

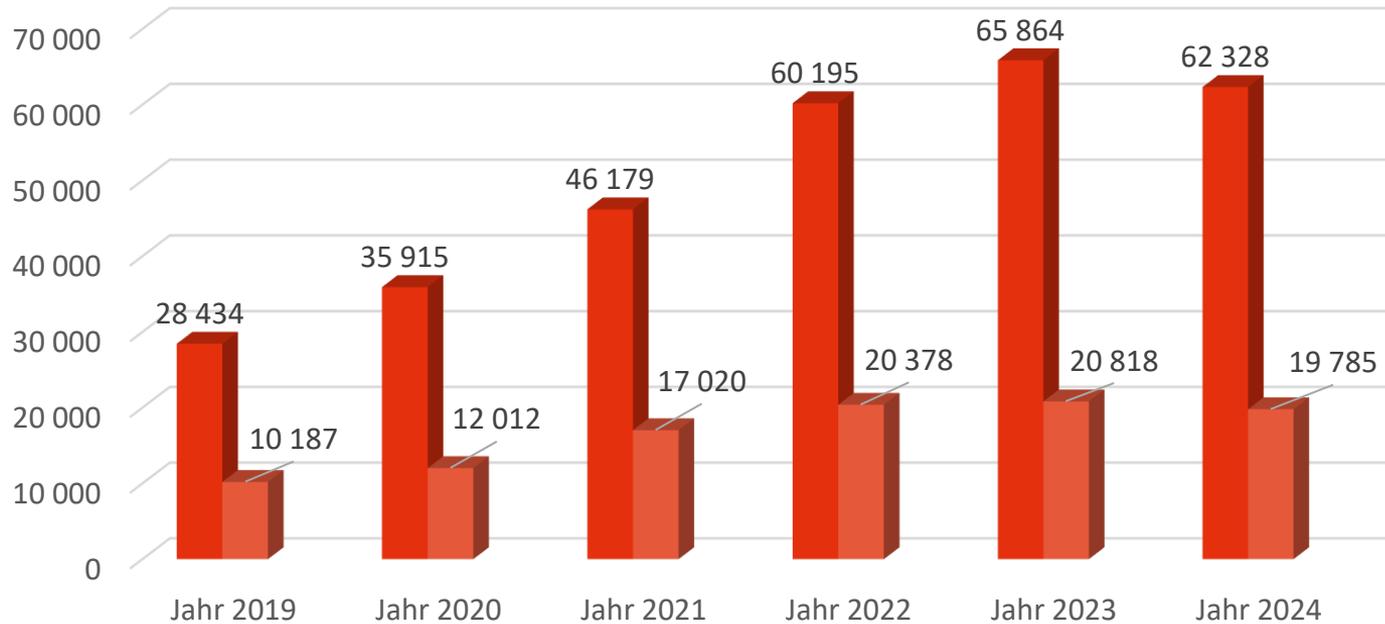
Cybercrime – Soll man Anzeigen?



Bundeskriminalamt, IT Rechtstag
Wien, 8. Mai 2025

Cybercrime - Entwicklung

Internetkriminalität



Cybercrime

- **Gesamtheitliche Aufgabe von Behörden, der Wirtschaft, Wissenschaft und Forschung und dem einzelnen Bürger**
- **Interdisziplinäre Zusammenarbeit zwischen Behörden, Organisationen und Experten**



- **Polizei und Staatsanwaltschaften zur Aufklärung und Strafverfolgung**
- **Datenschutzbehörde: Zum Schutz personenbezogener Daten**
- **Cert.at – Computer Emergency Response Team Austria für die Koordination der Reaktion auf Cyberangriffe**

Aktuelle Phänomene / Allgemein

The collage consists of several overlapping elements:

