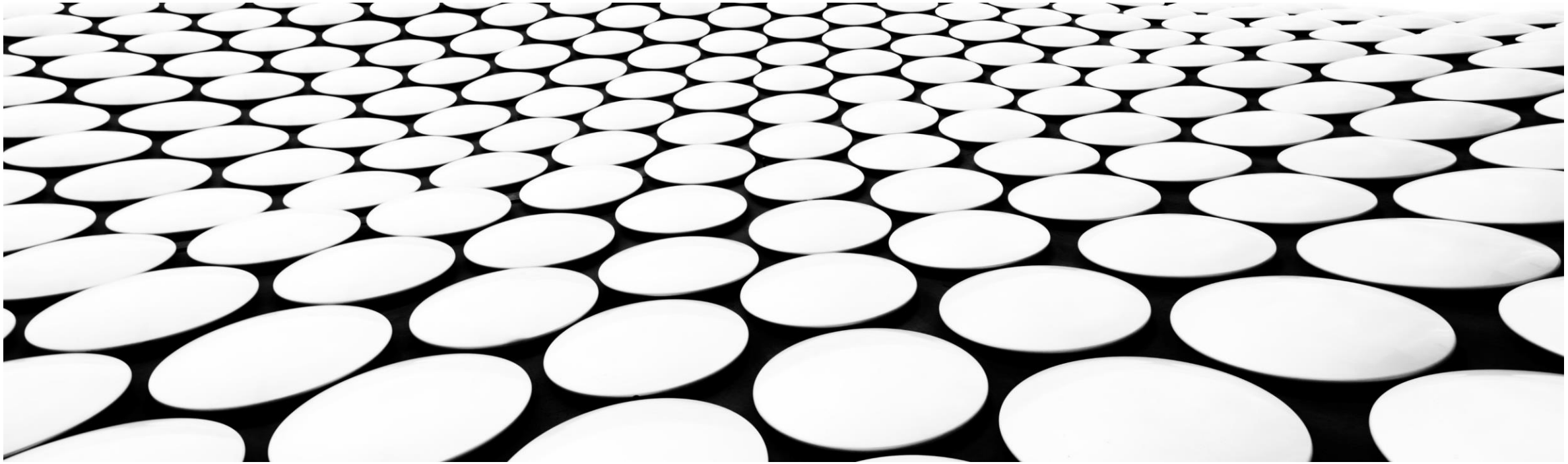
INTERNET - KRIMINALITÄT

WORLD WIDE WEB & DARK WEB – EIN FLUCH UND SEGEN ZUGLEICH



PHÄNOMENBEREICHE IM ALLTAG

Persönlichkeitsrechte
Identitätsdiebstahl
Personenbezogene Daten
Cybermobbing
BKA-Trojaner
WhatsApp – Smishing
Love Scam
Geldwäsche
IP-Spoofing
Enkeltrick
Postzustellung
Sexpressing
Sextortion
Microsoft – Anrufer
NFC-Betrug
Fake Shops
Dreiecksbetrug
Job – Angebote
Ping – Anrufe
Google Fonts
Warenbetrug
Warenagent & Finanzagent
Skimming
Fälschung beweiserheblicher Daten
Enkeltrick - Schockanruf
Datenveränderung – „gehackt“
Zollgebühren
Kreditvermittlungsbetrug
Gewinnversprechen
PaySafeCards
Phishing und Quishing
JA – Verträge

Welche Ziele verfolgt der Betrüger ?

Identitätsdiebstahl

und Zugangsdaten

- Personenbezogene Daten (Name, Vorname, Adresse, Telefonnummer, E-Mail)
- Zugangsdaten zum Bank – Konto und TAN
- Zugangsdaten E-Mail
- Zugangsdaten Verkaufsportale eBay, Amazon, Kleinanzeigen
- Zugangsdaten Bezahldienste (PayPal, Wise, etc)

Buchgeld

oder Wertgegenstände

- Digitales Geld als Überweisung
- Kryptowährung
- Abbuchung Geldbetrag über Handyrechnung
- Bezahlung per PaySafeCard
- Geldtransfer via PayPal, Sofortüberweisung
- Geldübertrag mittels Western Union
- Falscher Polizeibeamter und Enkeltrick

DER WEG DES GELDES IST FÜR ERMITTLUNGEN ENTSCHEIDEND !

WHATSAPP

Smishing = Betrug mittels SMS oder Nachrichten anderer Chatprogramme

Hallo Mama superdumm! Ich habe gerade mein handy verloren, überall gesucht und kann es nicht finden. Ich habe den schaden gemeldet und die versicherung angerufen und glücklicherweise wurde der schaden erstattet. Nur jetzt bin ich unter meiner alten nummer nicht mehr erreichbar, aber unter dieser nummer, kannst du sie gleich speichern? 12:03

Hallo Mama/Papa, Mein Handy ist kaputt und liest meine Sim-Karte nicht mehr. 01734670397 Kannst du mir ein nachricht auf Whatsapp schicken.

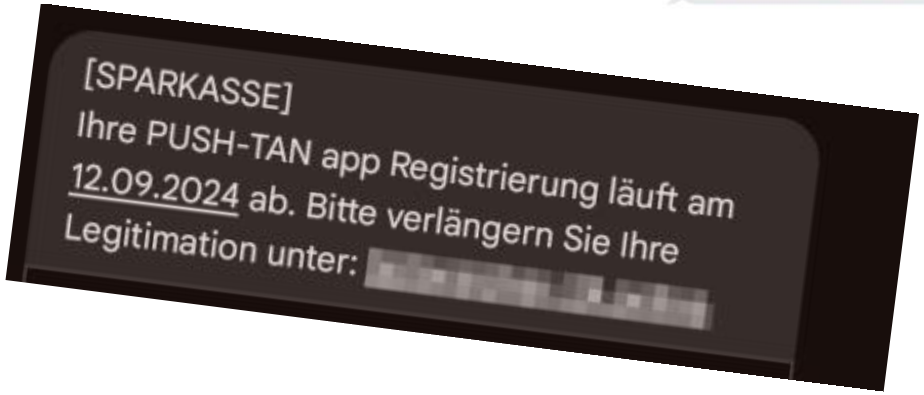
Hallo mama, rate mal wessen's Handy in der Waschmaschine gelandet ist. Du kannst diese Nummer einspeichern und die alte löschen 😣 19:30

Der Betrüger bittet darum, die alte Nummer zu löschen und kurz darauf erklärt er, dass er nicht mehr auf sein Bankkonto zugreifen kann, da er alle Zugangsdaten verloren hat. Angeblich braucht er Geld, um das neue Handy zu bezahlen. Das Geld hat er von einem Freund geliehen. Deshalb soll ein höherer Geldbetrag für das teure Smartphone auf die angegebene IBAN *sofort* überwiesen werden. Geld wird später an Mama oder Papa zurückgezahlt.

