POLIZEIPRÄSIDIUM SÜDHESSEN

GEMEINSAM SICHER IN HESSEN

Tatort Internet

„Sicher Surfen ist keine Wissenschaft“

Digitales Erbe

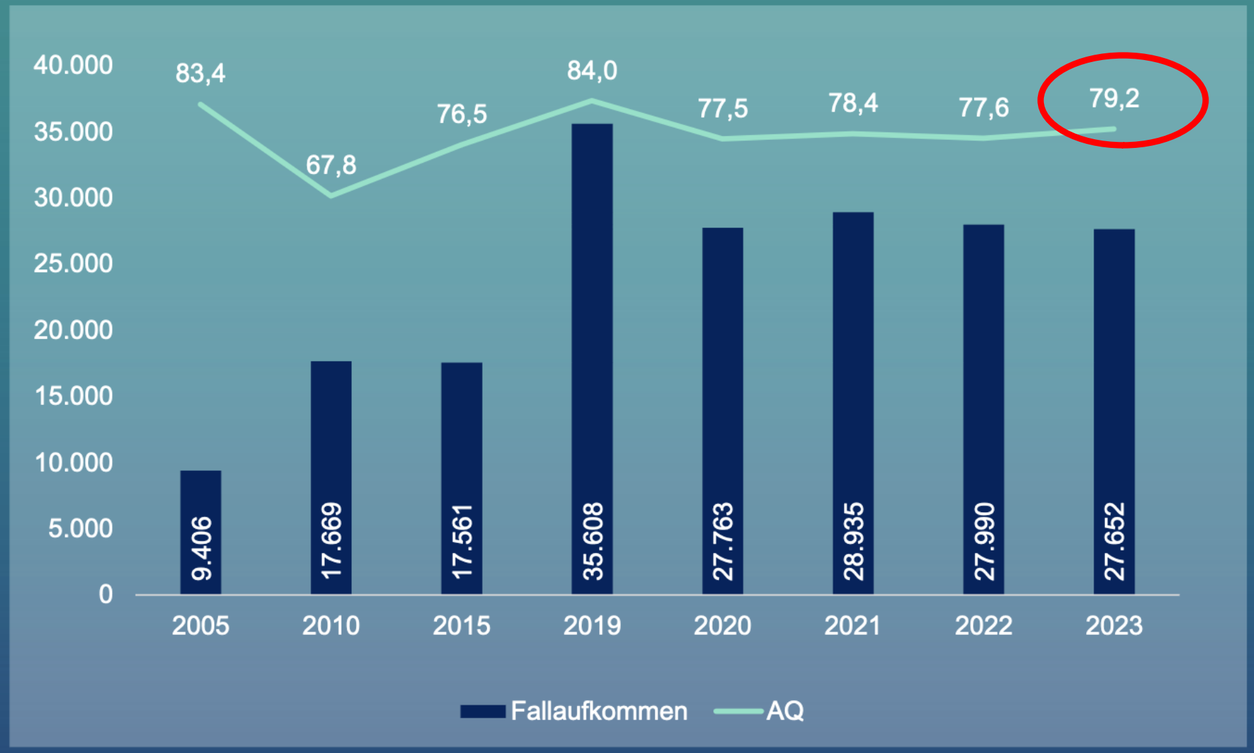
…über unseren digitalen Fußabdruck…

Michael Rühl
Stabsbereich Prävention
Fachberater Cybercrime
cybercrimepraevention.ppsh@polizei.hessen.de

GEMEINSAM SICHER IN HESSEN

Polizeiliche Kriminalstatistik Hessen 2023/24

INTERNETKRIMINALITÄT



- Straftaten mit Tatmittel Internet gesunken
- Einführung sicherer Zahlungsmethoden
- Viele Straftaten im Ausland – keine Erfassung
- Bargeldloses Bezahlen – Tatverdächtige anonym

CYBER-KRIMINALITÄT

Jeder Zehnte in Deutschland von Identitätsdiebstahl betroffen

27. März 2024 • 07:54 Uhr • 2 Min

- Übernahme Facebook Account
- Betrug im Online Handel
- Illegale Finanztransaktionen
- Unberechtigte Nutzung von Bildern und Videos (urheberrechtliche Verstöße)
- Abo-Betrug
- Vertragsabschlüsse mit falscher Identität
- …

POLIZEIPRÄSIDIUM SÜDHESSEN

GEMEINSAM SICHER IN HESSEN

Meist genutzte Schadsoftware und deren Funktionsweisen

Ransomware

Funktion: Veränderung von Dateien des Betriebssystems

1. Infektion durch Platzierung v. Schadprogrammen
2. Veränderung des Betriebssystems
3. Verschlüsselung von Daten
4. „Lösegeldforderung“

Keylogger

Funktion: Aufzeichnung und Übermittlung von Dateneingaben

1. Infektion durch Platzierung v. Schadprogrammen oder Hardware
2. Datenaufzeichnung und Versand
3. Missbrauch von Daten

Remote Access Funktionen

Steuerung von Rechnerhardware

- Botnetzaufbau/(D)DoS-Attacken *

1. Infektion durch Platzierung v. Schadprogrammen
2. Aufbau eines Botnetzes
3. Angriff über Rechnerverbund auf Opferrechner
4. Überlastung der Zielserver mit anschließender „Lösegeldforderung“