- Email:** From Österreichische Gesundheitskasse. Subject: Rückstattung. Includes fields for name, email, and registration number.
- News Article:** "Großer Skandal: ORF-Management verweigert Kommentar zu seinem Mitarbeiter Christoph Grisse mann". Includes a photo of a man and a Bitcoin logo with the text "HAT DAS SYSTEM BEREITS MEHR ALS: € 115.347.532,78".
- WhatsApp Messages:**
 - Message 1 (13:43): "Guten Tag, ... kam Zu unsere ... sowohl ihre Ka ... Ihr lebenslauf ... Online-Person ... favorisiert wur ... wir, Es wäre Te ... Nebenbeschä ... Sie Während l ... Durchführen K ... sind Leicht W ... ihre meinung ... ab. ★★★★★ ... Der zeit - sie e ... Sie Diese bew ... 😊 das tagess ... Und 1.000 euro und wird am gleichen Tag zur Verfügung gestellt 💰💰💰 sollten sie Interesse Haben, treten sie bitte via WhatsApp mit uns In Kontakt: +447961461432 📱"
 - Message 2 (13:01): "Halo mama/papa, mein Telefo... funktioniert nicht mehr. Dies... ist meine neue nummer schick... mir ein nachricht aber whats... app+436767395420"
 - Message 3 (11:24): "Ihr Paket wurde zurückge... sandt, da die Hausnummer im Paket fehlt. Bitte aktualisieren Sie die Versandinformatio... nen: <http://postataustria.cc/at>"
- Buttons:** "Weitermachen" at the bottom and "Berühren und halten, um zu reagieren" at the bottom right.

Fälle/LoopX

- 6 Mio. Schaden
- 6 Festnahmen

Salzburger Nachrichten E-Paper SN-Card

Abos Karriere Immobilien

SN.AT / PANORAMA / ÖSTERREICH

Millionenschaden durch Kryptobetrüger

von ANDREAS TRÖSCHER

Mittwoch
08. Mai 2024
04:02 Uhr

PLUS



1 Kommentar

Artikel drucken



Wer in Kryptowährungen investiert, verspricht sich meist schnell viel Geld.

Sechs Jahre lang ermittelt, sechs Millionen Euro Schaden aufgedeckt, sechs Verdächtige festgenommen. Dem Cybercrime Competence Center (C4) des Bundeskriminalamtes (BK) ist es in enger Kooperation mit der Wirtschafts- und Korruptionsstaatsanwaltschaft (WKStA) gelungen, eine mutmaßliche Betrügerbande auszuheben, die auf eine nahezu ...

Fälle/OP_Torman

- Auftragsmord via Darknet
- 15 Jahre Haft
- Weiterer Fall in Wien
 - 12 Jahre Haft



Ransomware Aktuell

- Am 7. März 2025 gestartet
- Ransomware as a Service
(80 % an Mieter/20% Entwickler)
- Bisher 3 bekannte Opfer
- 500.000 Euro in Bitcoin

VANHELING HEISST DAS NEUE RANSOMWARE-AS-A-SERVICE MODELL

30. April 2025

B2B
CYBER
SECURITY
NEWS

Cybercrime – Erstattung einer Anzeige

- **Recht auf strafrechtliche Verfolgung des Täters**
- - Eventuell Zivilrechtliche Ansprüche geltend machen

- **Ratschläge über Tätergruppierung, Schadsoftware**
- Eventuell Entschlüsselungstool erhalten



