Cybersicherheit für Privatpersonen

23. Januar 2025

Christian Weber

www.cyber-notfall-hilfe.de, Tel: 0160 970 30 893

Einkaufen

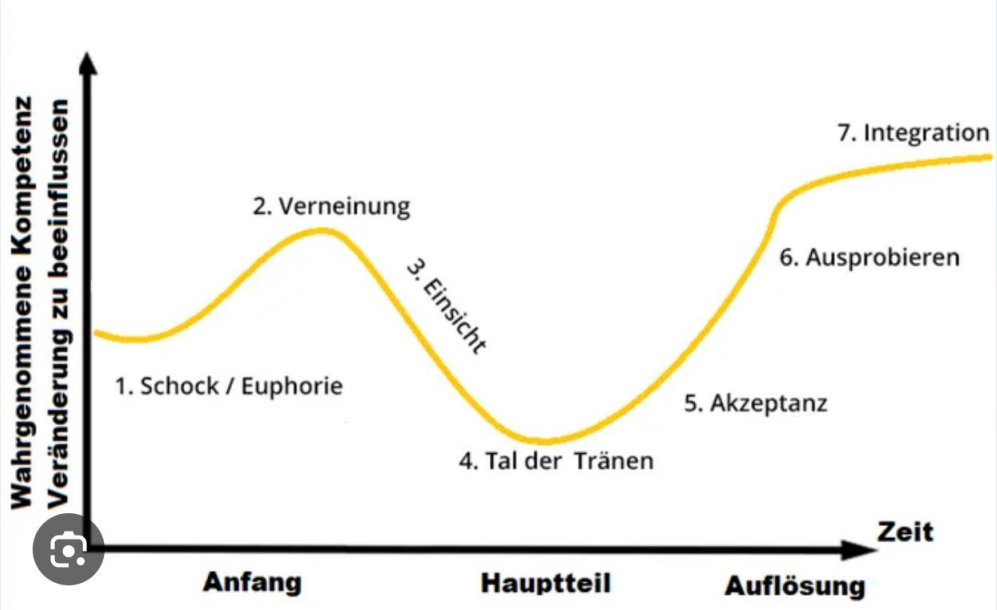
Self-Check-Out:
Der Kunde ist sein eigener Kassierer

Airport

Self-Check-In:
Alles in Eigenverantwortung

Parkplatzsystem

Schock + Ablehnung



www.cyber-notfall-hilfe.de

Online Banking

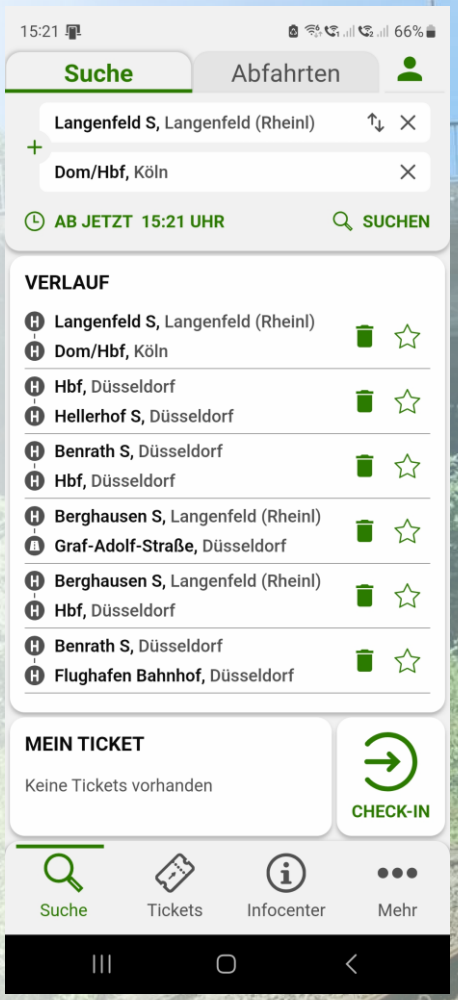
84% der Kunden nutzen Online Banking

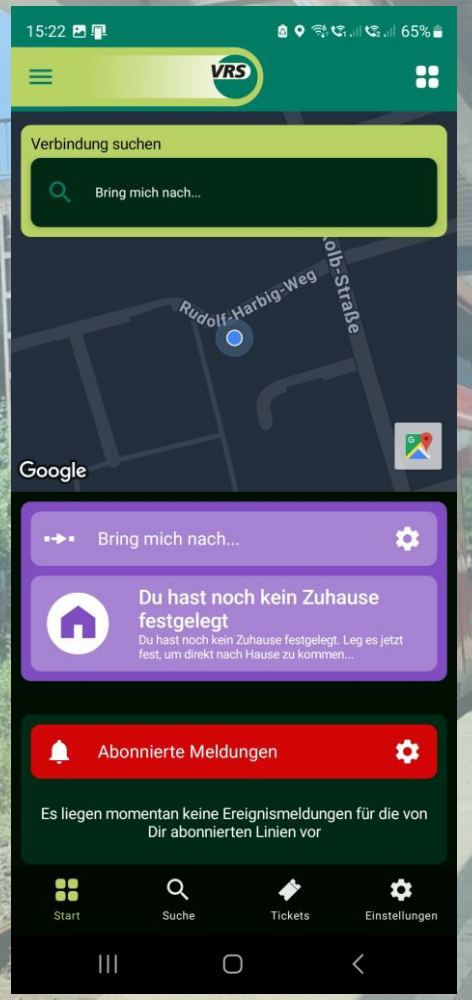
Reduzierung von Filialen!