* Distributed Denial of Service ((D)DoS) = Dienstverweigerung

POLIZEIPRÄSIDIUM SÜDHESSEN

GEMEINSAM SICHER IN HESSEN

Verbreitung von Schadsoftware

E4 PRÄVENTION

Emailempfang

Emails von seriös erscheinenden Absendern
oder über ausgespähte Accounts

POLIZEIPRÄSIDIUM SÜDHESSEN

GEMEINSAM SICHER IN HESSEN

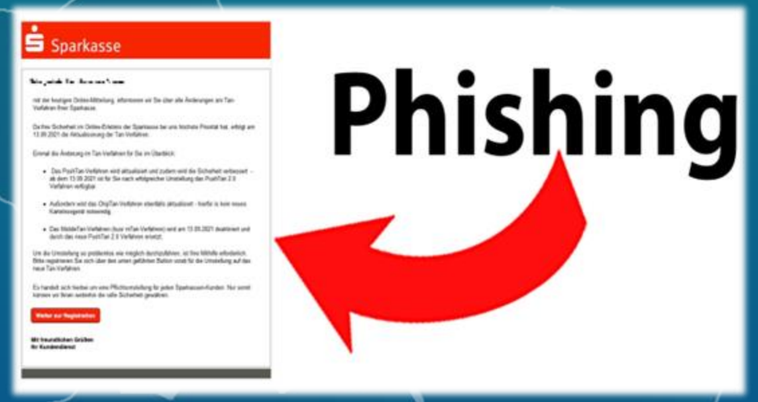
Wo liegen die

Gefahrenquellen ?

…beim Empfang und der Bearbeitung von Emails…

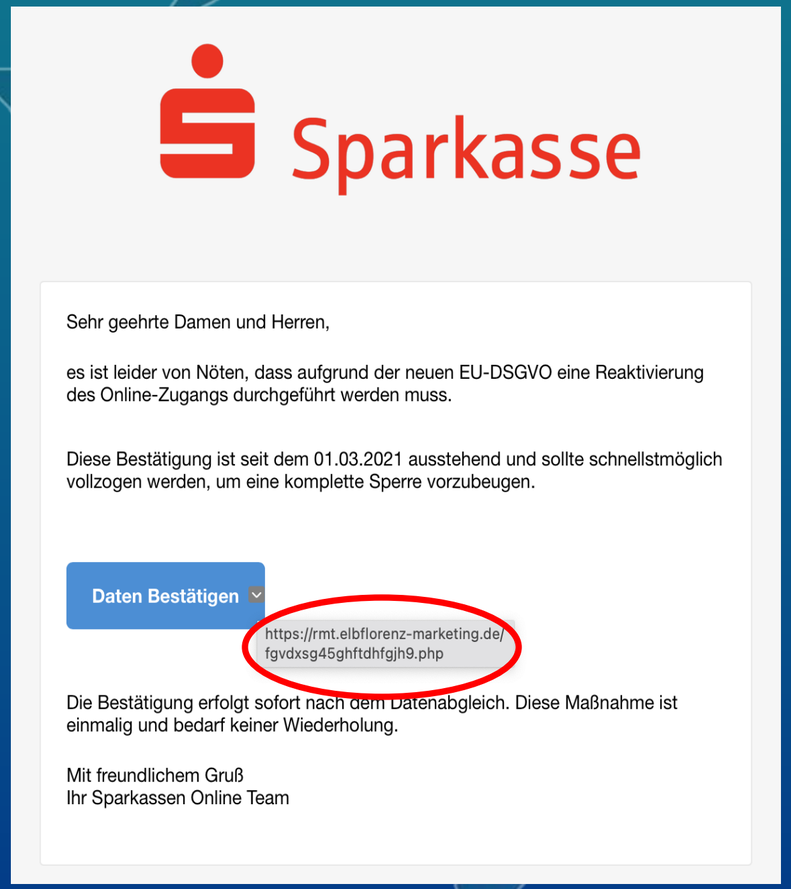
Hyperlinks

Phishing-Attacken



Fallstricke in Hyperlinks

Gefälschte oder falsche „URL“ (domain) erkennen / Phishing



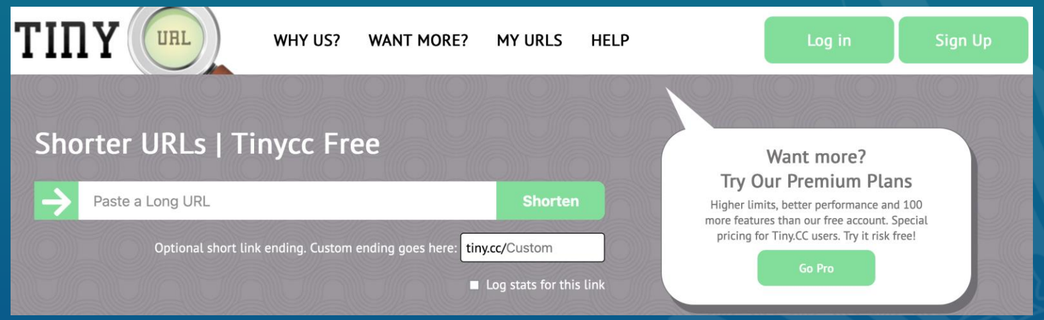
https://rmt.elbflorenz-marketing.de/fgvdxsg45ghftdhfgjh9.php

