Polizei

SAARLAND
Großes entsteht immer im Kleinen.

Tatort Internet – neue Gefahren durch die moderne Technik

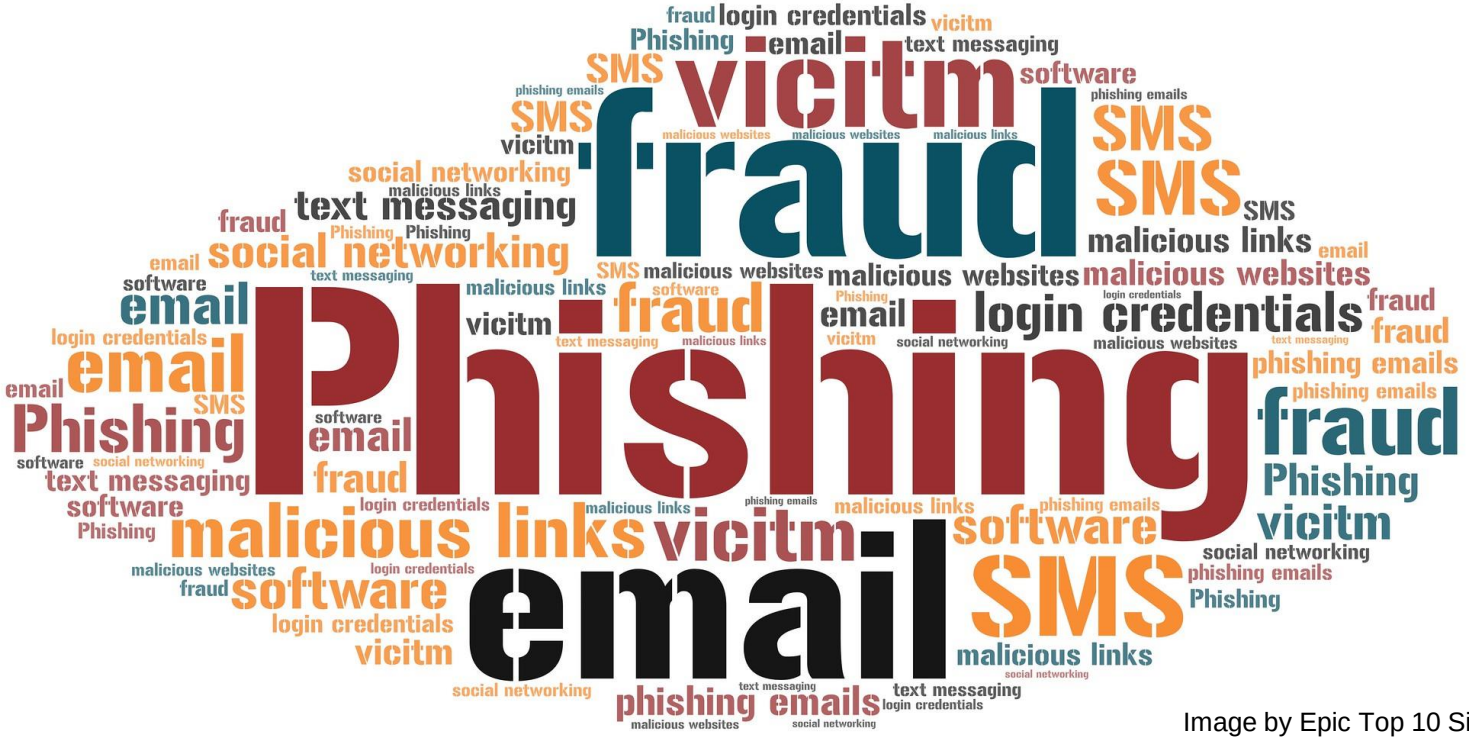


Image by Epic Top 10 Site

Saarlouis, 20. September 2022

Themen

- Was ist Cybercrime
- Datendiebstahl
- Schadsoftware
- Betrug, Agenten und Liebe
- „Fleißige“ Support Mitarbeiter
- Schutzmaßnahmen

Straftaten gegen

- das Internet
- andere Datennetze
- Informationstechnische Systeme (IT-Systeme)
- Daten innerhalb von IT-Systemen

Was genau versteht man eigentlich unter Cybercrime?

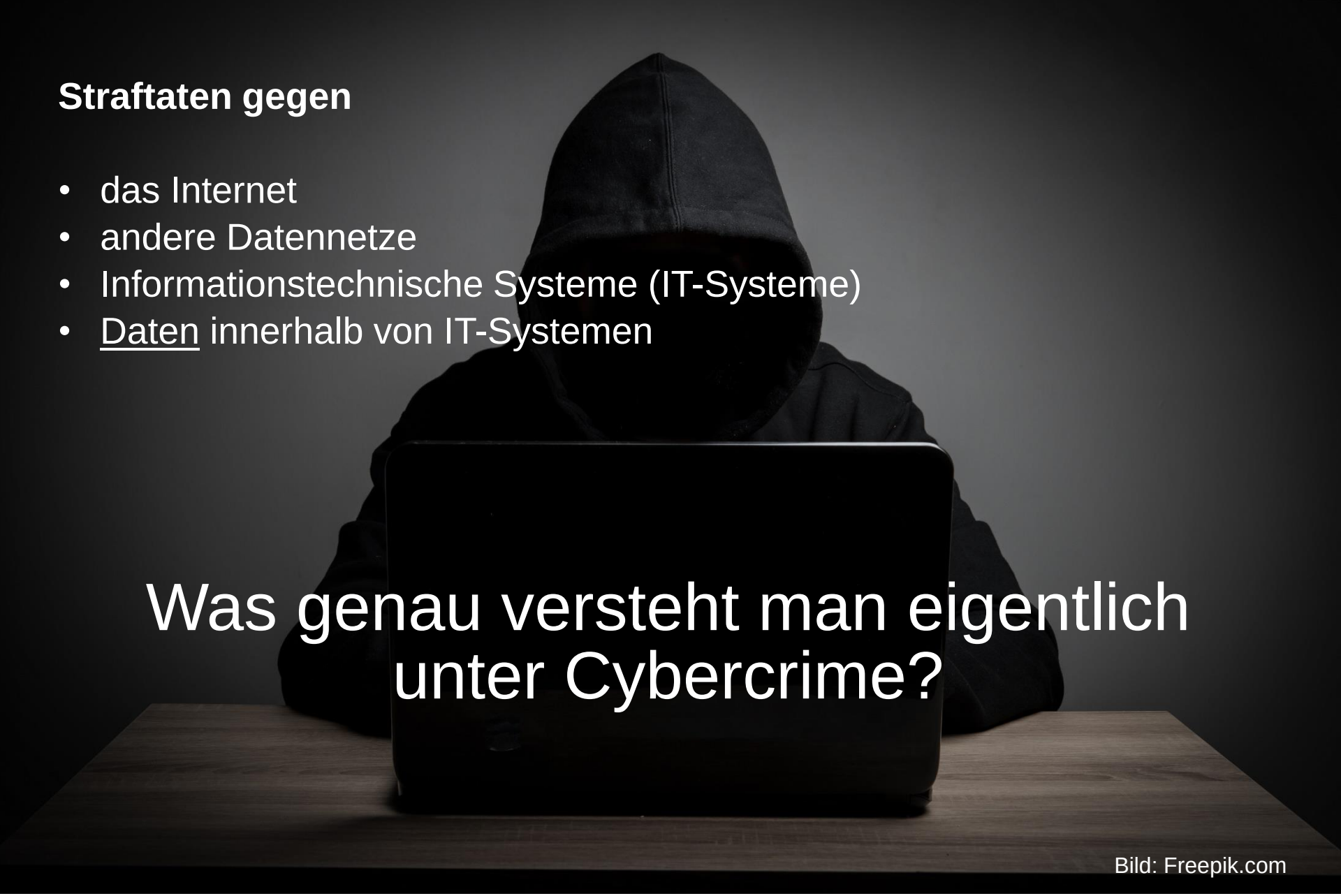


Bild: Freepik.com

Bekämpfung von Cybercrime im Landespolizeipräsidium des Saarlandes

Wie begegnet das Saarland den aktuellen Herausforderungen?

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)

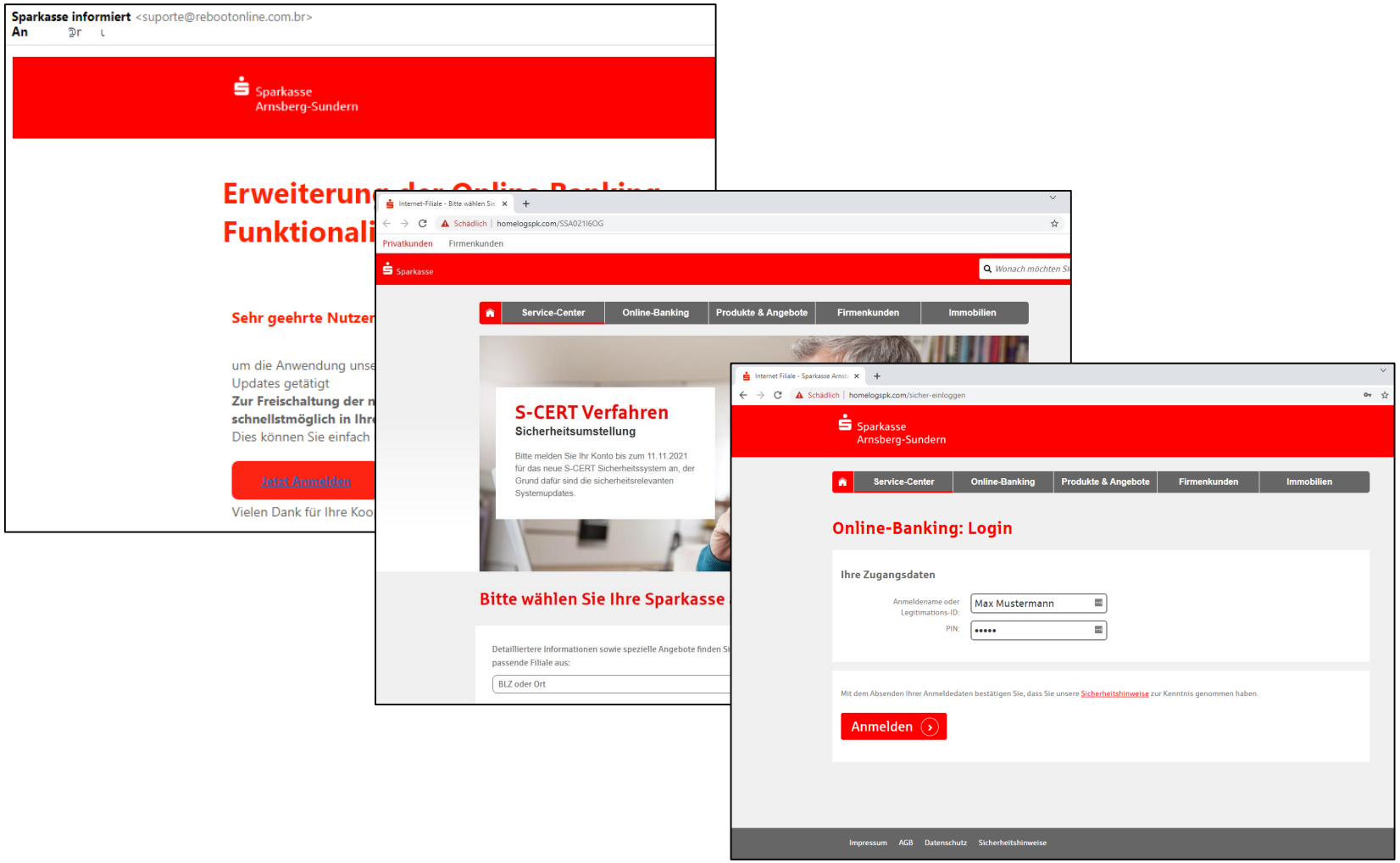
Ausspähen von Daten

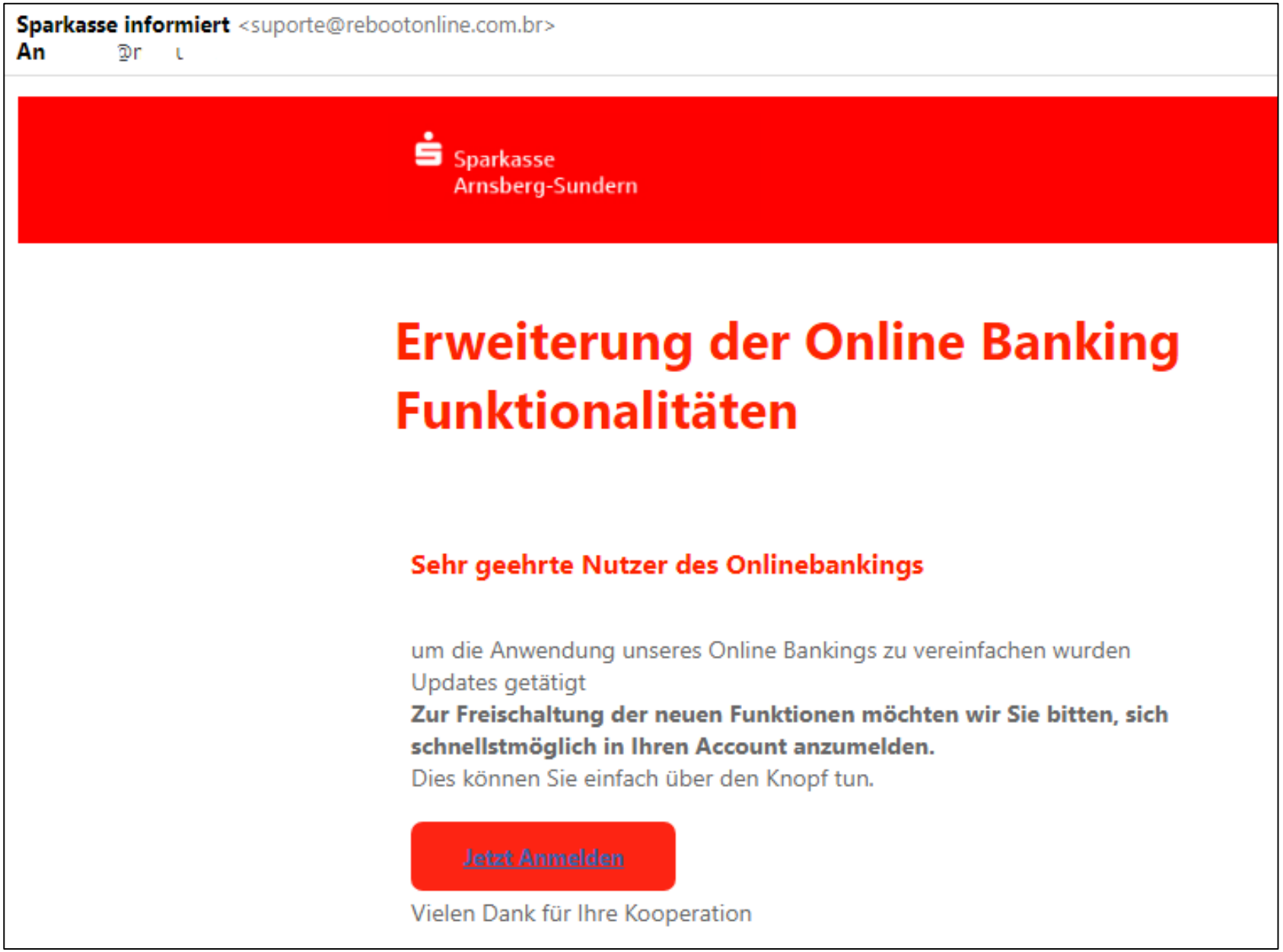
Wie gelangen Kriminelle an unsere Daten und was fangen sie damit an?