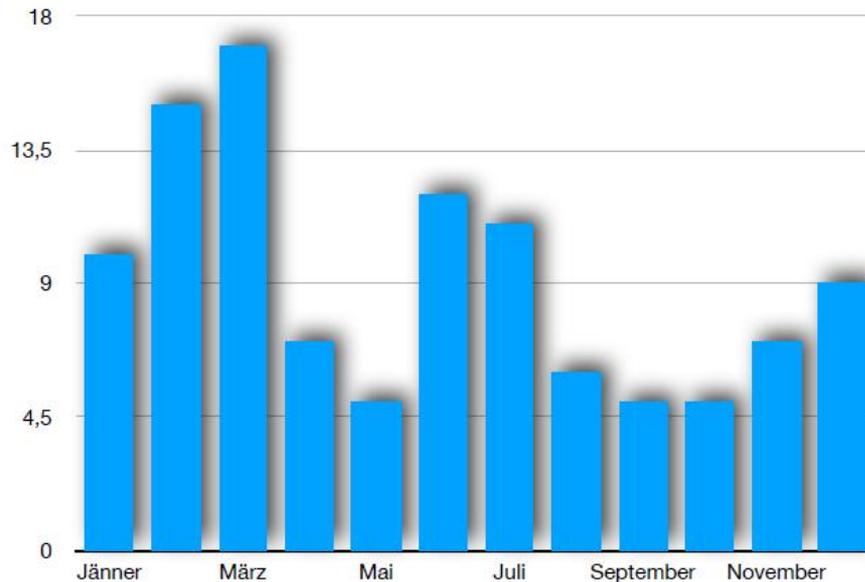
Cybercrime – Erstattung einer Anzeige

Ransomware-Angriffe entschlüsselt



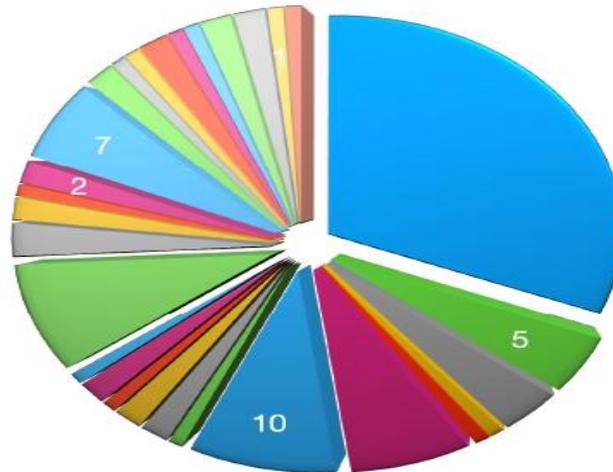
**Mitarbeiter des des Cybercrime-Center mit
Kollegen der japanischen Polizei in Wien**

Ransomware 2024



- 109 Fälle im Jahr 2024 in AT
 - Hohe Dunkelziffer
- Über 1.000 aktive Gruppen
- Lösegeldzahlungen in Milliardenhöhe jährlich weltweit