PHISHING

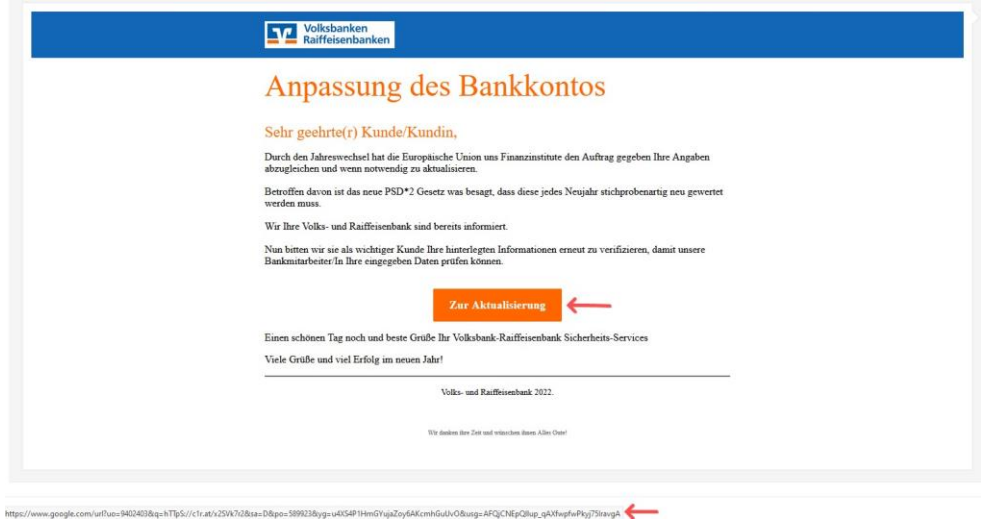
SMS-Nachricht
Heute, 17:54

Sparkasse: Ihr Zugriff auf die S-pushTAN App endet am 09.08.2024. Bitter verlängern Sie diesen jetzt unter: [redacted]



[SPARKASSE] Ihre T-App läuft in Kürze ab. Bitte aktualisieren Sie diese, um Ihr Online Banking weiterhin nutzen zu können.
https://[redacted] 23:44

Täter versuchen ihre Zugangsdaten zu erlangen. Per SMS oder WhatsApp oder E-Mail oder soziale Medien. Vom Bankzugriff bis hin zu Zugriffen auf Accounts für Verkaufsportale und Filmangebote.


Volksbanken Raiffeisenbanken

Anpassung des Bankkontos

Sehr geehrte(r) Kunde/Kundin,

Durch den Jahreswechsel hat die Europäische Union uns Finanzinstitute den Auftrag gegeben Ihre Angaben abzugleichen und wenn notwendig zu aktualisieren.

Betroffen davon ist das neue PSD*2 Gesetz was besagt, dass diese jedes Neujahr stichprobenartig neu gewertet werden muss.

Wir Ihre Volks- und Raiffeisenbank sind bereits informiert.

Nun bitten wir sie als wichtiger Kunde Ihre hinterlegten Informationen erneut zu verifizieren, damit unsere Bankmitarbeiter/In Ihre eingegeben Daten prüfen können.

Zur Aktualisierung

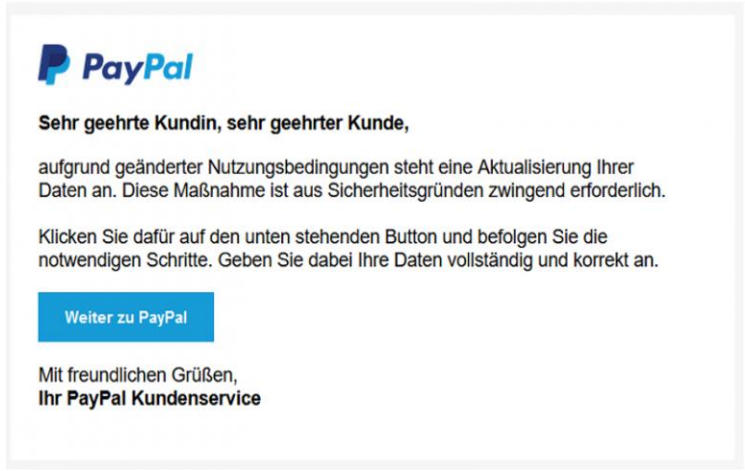
Einen schönen Tag noch und beste Grüße Ihr Volksbank-Raiffeisenbank Sicherheits-Services

Viele Grüße und viel Erfolg im neuen Jahr!

Volks- und Raiffeisenbank 2022.

Wir danken Ihre Zeit und wünschen Ihnen Alles Gute!

https://www.google.com/url?sa=i&url=[redacted]


PayPal

Sehr geehrte Kundin, sehr geehrter Kunde,

aufgrund geänderter Nutzungsbedingungen steht eine Aktualisierung Ihrer Daten an. Diese Maßnahme ist aus Sicherheitsgründen zwingend erforderlich.

Klicken Sie dafür auf den unten stehenden Button und befolgen Sie die notwendigen Schritte. Geben Sie dabei Ihre Daten vollständig und korrekt an.

Weiter zu PayPal

Mit freundlichen Grüßen,
Ihr PayPal Kundenservice

BETRUG MIT QR-CODE-PHISHING = QUISHING !!!

QR-CODES HABEN WESENTLICH MEHR INFORMATIONEN ALS STRICH-CODES !!! KANN JEDER ERSTELLEN !!!

QR-Codes werden auf Ladesäulen für Elektroautos oder Parkuhren überklebt. Täter verbreiten diese auf Plakaten. Auch falsche Strafzettel mit QR-Codes sind im Umlauf. Zudem werden gefälschte Briefe von Banken und Krankenkassen mit QR-Code verschickt. Auch bei Online-Banken wie C24-Bank werden Zugänge manipuliert. Wenn Sie einen QR-Code anklicken und einen Bestätigungscode eingeben, wird das Geld abgebucht !!!

Beim Parken am Besten App aus dem STORE – Apple oder Android – herunterladen. Keinen QR-Code nutzen !!!

POSTZUSTELLUNG

IN DEM FALL WILL DER TÄTER DATEN ERLANGEN UM DIESE ZU VERKAUFEN.

EIN BETRÜGER TÄUSCHT FAST IMMER ZEITDRUCK (DRINGEND) VOR !!!