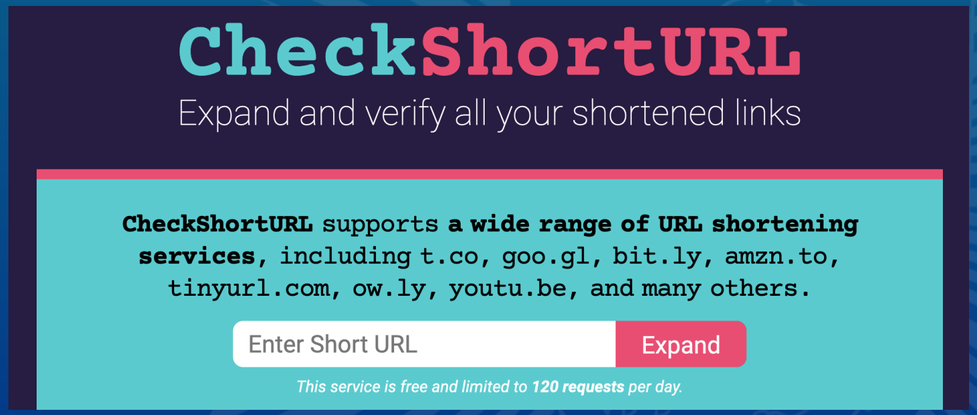
- Der „Wer-Bereich“ einer URL

POLIZEIPRÄSIDIUM SÜDHESSEN

GEMEINSAM SICHER IN HESSEN

TinyURL





E4 PRÄVENTION

GEMEINSAM SICHER IN HESSEN

Anlagen/Anhänge

GEMEINSAM SICHER IN HESSEN

Verschleierung der Identität des Angreifers

Manipulation des „verkürzten“ Emailheaders

Von: Sparkassen-Finanzgruppe <
Datum: 12.09.18 01:31 (GMT+01:00)
An: "
Betreff: Mitteilung zum Kundenkonto

Sparkasse

Sehr geehrte Damen & Herren,

unser Sicherheitssystem hat automatisierte Maßnah
Kundendaten abzublocken. Diese Maßnahmen bein
Kundendaten

Nach Abschluss des Vorgangs befindet sich Ihr Kun
aktuellen Stand der Sicherheitsbedingungen nach §
Bundesdatenschutzgesetzes.