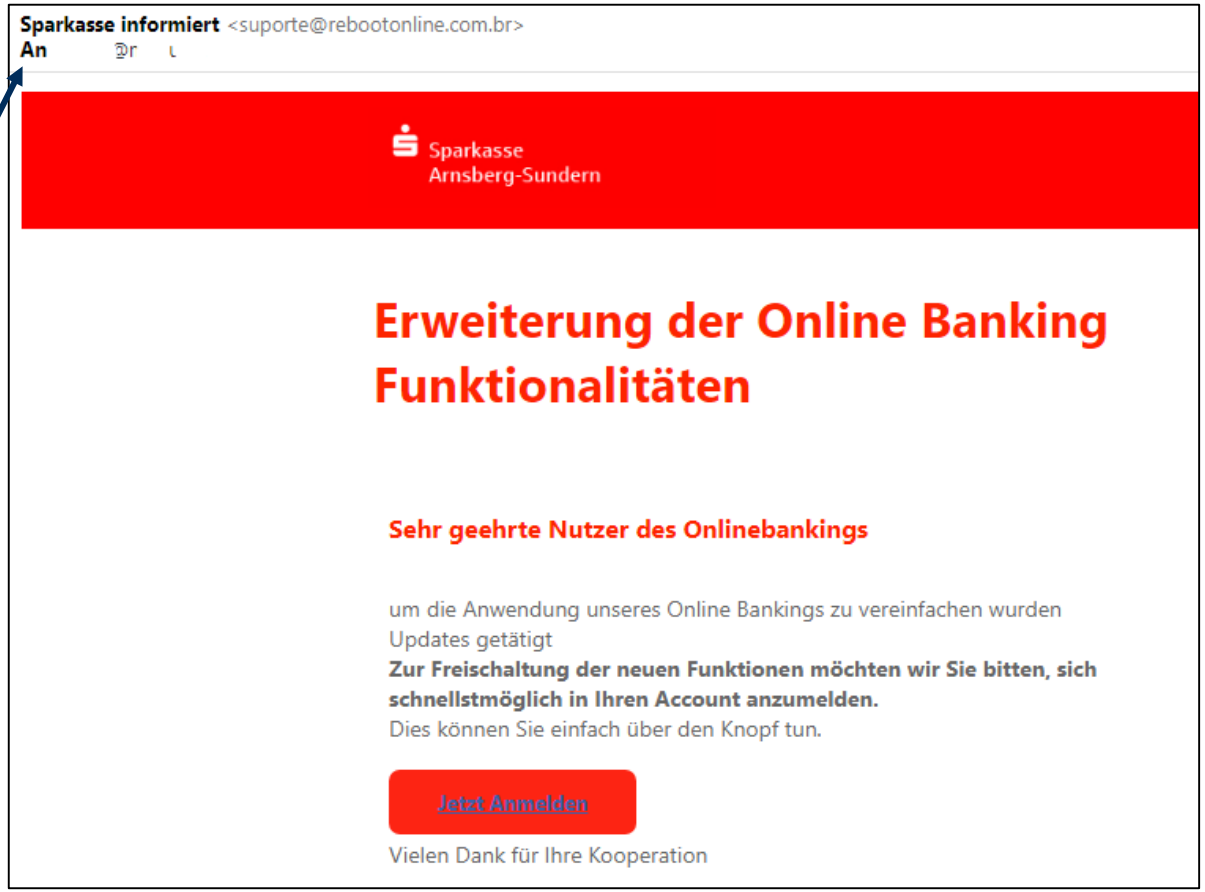
Phishing – Das Angeln nach Daten

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 aktuelles Beispiel

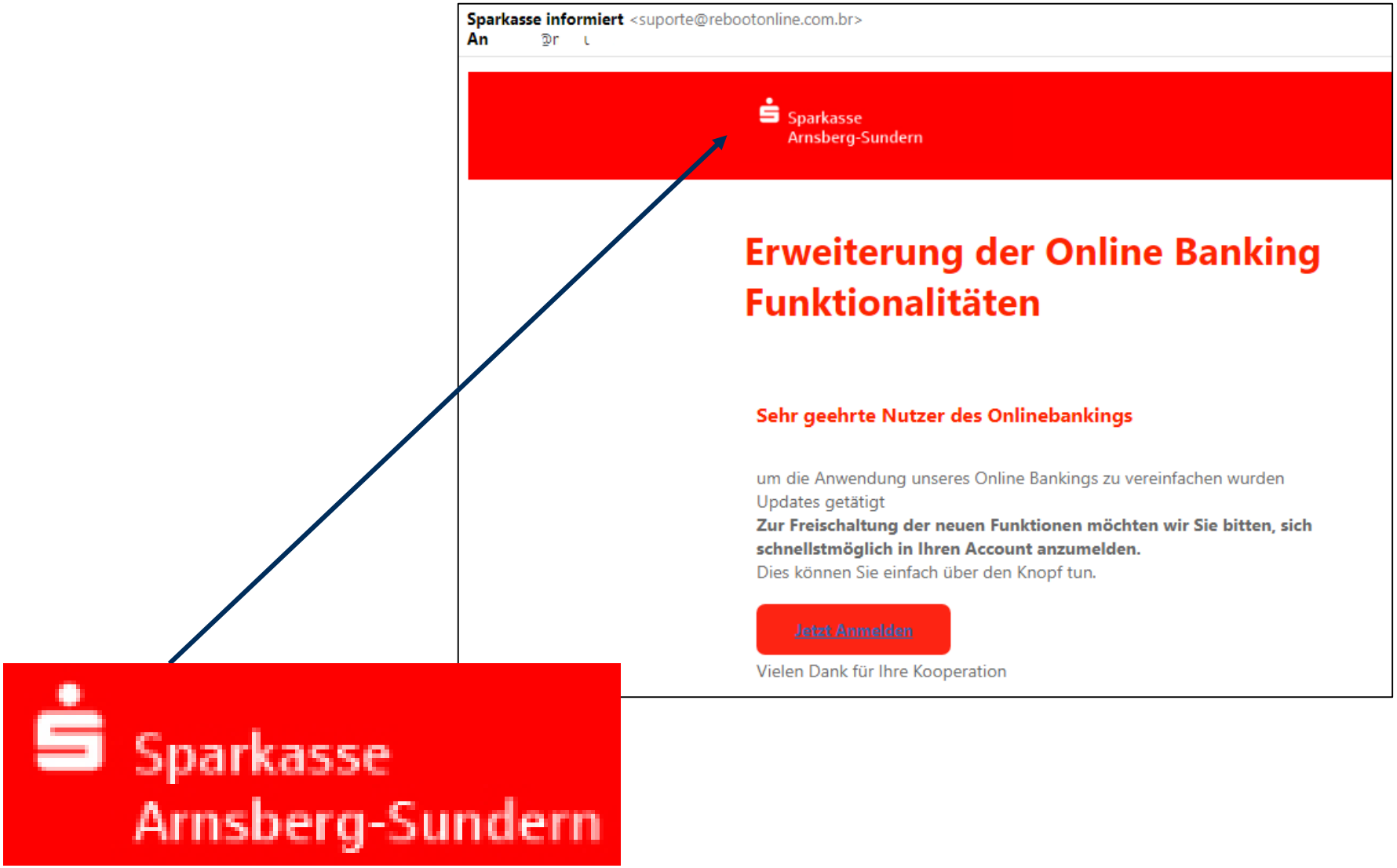



Sparkasse informiert <suporte@rebootonline.com.br>
An
Sparkasse
Arnsberg-Sundern
Erweiterung der Online Banking Funktionalitäten
Sehr geehrte Nutzer des Onlinebankings
um die Anwendung unseres Online Bankings zu vereinfachen wurden Updates getätigt
Zur Freischaltung der neuen Funktionen möchten wir Sie bitten, sich schnellstmöglich in Ihren Account anzumelden.
Dies können Sie einfach über den Knopf tun.
Jetzt Anmelden
Vielen Dank für Ihre Kooperation

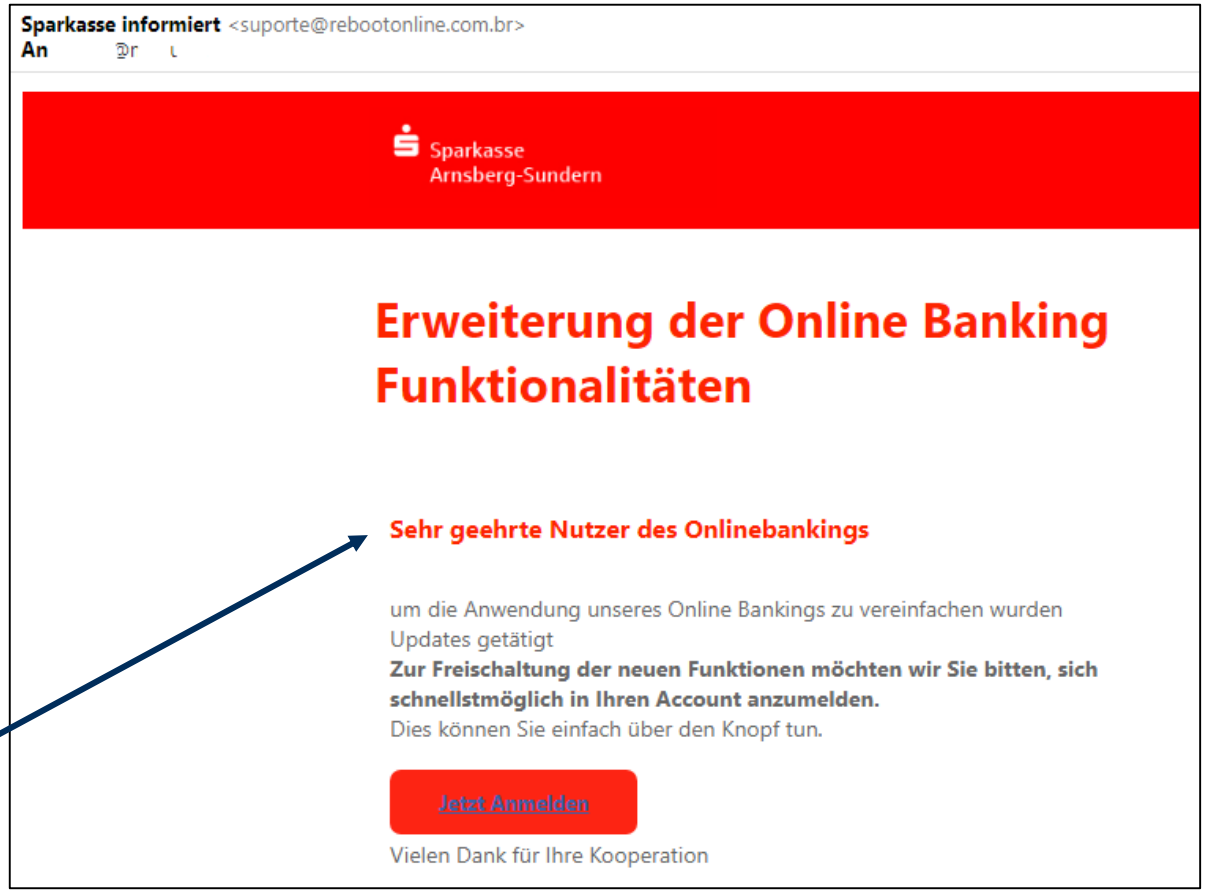


Sparkasse informiert <suporte@rebootonline.com.br>
An @r

ACHTUNG: Absender ist nicht die Sparkasse !!!



Bin ich Kunde bei genau dieser Sparkasse ?



Sehr geehrte Nutzer des Onlinebankings

um die Anwendung unseres Online Bankings zu vereinfachen wurden

Verdächtig: Persönliche Anrede fehlt !