Hallo lieber Kunde,

danke, dass Sie sich für uns entschieden haben. Um Ihr Paket zu liefern, bitten wir Sie, unsere Anweisungen zu befolgen. Klicken Sie bitte auf den untenstehenden Button, um auf unsere Seite weitergeleitet zu werden, und befolgen Sie die dort angegebenen Anweisungen.

VOLLSTÄNDIGER VERSAND HIER

HINWEIS: Dieser Link ist nur 48 Stunden gültig. Wenn Sie die Bestätigung innerhalb dieser zeit nicht abgeben, wird Ihr Paket an den Absender zurückgesandt.

Herzliche Grüße,
Das DHL EXPRESS Kundenservice-Team

DHL

AKTUALISIERUNG IHRER LIEFERADRESSE

Sehr geehrte/r

wir hoffen, diese Nachricht erreicht Sie in bester Verfassung. Es liegt eine wichtige Angelegenheit bezüglich eines Pakets für Sie vor, das derzeit aufgrund einer falschen Lieferadresse nicht zugestellt werden konnte.

Paketdetails:

Liefercode: [redacted]
Rücksendegebühr: 2,99 €
Um sicherzustellen, dass Ihr Paket erfolgreich zugestellt wird, bitten wir Sie, die folgenden Schritte zur Korrektur Ihrer Lieferadresse zu befolgen:

Schritte zur Aktualisierung Ihrer Lieferadresse:

Klicken Sie auf den folgenden Link:

Nachlieferung

Bearbeiten Sie Ihre Lieferadresse: Fügen Sie die korrekten Angaben hinzu und bestätigen Sie die Änderungen.
Bitte beachten Sie, dass eine Rücksendegebühr in Höhe von 2,99 € anfällt. Dies dient dazu, die Kosten für die erneute Zustellung zu decken.

Für jegliche Unterstützung oder Fragen steht Ihnen unser Kundensupport rund um die Uhr zur Verfügung.

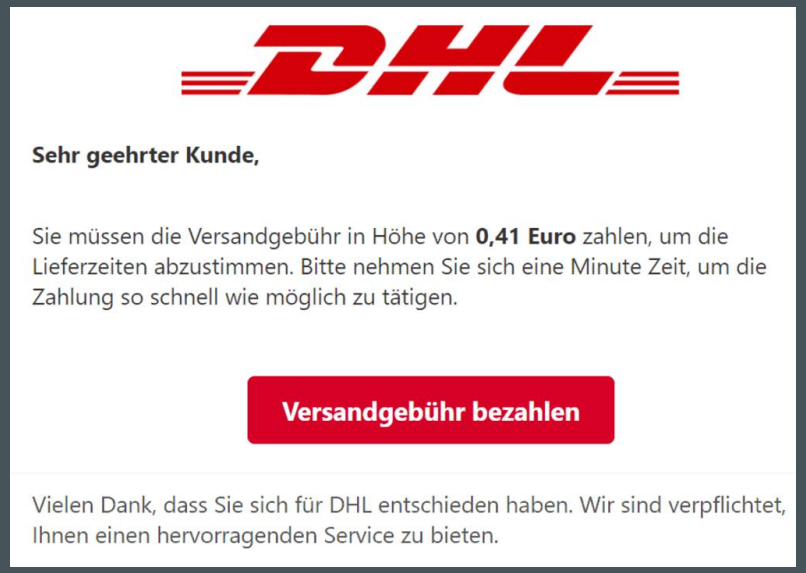
Wir danken Ihnen für Ihre sofortige Aufmerksamkeit und Mitarbeit, um eine reibungslose Zustellung Ihres Pakets sicherzustellen.

Mit freundlichen Grüßen,

ZOLLGEBÜHREN UND WEITERE KOSTEN

BETRÜGER FORDERT SCHNELLES HANDELN, UM FOLGEKOSTEN ZU VERMEIDEN ODER DIE RÜCKSENDUNG DER WARE ZU VERHINDERN. ER BESTEHT AUF SOFORTIGE BEZAHLUNG DURCH ÜBERWEISUNG UND BEZAHLDIENSTE.

Seriöse Unternehmen, Banken, Polizei, Behörden, Gerichte, Schulen und Ämter fragen NIEMALS Zugangsdaten oder Kontaktdaten auf diesem Wege an. Solche Nachrichten werden IMMER von den Betrügern versandt.



WARENBETRUG

Geld bezahlt, keine Ware = Warenbetrug

Ware versandt, kein Geld erhalten = Warenkreditbetrug

- Verkäufer bietet für den Interessenten eine ansprechende Ware für scheinbar billigen Preis als Schnäppchen an
- Kontaktaufnahme mittels Chat bei www.kleinanzeigen.de oder www.ebay.de oder andere Verkaufsportale
- Nach Einigung über Verkaufspreis und Versandkosten, sendet der Käufer dem Verkäufer die Adressdaten mit Name und Vorname, damit die Ware schnellstmöglich zum Empfänger versendet werden kann.
- Verkäufer (Betrüger) bittet um Bezahlung via PayPal mit der Option „Freunde und Familie“
- Es besteht **KEIN KÄUFERSCHUTZ**
- WARE wird niemals geliefert !!!
- In diesen Fällen wurde der Account eines Anderen z.B. bei www.kleinanzeigen.de vom Betrüger „gehackt“ und zum Verkauf missbraucht. Standort und Anzeigename wurden geändert, aber die echten personenbezogenen Daten des eigentlichen Account – Inhabers wurden belassen.

IDENTITÄTSDIEBSTAHL BEI KLEINANZEIGEN.DE

Genauso wie beim Warenbetrug nimmt der Täter Kontakt über den Chat auf. Man wird sich handelseinig, doch in dem Fall möchte der Täter vom Käufer einen Nachweis über seine Identität haben.

Als Vertrauensbeweis sendet er im Vorfeld schon mal die Screenshots von seinem Personalausweis zu. Natürlich handelt es sich hierbei um einen gestohlenen oder total gefälschten Ausweis mit Echtdaten von existierenden Personen oder fiktiven Daten, welche frei erfunden worden sind.

Als ehrlicher Käufer sendet man anschließend die Screenshots von seinem echten gültigen Personalausweis. Jetzt hat der Täter schon gewonnen !

Mit den erhaltenen Screenshots des Ausweises betrügt er sein nächstes Opfer und erhält schon wieder einen neuen „frischen“ Ausweis für die nächste Tatbegehung. Diese Betrugskette verlängert sich Glied für Glied.

Solche Ausweise werden auch auf andere Weise durch Webseiten der Betrüger erlangt. Näheres dazu auf beim Thema JOB – ANGEBOTE von den Betrügern.

DATENVERÄNDERUNG

WARUM HAT DER TÄTER ZUGRIFF AUF MEINEN ACCOUNT ?