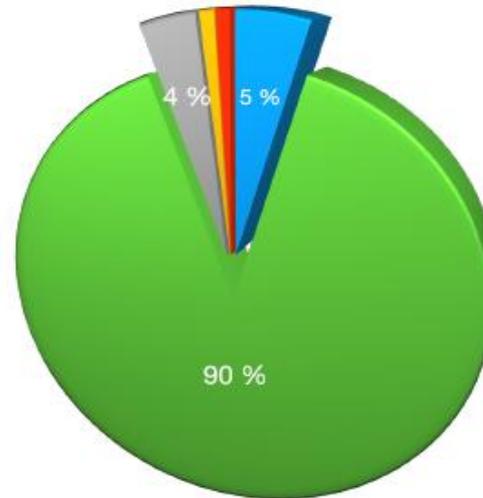
Cybercrime – Ransomware 2024 - Akteure



Top 5 der Ransomware Akteure

1. LockBit 3.0
2. Qilin
3. 8base
4. Akira
5. INC

Cybercrime – Ransomware 2024 - Opfer



5 Privatpersonen
98 Unternehmen
4 Forschungs- und Bildungseinrichtungen
1 Behörde
1 Kritische Infrastruktur

Ransomware Top 5

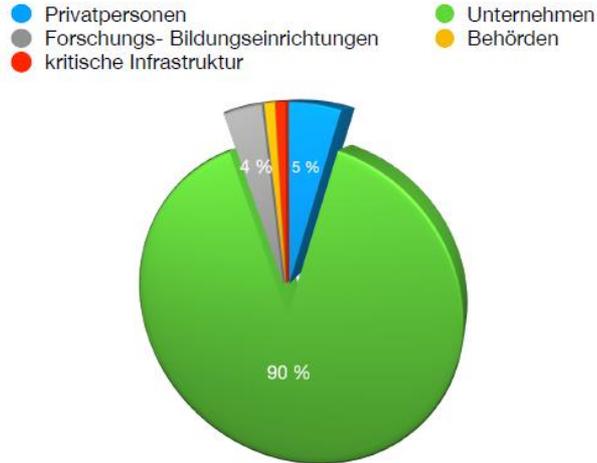


Abbildung 4: Opferverteilung

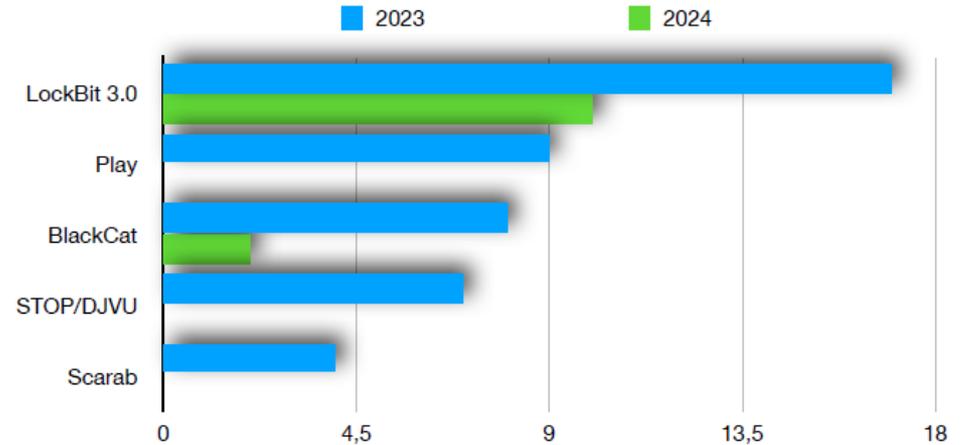


Abbildung 7: Vergleich Top 5 aus 2023/2024

Cybercrime – No More Ransom

- Initiative der National High Tech Crime Unit der niederländischen Polizei, Europols europäischem Cybercrime Center, Kaspersky und McAfee.
- Ziel des Projektes Ransomware Infektionen zu vermeiden
- Informationen über Ransomware, welche Gegenmaßnahmen getroffen werden und Opfern bei der Entschlüsselung zu helfen.



Cybercrime – No More Ransom – Crypto Sheriff

Verschlüsselte Dateien hier hochladen (Dateigröße darf nicht 1 MB überschreiten)



Erste verschlüsselte Datei vom PC auswählen



Zweite verschlüsselte Datei vom PC auswählen

Geben Sie unten eine E-Mail, Webseite, onion und/oder- Bitcoin-Adresse ein, die Sie in der LÖSEGELDFORDERUNG vorfinden Anmerkung: Seien Sie bei der Rechtschreibung besonders genau.

[Oder laden Sie die Datei \(.txt oder .html\) mit der Lösegeldforderung der Kriminellen hier hoch.](#)

Suche starten!

Cybercrime - Anzeigeerstattung Erstmaßnahmen

- **Bewahren Sie Ruhe, gehen sie strukturiert vor.**
- **Keine Veränderungen am Gerät, dem Systembetrieb oder an den Daten**
- **Kommunikation zum Cybercrime Vorfall auf einem nicht infizierten System**
- **Eventuell die kostenlose 24h-Cyber Security Hotline der WKO 0800 888 133**



Cybercrime - Anzeigeerstattung Fragen



- **Welche Systeme sind auf welche Weise betroffen?**
- **Welche Nachweise haben Sie, dass widerrechtlich auf Dateien oder Protokolle zugegriffen wurde (verändert, gelöscht, kopiert, Nutzerrechte verändert...)?**
- **Existieren Protokollinformationen (Ausgangspunkt des Angriffes, Serverkennungen...)?**
- **Wurden Programme installiert oder Daten auf das System kopiert?**
- **Wurden Datei- oder Konfigurationsänderungen vorgenommen?**
- **Wurden Log-Einträge oder gar ganze Logdateien gelöscht?**
- **Wurden wichtige Schutzmechanismen des Systems deaktiviert (z.B. Virens Scanner)?**

