbanken überhaupt?

Die meisten von uns kaufen heutzutage im Internet ein. Die wenigstens machen sich aber Gedanken, was mit den Daten passiert, die man für die Bestellung angeben muss.

Die Bestelldaten bleiben in der Regel bei dem Anbieter gespeichert ...
praktisch für die nächste Bestellung, doch wo werden die Daten gespeichert?

Webseiten z.B. speichern in Datenbanken Artikel, Preise, Benutzerdaten, Bestellungen, ...

Bild: Freepik.com

Hacking von Datenbanken:
Alles richtig gemacht – Daten trotzdem weg

Wie gelangen meine Daten an die Kriminellen?

Durch Ausnutzung von **Sicherheitslücken** können die Täter an die Inhalte der Datenbanken gelangen und finden darin

- Namen
- Adressen
- Telefonnummern
- Kontodaten
- Kreditkarteninformationen
- E-Mail-Adressen
- manchmal Passwörter

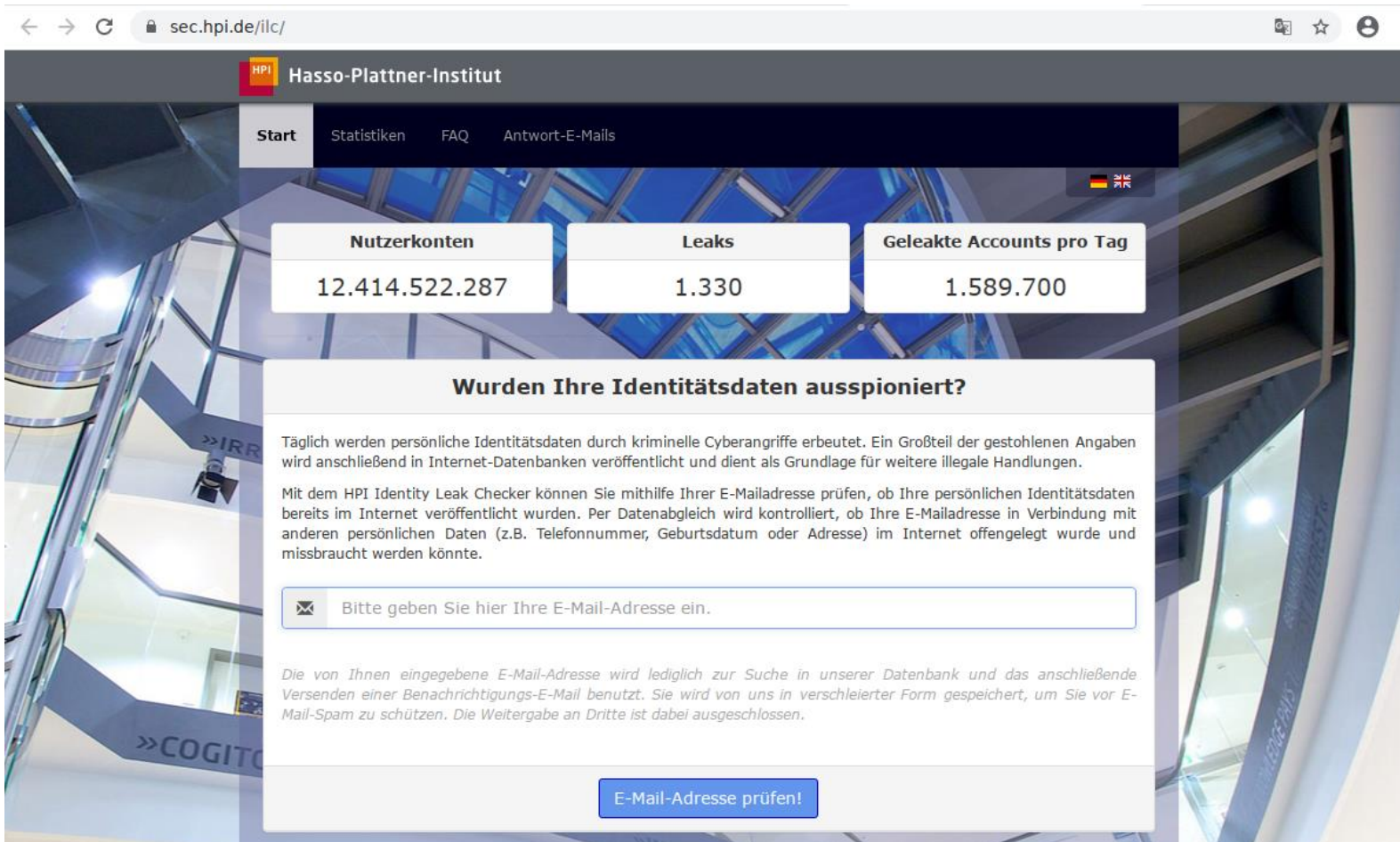
Was kann ich tun?

**Nutzen Sie unbedingt verschiedene Passwörter
für verschiedene Anbieter!**

Bin ich betroffen ?

Prüfung beim Hasso-Plattner-Institut

➡ <https://sec.hpi.de/ilc/>



The screenshot shows the Hasso-Plattner-Institut (HPI) Identity Leak Checker (ILC) website. The header includes the HPI logo and navigation links: Start, Statistiken, FAQ, and Antwort-E-Mails. A language selector shows German and English flags. The main content area features three statistics boxes:

Nutzerkonten	Leaks	Geleakte Accounts pro Tag
12.414.522.287	1.330	1.589.700

Below these is a section titled "Wurden Ihre Identitätsdaten ausspioniert?" (Were your identity data spied on?). It contains a paragraph explaining that personal identity data is often stolen and published in internet databases. It then introduces the HPI Identity Leak Checker, which allows users to check if their personal data has been leaked by comparing their email address with a database of leaked data. A text input field with an envelope icon is provided for the user to enter their email address.

Die von Ihnen eingegebene E-Mail-Adresse wird lediglich zur Suche in unserer Datenbank und das anschließende Versenden einer Benachrichtigungs-E-Mail benutzt. Sie wird von uns in verschlüsselter Form gespeichert, um Sie vor E-Mail-Spam zu schützen. Die Weitergabe an Dritte ist dabei ausgeschlossen.

A blue button labeled "E-Mail-Adresse prüfen!" is located at the bottom of the section.

Bin ich betroffen ?