Der Täter verschafft sich durch verschiedene Programme und Algorithmische Abfolgen Zugriff auf das E-Mail-Konto. Es werden auch Server von Betreibern (T-Online, Facebook, etc) „gehackt“.

Anschließend aktiviert er im E-Mail-Account eine Umleitung auf seine eigene E-Mail-Adresse. Auch das Passwort wird verändert.

Sobald der Täter Zugriff auf die E-Mail-Adresse hat, testet er bei Verkaufsplattformen wie ebay, kleinanzeigen oder Amazon den Zugang mit falschen Passwörtern. Sofort wird ihm angeboten das Passwort zurückzusetzen. Nun erhält er den Link auf die gehackte umgeleitete E-Mail und kann alles ändern und hat vollen Zugriff.

JOB – ANGEBOTE VOM BETRÜGER – KANN DAS ÜBERHAUPT LEGAL SEIN ?

Betrüger bieten über ihre eigenen Webseiten auf ausländischen Servern Jobs für Heimarbeit an. Interessierte melden sich auf deren Webseite und geben dort ihre personenbezogenen Daten an.

Zur Legitimierung wird wie beim Postident-Verfahren ein Video von den Interessenten aufgezeichnet. Zudem muss man den Personalausweis mit Vorder- und Rückseite in die Kamera halten.

Jetzt hat der Betrüger alles was er braucht. Von dem Ausweis kann er Screenshots machen und diese zum Warenbetrug benutzen. Mit dem Video und den Ausweisdaten kann der Täter neue Bankkonten wie bei den deutschen Online – Banken N24 Bank, BunQ oder Solarisbank eröffnen. Diese Konten werden dann zur Geldwäsche verwendet und nach wenigen Tagen werden weitere Konten mit den gleichen Daten eröffnet. Das erlangte Geld wird dann auf andere Konten ins Ausland umverteilt– vorzugsweise Litauen, Frankreich oder England. Teilweise werden die Gelder in Kryptowährung (Ethererum gewechselt).

GELDWÄSCHE UND FINANZAGENT

TÄTER SCHREIBEN AUCH ZUKÜNFTIGE OPFER UND MITTÄTER PER E-MAIL ODER AUCH ÜBER SOZIALE MEDIEN AN, ES WIRD ANGEBOTEN EINEN JOB MIT GROßZÜGIGER ENTLOHNUNG ANZUNEHMEN. SIE MÜSSEN LEDIGLICH GELD VON KUNDEN IHRES UNTERNEHMENS IM AUSLAND ANNEHMEN UND ALS EINE ART BUCHMACHER AN IHRE ANDEREN UNTERNEHMENSZWEIGE ODER ENDKUNDEN WEITERLEITEN. NATÜRLICH FÜHREN ALLE VERSTRICKUNGEN WIEDER ZU WEITEREN TÄTERN DER ORGANISATION.

WARENAGENT

Der Warenagent arbeitet ebenfalls für die Betrüger. Diesmal hat die Person aber nicht die Aufgabe Geld zu transferieren, sondern Ware neu zu verpacken und weiter zu senden. Oftmals im Zusammenhang mit LOVE SCAMMING.

Die Waren werden von den Betrügern mittels rechtswidrig erlangter Kreditkarten bei Online Shops bestellt und an die Adresse des Warenagenten geschickt. Dieser verpackt sie neu und schickt sie an die Adressen anderer Postkasten – Firmen (Firmensitz bei leerstehenden Gebäuden) oder DHL Paketstationen oder sogar an Endkunden weiter, welche tatsächlich an der angegebenen Adresse nicht wohnhaft sind, aber den Postboten das Paket vor Ankunft entlocken.

Betrüger kaufen Waren bei Online – Shops mittels der „gehackten“ E-Mail-Adressen, erlangten personenbezogenen Daten aus anderen Straftaten wie beim Warenbetrug oder Job Scamming, sowie durch Datenklau auf den Servern anderer Unternehmen. Diese Daten werden als Pakete im Dark Web zwischen den Betrügern gehandelt.

LOVE SCAMMING

DER BETRÜGER SPIELT DIE GROßE LIEBE AUS DEM AUSLAND VOR. OFTMALS VERMÖGEND UND STATUS WIE ÄRZTE IM KRIEGSGEBIET. NACH VIELEN SCHÖNEN WORTEN WIRD DAS VERTRAUEN GEWONNEN. ES WIRD DANN EIN GELDENGPASS VORGEGAUKELT, DAMIT DIE VERLIEBTE SEELE AUSHILFT. GELD WIRD INS AUSLAND TRANSFERIERT.

Der Täter gewährt nicht selten der Neuen Liebe Zugriff auf sein Konto. Sie ist einsam, verliebt und vertraut ihm. Deshalb darf sie in seinem Auftrag sogar Geldtransfers auf seinem Konto tätigen. Jedoch nutzt sie hierfür den Link von ihm. Dieser führt zu einer täuschend echt aussehenden Bankseite. Das Konto ist gar nicht exisitent, sondern nur ein Programm. Irgendwann wird der Zugriff geblockt und er benötigt dringend Geld. Da er reich ist, werden ihr riesige Summe wie 100.000 Euro versprochen als Entschädigung für die Hilfe. Sie überweist mehrere 10.000 Euro bis sie schließlich Pleite ist.
Manchmal werden Notsituationen vorgespielt. Ein erkranktes Kind oder eigene Krankheit welche verhindern zur Bank zu gehen und deshalb nur kurzzeitig Gelder als Nothilfe nötig sind. Sie zahlt wieder und hofft auf Rückzahlung.

Der Betrug mit der LIEBE ist weit verbreitet und vor allem alte Menschen sehnen sich danach und werden Opfer.

FAKE SHOPS

FAKE SHOPS SEHEN AUF DEN ERSTEN BLICK UNFASSBAR SERIÖS AUS UND WERBEN MIT UNSCHLAGBAREN WAREN-ANGEBOTEN ÄHNLICH WIE BEI TEMU. DIESE WEBSEITEN HABEN BETRÜGER ONLINE GESTELLT. SIE ERLANGEN DADURCH DATEN UND GELD. ABER WIE KANN ICH SOLCHE BETRÜGERISCHEN FAKE-SHOPS ERKENNEN?