THIS WEBSITE HAS BEEN SEIZED

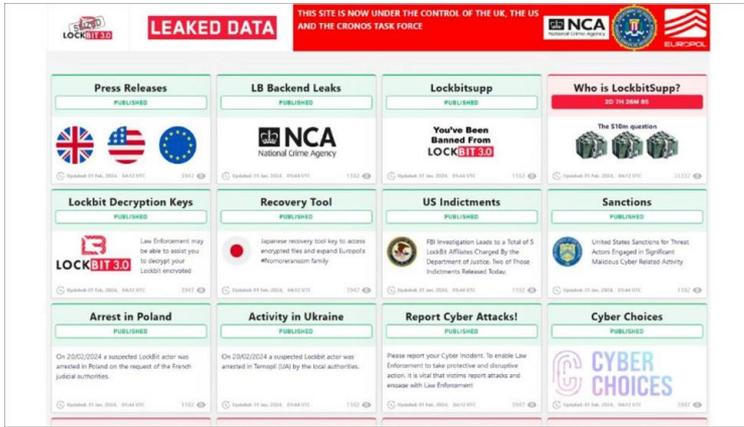
Z-Library's domains have been seized by the Federal Bureau of Investigation in accordance with an international request or warrant issued by the United States District Court for the Eastern District of New York. These seizures were possible because of international law enforcement and private sector coordination including the partners listed below.



 Federal Ministry
Republic of Austria
Interior

Criminal Intelligence Service Austria





LEAKED DATA THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

Press Releases
PUBLISHED
UK, USA, EU logos

LB Backend Leaks
PUBLISHED
NCA National Crime Agency logo

Lockbitsupp
PUBLISHED
You've Been Banned From LOCKBIT 3.0

Who is LockbitSupp?
PUBLISHED
The \$16m question

Lockbit Decryption Keys
PUBLISHED
LOCKBIT 3.0 Law Enforcement may be able to assist you to decrypt your Lockbit encrypted

Recovery Tool
PUBLISHED
Japanese recovery tool key to access encrypted files and expand Europe's ransomware family

US Indictments
PUBLISHED
FBI Investigation Leads to a Total of 5 Lockbit Affiliates Charged By the Department of Justice. Two of Those Indictments Released Today

Sanctions
PUBLISHED
United States Sanctions for Threat Actors Engaged in Significant Malicious Cyber Related Activity

Arrest in Poland
PUBLISHED
On 20/02/2024 a suspected Lockbit actor was arrested in Poland on the request of the French judicial authorities

Activity in Ukraine
PUBLISHED
On 20/02/2024 a suspected Lockbit actor was arrested in Ternopil (UA) by the local authorities

Report Cyber Attacks!
PUBLISHED
Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action. It is vital that victims report attacks and engage with Law Enforcement

Cyber Choices
PUBLISHED
CYBER CHOICES logo



THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

LOCKBIT logo surrounded by flags of various countries including UK, USA, Germany, France, Finland, Netherlands, Sweden, Australia, Canada, and Switzerland.

Logos of participating law enforcement agencies: NCA, MOCU, EUROPOL, POLITIE, Kanton Zürich, Devon County Council, SH, POLIISI, and others.



EURPOL **OPERATION CRONOS**

10 < COUNTRIES IN TASKFORCE CRONOS />

2 < ARRESTS />

MORE THAN 200 < CRYPTOCURRENCY ACCOUNTS FROZEN />

34 < SERVERS TAKEN DOWN />

14 000 < ROGUE ACCOUNTS CLOSED />

< LAW ENFORCEMENT HAS TAKEN CONTROL OF THE TECHNICAL INFRASTRUCTURE AND LEAK SITE />



Fälle/Phishing Takedown



- Eine der größten phishing-as-a-service Plattformen weltweit
- 37 Festnahmen
- Mehrere 10.000 User
- \$ 249 Monatsgebühr
- Phishing-Dienste mit Bezug zu Banken, Zustelldienste, Telekommunikation etc.