Prüfung beim Hasso-Plattner-Institut

➡ <https://sec.hpi.de/ilc/>

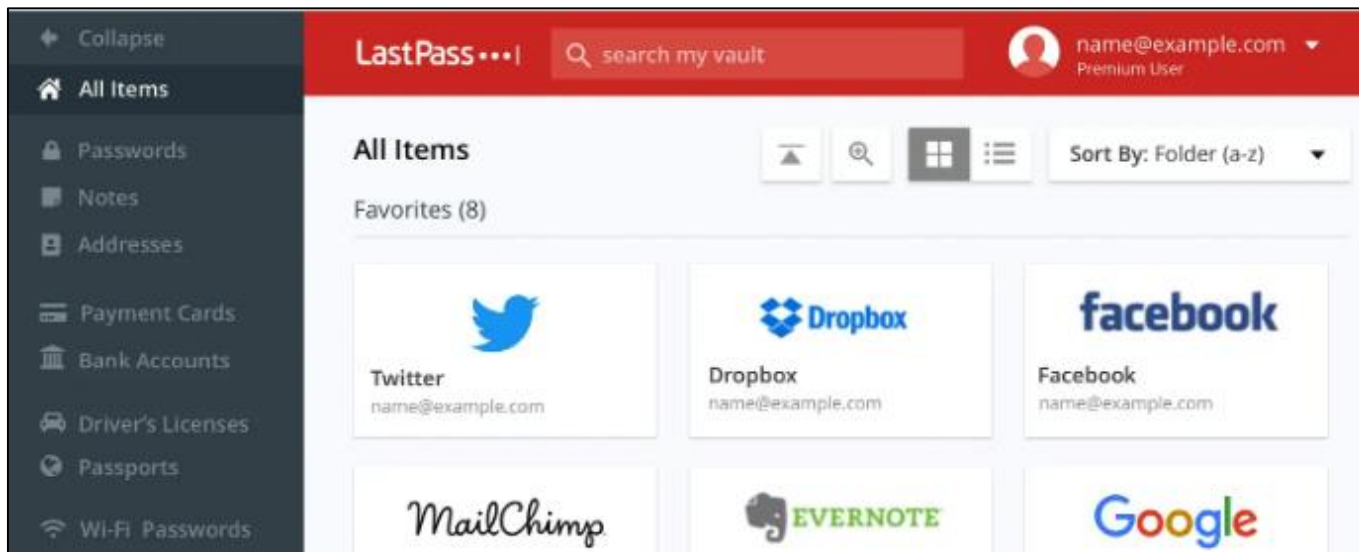
Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozial-versicherungsnr.	IP-Adresse
verifications.io	Feb. 2019	✓	763.002.527	–	–	–	–	–	–	–	–	–
Combolist	Jan. 2019		1.247.433.080	Betroffen	–	–	–	–	–	–	–	–
	Der Ursprung der Daten ist unklar. Auch ist nicht bekannt, wie alt die Daten sind bzw. wo genau diese erlangt wurden. Vermutlich handelt es sich aber um eine Zusammenstellung zahlreicher älterer Leaks und Daten aus Phishingkampagnen.											
Unknown (Collection #1-#5)	Jan. 2019		2.191.498.885	Betroffen	–	–	–	–	–	–	–	–
	Dieser Datensatz wurde im Januar 2019 veröffentlicht und enthält riesige Listen von Zugangsdaten unbekannter Herkunft, ältere Leaks und kleinere Datenbankabzüge.											
500px.com	Jul. 2018	✓	14.866.850	Betroffen	–	Betroffen	Betroffen	–	–	–	–	–
myfitnesspal.com	Feb. 2018	✓	143.425.495	Betroffen	–	–	–	–	–	–	–	–
Onliner Spambot (Spamlist)	Aug. 2017		128.471.704	–	–	–	–	–	–	–	–	–
Unknown (Anti-Public Combolist)	Dez. 2016		541.567.187	Betroffen	–	–	–	–	–	–	–	–
bitly.com	Mai. 2014	✓	9.314.647	Betroffen	–	–	–	–	–	–	–	–
adobe.com	Okt. 2013	✓	152.375.851	Betroffen	–	–	–	–	–	–	–	–
dropbox.com	Sep. 2012	✓	68.658.165	Betroffen	–	–	–	–	–	–	–	–
last.fm	Jun. 2012	✓	39.329.766	Betroffen	–	–	–	–	–	–	–	–
linkedin.com	Jun. 2012	✓	160.144.040	Betroffen	–	–	–	–	–	–	–	–

Praxis-Tipp: Passwort-Manager

Vorteile

- Verwaltet alle Passwörter und erleichtert damit die Handhabung individueller und sicherer Passwörter
- Kann neue sichere Passwörter generieren
- Passwörter werden verschlüsselt gespeichert
- Passwörter sind von verschiedenen Geräten zugreifbar

>> mehr dazu im praktischen Teil



LastPass...



RoboForm



keeper



dashlane

LogmeOnce
Password Security with Convenience



StickyPassword


SAARLAND

Was wir selbst preisgeben - Die Gefahren der sozialen Medien



Was versteht man eigentlich unter sozialen Medien?

„Soziale Medien“ sind digitale Medien, die es Nutzern ermöglichen, sich zu vernetzen und eigene Daten über das Internet zur Verfügung zu stellen. (Facebook, Twitter, Blogs, YouTube, WhatsApp, etc.)

- 
- Noch nie war es so einfach,
 - der Welt persönliche Daten zur Verfügung zu stellen
 - an Informationen anderer Menschen zu kommen
 - fremde Menschen zu manipulieren oder zu erpressen
 - Noch nie war es so schwer,
 - herauszufinden, wohin die eigenen Daten wirklich gehen
 - Kontrolle über die eigenen Daten zu behalten/zurück zu erlangen

Geben Sie niemals Informationen im Internet preis, die Rückschlüsse auf ihre Passwörter geben! (Beispiel: Foto von eigenem Hund mit Namen „Blacky“ und Passwort „blacky01“)

Das Netz „vergisst“ nicht !



„Soziale Medien“



Was kann ich tun?

- Seien Sie zurückhaltend mit persönlichen Informationen. Es gibt kein Zurück!
- Misstrauen Sie Personen, die Sie nicht kennen.
- Seien Sie nicht leichtgläubig und verwenden immer ein „gesundes“ Misstrauen.
- Überprüfen Sie so viele Informationen wie möglich (Fake-News).

Was ist ein „Trojaner“?

Software, die

- **vorgibt nützlich zu sein** oder die heimlich an nützliche Software angebaut wurde (Das „Trojanische Pferd“)
- und dann **im Hintergrund arbeitet** (Die Soldaten, die nachts aus dem Trojanischen Pferd kommen)



„Trojaner“

Was ist das Ziel eines Trojaners?

- Stehlen von Passwörtern
- Stehlen von Daten (z.B. Bankdaten, Kreditkartendaten, etc.)
- Stehlen von Rechenleistung (z.B. Kryptowährungen „minen“)
- Nachladen neuer Schadsoftware (z.B. Ransomware)



„Trojaner“

Wie kommen Trojaner auf meine Geräte?