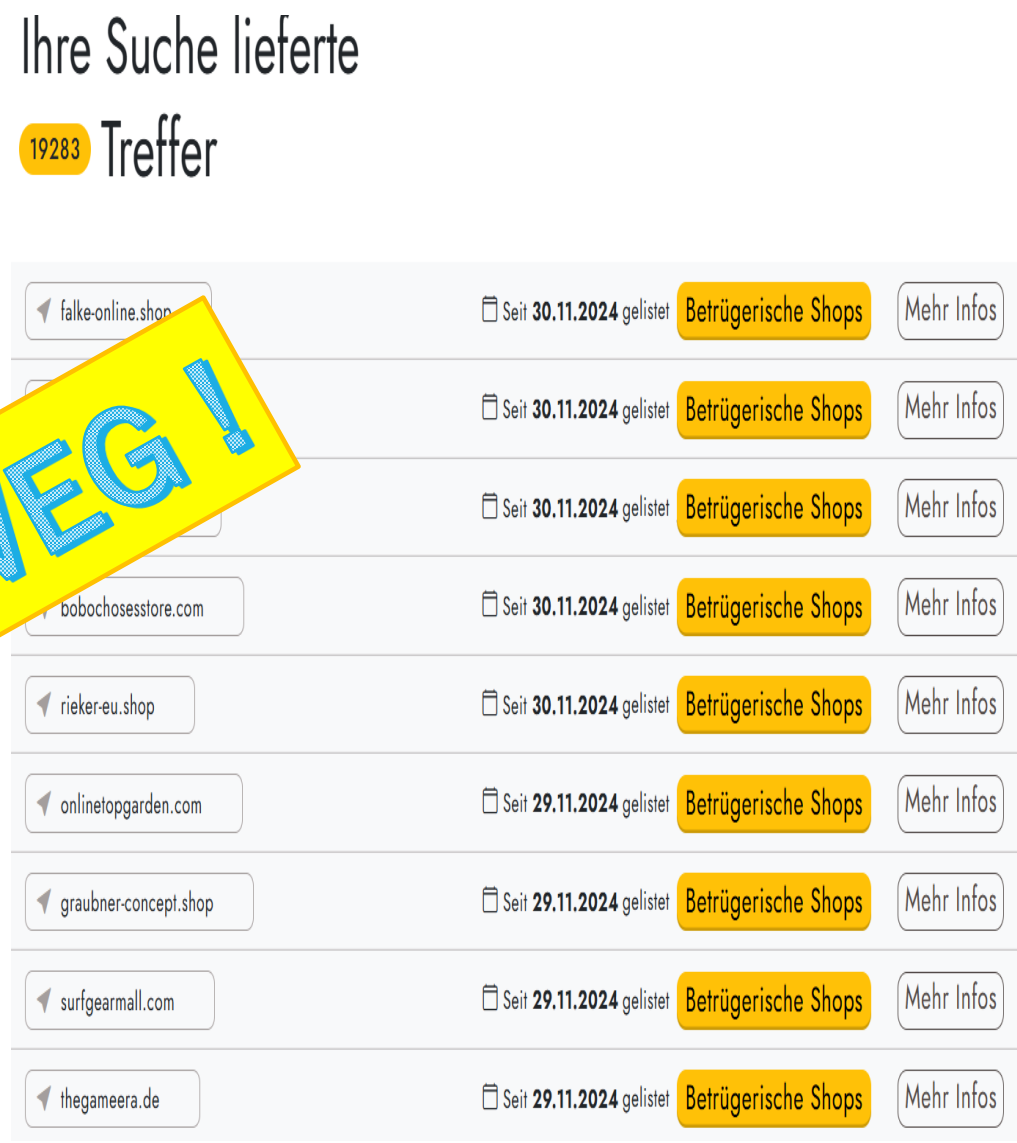
Sehr viele Fake – Shops sind bereits bei der Verbraucherzentrale bekannt und können dort mit der Webadresse erkannt werden.
Ein seriöser Anbieter eines Online – Shops ist persönlich per Telefon erreichbar und nicht nur per E-Mail. Eine Bandansage mit der Bitte eine E-Mail zu schreiben, ist immer verdächtig.
Sobald man das Formular zur Bestellung ausgefüllt hat, sollte man unverzüglich eine Bestätigungs-E-Mail erhalten. Diese werden bei Betrügern meistens nicht versendet, da sonst die Protokolle der E-Mail (HEADER) übermittelt werden.
Ein absolutes Erkennungszeichen ist der Bezahlvorgang. Es wird oftmals PayPal oder andere Dienste angeboten, aber diese funktionieren angeblich aufgrund Wartungsarbeiten oder Störungen nicht. Deshalb wird eine Sofortüberweisung angeboten. Das Geld wird in Echtzeit übertragen und kann nicht mehr zurückgeholt werden. Ohne Käuferschutz auf keinen Fall Geld transferieren.

Als die Anzeigenerstatterin zur Polizei kam, um eine Anzeige wegen Warenbetrugs gegen Betreiber von spielzeugwaren.net zu erstatten, existierte diese Webseite nicht mehr.

Inzwischen haben die Betrüger ihre DOMAIN geändert. Genauso wie bei den Konten für Geldwäsche sind solche Webseiten nur kurzfristig verfügbar.

Angebote werben mit Billigpreis und Zeitdruck (nur noch 1 Produkt auf Lager, Angebot gültig nächsten 5 Stunden)

FINGER WEG !



E-MAIL UND HEADER – ENORM WICHTIG FÜR STRAFVERFOLGUNG

```
Return-Path: <user31232@lws01.ldn5.groupnbt.net>
Received:
from mail.vz-nrw.de ([unix socket]) by mail (Cyrus
v2.2.13-Debian-2.2.13-10+etch4) with LMTPA; Tue, 04 Jan 2011 20:08:52
+0100
X-Sieve:
CMU Sieve 2.2
Envelope-to: finanzwissen@vz-nrw.de
Delivery-date: Tue, 04 Jan 2011 20:08:52 +0100
Received: from [172.16.1.4] (helo=astaro.vz-nrw.de) by
mail.vz-nrw.de with esmtp (Exim 4.63) (envelope-from
<user31232@lws01.ldn5.groupnbt.net>) id 1PaCFY-00015E-Kb for
finanzwissen@vz-nrw.de; Tue, 04 Jan 2011 20:08:52 +0100
Received: from lws01.netbenefit.co.uk ([62.128.158.4]:49352
helo=lws01.ldn5.groupnbt.net) by astaro.vz-nrw.de with esmtps
(TLSv1:AES256-SHA:256) (Exim 4.69) (envelope-from
<user31232@lws01.ldn5.groupnbt.net>) id 1PaCFW-0005Dx-26
for finanzwissen@vz-nrw.de; Tue, 04 Jan 2011 20:08:50
+0100
Received: from user31232 by lws01.ldn5.groupnbt.net with local
(Exim 4.63) (envelope-from <user31232@lws01.ldn5.groupnbt.net>) id
1PaCFW-0000pj-4q for finanzwissen@vz-nrw.de; Tue, 04 Jan 2011 19:08:50
+0000
X-CTCH-RefID:
str=0001.0A0B0205.4D237042.0231:SCFSTAT3589785,ss=1,fgs=0
An: finanzwissen@vz-nrw.de
Betreff: Achtung! Ihr PayPal-Konto wurde begrenzt!
```

Beim Versenden von E-Mails werden im Hintergrund Protokolle gefertigt. Diese werden im HEADER gesichert. Unter „Eigenschaften“ oder „Mehr Informationen“ kann jedermann diese abrufen.