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

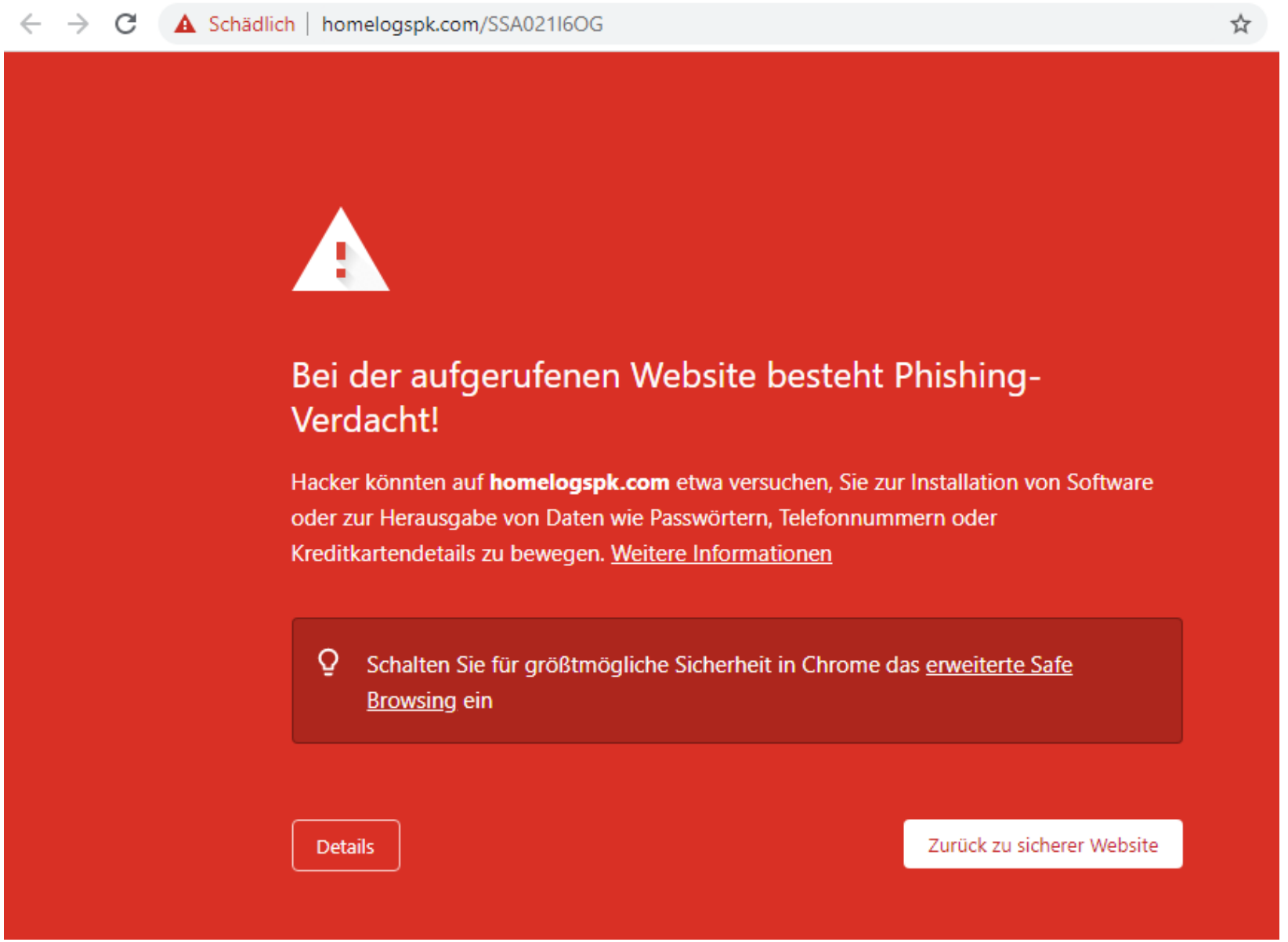
Sparkasse
Arnsberg-Sundern

Erweiterung der Online Banking Funktionalitäten

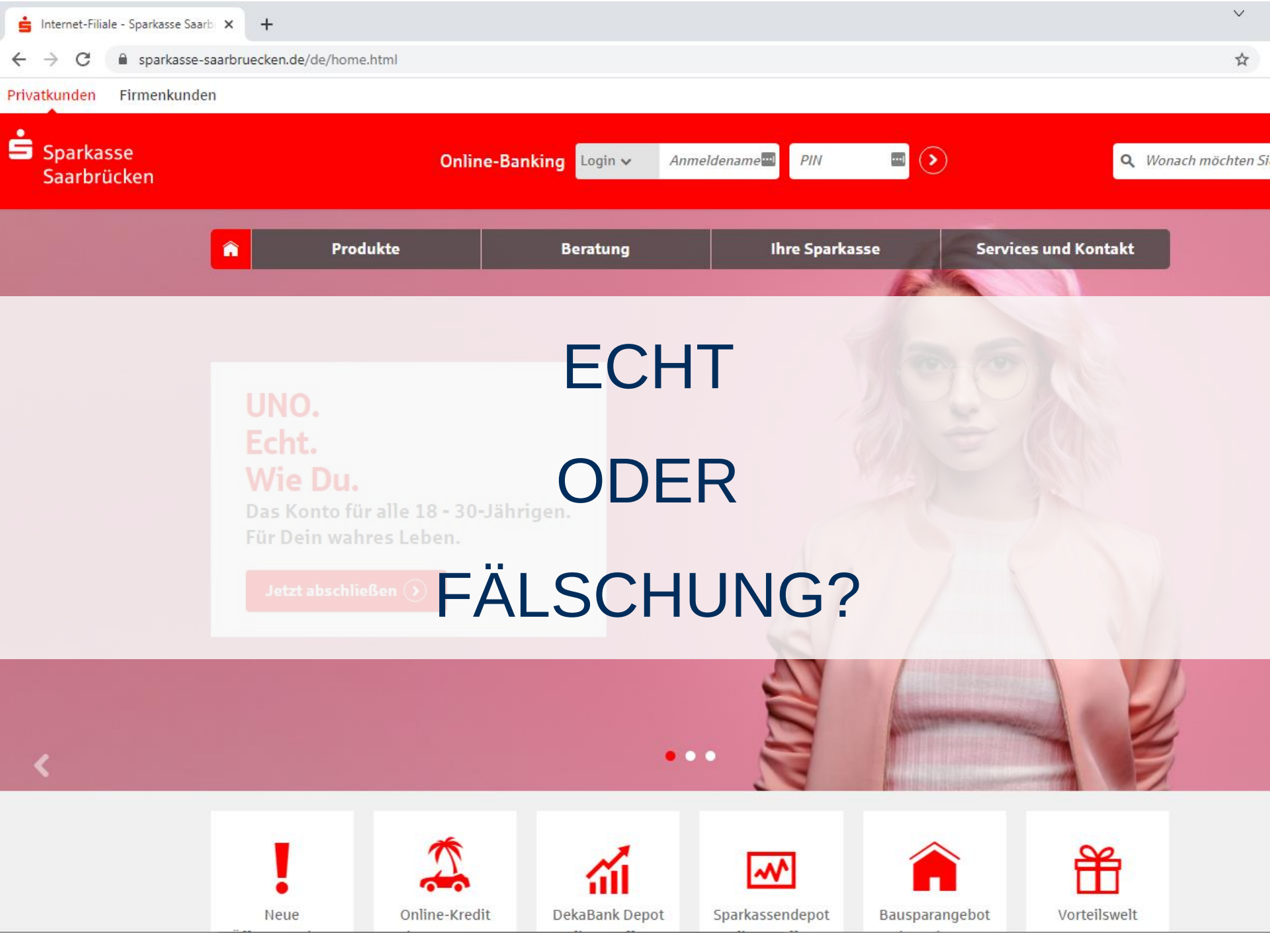
Sehr geehrte Nutzer des Onlinebankings

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.

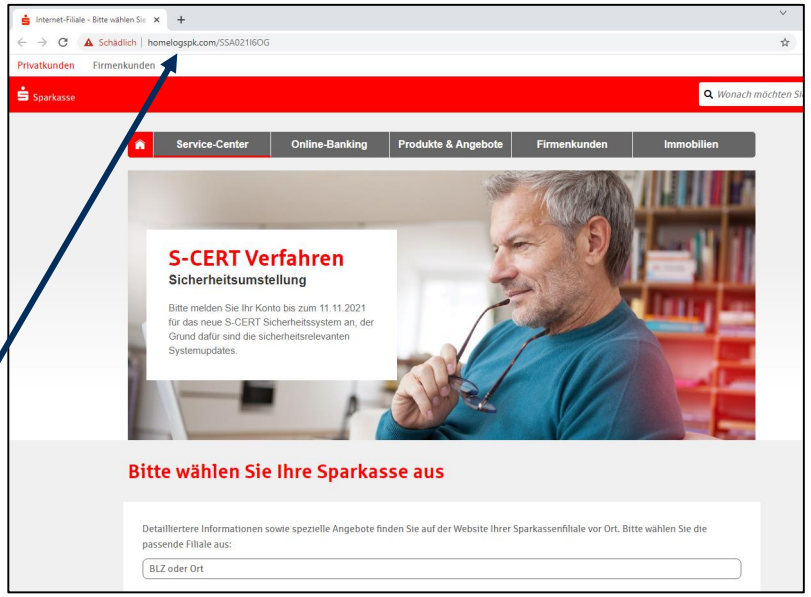
Vielen Dank für Ihre Kooperation

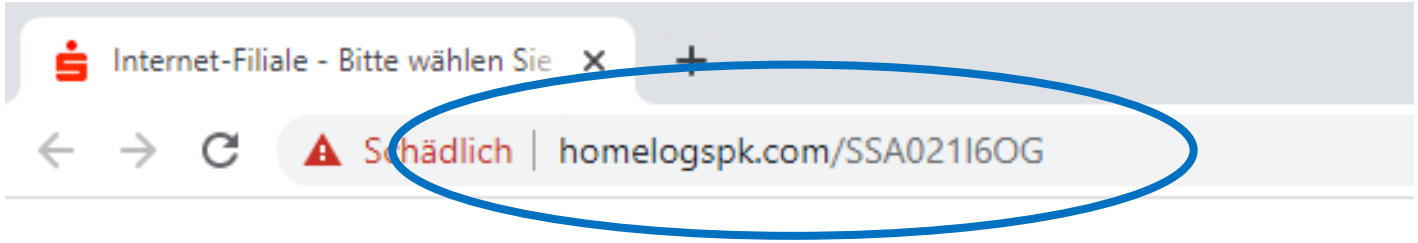

Schädlich | homelogspk.com/SSA021I6OG
Bei der aufgerufenen Website besteht Phishing-Verdacht!
Hacker könnten auf homelogspk.com etwa versuchen, Sie zur Installation von Software oder zur Herausgabe von Daten wie Passwörtern, Telefonnummern oder Kreditkartendetails zu bewegen. Weitere Informationen
Schalten Sie für größtmögliche Sicherheit in Chrome das erweiterte Safe Browsing ein
Details
Zurück zu sicherer Website

Internet-Filiale - Bitte wählen Sie
Schädlich | homelogspk.com/SSA021I6OG
Privatkunden
Firmenkunden
Sparkasse
Wonach möchten Sie
Service-Center
Online-Banking
Produkte & Angebote
Firmenkunden
Immobilien
S-CERT Verfahren
Sicherheitsumstellung
Bitte melden Sie Ihr Konto bis zum 11.11.20
für das neue S-CERT Sicherheitssystem an, der
Grund dafür sind die sicherheitsrelevanten
Systemupdates.
ECHT
ODER
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:
BLZ oder Ort


Internet-Filiale - Sparkasse Saarb
sparkasse-saarbruecken.de/de/home.html
Privatkunden
Firmenkunden
Sparkasse Saarbrücken
Online-Banking
Login
Anmeldename
PIN
Produkte
Beratung
Ihre Sparkasse
Services und Kontakt
UNO.
Echt.
Wie Du.
Das Konto für alle 18 - 30-Jährigen.
Für Dein wahres Leben.
Jetzt abschließen
ECHT
ODER
FÄLSCHUNG?
Neue
Online-Kredit
DekaBank Depot
Sparkassendepot
Bausparangebot
Vorteilswelt

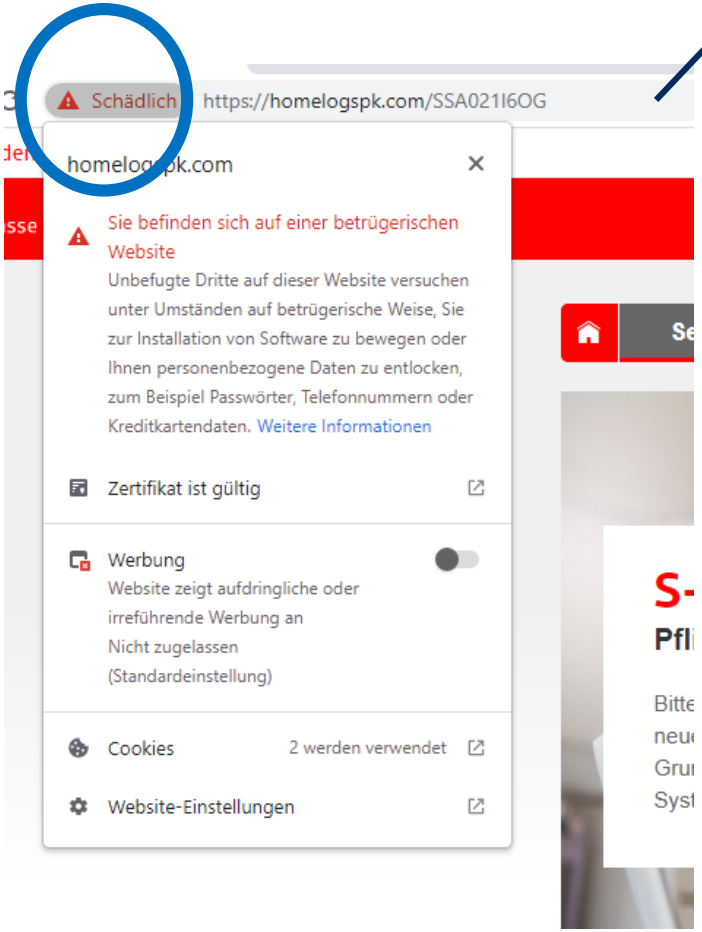
Internet-Filiale - Bitte wählen Sie
Schädlich | homelogspk.com/SSA021I6OG
Privatkunden
Firmenkunden
Sparkasse
Wonach möchten Sie
Service-Center
Online-Banking
Produkte & Angebote
Firmenkunden
Immobilien
S-CERT Verfahren
Sicherheitsumstellung
Grund dafür sind die sicherheitsrelevanten
Systemupdates.
Das ist die Fälschung!
Aber wie kann ich das erkennen?
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

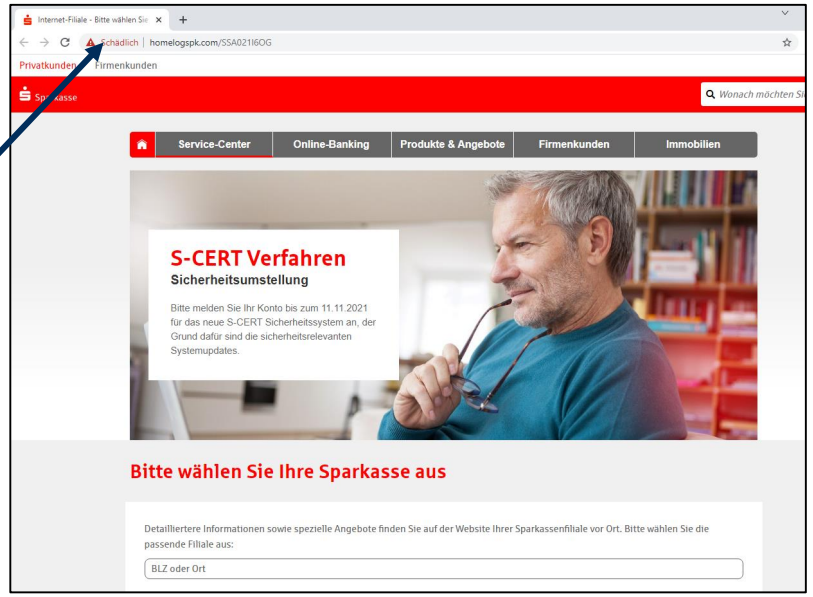




URL (Adresse im Browser) prüfen !