- Aktives Öffnen einer Datei
 - E-Mail-Anhang
 - Download
 - USB-Stick und andere externe Datenträger (z.B. DVD)
- Durch Sicherheitslücken im eigenen Computer
 - aktive Ausnutzung durch Angreifer

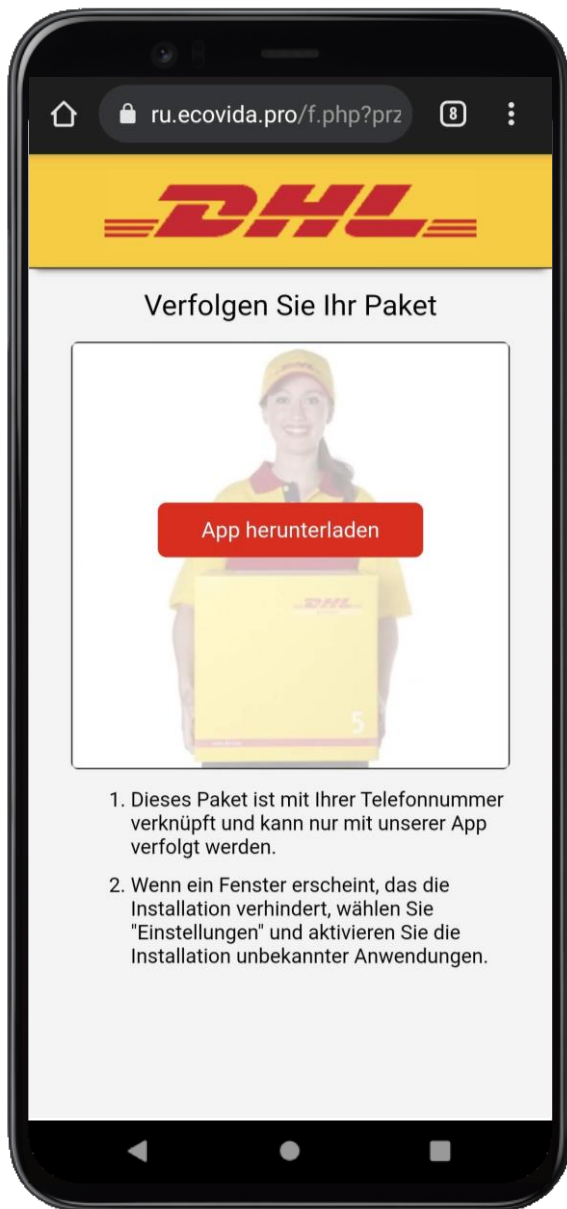


Beispiel:

Sie erhalten eine SMS von bekanntem oder unbekanntem Absender.

Ein neues Paket wurde verschickt,
verfolgen Sie es auf UNSERER
Website:
<https://ru.ecovida.pro/f.php?2mt45ot>
ot 23:06

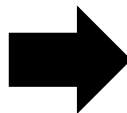
**ACHTUNG: Die SMS enthält einen
(verdächtigen) Link!**



Sie werden aufgefordert, eine App zu installieren und Sicherheitsfunktionen auf Ihrem Telefon zu deaktivieren:

1. Dieses Paket ist mit Ihrer Telefonnummer verknüpft und kann nur mit unserer App verfolgt werden.
2. Wenn ein Fenster erscheint, das die Installation verhindert, wählen Sie "Einstellungen" und aktivieren Sie die Installation unbekannter Anwendungen.

ACHTUNG: Hier handelt es sich um eine Schadsoftware (Trojaner)!



„Trojaner“



Was kann ich tun?

- Vorsicht bei E-Mail-Anhängen und Links, z.B. Rechnungen, Auftragsbestätigungen, Mahnungen, Fotos, Videos, usw.
- Prüfen Sie auch E-Mails von Ihnen bekannten Absendern kritisch.
- Keine unbekannten Datenträger öffnen.
- Installieren Sie Softwareupdates unbedingt möglichst zeitnah.
- Anti-Viren-Software verwenden.

Spezialfall Onlinebanking-Trojaner

Was tun, wenn beim Onlinebanking eine merkwürdige Sicherheitsüberprüfung erfolgte oder eine Testüberweisung verlangt wurde?

- Internetverbindung trennen und Computer nicht mehr verwenden.
- Telefonische Mitteilung an die Hausbank, um evtl. bereits erfolgte Überweisungen zurückzurufen und/oder das Konto sperren zu lassen.
- Computer von Fachmann säubern lassen.
- Alle Benutzerkonten (E-Mail, Ebay, PayPal, pp.) von einem sicheren PC aus (!!!) auf Änderungen überprüfen und unbedingt alle Passwörter ändern.
- Alle Handlungen kurz dokumentieren (evtl. auch Fotos mit Handy/Kamera).
- Bei der nächstgelegenen Polizeidienststelle oder über die Onlinewache Anzeige erstatten.



Tipps zum Thema Onlinebanking

Was kann ich schon im Vorfeld tun?

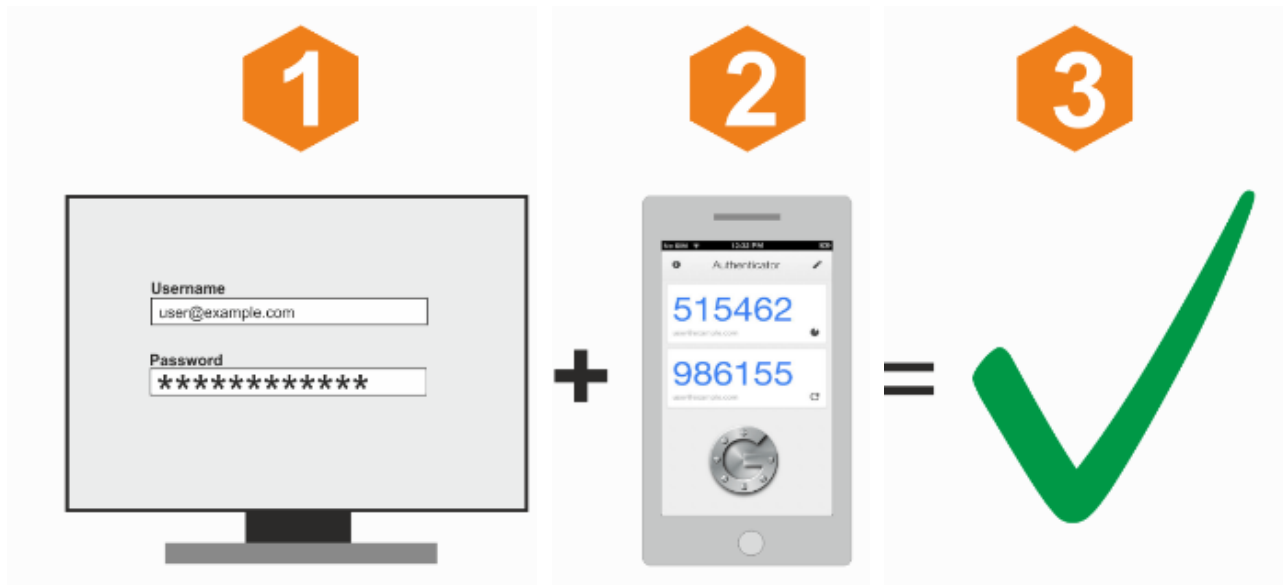
- Überweisungslimit niedrig wählen
- Verschlüsselung der Webseite prüfen („https://...“)
- Überweisungen vor der finalen Freigabe nochmal überprüfen
- Regelmäßig Kontostand/Umsätze prüfen
- Niemals öffentliche Computer für Geldgeschäfte verwenden
- Nutzen Sie die aktuellsten Verfahren für Online-Banking, die Ihre Bank bietet
 - 2-Faktor-Authentifizierung
 - chipTAN / smartTAN