UNBEDINGT markieren und kopieren in eine WORD – DATEI und der Polizei übergeben !!!

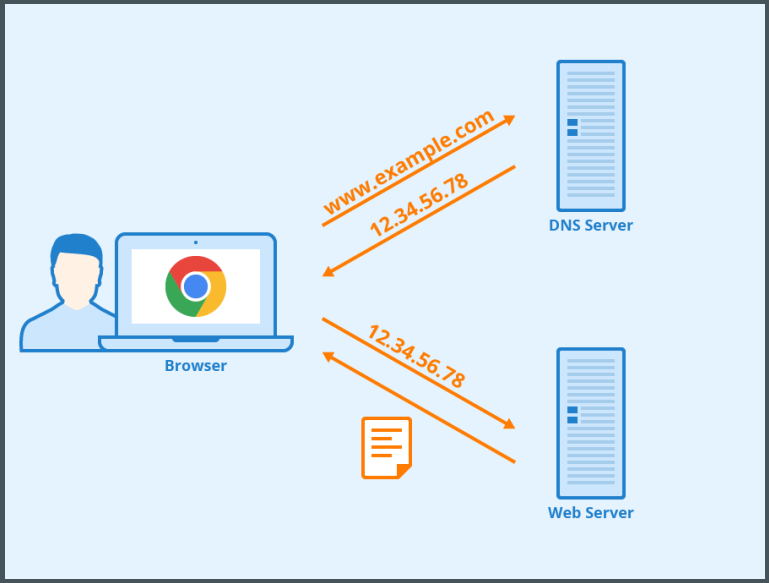
Sie können im E-Mail-Header folgende Informationen ermitteln:

- die E-Mail-Adresse des Absenders
- die IP-Adresse des Absenders (und damit den tatsächlichen Absender!)
- die Empfänger der E-Mail
- das Datum des Versands
- den Betreff der E-Mail

WAS IST EINE IP – ADRESSE ?

WENN DER POSTBOTE AN SIE EINE LIEFERUNG HAT ODER EINEN BRIEF ZUSTELLEN WILL, BENÖTIGT ER IHRE WOHNADRESSE, ALSO DIE STRAßE, HAUSNUMMER UND AUCH DEN ORT MIT POSTLEITZAHL.

IM INTERNET WERDEN DIE ADRESSEN ALS IP – ADRESSEN BEZEICHNET UND SCHAUEN SO AUS: 192.188.63.42



Jede Webseite hat eine STATISCHE IP – Adresse. Natürlich kann sich niemand diese Zahlenfolge merken. Wir schreiben z. B. www.example.com und der Computer im Internet (Domain-Name-Server) wandelt es in die IP-Adresse um.

Wenn sich eine Person über den Browser ins World Wide Web einwählt, erhält er vom Provider (T-Online, AOL, Kabel Deutschland) eine DYNAMISCHE IP – Adresse. Diese wird immer wieder neu vergeben, aber Datum, Uhrzeit und Telefonanschluss werden protokolliert. Jeder Provider hat nur ein begrenztes Kontigent an IP – Adressen.

IP-Adressen verraten den Weg der Daten bis zum Ziel !!!

KÄUFERSCHUTZ

- Seriöse Bezahldienste wie bei www.ebay.de integriert oder auch PayPal bieten grundsätzlich einen Käuferschutz an.
- Betrüger drängen immer darauf, dass Zahlungen sofort zu leisten sind, um sich ein Angebot zu sichern. Deshalb bieten sie auch Sofortüberweisung oder PayPal mit der Option „Freunde und Familie“ an. Bei diesen Geldtransfers gibt es keinen Käuferschutz. Geld weg für immer.
- Lediglich bei Einzugsermächtigungen oder Abbuchungen kann man das Geld über seine Bank zurückfordern.
- In dem Zusammenhang möchte ich noch die KUNO – Sperrung bei der Polizei vorstellen.

KUNO
Karten Sperrdienst für
SEPA-Lastschriftzahlungen

Sollte jemand aufgrund Diebstahl oder Verlust eine EC – Karte verlieren, dann wird oftmals nur die Bank informiert. Die Bank sperrt die Karte für Zahlungen mittels PIN oder per Unterschrift – Verfahren. Jedoch kann jede Bankkarte bis zum Ablauf ihrer Gültigkeit weiterhin im Handel als bargeldloses Bezahlungsmittel eingesetzt werden. Diese Karten können 8 bis 12 mal pro Monat mit Beträgen unter 50 Euro belastet werden. Dieses Geld wird von ihrem Konto nicht abgebucht, aber der Handel hat die Ware herausgegeben. Der Verlust wird vom Handel abgeschrieben, indem die Preise für alle Kunden angehoben werden. Deshalb nutzen Sie die Möglichkeit bei der Polizei. Nur die Polizei kann seit Februar 2006 diese Karte im Handel sperren.

RANSOMWARE - BKA TROJANER

Computer gesperrt und nur durch Bezahlung einer Geldsumme (Erpressung) kann der PC oder Laptop wieder in Betrieb genommen werden.

AUF KEINEN FALL BEZAHLEN.

Problem lässt sich durch Code – Eingabe oder anderer Software ohne bleibende Schäden beheben.

ERFINDER der Software BEREITS POLIZEILICH BEKANNT (Wohnsitz im Ausland).

Angebilch wurden Sexseiten aufgerufen und sofortiger Kontakt mit der ermittelnden Behörden ist erforderlich. Sie wollen Daten und Geld als eine Art Kaution um das Strafverfahren abzuwenden !

ERPRESSUNG PER E-MAIL

EUROPOL EC3 European Cybercrime Centre — INTERPOL — BUNDESPOLIZEI

STRUKTUREN IN ZUSAMMENARBEIT MIT INTERPOL – SICHERHEITSPOLIZEI & GENDARMERIE – EIDGENÖSSISCHES JUSTIZ- UND POLIZEIDEPARTEMENT

Interpol ist unter anderem dafür bekannt, Rote Notizen herauszugeben, d. h. Warndokumente, die nach ihrer Veröffentlichung die weltweite Jagd auf gesuchte Kriminelle ermöglichen. Diese Dokumente, die Identifikationsmerkmale und rechtliche Aspekte der gesuchten Personen enthalten, werden in allen 195 Mitgliedsländern verbreitet. Sie erleichtern die Arbeit der nationalen Polizeien erheblich, indem sie es ihnen ermöglichen, gesuchte Personen auf der Grundlage jeder beliebigen Kontrolle zum Zwecke der Auslieferung zu identifizieren, zu lokalisieren und festzunehmen.