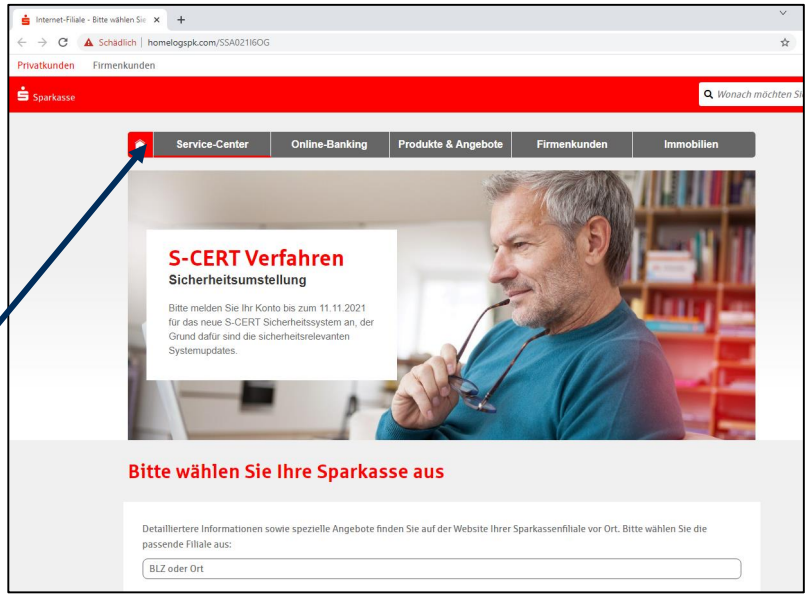
-> ACHTUNG !!! Das ist nicht die Seite der Sparkasse !!!





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 !!!

Internet-Filiale - Bitte wählen Sie

Schädlich | homelogspk.com/SSA021I6OG

Privatkunden Firmenkunden

Sparkasse

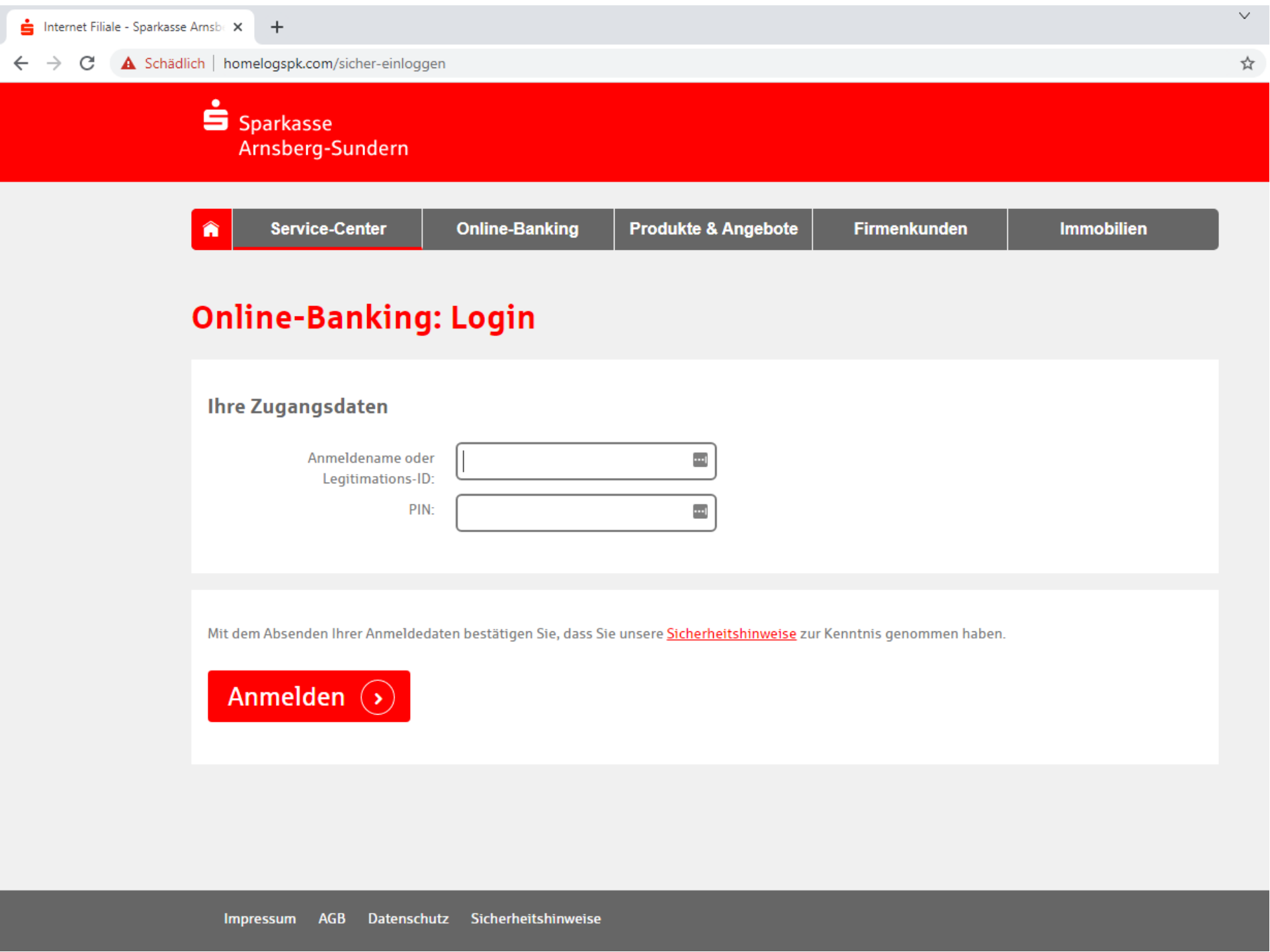
Wonach möchten Si

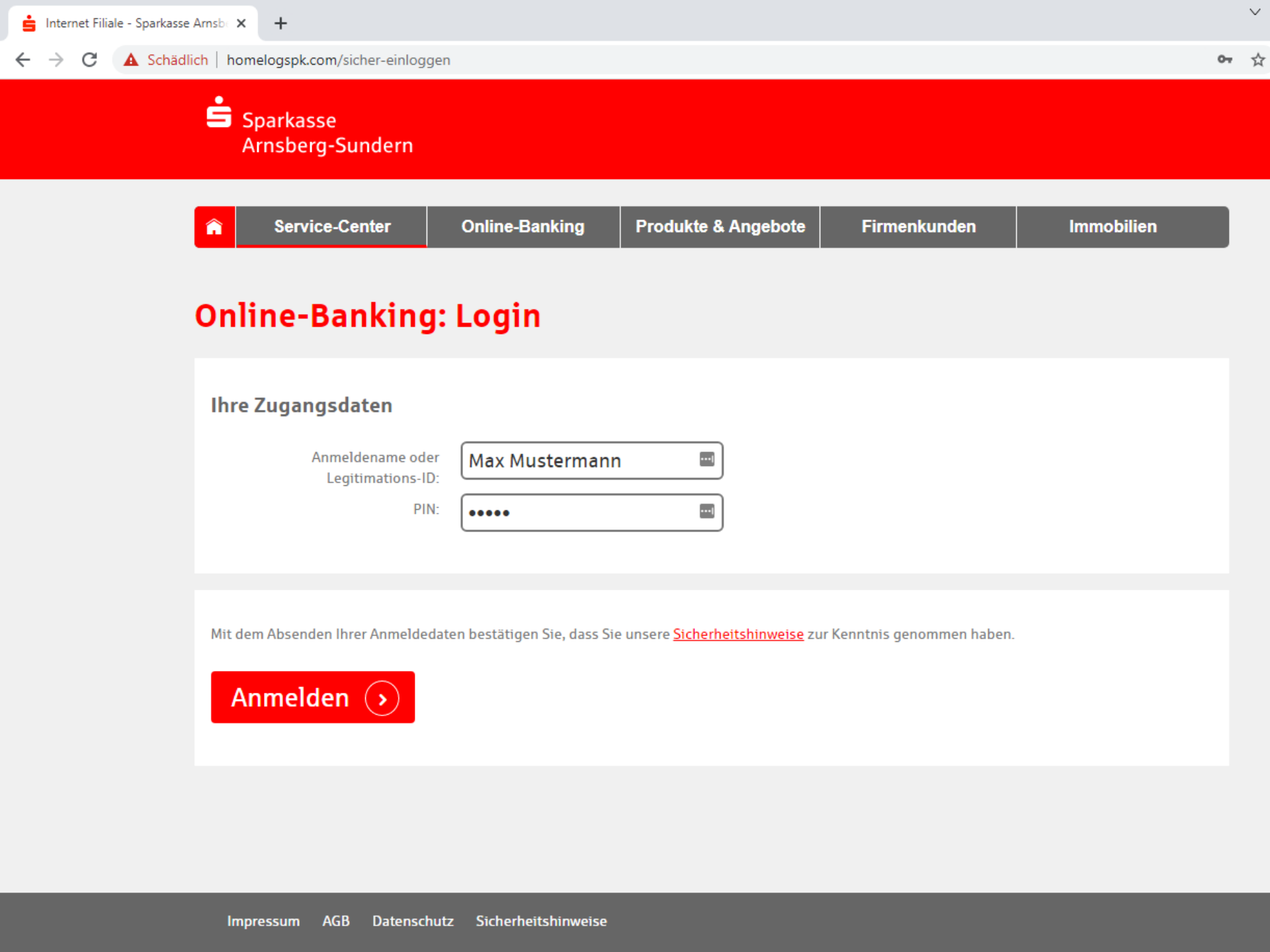
Service-Center | Online-Banking | Produkte & Angebote | Firmenkunden | Immobilien

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


Internet Filiale - Sparkasse Arnsb
Schädlich
homelogspk.com/sicher-einloggen
Sparkasse
Arnsberg-Sundern
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
Impressum
AGB
Datenschutz
Sicherheitshinweise


Internet Filiale - Sparkasse Arnsb
Schädlich | homelogspk.com/sicher-einloggen
Sparkasse
Arnsberg-Sundern
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
Impressum
AGB
Datenschutz
Sicherheitshinweise

Internet Filiale - Sparkasse Arnsb

Schädlich | homelogspk.com/sicher-einloggen?error=login-invalid

Sparkasse
Arnsberg-Sundern

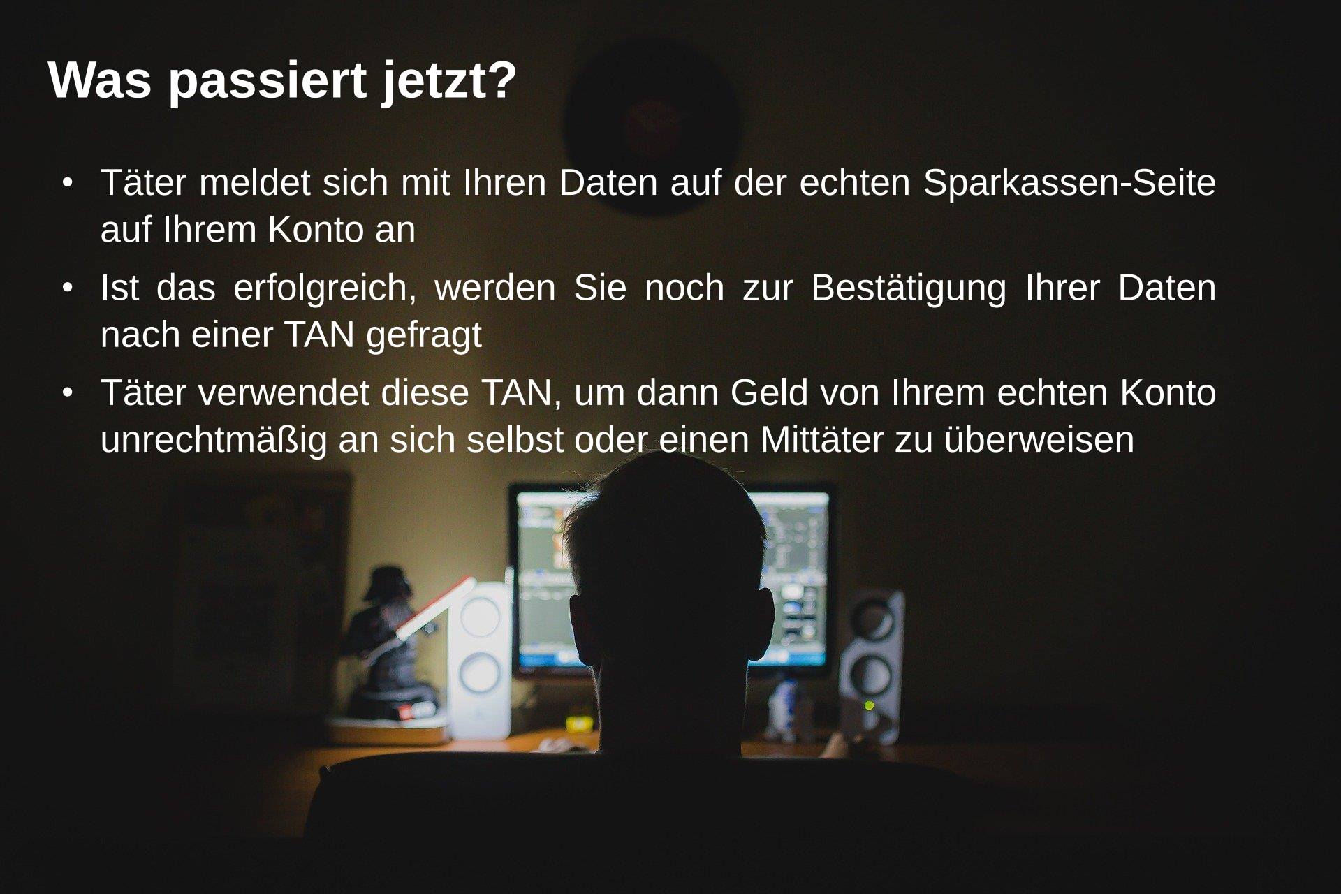
Service-Center | Online-Banking | Produkte & Angebote | Firmenkunden | Immobilien