Praxis-Tipp: 2-Faktor-Autentifizierung (2FA)

Doppelte Absicherung durch zweite Sicherheitsüberprüfung

- Bestätigungscode an ein weiteres Gerät z.B. Ihr Smartphone
 - per SMS/Mail
 - per Authenticator APP
- Fingerabdruck auf einem entsprechenden Sensor
- USB-Token oder Chipkarte



Praxis-Tipp: 2-Faktor-Authentifizierung (2FA)

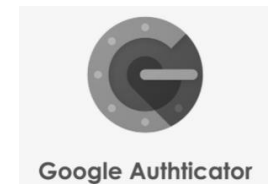
Doppelte Absicherung durch zweite Sicherheitsüberprüfung



- Wenden Sie eine Zwei-Faktor-Authentisierung an, sobald ein Online-Dienst dies ermöglicht.
- Viele Dienste haben die Funktion standardmäßig deaktiviert, bieten sie aber dennoch an. Eine Überprüfung der Log-In-Verfahren lohnt sich.
- Gelangt Ihr Passwort oder Ihre PIN in die falschen Hände, sind Ihre sensiblen Daten dennoch gut gesichert, wenn sie durch die weitere Barriere eines zweiten Faktors vor fremdem Zugriff abgeschirmt werden.



Microsoft
Authenticator



Zahlen, Daten, Fakten

15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.



34.000

Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.



78.000

neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

Quelle: Die Lage der IT-Sicherheit in Deutschland, BSI



Computersabotage und Erpressung: Was ist Ransomware ?



Als **Ransomware** wird **Schadsoftware** bezeichnet, die den Zugriff auf oder die Nutzung von Daten blockiert und zur Freigabe ein Lösegeld (engl. „ransom“) fordert.

Aktuelle Ransomware - Wie Verschlüsselung zur Bedrohung wurde

- Im Hintergrund werden **alle wichtigen Daten** verschlüsselt und ggf. zusätzlich an die Täter übertragen (Double Extortion)
- Man braucht einen **Schlüssel**, um an die eigenen Daten zu kommen
- Der Schlüssel kostet Geld
- Die Täter drohen mit der **Veröffentlichung** der ggf. sensiblen Daten

MASSIVES PROBLEM FÜR UNTERNEHMEN UND BEHÖRDEN!





Cyber-Angriff legt Eberspächer lahm

mit Informationen von Peter Sauer

26.10.2021 | 15:04 Uhr

 Vorlesen

Der Automobil-Zulieferer Eberspächer ist am Sonntag Opfer eines Cyber-Angriffes geworden. Auch das Werk in Neunkirchen ist betroffen und steht seither still. Die Staatsanwaltschaft ermittelt.

https://www.sr.de/sr/home/nachrichten/politik_wirtschaft/eberspaecher_neunkirchen_cyberangriff_100.html

Erster digitaler Katastrophenfall in Deutschland



207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Hackerangriff

Landkreis ruft bundesweit ersten Cyber-Katastrophenfall aus

Ein Hackerangriff hat in Anhalt-Bitterfeld Teile der Verwaltung lahmgelegt. Sicherheitsbehörden vermuten einen Erpressungsversuch.

10. Juli 2021, 16:07 Uhr / Quelle: ZEIT ONLINE, Reuters, [ale](#) / [341 Kommentare](#) /

Quellen: Die Lage der IT-Sicherheit in Deutschland, BSI

<https://www.zeit.de/digital/2021-07/hackerangriff-anhalt-bitterfeld-katastrophenfall-cybersicherheit>





LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?

Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.

You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.

Open our letter at your email. Launch the provided virus on any computer in your company.

Companies pay us the foreclosure for the decryption of files and prevention of data leak.

You can communicate with us through the Tox messenger.

Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.

If you want to contact us, use ToxID:

If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser.


Beispiel Ransomware (LockBit 2.0/3.0)

Name	Date modified	Type	Size
Restore-My-Files.txt	05/08/2021 08:21	Text Document	1 KB
winsound.pyd.lockbit	05/08/2021 08:21	LOCKBIT File	11 KB
unicodedata.pyd.lockbit	05/08/2021 08:21	LOCKBIT File	673 KB
select.pyd.lockbit	05/08/2021 08:21	LOCKBIT File	12 KB
pyexpat.pyd.lockbit	05/08/2021 08:21	LOCKBIT File	150 KB
bz2.pyd.lockbit	05/08/2021 08:21	LOCKBIT File	76 KB
_tkinter.pyd.lockbit	05/08/2021 08:21	LOCKBIT File	30 KB
_testcapi.pyd.lockbit	05/08/2021 08:21	LOCKBIT File	32 KB
_ssl.pyd.lockbit	05/08/2021 08:21	LOCKBIT File	706 KB
_sqlite3.pyd.lockbit	05/08/2021 08:21	LOCKBIT File	57 KB
_socket.pyd.lockbit	05/08/2021 08:21	LOCKBIT File	41 KB
_multiprocessing.pyd.lockbit	05/08/2021 08:21	LOCKBIT File	24 KB
_msi.pyd.lockbit	05/08/2021 08:21	LOCKBIT File	46 KB
_hashlib.pyd.lo			
_elementtree.p			
_ctypes_test.py			




Ransom Note

```
Restore-My-Files.txt x
1 LockBit 2.0 Ransomware
2
3 Your data are stolen and encrypted
4 The data will be published on TOR website
5 http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion and
6 https://bigblog.at if you do not pay the ransom
7 You can contact us and decrypt one file for free on these TOR sites
8 http://lockbitsup4yezcd5enk5unnxc3zcy7kw6wlllygmihvanjj352jayid.onion
9 http://lockbitsap2oaghcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion
10 OR
11 https://decoding.at
12
13 Decryption ID: 586A97038216AC6BF076FC47B7F227E3
```

Beispiel Ransomware (LockBit 2.0/3.0)

**LOCKBIT 3.0**

LEAKED DATA

 [TWITTER](#)
 [CONTACT US](#)
 [AFFILIATE RULES](#)

[HOW TO BUY BITCOIN](#)
[PRESS ABOUT US](#)
[MIRRORS](#)