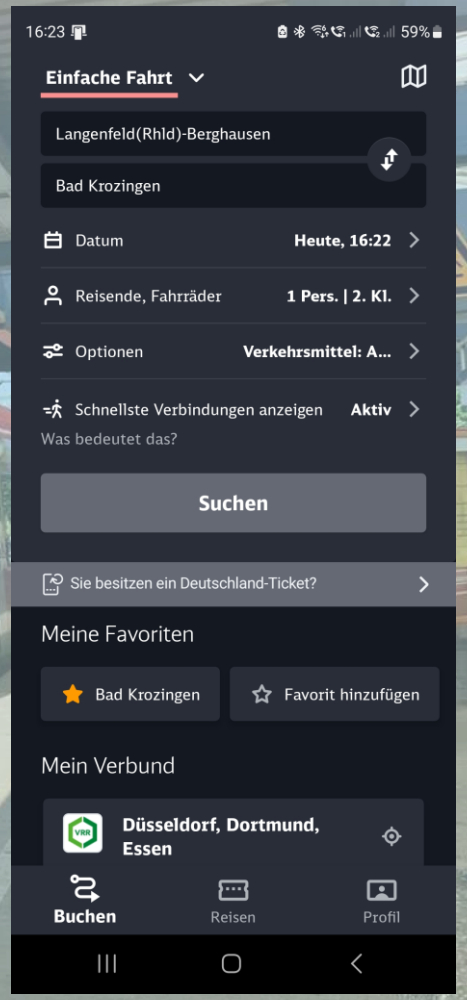
Bahn

Fahrpläne und Ticket

Mobilität alles in der App

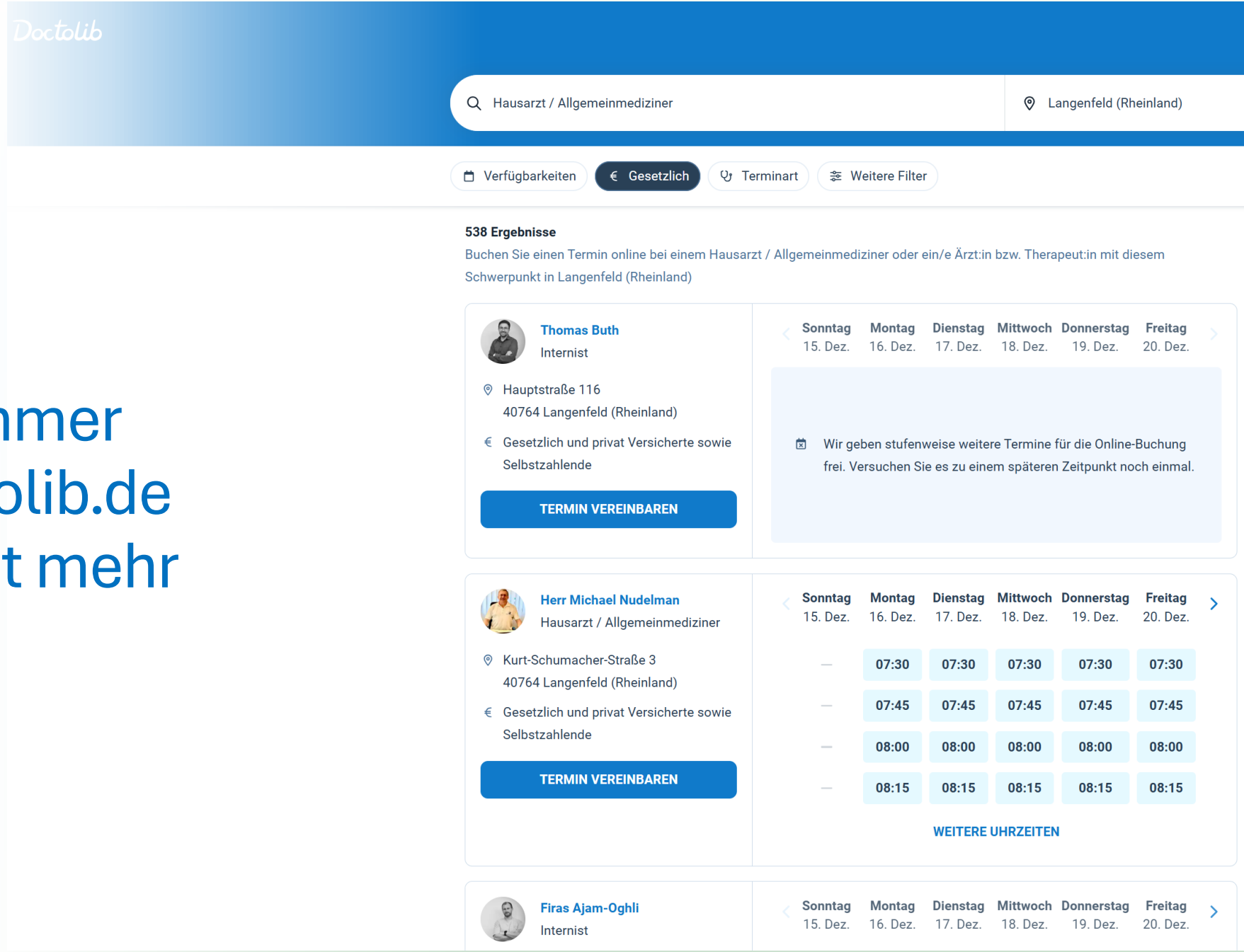






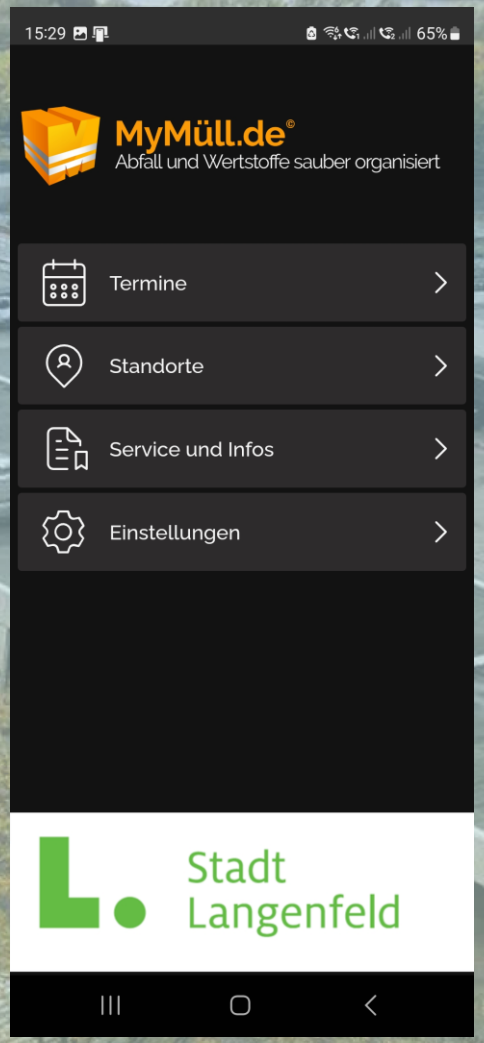
Arzttermine

Termine werden immer häufiger über doctolib.de reserviert und nicht mehr persönlich