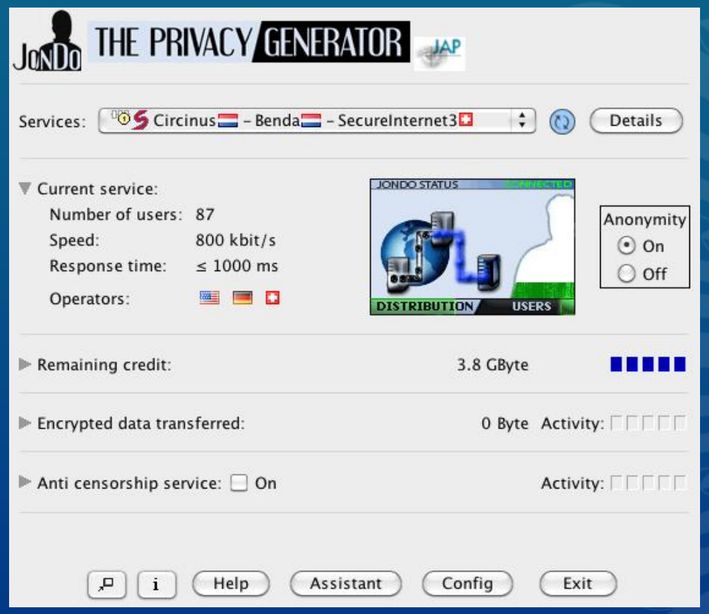
Fortfahren >>

Mit freundlichen Grüßen,
Ihre **Sparkassen-Finanzgruppe**

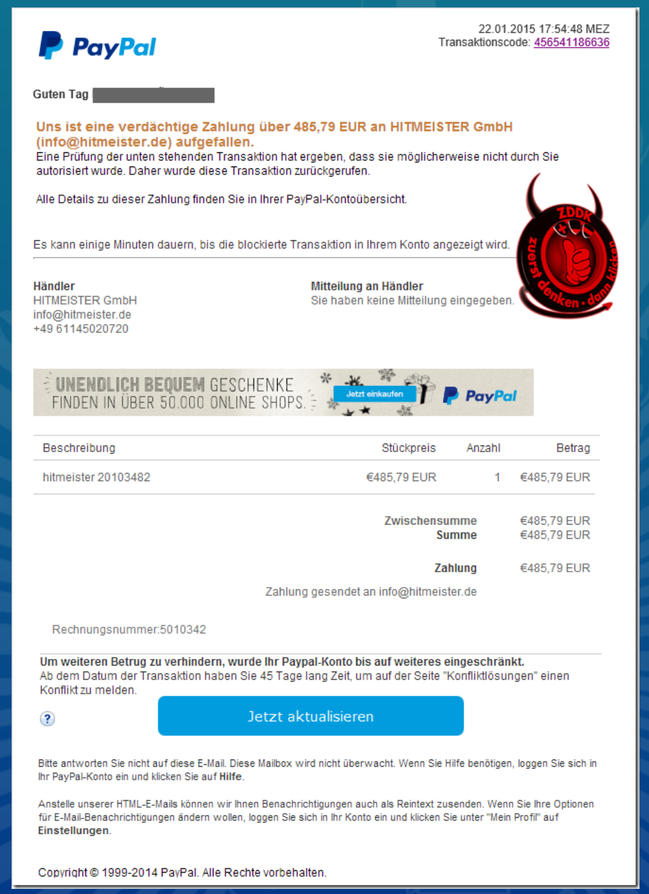
Betrügerische E-Mail

```
Return-Path: <info@caucastours.com>
Delivered-To: 3@2062321
Received: from imap-director-1.dovecot.xion.oxcs.net ([10.10.5.1])
     by imap-backend-45.dovecot.xion.oxcs.net with LMTP
     id GNJpLo/rRWDkAgAATYJhEw
     (envelope-from <info@caucastours.com>)
     for <3@2062321>; Mon, 08 Mar 2021 09:17:03 +0000
Received: from mx020l.vodafonemail.xion.oxcs.net ([10.10.2.20])
     by imap-director-1.dovecot.xion.oxcs.net with LMTP id IHAKLo/rRWAOFgAAKeNfSA
     ; Mon, 08 Mar 2021 09:17:03 +0000
Received: from mx007.vodafonemail.xion.oxcs.net (mta-11.mta.xion.oxcs.net [10.10.2.11])
     (using TLSv1.2 with cipher AECDH-AES256-SHA (256/256 bits))
     (No client certificate requested)
     by mx020l.vodafonemail.xion.oxcs.net (Postfix) with ESMTPS id 4DvCQl5MKyzdZSS
     for <ruehl.darmstadt@arcor.de>; Mon,  8 Mar 2021 09:17:03 +0000 (UTC)
Received: from fra1frontrelay09.vodafonemail.de (unknown [2.207.150.239])
     (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
     (No client certificate requested)
     by vsmx001.vodafonemail.xion.oxcs.net (Postfix) with ESMTPS id 4DvCQl5365zTgGj
     for <ruehl.darmstadt@arcor.de>; Mon,  8 Mar 2021 09:17:03 +0000 (UTC)
Received: from server1.ge (server1.ge [116.202.113.38])
     by fra1frontrelay09.vodafonemail.de (8.15.2/8.15.2/Debian-10) with ESMTPS id 1289H2iM030236
     (version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128 verify=NOT)
     for <ruehl.darmstadt@arcor.de>; Mon, 8 Mar 2021 10:17:03 +0100
Authentication-Results: fra1frontrelay09.vodafonemail.de; dmarc=pass (p=none dis=none) header.from=caucastours.com
Message-Id: <202103080917.1289H2iM030236@fra1frontrelay09.vodafonemail.de>
Received: from turnia.in (unknown [83.171.236.222])
     by server1.ge (Postfix) with ESMTPSA id 043427166157
     for <ruehl.darmstadt@arcor.de>; Mon,  8 Mar 2021 13:17:02 +0400 (+04)
Authentication-Results: server1.ge;
        spf=pass (sender IP is 83.171.236.222) smtp.mailfrom=info@caucastours.com smtp.helo=turnia.in
Received-SPF: pass (server1.ge: connection is authenticated)
From: "Ihre Spk Online" <info@caucastours.com>
Subject: =?utf-8?B?UHLDvGZlbmcgZXJmb3JkZXJsaWNo?=
To: "ruehl.darmstadt" <ruehl.darmstadt@arcor.de>
Content-Type: multipart/alternative; boundary="WOZruiRlT9yNqMFxffXi=_f8l8R2IapE7e"
MIME-Version: 1.0
Date: Mon, 8 Mar 2021 10:17:02 +0100
X-purgate-type: clean
X-purgate-Ad: Categorized by eleven eXpurgate (R) http://www.eleven.de
X-purgate: clean
X-purgate: This mail is considered clean (visit http://www.eleven.de for further information)
X-purgate-size: 13115
X-purgate-ID: 149169::1615195023-0000052B-F87A182A/0/0

This is a multi-part message in MIME format

--WOZruiRlT9yNqMFxffXi=_f8l8R2IapE7e
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline

Ihr Konto: Best=C3=A4tigung Ihrer Daten erforderlich img { max-width: =
100%; } body { -webkit-font-smoothing: antialiased; -webkit-text-size-=
adjust: none; width: 100% !important; height: 100%; line-height: 1.6em=
; } body { background-color: #f6f6f6; } @media only screen and (max-wi=
dth: 640px) { body { padding: 0 !important; } h1 { font-weight: 800 !i=
mportant; margin: 20px 0 5px !important; } h2 { font-weight: 800 !impo=
rtant; margin: 20px 0 5px !important; } h3 { font-weight: 800 !importa=
nt; margin: 20px 0 5px !important; } h4 { font-weight: 800 !important;=
 margin: 20px 0 5px !important; } h1 { font-size: 22px !important; } h=
2 { font-size: 18px !important; } h3 { font-size: 16px !important; } .=
container { padding: 0 !important; width: 100% !important; } .content =
{ padding: 0 !important; } .content-wrap { padding: 10px !important; }=
 .invoice { width: 100% !important; } }  =20
```

Nutzung von Proxyservern



Hyperlinks



Ermittlungsansätze – Beispiel erw. Emailheader

Tim Gabel – Amazn Eingang...r.de (Arcor) 9. März 2024 um 15:51
Michael || Sondermeldung für Sie – Vorgang Nr. #1709995916 / ruehl.darmstadt@arcor.de /
An: Michael Rühl

Guten Tag Michael Rhl,

Fantastische Nachrichten!: Ein unerwartetes Geschenk ist fast bei Ihnen.