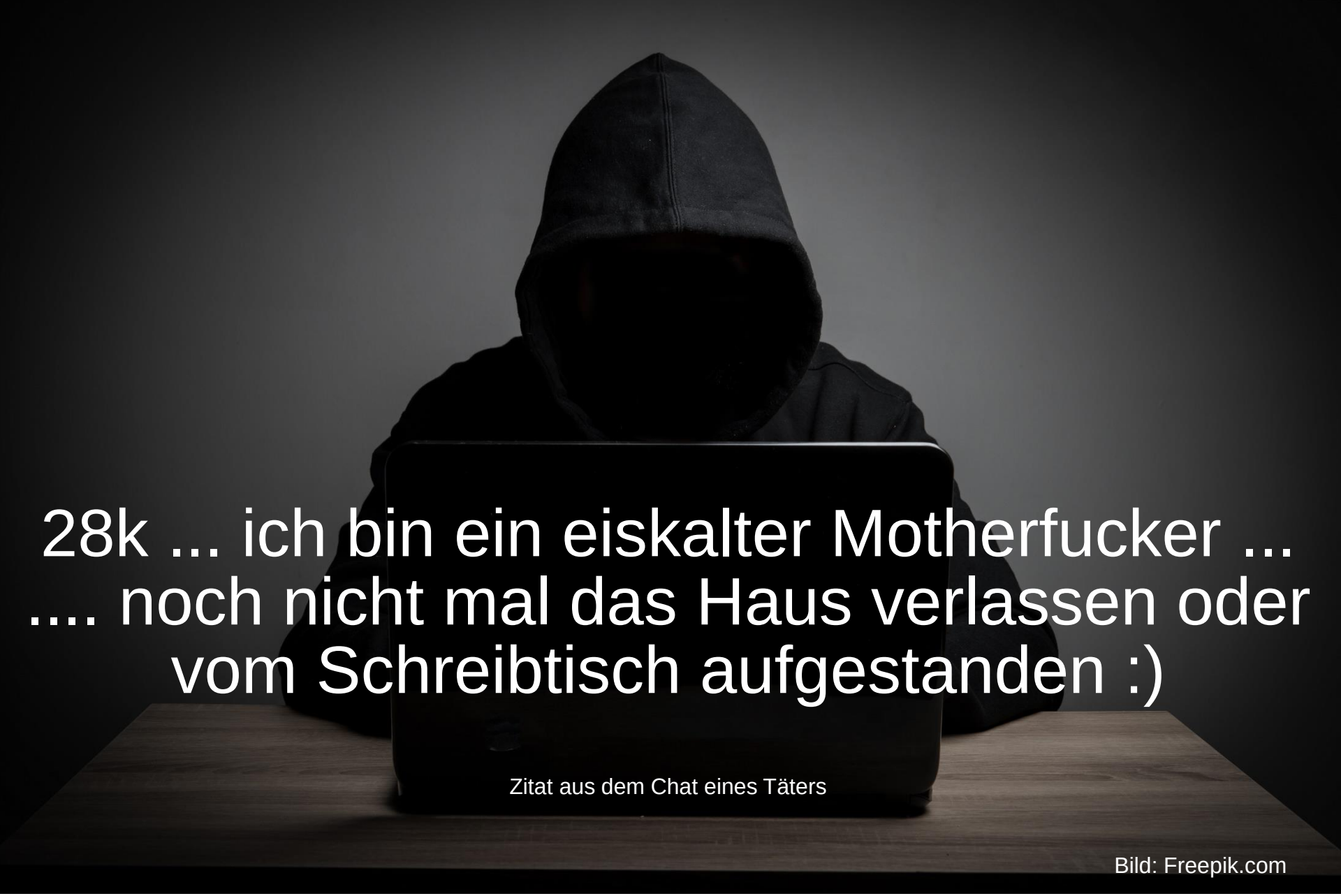
Überprüfung wird durchgeführt

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.

Was passiert jetzt?

- 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

Wie erkenne ich die echten Internet-Seiten ?

Internet-Filiale - Sparkasse Saarb

sparkasse-saarbruecken.de/de/home.html

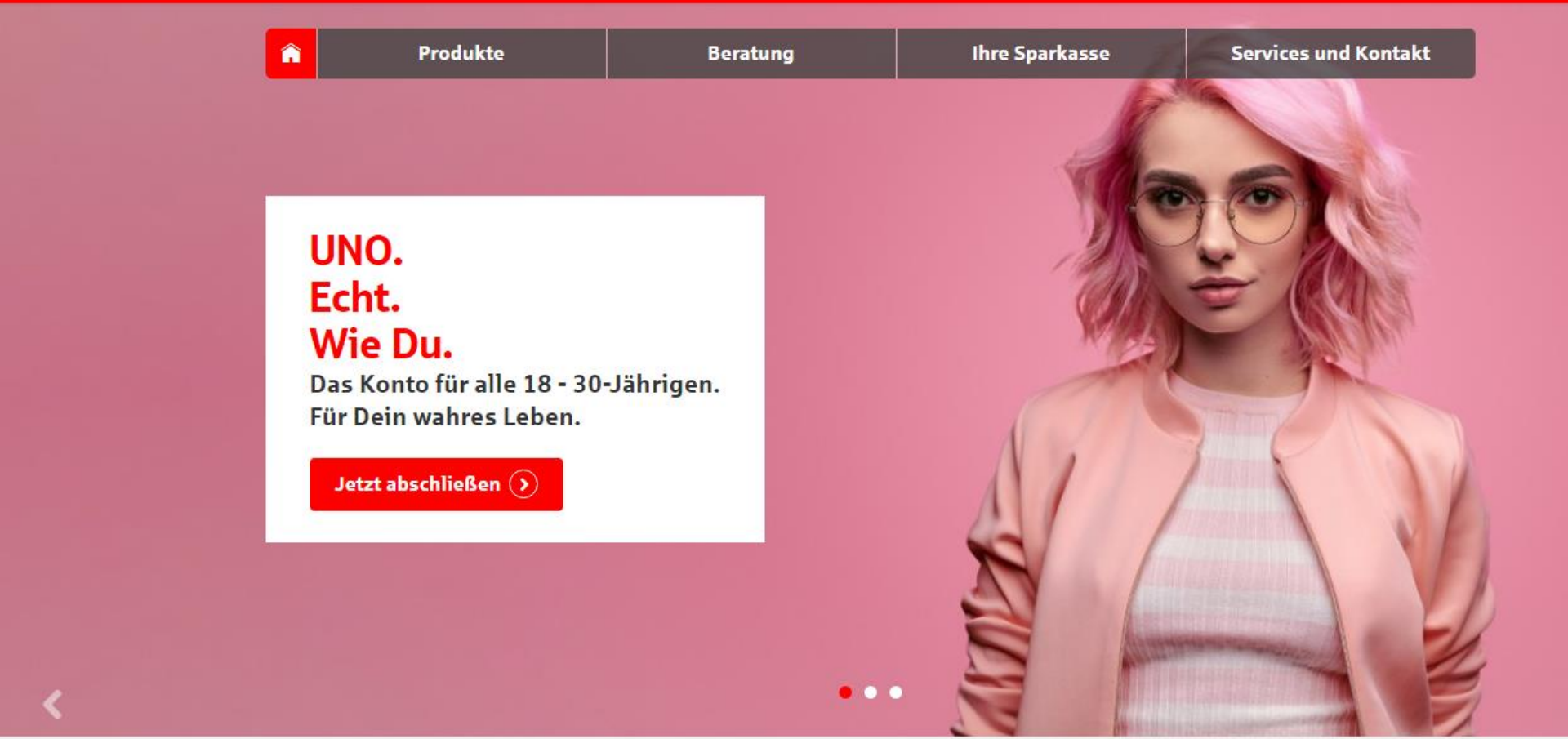
Privatkunden Firmenkunden

Sparkasse Saarbrücken

Online-Banking Login Anmeldename PIN

Wonach möchte

Produkte | Beratung | Ihre Sparkasse | Services und Kontakt



Neue

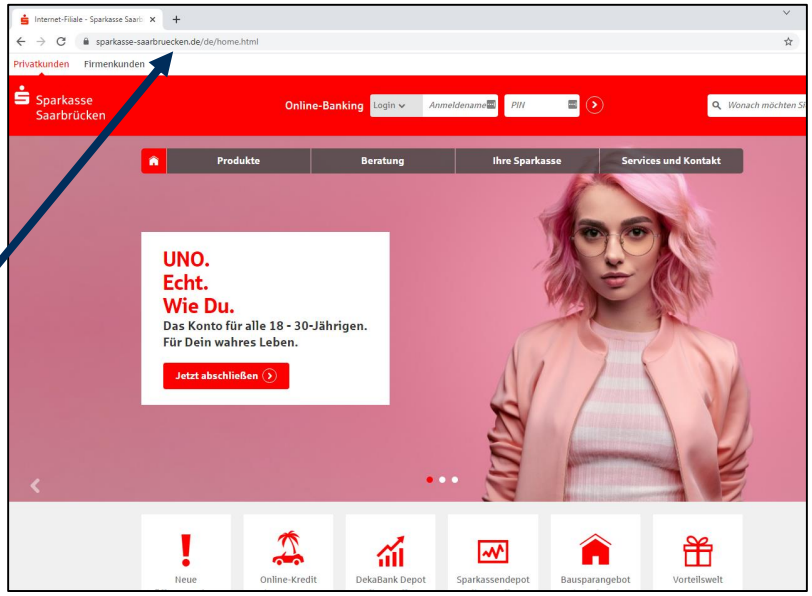
Online-Kredit

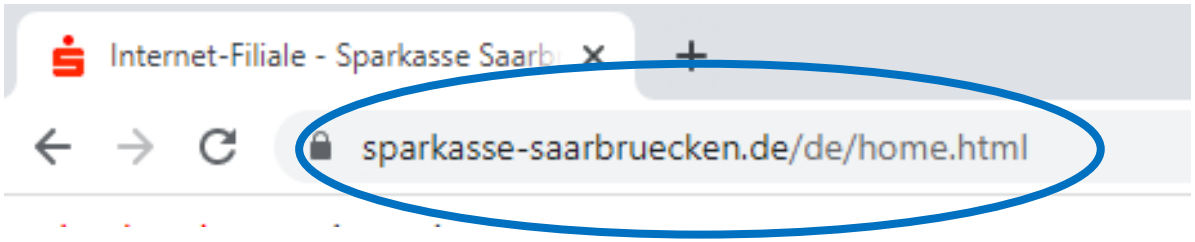
DekaBank Depot

Sparkassendepot

Bausparangebot

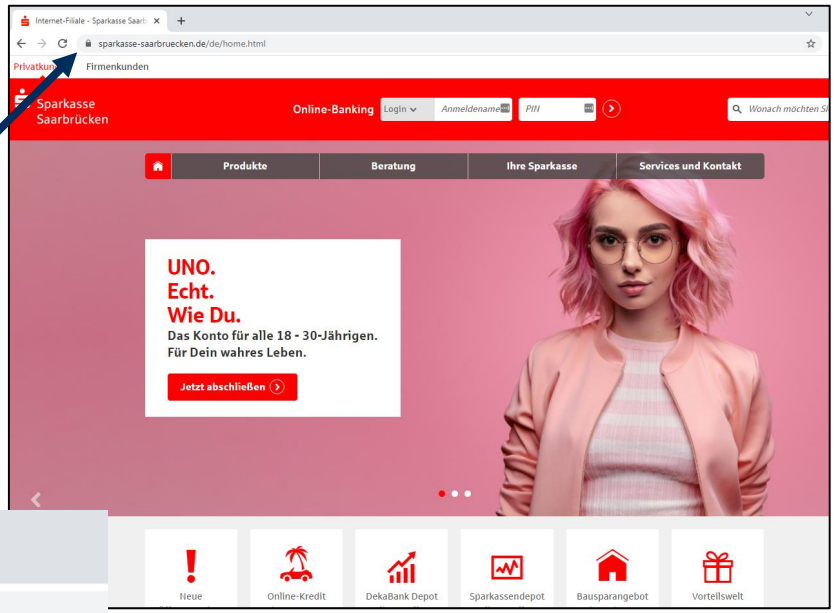
Vorteilswelt

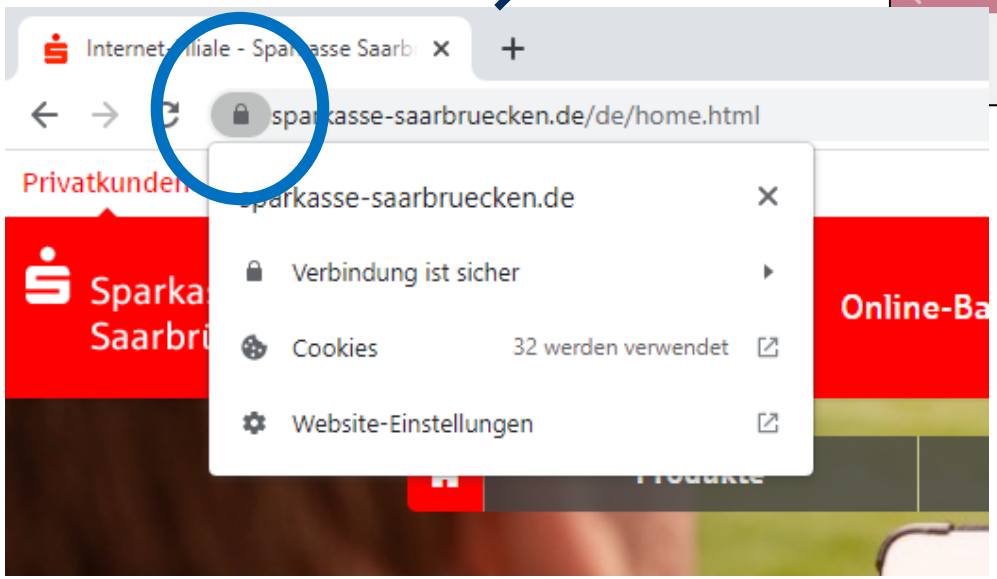




URL (Adresse im Browser) prüfen !