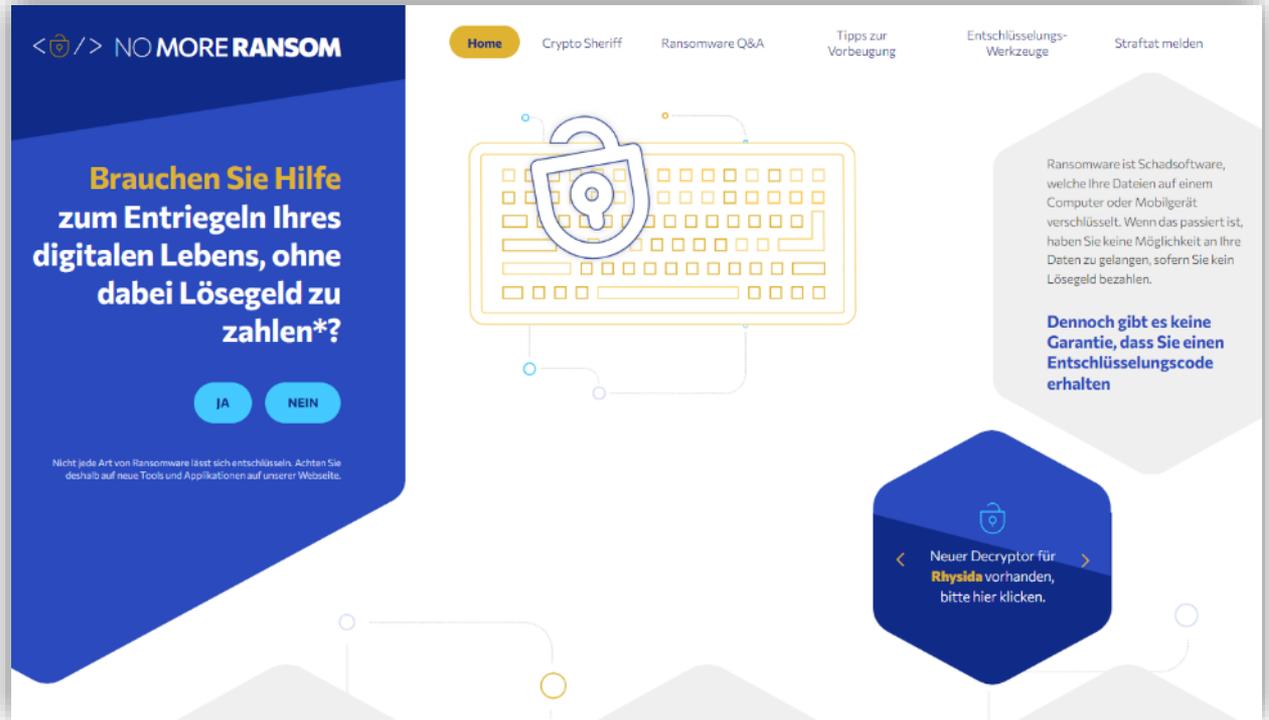
Quick Check Liste – Cybercrime Anzeige

- Bewahren sie Ruhe und gehen sie strukturiert vor
- Vermeiden sie Veränderungen am Gerät, die Beweise verändern/vernichten
- Nutzen sie die kostenlose WKO Cyber-Security Hotline – 0800 888 133
- Bereiten sie sich auf die Anzeige vor (gesicherte Beweismittel, Kopien, Ereignisprotokoll, Tatzeiträume, Tatorte, Schäden..)
- Sammeln sie Informationen zu betroffenen Systemen, Datei- oder Konfigurationsänderungen, gelöschte Log-Einträge, deaktivierte Schutzmechanismen
- Stellen sie Personen- und Kontaktdaten zur Verfügung

Quick Check Liste – Cybercrime Prävention

- Erstellen sie einen Ablaufplan/Notfallplan
- Erstellen einer Notfalltelefonliste (interne und externe Kontakte)
- Erstellen einer Verständigungsliste nach Prioritäten
- Erstellen von internen Leitfäden und Handlungsanweisungen
- Erstellen einer Kurzversion von Verhaltensinformationen
- Bestimmung einer Vertretung des Unternehmens nach Außen
- Halten sie Uhrzeit und die richtige Zeitzone auf allen Systemen aktuell
- Üben sie den Ablauf im Rahmen von jährlichen Übungen

Prävention



< /> NO MORE RANSOM

Brauchen Sie Hilfe zum Entriegeln Ihres digitalen Lebens, ohne dabei Lösegeld zu zahlen*?