Langenfelder Müllkalender

Weg vom Papier, hin zur App

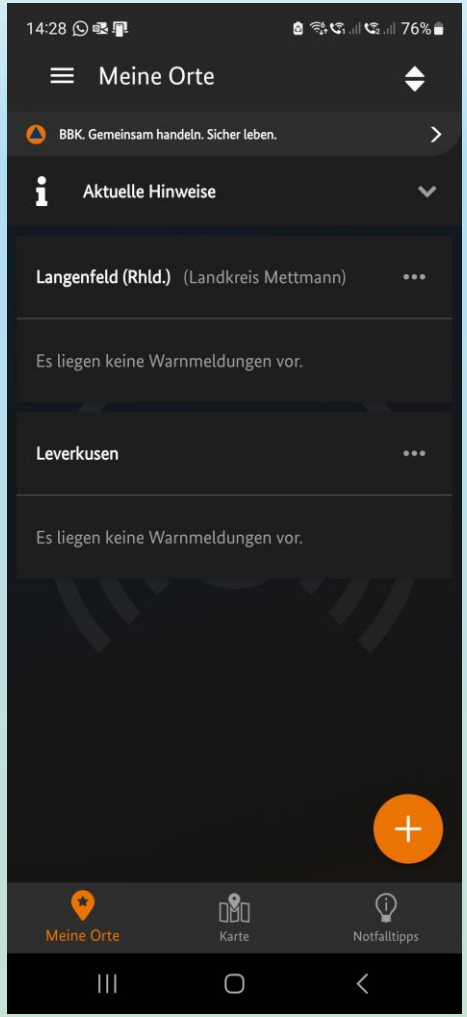


www.cyber-notfall-hilfe.de

Notfall Information

NINA

Die Warn-App NINA dient, der Bevölkerung wichtige bzw. dringende Warnmeldungen zukommen zu lassen.