-> PLAUSIBEL

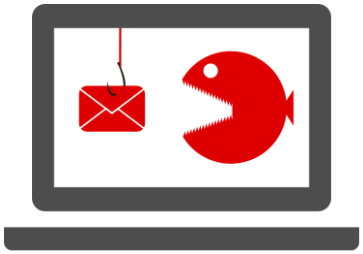




Zertifikat (Digitale Identitätsprüfung für die URL) prüfen !

-> GÜLTIG (keine unbemerkte Umleitung)

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 Konsequenzen** (Konto- oder Accountsperrung, Kosten, pp.).

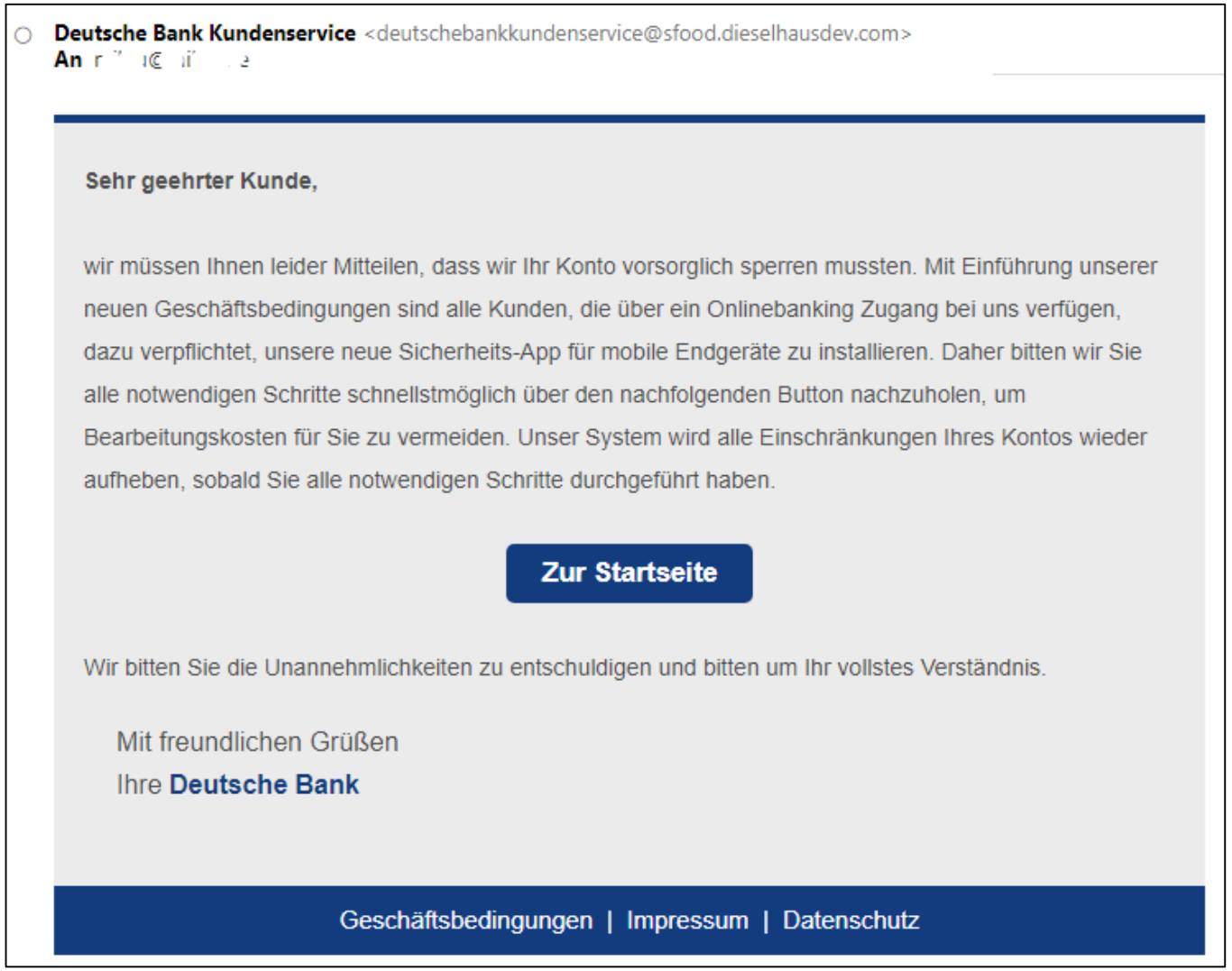
4. Sie klicken auf den Link.

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.

Weitere Beispiele Phishing E-Mail



Deutsche Bank Kundenservice <deutschebankkundenservice@sfood.dieselhausdev.com>
An

Sehr geehrter Kunde,

wir müssen Ihnen leider Mitteilen, dass wir Ihr Konto vorsorglich sperren mussten. Mit Einführung unserer neuen Geschäftsbedingungen sind alle Kunden, die über ein Onlinebanking Zugang bei uns verfügen, dazu verpflichtet, unsere neue Sicherheits-App für mobile Endgeräte zu installieren. Daher bitten wir Sie alle notwendigen Schritte schnellstmöglich über den nachfolgenden Button nachzuholen, um Bearbeitungskosten für Sie zu vermeiden. Unser System wird alle Einschränkungen Ihres Kontos wieder aufheben, sobald Sie alle notwendigen Schritte durchgeführt haben.

Zur Startseite

Wir bitten Sie die Unannehmlichkeiten zu entschuldigen und bitten um Ihr vollstes Verständnis.

Mit freundlichen Grüßen
Ihre **Deutsche Bank**

Geschäftsbedingungen | Impressum | Datenschutz

Weitere Beispiele Phishing E-Mail

HypoVereinsbank <noreply@hypovereinsbank.de>
An

HypoVereinsbank

Kunde Hypovereinsbank

Ihr Profil hat sich weiterentwickelt. Schützen Sie Ihre Konten, indem Sie die Aktualisierung Ihres Sicherheitsbereichs aktivieren.

Update

*Bitte behalten Sie den Bildschirm im Auge und haben Sie Geduld, während die Anleitung geladen wird. Dies kann mehr als 10 Minuten dauern.

*Bitte verlassen Sie die Ladeseite nicht, um den nächsten Schritt zu sehen.

Weiteres Beispiel Phishing E-Mail

amazon.com

Wir brauchen Ihre Hilfe,

Wir benötigen ihre Hilfe damit es für sie weiterhin möglich ist ihr Amazon Konto wie gewohnt nutzen zu können.

Wo liegt das Problem?

Auf ihrem Amazon Kundenkonto wurde eine Bestellung getätigt welche auf eine nicht von ihnen angegebene Lieferadresse gesendet werden sollte.

Unser Sicherheitssystem hat diese Bestellung erkannt und storniert.
Wir bitten sie daher ihr Mitgliedskonto schnellstmöglich zu verifizieren um weiteren Komplikationen vorzubeugen.

Nach erfolgreicher Verifizierung können sie ihr Konto wieder im vollen Umfang nutzen.

Damit sie ihr Konto wieder uneingeschränkt nutzen können, verifizieren sie sich bitte durch Abgleich ihrer Daten als rechtmäßiger Besitzer.

Nach erfolgreicher Verifizierung können sie ihr Konto wieder im vollen Umfang nutzen.

Ihr Amazon Kundenservice

Was mache ich jetzt?

Nutzen Sie zur Verifizierung folgenden Link:

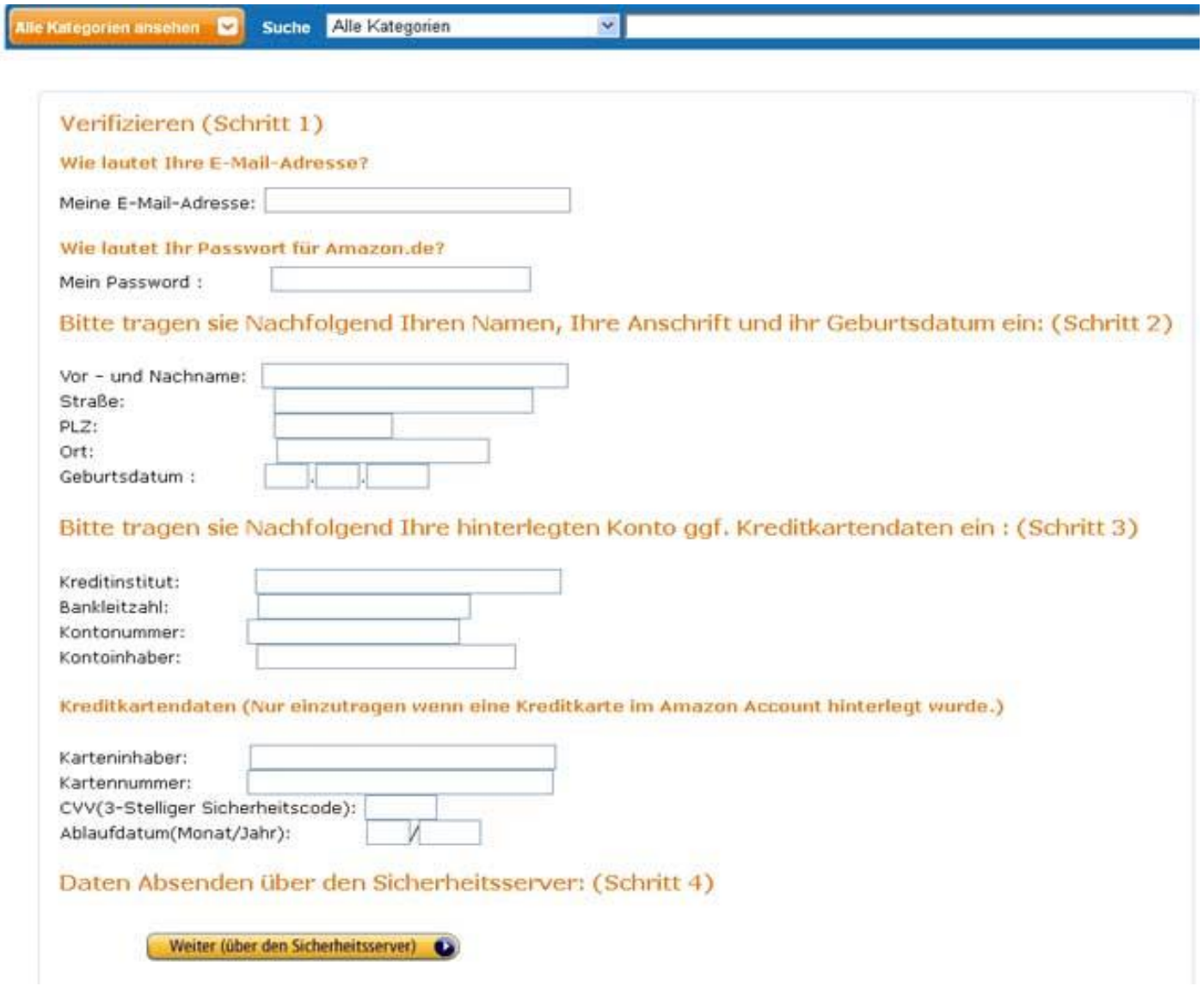
Konto jetzt verifizieren

Der Link zur Verifikation zeigt auf http://www.**amazon-kundencenter**.de/verifizierung.

Die Domain www.amazon-kundencenter.de hat jedoch mit www.amazon.de nichts zutun!

Klicken sie auf den Link, gelangen sie zur Webseite der Kriminellen, die der Webseite von Amazon „täuschend ähnlich sieht“…

Typische Phishing-Webseite mit Amazon-Layout



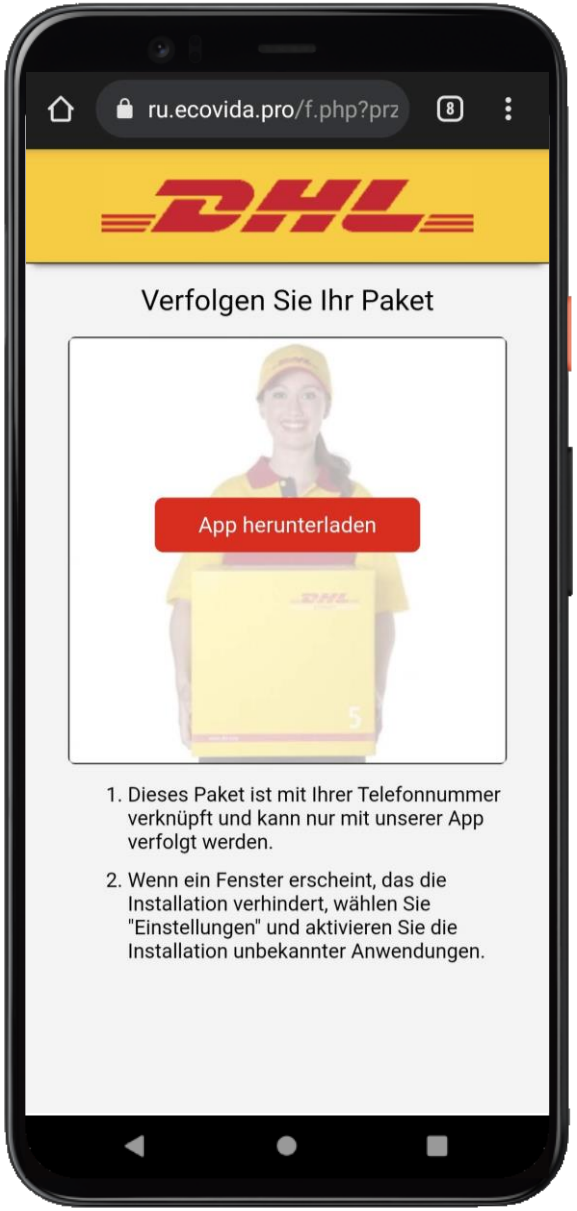
Sonderform Spam SMS:

„SMS“ + „Phishing“ = „Smishing“

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?2mt45otot 23:06

ACHTUNG: Die SMS enthält einen (verdächtigen) Link!