JA **NEIN**

Nicht jede Art von Ransomware lässt sich entschlüsseln. Achten Sie deshalb auf neue Tools und Applikationen auf unserer Webseite.

Home Crypto Sheriff Ransomware Q&A Tipps zur Vorbeugung Entschlüsselungs-Werkzeuge Straftat melden

Ransomware ist Schadsoftware, welche Ihre Dateien auf einem Computer oder Mobilgerät verschlüsselt. Wenn das passiert ist, haben Sie keine Möglichkeit an Ihre Daten zu gelangen, sofern Sie kein Lösegeld bezahlen.

Dennoch gibt es keine Garantie, dass Sie einen Entschlüsselungscode erhalten

Neuer Decryptor für Rhapsida vorhanden, bitte hier klicken.

<https://www.nomoreransom.org/>

Prävention

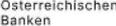
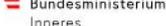
- <https://www.phishen-impossible.at/>
- Die 4 häufigsten Phishing-Attacken
 - Online-Banking
 - Tech Support
 - Paketdienst
 - Finanzamt



MACHEN WIR
PHISHEN
IMPOSSIBLE!

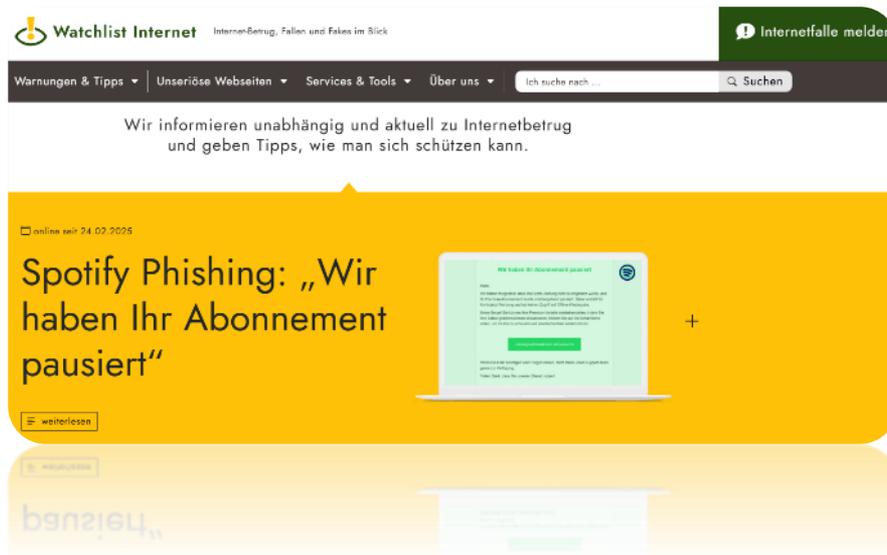
Phishing bedeutet Datendiebstahl. Mit Phishing-Nachrichten versuchen Betrüger, an Passwörter, Bankdaten oder andere sensible Informationen zu gelangen. Hier erfährst du, wie du deine persönlichen Daten schützen kannst.

MEHR ERFAHREN

Eine Initiative von  Österreichischen Banken  PSA  Bundesministerium Inneres

in Kooperation mit  Watchlist Internet

Prävention



<https://www.watchlist-internet.at/>

- Aktuelle Warnungen
- Newsletter / Apps / Channels
- Fakeshop – Detector
- Awareness Playbooks
- Webinare
- Erklärvideos
- Meldfunktion

Danke für Ihre
Aufmerksamkeit!



MinRat Klaus MITS, B.A., M.A.
Bundeskriminalamt