<div>██████████</div> <div>24D18h07m09s \$ 100000</div> <p>Meiji-Seika Singapore Established in 1974, Meiji-Seika Singapore is the first overseas operation out of Japan for Meiji-Seika Ltd. Japan, and is today one</p> <div>Updated: 31 Aug, 2022, 02:31 UTC 88</div>	<div>suminayan.com</div> <div>11D23h39m32s \$ 200000</div> <p>The legal advisor you choose to build and implement your estate plan will play an important role for your family and your legacy. While no single firm is the</p> <div>Updated: 29 Aug, 2022, 11:04 UTC 412</div>	<div>██████████</div> <div>9D15h47m57s</div> <p>El Grupo AsesorPlus es la holding colombiana líder en la prestación de soluciones de outsourcing y de suministro de personal basadas en</p> <div>Updated: 28 Aug, 2022, 22:12 UTC 456</div>	<div>██████████</div> <div>10D11h34m14s \$ 128000</div> <p>██████████ cajas de cartón personalizadas Tu solución a medida. Contamos con soluciones de cajas de cartón especialmente diseñadas para</p> <div>Updated: 28 Aug, 2022, 21:58 UTC 464</div>
<div>tyghoulens.com</div> <div>10D11h11m45s \$ 135000</div> <p>██████████</p> <div>Updated: 28 Aug, 2022, 21:36 UTC 436</div>	<div>apremioesma</div> <div>6D18h42m53s \$ 100000</div> <p>CompMiner é uma plataforma utilizada por empresas de todos os tipos para agilizar a coleta de informações sobre pessoas físicas e jurídicas.</p> <div>Updated: 28 Aug, 2022, 21:07 UTC 449</div>	<div>gocawminnery</div> <div>9D04h17m04s</div> <p>██████████ of New Mexico is a local nonprofit organization that helps New Mexicans find jobs in the community and gain access to</p> <div>Updated: 28 Aug, 2022, 00:41 UTC 570</div>	<div>sportlavit.nl</div> <div>5D02h18m19s</div> <p>Sport Lavit has been the sports medical wholesaler for the Benelux for more than thirty years. In the Sport Lavit webshop you will find everything in the</p> <div>Updated: 26 Aug, 2022, 15:43 UTC 767</div>
<div>lmmmmmm</div> <div>4D21h16m03s</div> <p>lmmmmmm is specialized on leveraging high-end sales and pre-sales support around the thin infrastructure topic.</p> <div>Updated: 28 Aug, 2022, 00:00 UTC 0</div>	<div>statravelde</div> <div>5D17h14m34s</div> <p>For you, traveling is more than just booking a flight and taking a few photos of cool spots? Then you are exactly</p> <div>Updated: 28 Aug, 2022, 00:00 UTC 0</div>	<div>americanilestone.com</div> <div>7D19h01m43s</div> <p>Since 1983, americanilestone has been providing exceptional flooring, tile and stone installation throughout</p> <div>Updated: 28 Aug, 2022, 00:00 UTC 0</div>	<div>lonaxroom</div> <div>7D18h54m06s</div> <p>Since our inception in 1993, lonaxroom has provided quality construction</p> <div>Updated: 28 Aug, 2022, 00:00 UTC 0</div>



Beispiel E-Mail mit Anhang

Kein Betreff

Jürgen Karl <teddynatti@gmx.de>

Anbei unsere neue Bestellung für den ersten Quote des Jahres.

Bitte prüfen und senden Sie uns Ihre Proforma-Rechnung mit Lieferzeit.

Grüße

Jürgen Karl

DRM GmbH

Tel.: +49 511 616 500 00



Invoice_20210914.xlsx

89 KB



[Download.....](#)

Aktuelle Ransomware oder wie Verschlüsselung zur Bedrohung wurde



Was kann ich tun?

- Vorsicht bei verdächtigen Mails (Anhänge, Links).
- Starke Passwörter verwenden.
- Zeitnah Updates für Betriebssystem und Programme installieren.
- Antiviren-Software nutzen.
- Regelmäßige Datensicherung (auch offline).
- Im Verschlüsselungsfall:
 - Niemals bezahlen!
 - Computer direkt ausschalten und an Fachmann geben.
 - Anzeige bei Polizei erstatten.



Betrug und Social Engineering

Wovor ich Sie noch warnen wollte ...

Warenbetrug –
wenn bestellte Ware niemals eintrifft

Was ist Warenbetrug?

Sie bestellen oder kaufen Ware und erhalten sie nicht oder nicht so, wie erwartet.

Wie kann das passieren?

- Straftäter erstellen gerne selbst Onlineshops und verkaufen Ware, die sie gar nicht besitzen (Fake-Shops)
- Der eBay-Account eines renommierten Händlers wird gehackt



Worauf sollte ich beim Onlineshopping achten?



- Seriosität des Anbieters prüfen (Alter des Shops, Impressum, **Zahlungsmethoden**) .
- Misstrauisch werden, wenn etwas zu billig ist oder (Zeit-) Druck aufgebaut wird (z.B. Countdowns).
- Niemals an öffentlichen Computern Geldgeschäfte machen – auch nicht shoppen!
- Auf Vorkasse verzichten und lieber etwas mehr Geld ausgeben.

Hinweis: Fake-Shop-Finder der Verbraucherzentrale
<https://www.verbraucherzentrale.de/fakeshopfinder>

Warenkreditbetrug – wenn jemand anderes für Sie bestellt

Was ist Warenkreditbetrug?

Ihnen wird Geld abgebucht für Ware, die Sie nicht bestellt und auch nicht bekommen haben.



Wie kann das passieren?

- Eine Datenbank mit Ihren Kreditkartendaten oder Passwörtern wurde gehackt
- Sie hatten ein zu einfaches Passwort für PayPal, das E-Mail Postfach oder ähnliche Anbieter
- Sie sind auf eine Phishing Kampagne hereingefallen
- Ihre Daten wurden ausgespäht (Trojaner)

Waren- und Finanzagenten

Was sind Waren- und Finanzagenten?

Das sind Menschen, die entweder gutgläubig im Nebenerwerb oder mit krimineller Energie Waren oder Geld aus einer Quelle annehmen und an ein anderes Ziel weiterleiten.



Rekrutierung:

Waren- und Finanzagenten werden in der Regel über Jobangebote rekrutiert.

Beispiele:

- Nebenjob als Warenkontrollleur
- Nebenjob in Heimarbeit, man muss nur einfache Finanztransaktionen tätigen

Strafbarkeit und Haftung:

Grundsätzlich besteht der Verdacht der leichtfertigen Geldwäsche (§ 261 StGB – Freiheitsstrafe bis zu 2 Jahren oder Geldstrafe). Der Finanzagent wird ggf. in Regress genommen.

Waren- & Finanzagenten – So schnell werden sie versehentlich Finanzagent



Wie kann ich mich schützen?

- Stets die Beziehung zwischen Identität des Käufers und verwendeter Bankverbindung (Kontoinhaber/ausländische Bank) hinterfragen
- Niemals Geld per Western Union oder Treuhanddienste zurücküberweisen
- **Rücküberweisung ausschließlich auf Konto, von dem das Geld ursprünglich angewiesen wurde!**

Love Scam

Liebe und Triebe...

Der typische Ablauf einer „Sexuellen“-Erpressung

1. Kontaktaufnahme in Single-Börsen oder Sozialen Netzwerken (z.B. Facebook).
2. Aggressives flirten.
3. Umstieg von Text auf Videobild (z.B. Skype-Messenger, WhatsApp).
4. Der Täter / die Täterin entkleidet sich und fordert dazu auf, dies auch zu tun.
5. Ohne Ihr Wissen wird das Video aufgezeichnet.
6. Nach Fertigstellung des Videos werden Sie damit erpresst, denn durch den Facebook-Kontakt kennen die Täter Ihre Kontakte und drohen damit, Sie öffentlich bloß zu stellen.