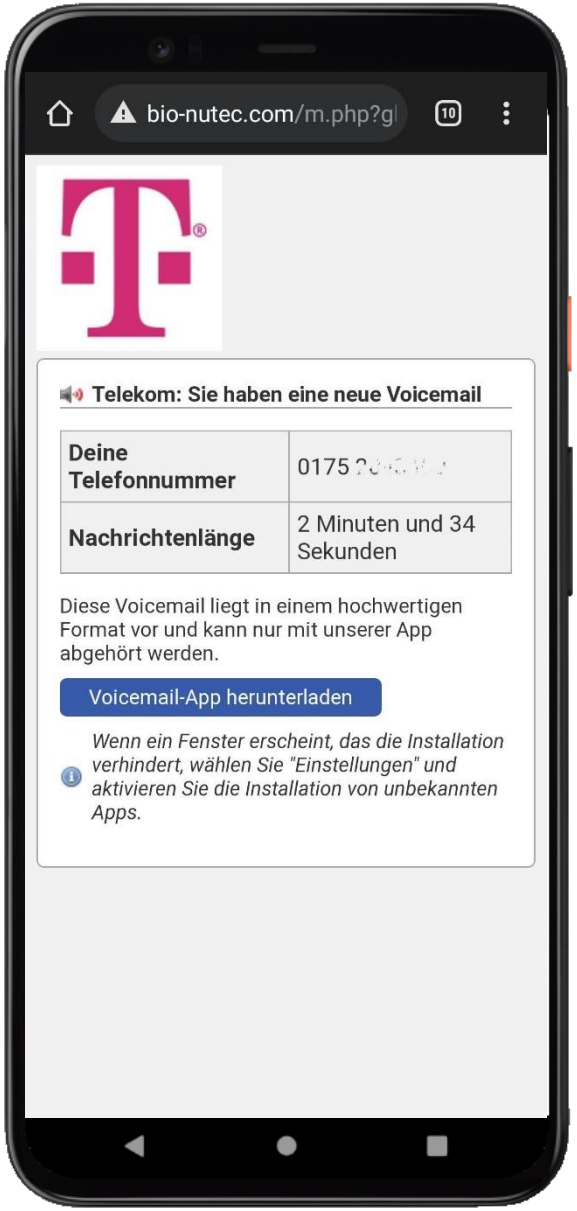


Sie werden aufgefordert, eine App zu installieren und Sicherheitsfunktionen auf Ihrem Telefon zu deaktivieren:

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!

+49 160
+49 160
Sie - haben einen verpassten [sb4] Anruf. Der Anrufer hat Ihnen - eine Nachricht . hinterlassen http://bio-nutec.com/m.php ?hehu1mag
1min
Unverschlüsselte SMS


bio-nutec.com/m.php?gl
Telekom: Sie haben eine neue Voicemail
Deine Telefonnummer
0175
Nachrichtenlänge
2 Minuten und 34 Sekunden
Diese Voicemail liegt in einem hochwertigen Format vor und kann nur mit unserer App abgehört werden.
Voicemail-App herunterladen
Wenn ein Fenster erscheint, das die Installation verhindert, wählen Sie "Einstellungen" und aktivieren Sie die Installation von unbekannten Apps.

Phishing – Das Angeln nach Daten

Was kann ich tun?

- Verdächtigen eletronischen 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 grundätzlich 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.

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)

=> Vorsicht bei kostenlosen Angeboten

„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

„Trojaner“

Was ist das Ziel eines Trojaners?

- Stehlen von Passwörtern
- Stehlen von Bankdaten oder Kreditkartendaten
- Stehlen von Rechenleistung (z.B. Cryptowährungen „minen“)
- Nachladen neuer Schadsoftware (z.B. Ransomware)
- Selten Erpressung

„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

Wie können Kriminelle noch unsere Daten gelangen?

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

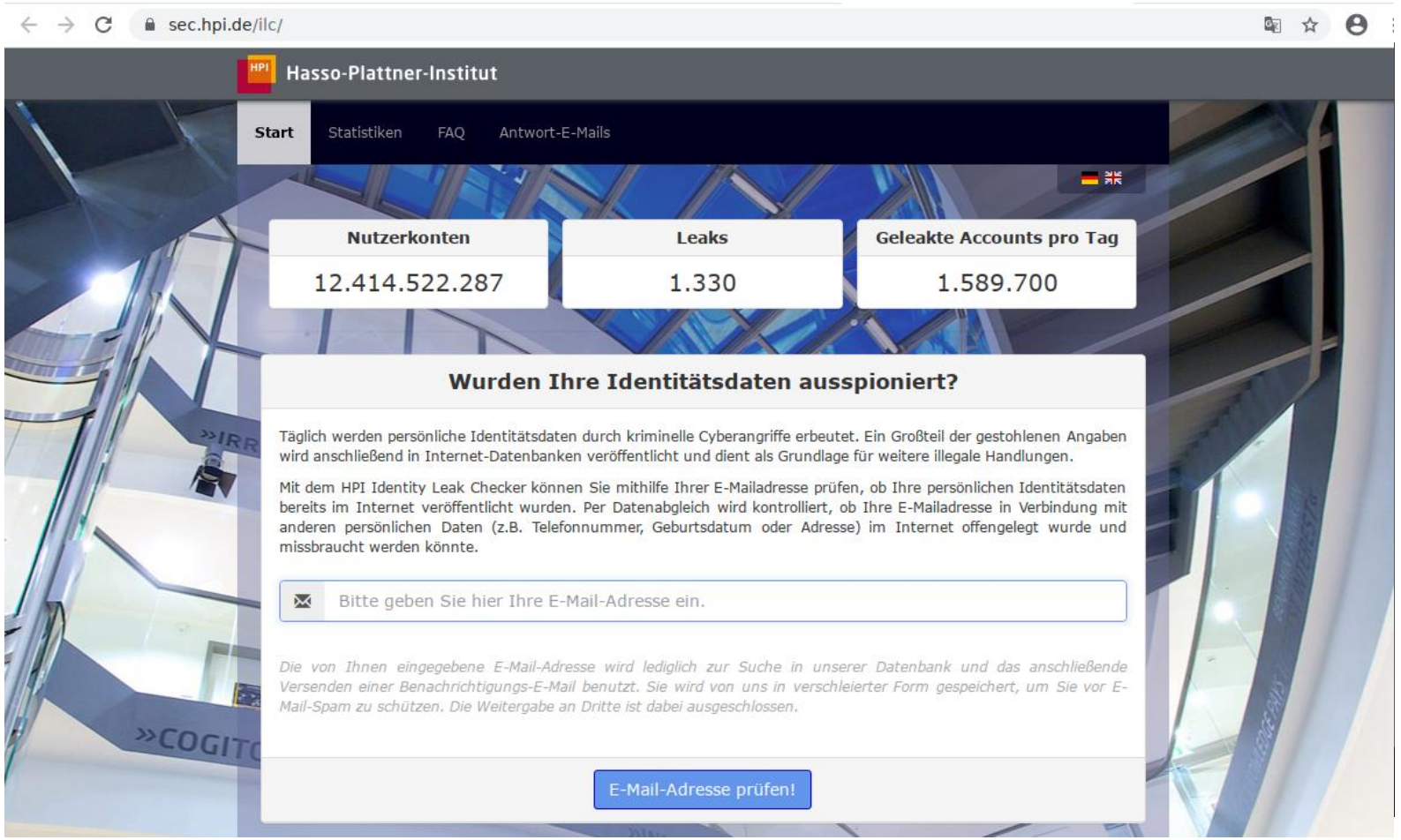
Was kann ich tun?

Nutzen Sie unbedingt verschiedene Passwörter für verschiedene Anbieter!

Bin ich betroffen ?

Prüfung beim Hasso-Plattner-Institut

https://sec.hpi.de/ilc/



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	–	–	–	–	–	–	–	–

Was wir selbst preisgeben -
Die Gefahren der sozialen Medien

Was versteht man eigentlich unter sozialen Medien?

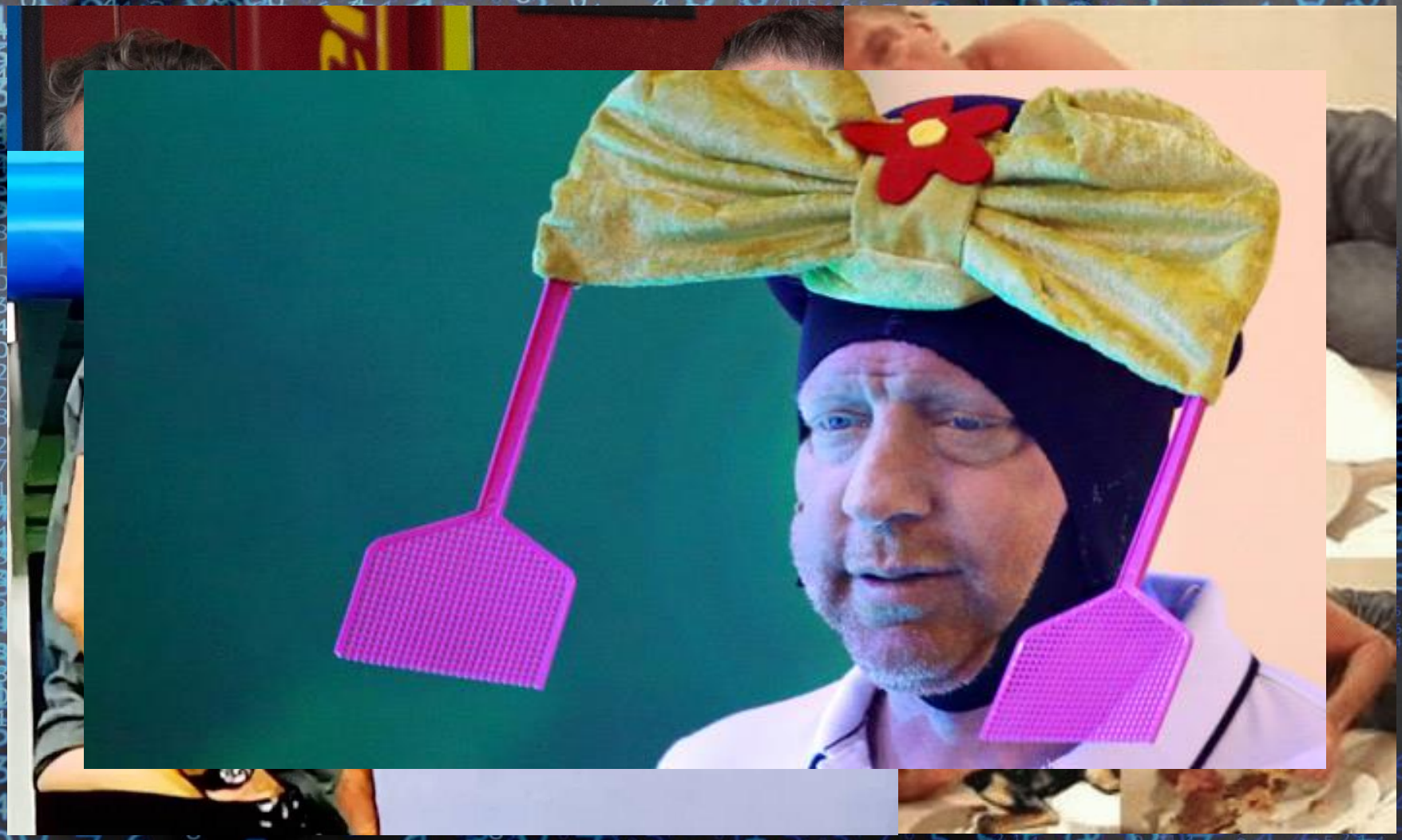
„Soziale Medien“ sind digitale Medien, die es Nutzern ermöglichen,
sich zu vernetzen und eigene Daten über das Internet zur Verfügung zu stellen.
(Facebook, Twitter, Blogs, YouTube, WhatsApp, etc.)

- 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 Ransomware ?

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

Die Anfänge der Ransomware – Ransomware 1.0

Die erste Generation dieser Art von Software (Ransomware 1.0) blockiert **scheinbar** die Computernutzung bis Geld für die Freischaltung des Computers gezahlt wurde.

Merkmale

- Täter geben sich oft als Behörde aus
- Ihnen wird vorgetäuscht, der Computer sei wegen illegaler Handlungen gesperrt worden
- Es wird eine Lösung durch Bezahlung von Geld angeboten (Paysafe-, Amazon-, iTunes-Guthaben, ..)
- Oft Zeitdruck

Beispiele für klassische Ransomware 1.0

Ransomware 2.0 -
Wie Verschlüsselung zur Bedrohung wurde

Was hat sich geändert ?

- Im Hintergrund werden **alle wichtigen Daten** verschlüsselt und ggf. zusätzlich an die Täter übertragen
- Man braucht nun 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 !

Cyber-Angriff legt Eberspächer lahm

mit Informationen von Peter Sauer 26.10.2021 | 15:04 Uhr

Vorlesen

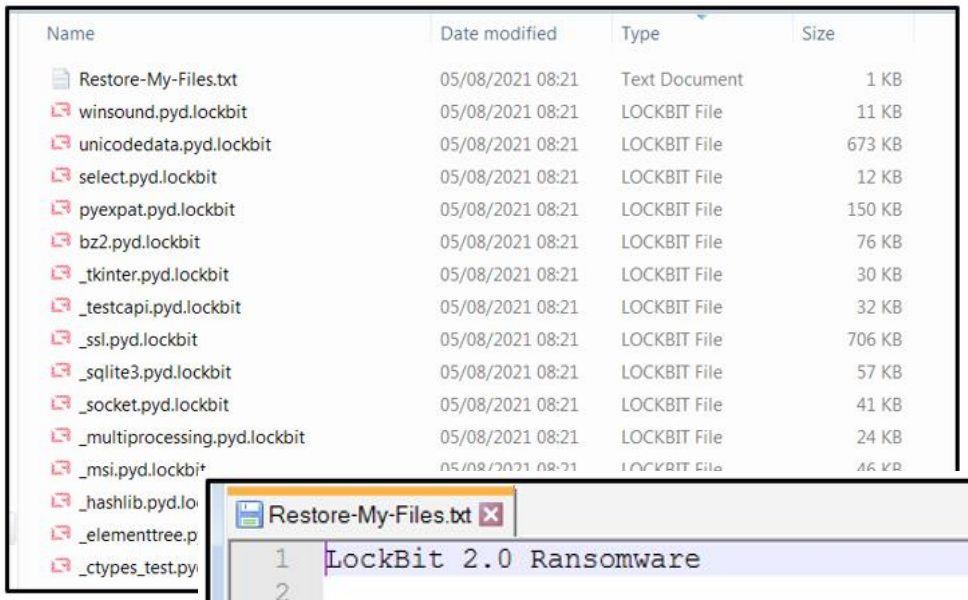
Der Automobil-Zulieferer Eberspächer ist am Sonntag Opfer eines Cyber-Angriffes geworden. Auch das Werk in Neunkirchen ist betroffen und steht seither still. Die Staatsanwaltschaft ermittelt.