Unser Team hat vor einigen Tagen den Kontakt zu Ihnen gesucht (per E-Mail und Telefon) – leider ohne Rückmeldung. Aber keine Sorge, wir sind hier, um zu helfen, indem wir Ihnen einen neuen Zugang zu unserem Kundenportal bieten, damit Sie nichts verpassen.

@ruehl.darmstadt@arcor.de, öffnen Sie bitte Ihren exklusiven Link hier

Wir möchten diese Gelegenheit nicht verstreichen lassen, ohne Ihnen für Ihre Treue zu Amazon zu danken. Wir schätzen Ihr Engagement sehr und blicken erwartungsvoll Ihrer Rückmeldung entgegen.

Viele Grüße,

Tim Gabel – Amazn – Ihr persönlicher Amazon-Berater

🌟 *Anhang: Ihre Erinnerung an unser letztes Gespräch für eine nahtlose Kommunikation.*

Hallo Michael Rhl,

Seit Beginn der Woche liegt ein wichtiger Punkt bezüglich Ihres Amazon-Kontos (ruehl.darmstadt@arcor.de) vor, den wir gerne abschließen möchten. Durch Ihre Teilnahme an unseren Aktionen wurden Sie automatisch in unser neuestes Kontest aufgenommen, und die Gewinner stehen fest – nur Ihre Bestätigung fehlt noch!

Zögern Sie nicht, Ihren Preis zu beanspruchen

Ohne eine Bestätigung bis zum (09.03.2024) wird eine Datenlöschung unumgänglich. Eine nachträgliche Geltendmachung des Gewinns ist somit ausgeschlossen.

Tim Gabel – Amazn Eingang...or.de (Arcor) 9. März 2024 um 15:51
Michael || Sondermeldung für Sie – Vorgang Nr. #1709995916 / ruehl.darmstadt@arcor.de /
An: Michael Rühl

Content-Type: multipart/mixed;
boundary="b1_sAWywqnOPTCzUvbJChJSBrpboxXeSshUjSGzVJmq6v0"
Mime-Version: 1.0
Authentication-Results: mx5.vodafonemail.de/4TsQww2vzqzJqyp; dkim=pass (2048-bit key; unprotected) header.d=rewardyouget.com header.i=@rewardyouget.com header.a=rsa-sha256 header.s=key header.b=cm2UvjUX; dkim-atps=neutral
X-Purgate-Type: clean
Dkim-Signature: a=rsa-sha256; bh=oPcpDQmzGKRVQI8yxHp8tU7IVAabw5ne6MAtZjDu+Iw=; c=relaxed/relaxed; d=rewardyouget.com; h=MIME-Version:Message-ID:From:To:Subject:Date; s=key; t=1709995920; v=1; b=cm2UvjUXIjuSLpAQXTevrOjXPclhWtCZLYuOpNKo1++uyp/yAfypRccXVA/0n1Heo6ox03F6
ROcPc9pN2E3sGhnA0A2BKUjewNjC9mkTbQlCjpXjShS4jn+UksKVfr///x1dZbMPxgBx60ZR5+rDPhLyyOw6YoPm8KdJu1ElOKByxCnVZy6SlOZG0vAu6pkBrK3Y/yU2c74dAoAYEmbvoEsaCCNf4y1GU0gEPh++B2AOuC0Fyr8CjVOh9JGK+JegAi7Mbk1Grkj4CS5npTwSdiz9xfM7ONk6PFaBuy/HdUi4elNslcFK7bGdF3/diHtrKiaI86FfwCBZZLgFtC1fuw==
X-Priority: 3
Return-Path: <doh-m@rewardyouget.com>
X-Mailer: nlserver, Build 6.7.0
X-Purgate-Size: 47841
X-Purgate-Ad: Categorized by eleven eXpurgate (R) http://www.eleven.de
Received: from RelayQueue03 (mailbackend03 [10.6.0.92]) by mailbackend03 with SMTP (envelope-from <doh-m@rewardyouget.com>); Sat, 09 Mar 2024 15:52:08 +0100
Received: from ql0y.rewardyouget.com (ql0y.rewardyouget.com [37.59.78.203]) (using TLSv1.3 with cipher TLS_AES_128_GCM_SHA256 (128/128 bits) key-exchange X25519 server-signature RSA-PSS (2048 bits) server-digest SHA256) (No client certificate requested) by mx5.vodafonemail.de (Postfix) with ESMTPS id 4TsQww2vzqzJqyp for <ruehl.darmstadt@arcor.de>; Sat, 9 Mar 2024 14:51:57 +0000 (UTC)
<sAWywqnOPTCzUvbJChJSBrpboxXeSshUjSGzVJmq6v0@rewardyouget.com>
X-Purgate: This mail is considered clean (visit http://www.eleven.de for further information)
X-Purgate: clean
X-Purgate-Id: 149169::1709995920-E67FB11D-98318B25/0/0