www.cyber-notfall-hilfe.de

Notfall Information

Mit nora können Notrufe abgesetzt werden können. Sie ermöglicht insbesondere Menschen mit Sprach- und Hörbehinderung Notrufe abzusetzen

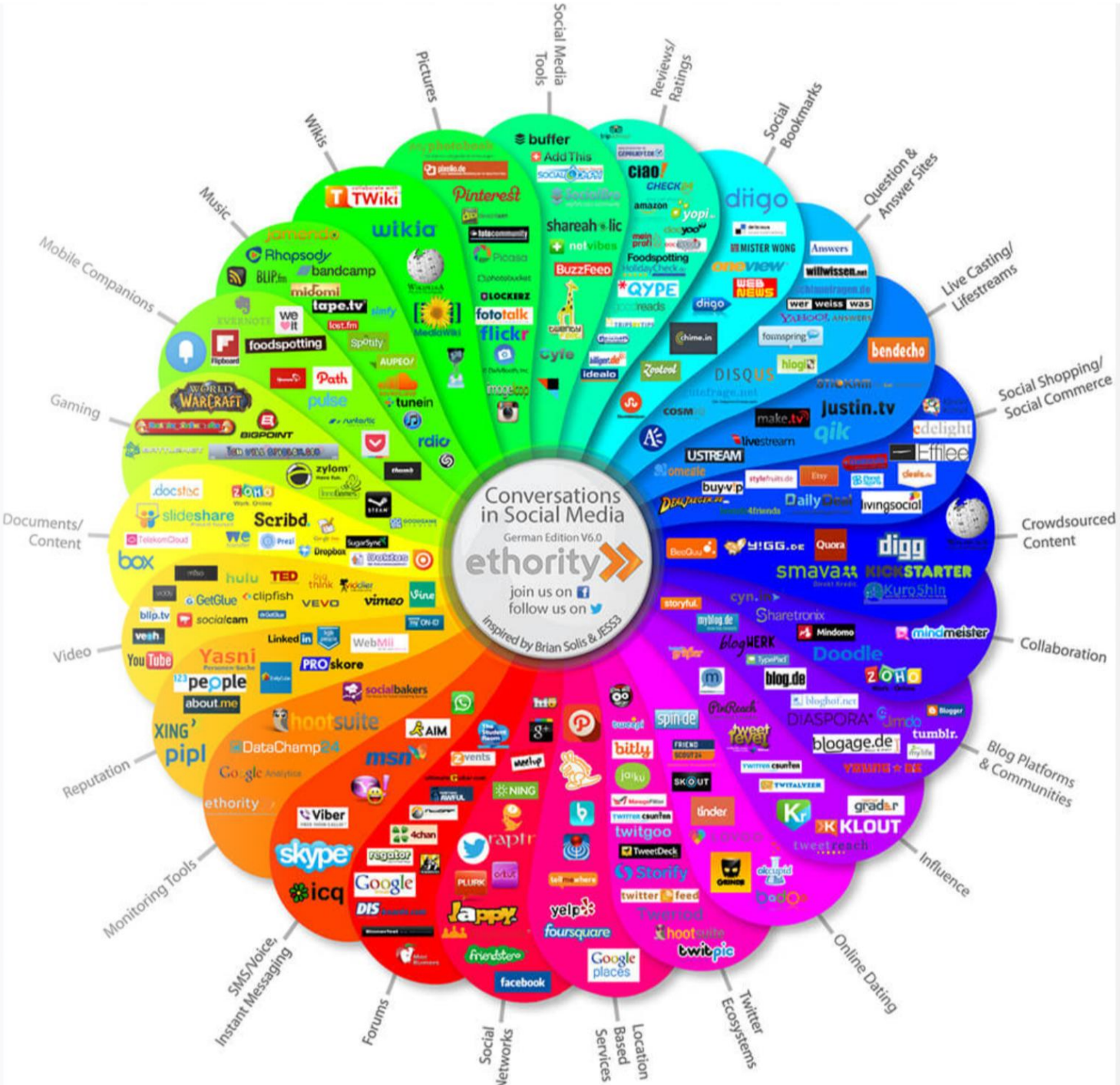
Versicherungen

Alle Dokumente in der App:

- Vertragsunterlagen
- Schadensmeldung
- Formulare

Apps

Weltweit genutzten Apps



zurückrufen.

Die nächsten Videos

Russische Hacker: Greifen Firefox-User an

Achtung Betrug: Mit Notruf 116 116

Vorsicht, Falle: Amazon verschenkt keine Notebooks

BSI: Warnt vor aktueller Lage im Internet

Spam-Anrufe: Vorsicht bei diesem Anruf aus den Niederlanden

PayPal: Betrüger versenden gefährliche Phishing-Mails

Niemand, ob jung oder alt, sollte sorglos im Internet unterwegs sein.
Cyberkriminelle finden immer wieder neue Wege, um an Daten oder Geld von Nutzerinnen und Nutzer zu gelangen.