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

Beispiel Ransomware 2.0 (LockBit 2.0/3.0)

SAARLAND

Beispiel Ransomware 2.0 (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.lockbi	05/08/2021 08:21	LOCKBIT File	46 KB
_hashlib.pyd.lo			
_elementtree.p			
_ctypes_test.py			

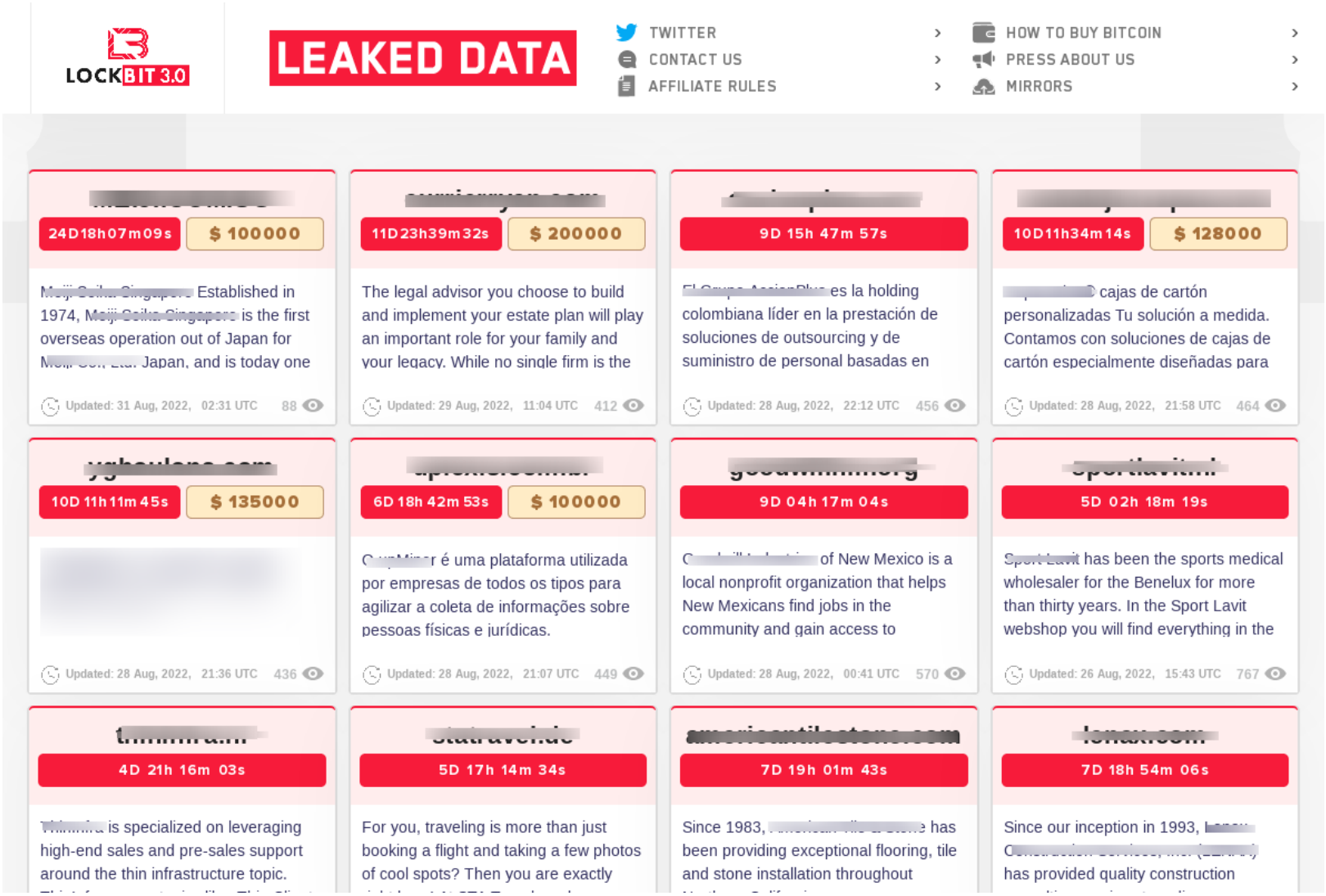
Ransom Note

Restore-My-Files.txt

```
1  LockBit 2.0 Ransomware
2
3  Your data are stolen and encrypted
4  The data will be published on TOR website
   http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion and
   https://bigblog.at if you do not pay the ransom
5  You can contact us and decrypt one file for free on these TOR sites
6  http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid.onion
7  http://lockbitsap2oaghcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion
8  OR
9  https://decoding.at
10
11 Decryption ID: 586A97038216AC6BF076FC47B7F227E3
```


SAARLAND

Beispiel Ransomware 2.0 (LockBit 2.0/3.0)



SAARLAND

Ransomware 2.0 oder wie Verschlüsselung zur Bedrohung wurde

Was kann ich tun?

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

Was ist ein DDoS Angriff?

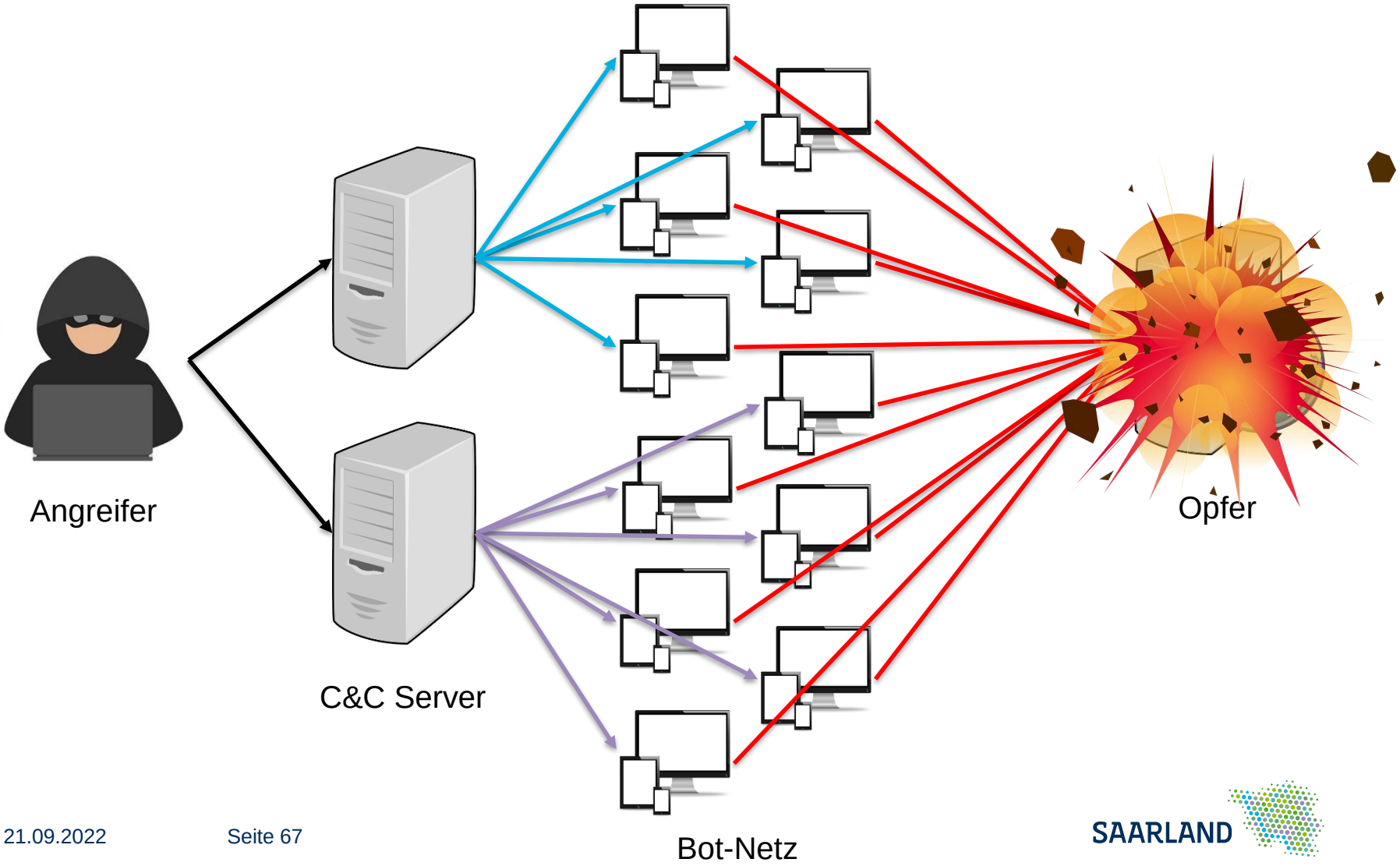
(Distributed Denial of Service)

DDoS-Angriffe…
und wieso **Sie** Teil des Problems sein könnten

Ein DDoS-Angriff (Distributed Denial of Service) ist ein Angriff auf eine Webseite oder Dienst mit dem Ziel, diese oder diesen für eine gewisse Zeit lahm zu legen.

Dazu schießen zehntausende oder hunderttausende Computer Datenpakete gleichzeitig auf das Ziel, welches dann solange den Dienst verweigert, bis der Ansturm aufhört.

DDoS-Angriffe…
und wieso **Sie** Teil des Problems sein könnten



SAARLAND

DDoS-Angriffe…
und wieso **Sie** Teil des Problems sein könnten

Wo ist das Problem?

- Hoher Schaden für Unternehmen, die Geld mit ihrer Webseite verdienen
- Angreifer sind während des Angriffs oft nicht aufspürbar
- Angriffe kommen häufig von **privaten Computern oder Geräten**, die auf der ganzen Welt verteilt sind

DDoS-Angriffe…
und wieso **Sie** Teil des Problems sein könnten

Jedes internetfähiges Gerät kann Teil eines Bot-Netzes durch die Infektion
mit einer Schadsoftware werden. Ein Bot-Netz kann so aus Millionen von Bots bestehen.

Abbildungen beispielhaft

DDoS-Angriffe…
und wieso jeder von uns Teil des Problems ist

Was kann ich tun?

- Keine Standard-Passwörter (z.B. vom Hersteller vergeben) verwenden, sondern immer eigene starke Passwörter vergeben.
- Regelmäßig Updates durchführen.
- Wenn das Gerät nicht gebraucht wird: herunterfahren bzw. ausschalten.
- Keine Software aus unsicheren Quellen installieren.
- Keine Datenträger, die man auf der Straße findet, verwenden.
- Geräte, die nicht mit dem Internet verbunden sein müssen, nicht mit dem Internet verbinden.

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 (Fakeshops)
- Der eBay-Account eines renommierten Händlers wird gehackt

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)

Warenbetrug und Warenkreditbetrug

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: Fakeshop-Finder der Verbraucherzentrale
https://www.verbraucherzentrale.de/fakeshopfinder

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 Warenkontrolleur
- 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

1. Sie **verkaufen ein Auto** im Internet für 10.000€
2. Ein Interessent meldet sich (oft aus dem EU-Ausland)
3. Er will das Auto im Auftrag eines anderen kaufen und überweist Ihnen 10.000€.
4. Er tritt vom Kaufvertrag zurück und schildert eine herzzerreißende Geschichte
5. Sie sollen 9.700 Euro bitte zurücküberweisen – aber auf ein anderes Konto
6. Sie dürfen die 300 Euro Differenz behalten – „für Ihre Unannehmlichkeiten“
7. Einige Tage später fordert ein Ihnen unbekannter Dritter seine 10.000€ zurück

Was ist passiert?

Täter haben die Zugangsdaten zum Bankkonto des Eigentümers der 10.000€ erlangt und Sie als Zwischenstation missbraucht, um Spuren zu verwischen und die Ermittlungen in die Länge zu ziehen und zu erschweren

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…

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/ Aufnehmen von Videos statt, es gibt nur diese eine Spam-E-Mail. Durch Anzeige der **eigenen E-Mailadresse** als Absenderadresse wird Authentizität vorgetäuscht.

Love Scam
Liebe und Triebe…

Romance-/Love Scam

- Kontakt über Single-Börse oder teilweise auch z.B. Kleinanzeigen
-
- 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.

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!

SAARLAND

Tipps für Chats, Foren, Soziale Netzwerke und Handelsplattformen

Wie sollte ich mich grundsätzlich verhalten?

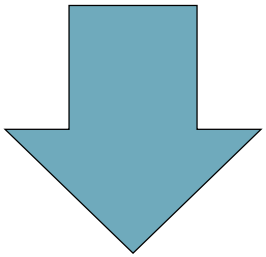
- Seien Sie zurückhaltend mit persönlichen Informationen. Es gibt kein Zurück!
- Überprüfen Sie so viele Informationen wie möglich.
- Lassen Sie sich nicht auf andere, externe Seiten locken.
- **Lassen Sie sich nicht unter Druck setzen!**
- Überweisen Sie kein Geld und schicken sie keine Waren an „neue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

SAARLAND

Wie kann ich mit 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!

Wie kann ich mich schützen?

Generelle Handlungsempfehlungen

- E-Mails, auch von vermeintlich bekannten Absendern, **grundsätzlich misstrauen**. Niemals unbekannte **Datei-Anhänge** oder Rechnungen öffnen.

- Vermeiden sie das Klicken von **Links in E-Mails**. Gehen sie lieber selbst über die Eingabe der Webadresse im Browser auf Webseiten (Amazon, PayPal …).

- Niemals Passwörter, Zugangsdaten, wichtige Personendaten oder Personalausweisscans ungeschützt auf dem Computer speichern (Passwort-Safe, Zettel nutzen)

Wie kann ich mich schützen?

Generelle Handlungsempfehlungen

- **Updates** für Betriebssystem & sonstige Software möglichst zeitnah durchführen.
- **Antiviren-Software** installieren und aktiv und aktuell halten.
- Für verschiedene Dienste (E-Mail, Ebay, PayPal, Amazon, Foren) immer **verschiedene Passwörter** benutzen.

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