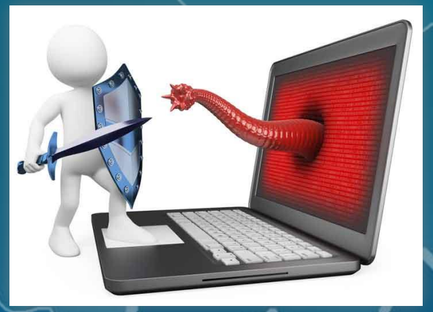
POLIZEIPRÄSIDIUM SÜDHESSEN

GEMEINSAM SICHER IN HESSEN

„Klick- und Surfverhalten“

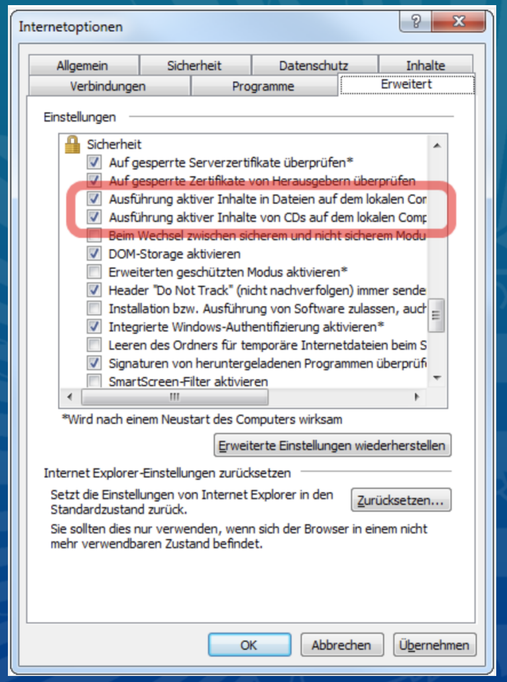
Eigenständige Fortbildung

Prof. Virenschutz
(Systemadministrator)

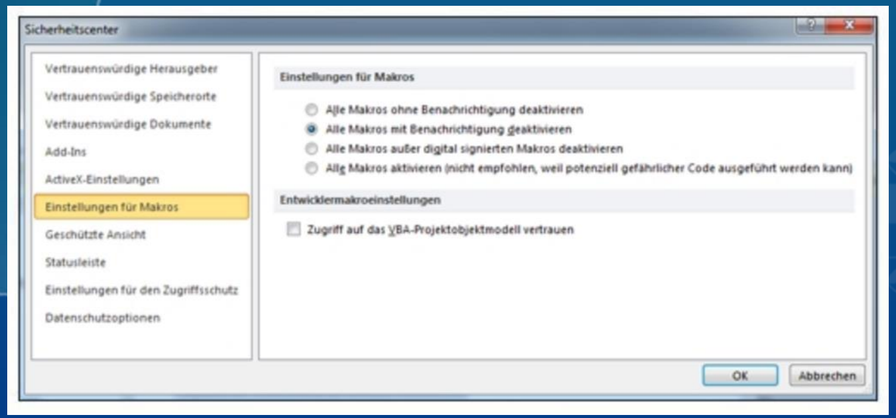


Updates der meist genutzten Programme
(Systemadministrator)

Aktive Inhalte / Macros limitieren oder inaktiv schalten
(Systemadministrator)



Angepasste, regelmäßige
BackUp/Serversicherung
(Systemadministrator)