Wir leiten kurz nach einer Cyber-Infiltration rechtliche Schritte gegen Sie ein, um :

Kinderpornografie-Pädophilie-Cyberpornografie-Online-Masturbation

Zu Ihrer Information: Der Gesetzgeber hat erklärt, dass in Fällen, in denen die im Strafgesetzbuch vorgesehenen Verbrechen und Vergehen mithilfe eines Telekommunikationsnetzes begangen werden, die vorgesehenen strafrechtlichen Strafen verschärft werden.

Nach einer Untersuchung bestätigen wir, dass Sie diese Straftaten begangen haben, d. h. den Erwerb, den Besitz, die Anzeige, die Übertragung und den Abruf von Bildern und Videos mit exhibitionistischem oder kinderpornografischem Inhalt über das Internet (Anzeigenseiten, Seiten mit pornografischem Inhalt, Datingseiten, soziale Netzwerke).

Während der Untersuchung haben wir auch beobachtet, dass obszöne Inhalte von Ihnen auf Webseiten oder Netzwerken mit hohem Publikumsverkehr, auf denen sich viele 16-Jährige tummeln, verbreitet wurden.

Wenn Nacktheit auf diese Weise zur Schau gestellt wird, stellt dies eine Straftat der sexuellen Zurschaustellung vor der Öffentlichkeit und vor Minderjährigen unter 16 Jahren dar. Dieses Vergehen wird nach dem Gesetz streng bestraft.

Historische Bilder, nackte Videos von Ihnen und Minderjährigen, die durch Cyber-Infiltration aufgezeichnet wurden, stellen Beweise für Ihre Straftaten dar.

Sie werden gebeten, sich per E-Mail zu melden, indem Sie Ihre Rechtfertigungen schreiben, damit diese geprüft und verifiziert werden können, um die Sanktionen zu bewerten; dies muss innerhalb einer strikten Frist von 48 Stunden geschehen. Nach Ablauf dieser Frist müssen wir unseren Bericht an das Gericht in Ihrer Region weiterleiten, damit ein Haftbefehl gegen Sie ausgestellt werden kann.

Sie werden dann im Nationalen Register für Sexualstraftäter (NDSR) erfasst. In diesem Fall wird Ihre Akte auch an Vereinigungen zur Bekämpfung der Pädophilie und an die Medien zur Veröffentlichung als im NDSR registrierte Person weitergeleitet.

Frau NICOLLETA DELLA VALLE,
INTERPOL-DIREKTORIN
GENERALDIREKTION VON INTERPOL
Anschrift: Guisanplatz 1ACH-3003 Bern

NICOLLETA DELLA VALLE
DIRECTRICE DE FEDPOL

SEXTORTION – ERPRESSUNG NACH VERSENDEN VON NACKTFOTOS ODER VIDEOS

Dieses Phänomen ist leider öfters verbreitet, als man annimmt. Sowohl Jugendliche als auch Erwachsene chatten mit völlig fremden Menschen, welche für sie als zukünftige Partnerschaft in Betracht kommen. Der Chat verläuft immer mehr in sexueller Ausrichtung, bis letztendlich der Betrüger mit dem Fake – Account und falschen Bildern das Opfer dazu bringt auch echte freizügige Bilder, sowie Nacktfotos und Videos zu senden.

Jetzt ist das Opfer in die Falle getappt.

Nun zeigt der Betrüger seine wahre Absichten. Inzwischen hat der Betrüger alle Kontaktdaten ausgespäht und droht dem Opfer die Bilder an seine Freunde, Arbeitskollegen, seiner Familie und an all seine Kontakte zu senden. Er kann dies nur vermeiden, indem er Geld bezahlt. Jugendliche kaufen in dem Fall PaySafeCards von Google, Nintendo, Amazon oder Apple. Die CODES sind bares Geld wert und werden dem Täter übermittelt. KEIN EINZELFALL.

Beim Enkeltrick werden überwiegend ältere Menschen als Opfer ausgesucht und vorher auch ausspioniert.

Der Betrüger hat es auf das Geld abgesehen und will mit allen Mitteln unter größtem psychischen Druck die alten Menschen zu Zahlungen oder Geldübergaben bewegen. Es gibt unendlich viele Varianten.

Stimme des angeblichen Enkel ruft an und fragt ob die Oma ihn noch kennt. Er schildert eine finanzielle Notlage.

Ein angeblicher Polizeibeamter, Richter oder Staatsanwalt ruft von einer Unfallstelle an. Der Sohn oder Enkel hat eine Frau und ein kleines Kind totgefahren. SCHOCKANRUF

Die Oma soll viel Geld bezahlen oder Schmuck einem Beamten übergeben, damit der Sohn nicht eingesperrt wird. Hier wird mit Ängsten gespielt. Alle Daten der Oma sind den Tätern im Vorfeld bekannt !!!

Achtung! Falscher Polizist!

Einbruchserien

Ähnlich wie beim Enkeltrick mit dem fingierten Unfall und der angeblich tödlich verunglückten Person machen die Betrüger älteren Menschen Angst. Sie rufen an und erzählen, dass in der letzten Zeit sehr viele Einbrüche in der Wohngegend waren und sie deshalb alles Bargeld bei der Polizei sicherstellen.

Die ältere Person wird aufgefordert das Geld in einem Sack oder ähnlichem Behältnis vor die Tür zu stellen und die Täter kommen tatsächlich vorbei und holen das Geld ab. Die Geschädigten melden sich oft erst, wenn sie die Geschichte einem Verwandten erzählt haben oder wieder etwas Geld von der Polizei zurückwollen, um sich etwas kaufen zu können.

Alle Rufnummern sind entweder unterdrückt und mittels Internet erstellt oder handelt sich sogar um IP – Spoofing.

TODESANZEIGEN

AUCH WENN ES EINEM SEHR MAKABER ERSCHEINT, SCHRECKEN TÄTER NICHT MAL VOR DEM TOD ZURÜCK. SIE STUDIEREN REGELRECHT DIE TODESANZEIGEN UND DEREN ANGEHÖRIGE.