Der Betrüger braucht Deine Zugangsdaten (Benutzername, Passwort, PINs) oder deine Hilfe!

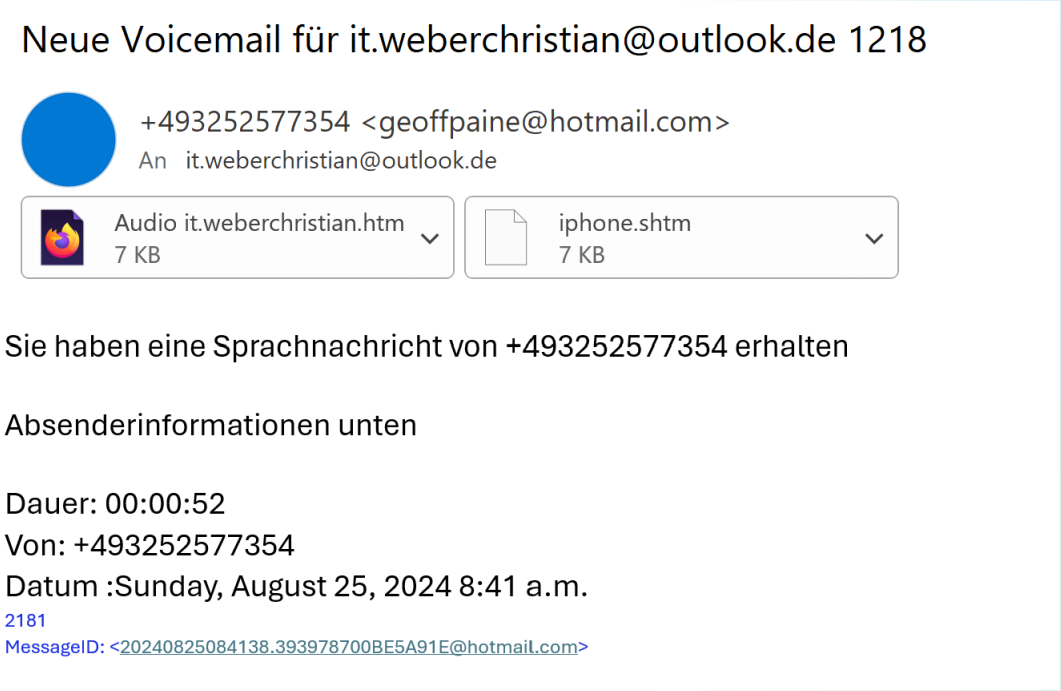
Das wollen wir verhindern!

Die wichtigsten Angriffsmethoden

Phishing	Phishing ist eine betrügerische Methode, bei der Angreifer versuchen, durch gefälschte E-Mails oder Websites persönliche und sensible Informationen wie Passwörter oder Kreditkartendaten zu stehlen.
Social Engineering	Versuch, Menschen dazu zu bringen, sensible Informationen preiszugeben oder bestimmte Handlungen auszuführen, indem man ihre Vertrauenswürdigkeit oder ihr Unwissenheit ausnutzt (z.B. Enkel-Trick).
Identitätsdiebstahl	Identitätsdiebstahl ist der unbefugte Gebrauch der persönlichen Daten (Name, Wohnort, Geburtsdatum, Bankdaten…) einer anderen Person, um sich als diese auszugeben und oft betrügerische Handlungen durchzuführen.
Mailware	Malware ist schädliche Software, die entwickelt wurde, um Computer zu infizieren, zu beschädigen oder unbefugt darauf zuzugreifen.
Ransomeware	Ransomware ist eine Art von Schadsoftware, die den Zugriff auf Daten oder Systeme blockiert und ein Lösegeld fordert, um den Zugriff wiederherzustellen.

Cybersicherheit

Phishing



Neue Voicemail für it.weberchristian@outlook.de 1218

+493252577354 <geoffpaine@hotmail.com>
An it.weberchristian@outlook.de

Audio it.weberchristian.htm
7 KB

iphone.shtm
7 KB

Sie haben eine Sprachnachricht von +493252577354 erhalten

Absenderinformationen unten

Dauer: 00:00:52
Von: +493252577354
Datum :Sunday, August 25, 2024 8:41 a.m.
2181
MessageID: <20240825084138.393978700BE5A91E@hotmail.com>

Erkennungsmerkmale:

- **Unbekannte Telefonnummer**
- **Mailadresse (… @hotmail) unbekannt**
- **Anhang fordert Passwort**

Cybersicherheit

Phishing

Rückrufbitte vom 14.08.2024

LS

Liam Schuh <buero@vonderlee.com>
An it.weberchristian@outlook.de

Links und sonstige Funktionen wurden in dieser Nachricht deaktiviert. Verschieben Sie die Nachricht in den Posteingang, um diese Funktionen zu aktivieren.
Diese Nachricht wurde in das Nur-Text-Format konvertiert.