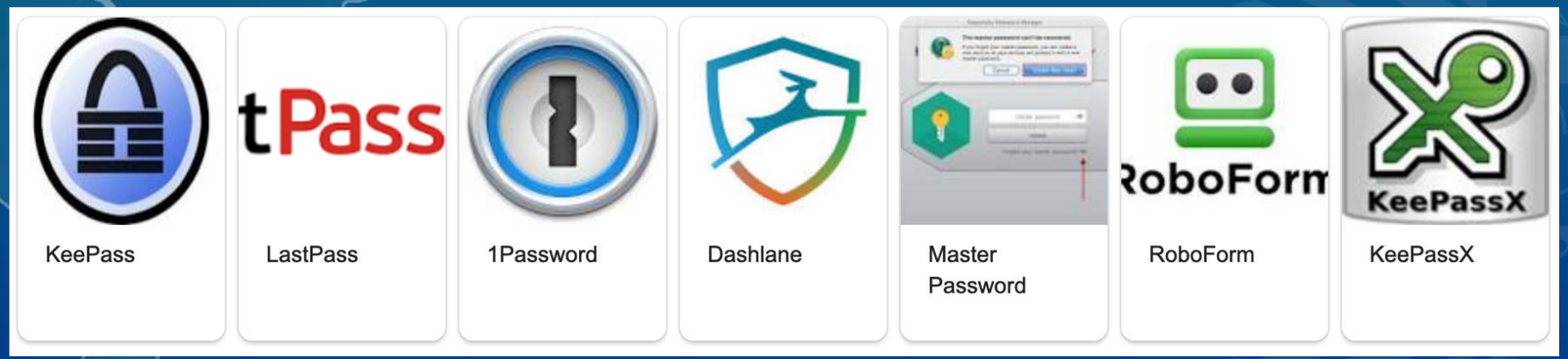


GEMEINSAM SICHER IN HESSEN

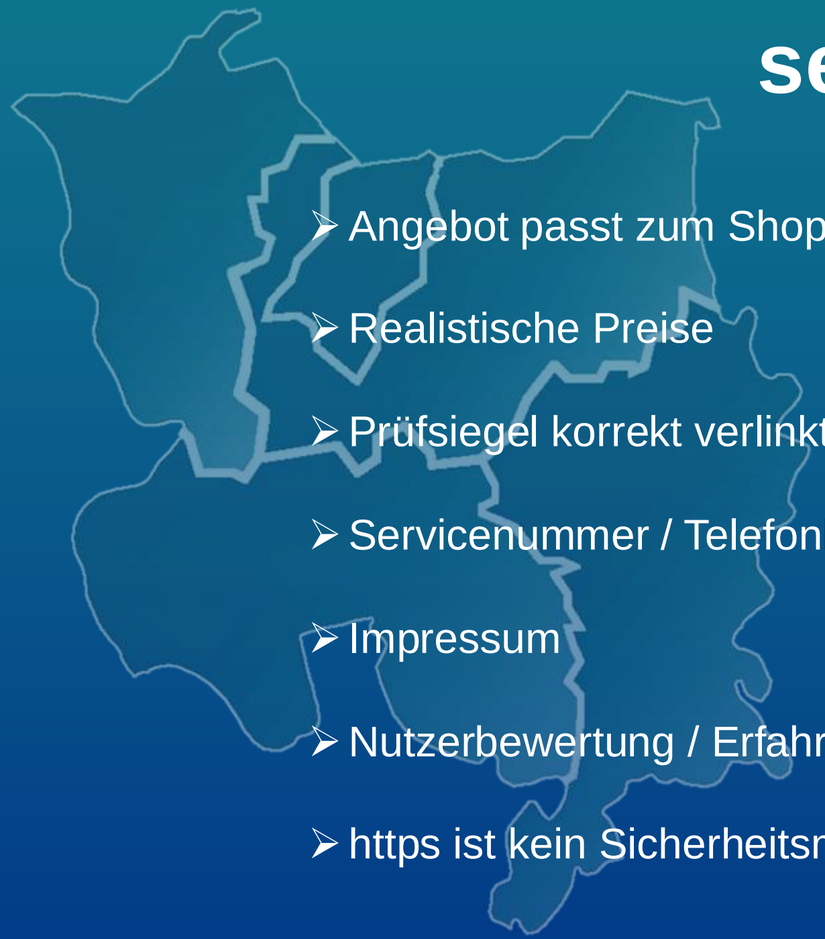
Passwortsicherheit

Sichere Passwörter

- 4 Merkmale
- So lang als möglich
- Regelmäßig wechseln
- 2 Faktoren Authentisierung



Merkmale seriöser Onlineshops



- Angebot passt zum Shop
- Realistische Preise
- Prüfsiegel korrekt verlinkt
- Servicenummer / Telefonkontakt
- Impressum
- Nutzerbewertung / Erfahrungen im Netz
- https ist kein Sicherheitsmerkmal

POLIZEIPRÄSIDIUM SÜDHESSEN

GEMEINSAM SICHER IN HESSEN

Onlinebanking

SMS TAN / Push TAN

TAN Generator

HBCI (Homebanking Computer Interface)

- Zertifizierte Bankingsoftware
- 2-Faktoren Authentifizierung
- Überweisungslimite setzen

Banking

POLIZEIPRÄSIDIUM SÜDHESSEN

GEMEINSAM SICHER IN HESSEN

Aktuelles

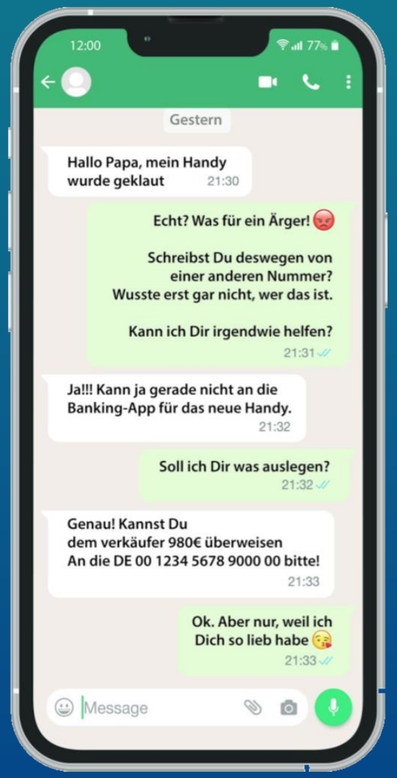
POLIZEIPRÄSIDIUM SÜDHESSEN

GEMEINSAM SICHER IN HESSEN

- Personen, die sie auf virtuellen Plattformen kennenlernen, sind nicht immer die, die sie vorgeben zu sein.
- Seien Sie misstrauisch, wenn ungewöhnlich hohe Gewinne versprochen werden.
- Schließen Sie Investments nur bei Banken oder Sparkassen ab, bei denen eine europäische Einlagensicherung besteht.
- Spekulationen mit Kryptowährungen unterliegen generell sehr großen Risiken.
- Die Durchsetzung zivilrechtlicher Forderungen gegenüber ausländischen Vertragspartnern ist sehr schwer bis unmöglich.
- Achten Sie bei Internetangeboten auf ein nachvollziehbares Impressum.
- Seien Sie vorsichtig bei der Herausgabe persönlicher Daten.
- Die Verbraucherzentrale bietet zu diesen und anderen Themen Beratungsangebote an.