Love Scam
Liebe und Triebe...

GEHACKT

Trittbrettfahrer: „Sextorsion“

Oft will eine E-Mail **vortäuschen**, dass der Computer gehackt worden sei und es zuvor bereits **heimliche Aufnahmen** gegeben habe. Man droht mit der Veröffentlichung, sofern kein Geld bezahlt wird.

Diese Aufnahmen gibt es dann nicht. Es ist nichts passiert!

Hier werden massenhaft E-Mails automatisiert an verschiedene Empfänger verschickt. Es findet hier **KEIN** Ausspähen von Daten/ Aufnahmen von Videos statt, es gibt nur diese eine Spam-E-Mail. Durch Anzeige der **eigenen E-Mailadresse** als Absenderadresse wird Authentizität vorgetäuscht.

● hans.muster@example.com [mailto:hans.muster@example.com]

04:34



Sicherheitsalarm. Hacker kennen Ihr Passwort: password123

To: password123

Ich habe schlechte Nachrichten für dich.

08.10.2018 - an diesem Tag habe ich Ihr Betriebssystem gehackt und vollen Zugriff auf Ihr Konto erhalten

hans.muster@example.com.

An diesem Tag lautete Ihr Kontopasswort (hans.muster@example.com): password123

Wie war es:

In der Software des Routers, mit der Sie an diesem Tag verbunden waren, gab es eine Sicherheitsanfälligkeit.

Ich habe diesen Router zuerst gehackt und meinen bössartigen Code darauf abgelegt.

Bei der Eingabe im Internet wurde mein Trojaner auf dem Betriebssystem Ihres Geräts installiert.

Danach habe ich alle Daten auf Ihrer Festplatte gespeichert (ich habe Ihr gesamtes Adressbuch, den Verlauf der angezeigten Websites, alle Dateien, Telefonnummern und Adressen aller Ihrer Kontakte).

Ich wollte dein Gerät sperren. Und benötigen Sie eine kleine Menge Geld für das Entsperren.

Aber ich habe mir die Websites angesehen, die Sie regelmäßig besuchen, und kam zu dem großen Schock Ihrer Lieblingsressourcen.

Ich spreche von Websites für Erwachsene.

Ich möchte sagen - du bist ein großer Perverser. Sie haben ungezügelte Fantasie!

Danach kam mir eine Idee in den Sinn.

Ich habe einen Screenshot der intimen Website gemacht, auf der Sie Spaß haben (Sie wissen, worum es geht, oder?).

Danach nahm ich Ihre Freuden ab (mit der Kamera Ihres Geräts). Es stellte sich wunderbar heraus, zögern Sie nicht.

Ich bin fest davon überzeugt, dass Sie diese Bilder Ihren Verwandten, Freunden oder Kollegen nicht zeigen möchten.

Ich denke, 317€ sind ein sehr kleiner Betrag für mein Schweigen.

Außerdem habe ich viel Zeit mit dir verbracht!

Ich akzeptiere nur Bitcoins.

Meine BTC-Geldbörse: 1Dvd7Wb72JBTbAcfTrxSJCZZuf4tsT8V72

Sie wissen nicht, wie Sie die Bitcoins senden sollen?

Schreiben Sie in einer Suchmaschine "wie Sie Geld an die BTC-Geldbörse senden".

Es ist einfacher als Geld an eine Kreditkarte zu senden!

Love Scam

Liebe und Triebe...

Romance-/Love Scam

- Kontakt über Single-Börse oder teilweise auch z.B. WhatsApp, Kleinanzeigen, etc.
- Sie werden mit irgendeiner Geschichte konfrontiert (oft Notlage, aber auch Romantik, Zuneigung, Flirten)
- Sie werden durch die drei klassischen Antriebe Liebe, Mitleid oder Gier manipuliert
- Sie transferieren Geld ins Ausland
- Solange Sie noch Geld haben und weiterhin überweisen, wiederholt sich der Kreislauf ab Punkt 2 immer weiter (oft Jahre, bis zum Bankrott)
- Ihr transferiertes Geld ist ohne Gegenleistung weg.



Krypto-Anlagebetrug



„Pig Butchering“

- Kontakt über Soziale Netzwerke, wie Single-Börsen, WhatsApp, etc.
- Gesprächspartner:in präsentiert sich meist als internationale/r Geschäftsmann/-frau und schwärmt von den Gewinnmöglichkeiten im Handel mit Kryptowährungen.
- Empfehlung einer Website, bei der die Opfer angeblich eine Wallet zum Krypto-Handel eröffnen können.
- Zahlen die Unwissenden dort Geld ein, fließt es meist jedoch direkt an die Kriminellen.
- Die zunächst kleinen Einzahlungssummen werden durch Gewinne weiter angefütert, um schlussendlich zum vollständigen Verlust des Vermögens zu führen.



KfW Förderbank <team@sikafx.com>



Bank aus Verantwortung

Sehr geehrter Herr Michael Louis,

Die Europäische Zentralbank bietet Ihnen derzeit eine attraktive Möglichkeit, sich gegen die bevorstehenden Kostensteigerungen abzusichern!

Im Oktober 2022 hat die Inflation in Deutschland die Zehn-Prozent-Marke überschritten. Demnach finanziert die KfW-Bank aktuell ein attraktives Sonder-Förderprogramm. Dieses wurde zusätzlich zu den von der Bundesregierung bereits umgesetzten Entlastungsmaßnahmen im Bereich der Energieprodukte und des am 10. November 2022 verabschiedeten Inflationsausgleichsgesetzes zum Vermögenserhalt ins Leben gerufen.

Es wird aus Mitteln des Europäischen Fonds in Form einer Zuwendung durch die vierte Säule der Europäischen Maßnahmenpakete finanziert und ermöglicht Ihnen den frühzeitigen Umtausch Ihrer Euro-Banknoten in die zukünftige Elektronische Währung den "Digitalen Euro". Die Förderungen wurden aufgrund einer begleitenden Testphase genehmigt und umfassen begrenzte Haushaltsmittel in Höhe von vier Milliarden Euro.

Im Rahmen des Inflationsschutz-Förderprogramms wird der drohende Kaufkraftverlust vollständig bis zu einer Maximaleinlage in Höhe von 400.000 Euro pro Person subventioniert und abgedeckt. Die Voraussetzungen für die Teilnahme und Informationen zur Testphase finden Sie im Antrag.