Guten Tag,

ich konnte Sie heute Vormittag nicht erreichen, nun bin ich selbst außer Haus.

Könnten Sie mich bitte morgen (Donnerstag) zurückrufen?

Vielen Dank im Voraus,

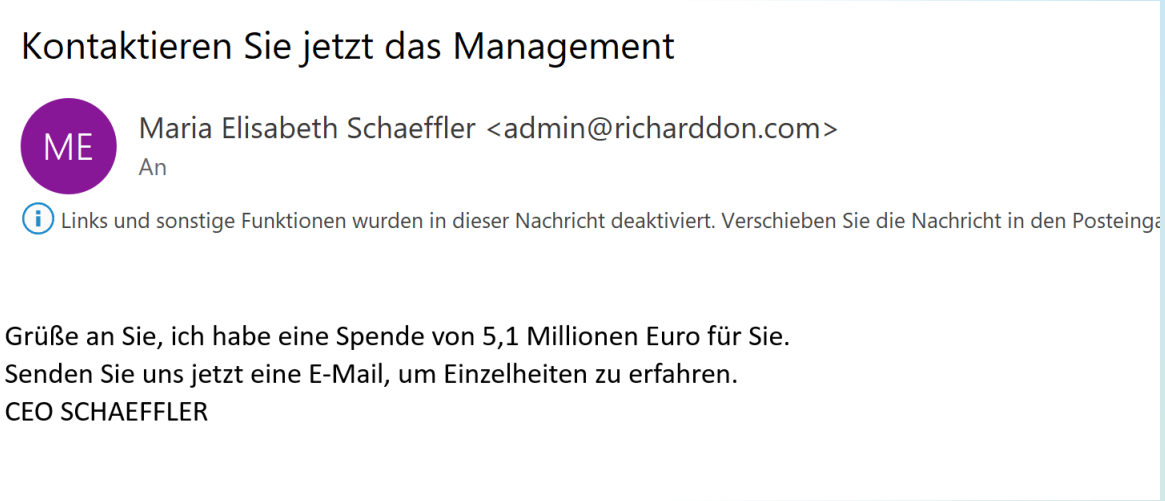
Liam Schuh
<https://www.vonderlee.com/ostat.php?link=568_02_04_58D_DE8F-4A9-01-03CF74213DE9B3C59028F3E3720F2FF6-8328E862A778EA9111>

Erkennungsmerkmale:

- **Unbekanter Absender**
- **Kein Grund für Rückruf genannt**
- **Ich hatte keinen Anruf erhalten**

Cybersicherheit

Phishing



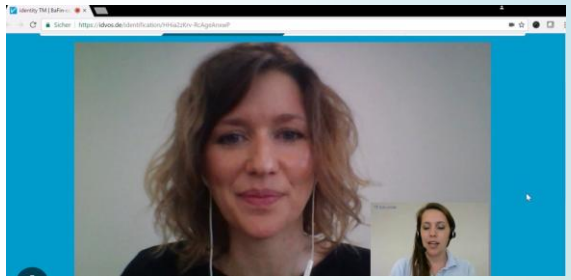
Erkennungsmerkmale:

- **Ködern mit Geldgeschenk (unrealistisch)**

Cybersicherheit

Identitätsdiebstahl – Beispiel 2

Bankkonto: Der Ausweis kann bei einem „nachlässigen“ Bank Mitarbeiter im Video ID Verfahren zur Eröffnung eines Kontos missbraucht werden.