GEMEINSAM SICHER IN HESSEN

Aktuelles



Michael Rühl
Stabsbereich Prävention
Fachberater Cybercrime
cybercrimepraevention.ppsh@polizei.hessen.de

POLIZEIPRÄSIDIUM SÜDHESSEN

GEMEINSAM SICHER IN HESSEN

Digitales Erbe

Was passiert mit unseren Daten nach dem Tod?

Deutschlandfunk v. 07.10.2020

https://www.deutschlandfunkkultur.de/digitales-erbe-nachlassverwaltung-per-app-100.html

GEMEINSAM SICHER IN HESSEN

Was versteht man unter dem „Digitalen Erbe“

Das digitale Erbe umfasst alle digitalen Spuren und Informationen, die eine Person hinterlässt, wie z.B. in E-Mail-, Social Media-, Onlinebanking/Onlinebroker Konten, Webshops…u.v.m.

Wer ist betroffen?

Jeder, der im Internet aktiv ist und dort persönliche Daten hinterlässt.

POLIZEIPRÄSIDIUM SÜDHESSEN

GEMEINSAM SICHER IN HESSEN

Bilder, Videos, Informationen

Social Media

- Name, Vorname
- Emailadresse
- Telefonnummer
- Persönl. Kontakte
- Adressbuch
- Fotos, Videos
- Persönl. Statements

GEMEINSAM SICHER IN HESSEN

Berufliche Netzwerke/Kontaktbörsen

XING

LinkedIn

- Name, Vorname
- Emailadresse
- Telefonnummer
- Berufl. Informationen
- Netzwerkadressen

ElitePartner
Akademiker & Singles mit Niveau

Parship

Abonements

- Name, Vorname
- Emailadresse
- Telefonnummer
- Adresse
- Kontoverbindungen
- Daten zur Zwei-faktorenauthentifizierung

Onlinebanking/Onlinebroker

“Digitales Vermögen“

Aktien, Wertpapiere, digitale Währungen

- Name, Vorname
- Emailadresse (2.Alt.)
- Telefonnummer
- Wohnanschrift
- Kontoverbindungen
- Daten zur Zwei-faktorenauthentifizierung

Onlineshopping

- Name, Vorname
- Emailadresse
- Telefonnummer
- Wohnanschrift
- Kontoverbindungen
- Daten zur Zwei-faktorenauthentifizierung

POLIZEIPRÄSIDIUM SÜDHESSEN

GEMEINSAM SICHER IN HESSEN

verbraucherzentrale

Beratung Bildung Politik Shop Marktbeobachtung
Beschwerde einreichen

Menü

Digitale Vorsorge, digitaler Nachlass: Was passiert mit meinen Daten?

Stand: 06.02.2025

Vorbeugen mit einer Vollmacht: Sie regelt was passiert, wenn Sie durch Krankheit oder Tod Ihre Online-Accounts nicht mehr verwalten können.

Teilen

verbraucherzentrale

Muster-Vollmacht für den digitalen Nachlass

Ich, [*Vor- und Zuname*], geboren am [*Geburtsdatum*] in [*Geburtsort*], wohnhaft in [*Anschrift mit Straße, Hausnr., PLZ und Ort*]

erteile hiermit eine Vollmacht für meinen digitalen Nachlass an:

Herrn/Frau [*Vor- und Zuname*] - nachfolgend Vertrauensperson genannt - geboren am [*Geburtsdatum*] in [*Geburtsort*], wohnhaft in [*Anschrift mit Straße, Hausnr., PLZ und Ort*]

Meine Vertrauensperson wird bevollmächtigt, meinen digitalen Nachlass so zu regeln, wie ich es in der hinterlegten Liste meiner Accounts festgelegt habe. Die Vertrauensperson kennt den Aufbewahrungsort dieser Liste. Diese Vollmacht ist nur wirksam, wenn die Vertrauensperson das Original dieser Vollmachtsurkunde besitzt und sie auf Verlangen vorlegen kann. Diese Vollmacht gilt über meinen Tod hinaus.

_____ _____

Ort, Datum Unterschrift

Michael Rühl
Stabsbereich Prävention
Fachberater Cybercrime
cybercrimepraevention.ppsh@polizei.hessen.de

POLIZEIPRÄSIDIUM SÜDHESSEN

GEMEINSAM SICHER IN HESSEN

Vielen Dank

Michael Rühl
Stabsbereich Prävention
Fachberater Cybercrime
cybercrimepraevention.ppsh@polizei.hessen.de