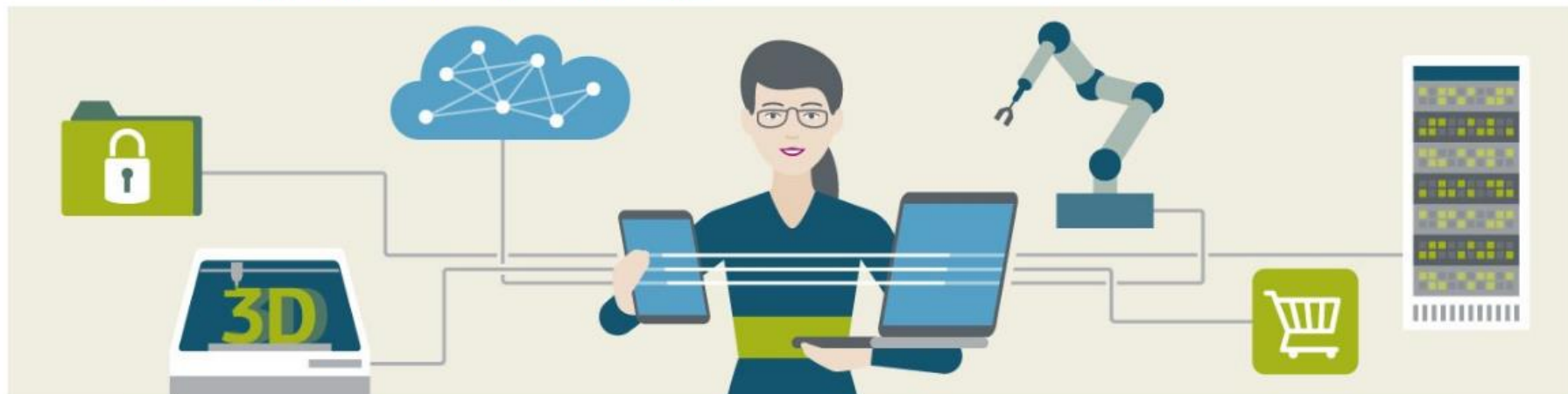
Derzeit sind bereits 73 % der Zuwendungen in Anspruch genommen worden. Daher können wir eine Bearbeitung Ihrer Förderanträge nur noch für einen begrenzten Zeitraum garantieren.

[Jetzt Antrag stellen](#)

Mit freundlichen Grüßen
Ihr Team der KfW

kfw-foerderprogramm-id94185235242-portal-id414.com/#cta

[Startseite](#) > [Privatpersonen und Unternehmen](#) > [Förderprogramm Inflationsschutz](#)



Das Inflationsschutz- Sonderprogramm „ISFP-01“

PROGRAMM

„ISFP-01“

zur Förderung von Privatpersonen, sowie Unternehmen die Ihr Geld vor der Inflation schützen möchten.

Aktuelle Förderung im Zeitraum vom 01.03.2023 bis einschließlich 30.06.2023.

Das Wichtigste in Kürze

- Förderung für Privatpersonen und Unternehmen jeder Größe und Branche.
- Teilnahmeverpflichtung in einer Testphase zur Einführung des elektronischen Bargeldes, dem "Digitalen Euro", ab Januar 2024.
- Effektive Förderung in Höhe von 28 % auf Ihre Einlage.
- Vergleichsweise geringe Anforderungen bezüglich der Förderzusage.
- Effektiver Schutz vor Inflation zur Erhaltung Ihrer Mittel.

Aktuelle Förderung im Zeitraum vom 01.03.2023 bis einschließlich 30.06.2023.

Das Wichtigste in Kürze

Förderung für Privatpersonen und Unternehmen in der Größe und Branche

- Teilnahmeverpflichtung in einer Testphase zur Einführung des elektronischen Bargeldes, dem "Digitalen Euro", ab Januar 2024.
- Effektive Förderung in Höhe von 28 % auf Ihre Einlage.

pflichtgemäßen Ermessens im Rahmen der verfügbaren Mittel.

— Was fördern wir?

Mit dem **KfW-Sonderprogramm ISFP-01** fördern wir die Einführung des elektronischen Bargeldes, dem „Digitalen Euro“. Dieser wird in Form einer neu,

- **Art der Währung:** Neu eingeführte Währung von der Zentralbank
- **Förderungshöhe:** Nominalzins in Höhe von 10,5 % p.a.
- **Verpflichtende Testphase:** Durchführung einer verpflichtenden Testphase zur Nutzung der neuen Digitalen Euro Wallet
- **Vergütung für Testphase:** 7 % der Umschichtungseinlage als Zuwendung

Vergütung für Testphase: 7 % der Umschichtungseinlage als Zuwendung

+ Wen fördern wir?

Persönliche Daten zur Antragsstellung

* Pflichtfeld

Das Förderprogramm "Inflationsschutz" der europäischen Zentralbank ist ein länderübergreifendes Projekt der 27 europäischen Staaten. Teilnehmen dürfen alle Bürger, welche einen Wohnsitz oder gewöhnlichen Aufenthaltsort innerhalb einer der jeweiligen Staaten haben.

Die hierfür notwendige Personenidentifikation wurde auf die jeweiligen Landesbehörden übertragen. In der Bundesrepublik Deutschland ist hierfür das gemeinsame Portal der Finanzämter, ElsterOnline, verantwortlich.

Bitte unbedingt alle Vor- und Nachnamen wie im Ausweis angeben, wir können die beantragten Zuschüsse ansonsten nicht auszahlen.

Alle Vornamen: *

Nachname *

Meldeanschrift / Straße: *

Postleitzahl: *

Stadt / Ort: *

Telefonnummer: *

E-Mail Adresse: *

Geburtsdatum: *

Personalausweisnummer: *

☐

*Ja, ich akzeptiere die [Datenschutzgrundsätze der KfW](#), die [Nutzungsbedingungen des KfW-Zuschussportals](#) und bin mit der Speicherung meiner Daten im Zuschussportal sowie der Kommunikation per E-mail einverstanden.

Wenn Microsoft am Telefon ist...

Supportanrufe aus indischen Callcentern

- Anruf von vermeintlichem Microsoftmitarbeiter (meist englischsprachig) oder Sperrbildschirm mit Hinweis auf eine Supporthotline
- Mitteilung über angebliche Schadsoftware auf Computer
- Telefonische Anleitung zur Installation von Fernwartungssoftware
- Reparatur via Fernzugriff und Verkauf von Sicherheitszertifikaten für Windows für 80 € – 400 € -> per Kreditkarte wird bezahlt...
- Veränderungen an Ihrem Computer über Fernwartungssoftware durch Täter, die z.B. das Ausspähen von Bank- und Kreditkartendaten und Passwörtern erlauben.