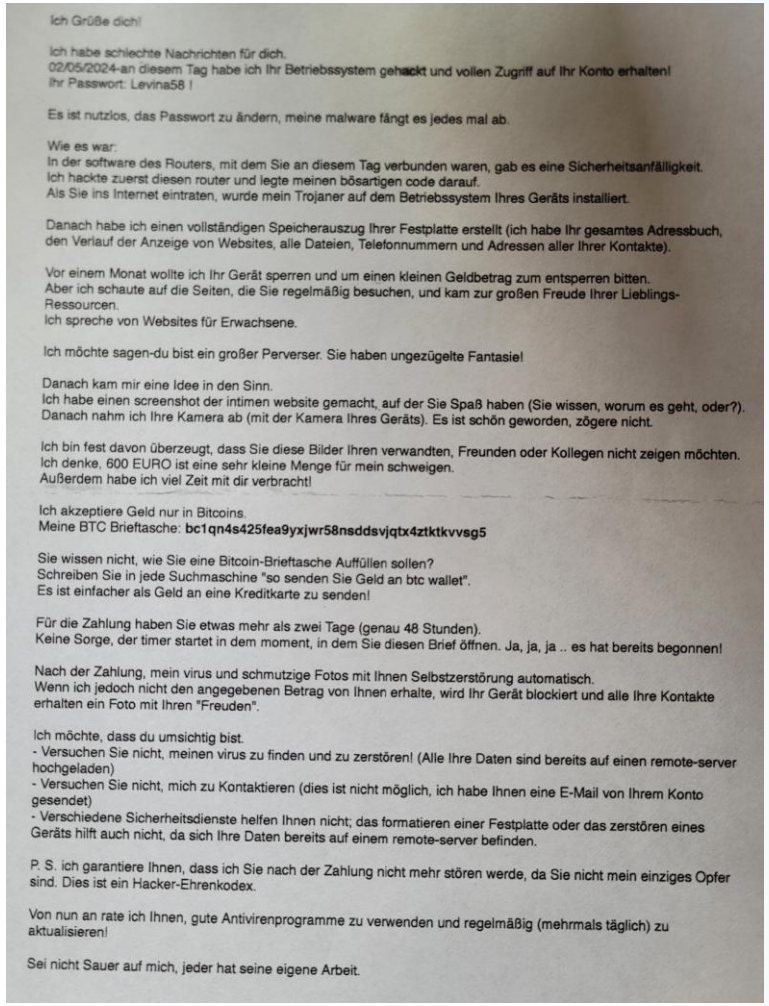


Eröffnen eines Bankkontos

Bei Identitätsdiebstahl meldet sich meist die Kriminalpolizei, nach Anzeige der Bank

Cybersicherheit

Erpressung



Ich Grüße dich!

Ich habe schlechte Nachrichten für dich.
02/05/2024-an diesem Tag habe ich Ihr Betriebssystem gehackt und vollen Zugriff auf Ihr Konto erhalten!
Ihr Passwort: Levina58 !

Es ist nutzlos, das Passwort zu ändern, meine malware fängt es jedes mal ab.

Wie es war:
In der software des Routers, mit dem Sie an diesem Tag verbunden waren, gab es eine Sicherheitsanfälligkeit.
Ich hackte zuerst diesen router und legte meinen bösartigen code darauf.
Als Sie ins Internet eintraten, wurde mein Trojaner auf dem Betriebssystem Ihres Geräts installiert.

Danach habe ich einen vollständigen Speicherauszug Ihrer Festplatte erstellt (ich habe Ihr gesamtes Adressbuch, den Verlauf der Anzeige von Websites, alle Dateien, Telefonnummern und Adressen aller Ihrer Kontakte).

Vor einem Monat wollte ich Ihr Gerät sperren und um einen kleinen Geldbetrag zum entsperren bitten.
Aber ich schaute auf die Seiten, die Sie regelmäßig besuchen, und kam zur großen Freude Ihrer Lieblings-Ressourcen.
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 Kamera ab (mit der Kamera Ihres Geräts). Es ist schön geworden, zögere nicht.

Ich bin fest davon überzeugt, dass Sie diese Bilder Ihren verwandten, Freunden oder Kollegen nicht zeigen möchten.
Ich denke, 600 EURO ist eine sehr kleine Menge für mein schweigen.
Außerdem habe ich viel Zeit mit dir verbracht!

Ich akzeptiere Geld nur in Bitcoins.
Meine BTC Brieftasche: **bc1qn4s425fea9yxjwr58nsddsvjqtx4ztktkvvsg5**

Sie wissen nicht, wie Sie eine Bitcoin-Brieftasche Auffüllen sollen?
Schreiben Sie in jede Suchmaschine "so senden Sie Geld an btc wallet".
Es ist einfacher als Geld an eine Kreditkarte zu senden!

Für die Zahlung haben Sie etwas mehr als zwei Tage (genau 48 Stunden).
Keine Sorge, der timer startet in dem moment, in dem Sie diesen Brief öffnen. Ja, ja, ja .. es hat bereits begonnen!

Nach der Zahlung, mein virus und schmutzige Fotos mit Ihnen Selbstzerstörung automatisch.
Wenn ich jedoch nicht den angegebenen Betrag von Ihnen erhalte, wird Ihr Gerät blockiert und alle Ihre Kontakte erhalten ein Foto mit Ihren "Freuden".

Ich möchte, dass du umsichtig bist.
- Versuchen Sie nicht, meinen virus zu finden und zu zerstören! (Alle Ihre Daten sind bereits auf einen remote-server hochgeladen)
- Versuchen Sie nicht, mich zu Kontaktieren (dies ist nicht möglich, ich habe Ihnen eine E-Mail von Ihrem Konto gesendet)
- Verschiedene Sicherheitsdienste helfen Ihnen nicht; das formatieren einer Festplatte oder das zerstören eines Geräts hilft auch nicht, da sich Ihre Daten bereits auf einem remote-server befinden.

P. S. ich garantiere Ihnen, dass ich Sie nach der Zahlung nicht mehr stören werde, da Sie nicht mein einziges Opfer sind. Dies ist ein Hacker-Ehrenkodex.

Von nun an rate ich Ihnen, gute Antivirenprogramme zu verwenden und regelmäßig (mehrmals täglich) zu aktualisieren!

Sei nicht Sauer auf mich, jeder hat seine eigene Arbeit.

Erkennungsmerkmale:

- **Erpressung**
- **Allgemeine Behauptungen**
- **Zeitdruck aufbauen**

Regelmäßig: Sei wachsam und schütze dich aktiv

1. E-Mail-Sicherheit: Öffne keine E-Mail-Anhänge oder Links von unbekannten Absendern.

2. Finanzkonten regelmäßig überprüfen: Kontrolliere deine Bank- und Kreditkartenabrechnungen sowie andere finanzielle Transaktionen regelmäßig.

3. Sicheres Bezahlen im Internet: Verwende möglichst eine Kreditkarte, da diese im Falle von Betrug besser abgesichert ist als eine Debitkarte.

4. Warnungen ernst nehmen: Beachte Warnungen und Hinweise von Banken, der Polizei oder anderen seriösen Stellen zu aktuellen Cyberbedrohungen.

5. Software-Updates regelmäßig durchführen: Aktualisiere regelmäßig dein Betriebssystem, Apps und Programme.

6. Vorsicht bei Downloads: Lade Dateien, Apps und Programme nur von offizieller und vertrauenswürdiger Quelle.

7. Datensicherung (Backups) durchführen: Sichere deine wichtigen Daten regelmäßig auf einer externen Festplatte oder in der Cloud (z. B. OneDrive, Google Drive).

8. Datenschutz-Einstellungen überprüfen: Überprüfe deine persönlichen Informationen in sozialen Medien und Online-Konten nur für dich oder einen eingeschränkten Personenkreis sichtbar sind.

9. Passwörter und Konten regelmäßig überprüfen: Ändere deine Passwörter in regelmäßigen Abständen und verwende dabei stets starke, einzigartige Kombinationen.

Vorsorge: Sichere deinen Computer und dein Handy

1. Starke Passwörter verwenden: Erstelle lange, komplexe und einzigartige Passwörter für jedes deiner Online-Konten. Verwende eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Nutze einen Passwortmanager, um Passwörter sicher zu generieren und zu speichern.

2. Zwei-Faktor-Authentifizierung (2FA) aktivieren: Aktiviere 2FA für wichtige Konten wie E-Mail, Social Media und Bankkonten.

3. Antivirensoftware: Installiere eine zuverlässige Antivirensoftware, wie Microsoft Defender oder Norton

4. Vertrauensperson definieren: Identifiziere eine Person deines Vertrauens (z. B. Kinder, Geschwister, Freunde), die im Notfall helfen kann.

5. Schutz vor Diebstahl und Verlust: Aktiviere Funktionen wie „Mein Gerät finden“ auf deinem Smartphone, um es bei Verlust oder Diebstahl zu orten und gegebenenfalls zu sperren oder zu löschen.

Bekannte Hackergruppen

Gruppe	Land (vermutet)	Typische Angriffsziele / Methoden bei Privatanwendern
Romance-Scammer (u. a. Westafrika)	Nigeria, Ghana (häufig genannt)	Betrügerische Online-Beziehungsanbahnung, finanzielle Erpressung/Abzocke
Tech-Support-Scams	Indien (häufig), global verteilt	Anrufe/Pop-ups vorgeblich vom „Support“ (Microsoft etc.), Abzocke & Malware
Emotet-Botnet (Phishing-Kampagnen)	Osteuropa (häufig vermutet)	Phishing-E-Mails, Banking-Trojaner, Datendiebstahl
STOP/DJVU-Ransomware	Variiert (teils Russland/Osteuropa)	Verschlüsselung von Dateien; Erpressung über Lösegeldforderungen
Fake-Onlineshops / Fake-Marktplätze	Global, oft EU/Osteuropa	Verkauf nichtexistierender Ware, Kreditkartenbetrug, Identitätsdiebstahl
Lottery/Inheritance-Scams (Nigerian Scam oder „419 Scam“)	Westafrika (u. a. Nigeria)	Vorspiegelung großer Gewinnsummen oder Erbschaften, Gebühren-Vorauszahlung
TrickBot (Banking-Trojaner)	Osteuropa (z. B. Russland/Ukraine)	Trojaner-Infektion über Phishing, Ausspähen von Zugangsdaten
Fake-Investment / Krypto-Scams	Weltweit (oft anonym verschleiert)	Versprechen hoher Renditen, Betrugsplattformen, Abgriff von Geld/Krypto

Wir kennen die Hackergruppen

Ein Nest der Angreifer

KK Park ist eine Online-Betrugsfabrik in Myanmar. Hier leben und arbeiten Tausende von Menschen vor allem aus Afrika und Asien - die meisten unter Androhung von Folter

Bild: Stefan Czimmek/DW

Cybersicherheit beginnt bei Ihnen – bleiben Sie wachsam, bleiben Sie geschützt!

Vielen Dank

Cyber-Notfall-Hilfe.de