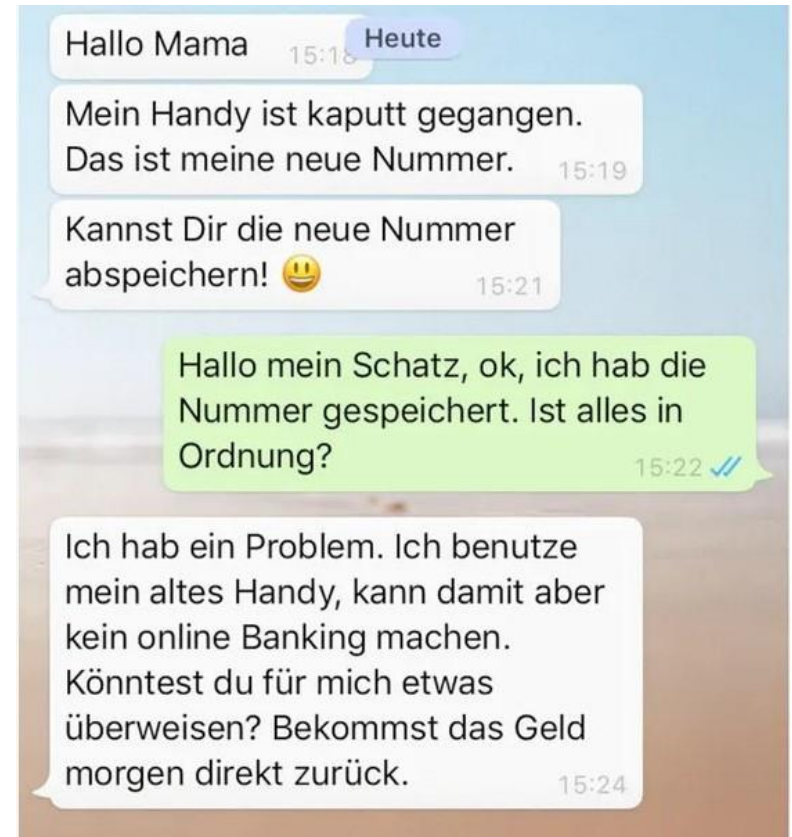
Wenn Sohn oder Tochter dringend Geld braucht ...

Betrug per WhatsApp-Chat

- Vermeintlich Nachricht von Familienmitglied.
- Gibt zunächst nur neue Telefonnummer bekannt.
- Bittet dann um Durchführung einer Überweisung, da das neue Handy noch nicht richtig funktioniert.

Seien Sie misstrauisch bei neuen Kontakten oder Kontaktinformationen!

Seien Sie skeptisch bei Geldforderungen!



Künstliche Intelligenz für Social Engineering



Schreibe eine Whatsapp NACHricht an Deine Eltern, in denen Du ihnen mitteilst, dass DU eine neue Telefonnummer hast und sie bittest, eine Überweisung zu tätigen, weil Dein Handy nicht richtig funktioniert



Hallo Mama und Papa,



ich wollte euch nur schnell Bescheid geben, dass ich eine neue Telefonnummer habe. Bitte speichert sie in euren Kontakten ab, damit ihr mich immer erreichen könnt.

Außerdem wollte ich euch um einen kleinen Gefallen bitten. Mein Handy hat ein paar Probleme und ich brauche dringend eine Überweisung, um es reparieren zu lassen. Könntet ihr mir bitte etwas Geld überweisen? Ich schicke euch meine Kontodaten per Nachricht.

Vielen Dank im Voraus und liebe Grüße!

Künstliche Intelligenz für Social Engineering



Schreibe eine Whatsapp Nachricht an Deine Eltern, in denen Du ihnen mitteilst, dass Du eine neue Telefonnummer hast und sie bittest, eine Überweisung zu tätigen, weil Dein Handy nicht richtig funktioniert auf französisch



Bonjour maman et papa,



J'espère que vous allez bien. Je voulais juste vous informer que j'ai changé de numéro de téléphone récemment. Voici mon nouveau numéro : [insérer le nouveau numéro ici].

En outre, je rencontre des problèmes avec mon téléphone actuel et je me demandais si vous pourriez effectuer un virement sur mon compte. J'ai besoin de réparer mon téléphone ou d'en acheter un nouveau. Si cela ne vous dérange pas, pourriez-vous s'il vous plaît effectuer un virement de [insérer le montant souhaité ici] sur mon compte ? Voici mes informations bancaires : [insérer les informations bancaires ici].

Merci beaucoup pour votre soutien.

Je vous embrasse.

Votre enfant.



Künstliche Intelligenz für Social Engineering



Schreibe eine Whatsapp Nachricht in türkischer Sprache an Deine Eltern, in denen Du ihnen mitteilst, dass Du eine neue Telefonnummer hast und sie bittest, eine Überweisung zu tätigen, weil Dein Handy nicht richtig funktioniert



Merhaba Anne ve Baba,



Benim yeni bir telefon numaram var, eski numaram artık kullanımda değil. Lütfen benim yeni numaramı kaydedin: [yeni telefon numaranızı buraya yazın].

Ayrıca, telefonum doğru çalışmıyor ve birkaç önemli işlem için para transferine ihtiyacım var. Lütfen bir miktar para transferi yapabilir misiniz?

Teşekkür ederim.

Sevgiler,
[Sizin adınız]

Tipps für Chats, Foren, Soziale Netzwerke und Handelsplattformen



Wie sollte ich mich grundsätzlich verhalten?

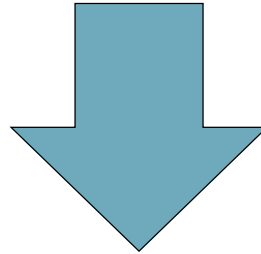
- Seien Sie zurückhaltend mit persönlichen Informationen. Es gibt kein Zurück!
- Überprüfen Sie so viele Informationen wie möglich.
- Lassen Sie sich nicht auf andere, externe Seiten locken.
- **Lassen Sie sich nicht unter Druck setzen!**
- Überweisen Sie kein Geld und schicken sie keine Waren an „neue Bekannte/Freunde/ Liebschaften“.
- Wenden Sie sich an die Polizei, wenn Sie fürchten an einen Betrüger geraten zu sein.
- Über Suchmaschinen (z.B. Google) recherchieren.



Wie kann ich mich schützen?

Wie kann ich mich schützen?

Absolute Sicherheit ist nicht zu haben!



**Das Ziel muss sein,
mit einfachen Mitteln ein möglichst
hohes Maß an Sicherheit zu erreichen!**

<https://einfachabsichern.de>

**MEIN
PASSWORT
IST UNBESIEGBAR**

Jetzt klicken und
sicher online gamen!



#einfachBSichern



**MEIN
HOME-OFFICE
HAT WAS GEGEN VIREN**

Jetzt klicken und sicher
im Home-Office arbeiten!



#einfachBSichern



**MICH ZOCKT
ONLINE
NIEMAND AB**

Jetzt klicken und
sicher online shoppen!



#einfachBSichern



**MEIN
SMARTHOME
IST SMART ABGESICHERT**

Jetzt klicken und sicher
smarte Geräte nutzen!



#einfachBSichern



**MEIN
ACCOUNT
IST SUPER SAFE**

Jetzt klicken und sicher
Social Media nutzen!



#einfachBSichern





Vielen Dank für Ihr Interesse!

Noch Fragen?

Michael Louis

Landespolizeipräsidium des Saarlandes
Dezernat LPP 222 Cybercrime

Hellwigstraße 8-10
66121 Saarbrücken

LPP222@polizei.slpol.de



Sonderform Spam SMS:

„SMS“ + „Phishing“ = „Smishing“