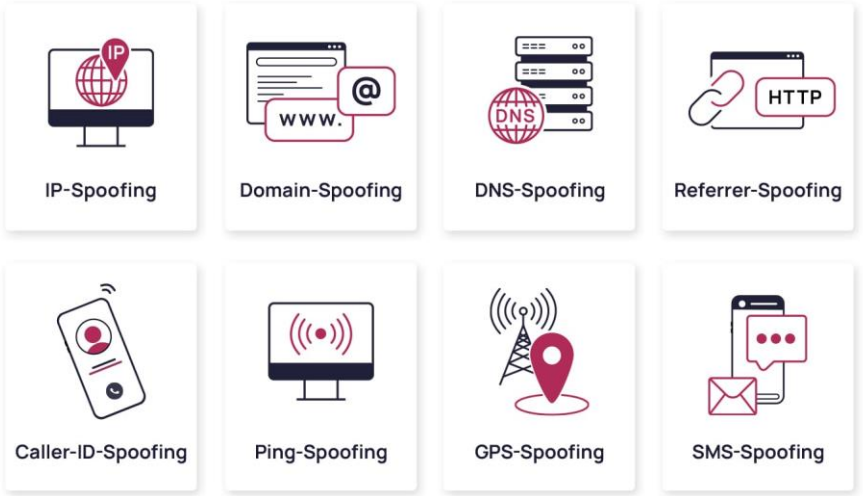
Die Hinterbliebenen sind in Trauer und sehr zugänglich. Ihnen wird vom Täter vorgegaukelt, dass sie ein entfernter Verwandter sind und unbedingt an der Trauerfeier teilnehmen wollen.

Unglücklicherweise haben sie nicht das nötige Kleingeld, da sie vom Ausland anreisen müssen. Deshalb hoffen sie auf eine Unterstützung. Das Ganze nur vorübergehend. Das Geld wird schließlich zurückgezahlt.

Leider stehen die Hinterbliebenen ohne die eingeladene Verwandtschaft am Grabmal und das Geld ist auch für immer weg.

Diese Masche wird von den gleichen Call-Center-Betrüger der organisierten Mafia vorgenommen, welche auch beim Enkeltrick äußerst aktiv sind.

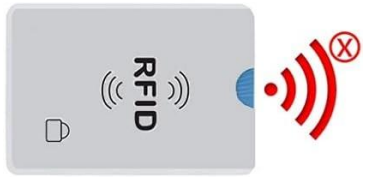
IP – SPOOFING & CALLER – ID - SPOOFING



Beim Spoofing wird eine echte vorhandene IP-Adresse oder echte Rufnummer vom Opfer verwendet, um eine andere Identität vorzutäuschen. Der Täter ruft an und lässt die echte Rufnummer der Polizei auf dem Display des Opfers anzeigen. In dem Fall ist die Polizei ein Opfer als Mittel zum Zweck. Dies geschieht alles über Server (Rechner permanent online im Internet). Das Ganze funktioniert auch mit Webadressen. Es gibt also immer das Opfer, dessen Daten verwendet werden und das Opfer, welches annimmt, das erste Opfer würde ihn kontaktieren.

NFC – NEAR FIELD COMMUNICATION

BEIM NFC handelt es sich um ein Daten-Übertagungssystem ähnlich wie WIFI, WLAN und Bluetooth. Reichweiten sind jedoch unterschiedlich. NFC bis 10 bis 20 cm, WLAN 100 bis 300 Meter, Blutooth bis 10 Meter.



Eine Bankkarte mit dem Sende-Symbol sendet automatisch beim Bargeldlosen Zahlen die Kontodaten an das Lesegerät im Geschäft. Sogenannte POS – Terminals.

Sind diese Karten in der Geldbörse und ein Betrüger läuft mit einem Zahlungsmittel-Lesegerät vorbei, kann er automatisch von Ihrer Karte Geld abbuchen lassen !!!

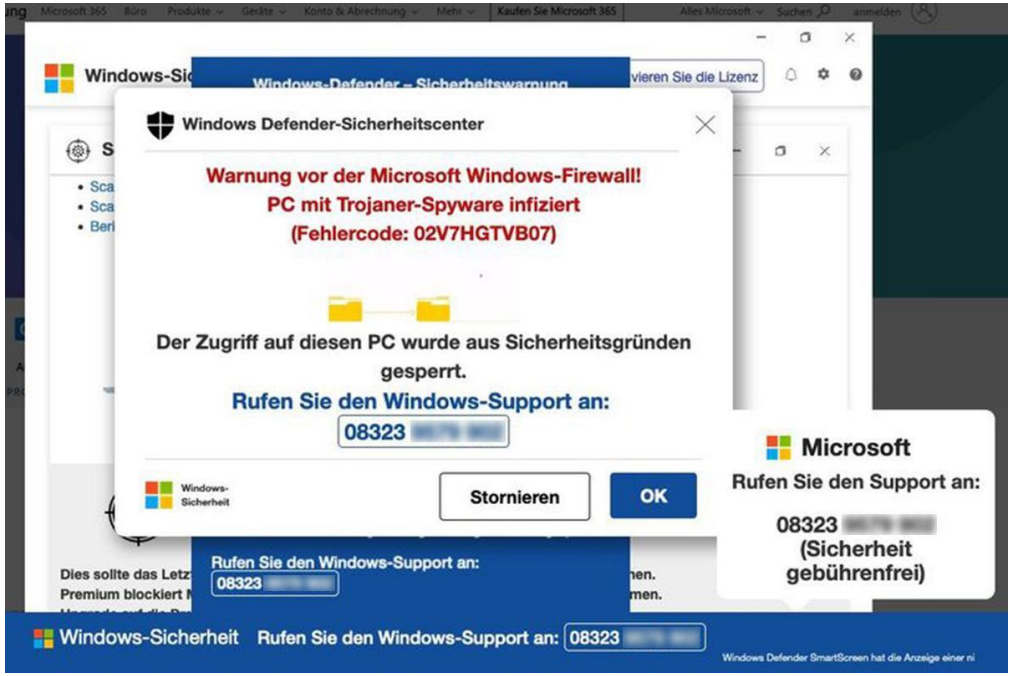
Solche Kartenlesegeräte kann JEDER frei kaufen. Betrüger koppeln ihr Handy und geben den Geldbetrag bis 50 Euro ein. Dann laufen Sie bei Ihnen vorbei und Sie überweisen kontaktlos !

Sie können sich schützen, indem Sie Blocker einsetzen. Überlagerung zweier Karten mit NFC hilft nicht !!!

Google Pay und Apple Pay sind wesentlich sicherer, da keine Echtdaten von Konten übertragen werden !!!

MITARBEITER VON MICROSOFT

Angeblicher Mitarbeiter von Microsoft ruft bei Ihnen auf dem Festnetz oder Mobiltelefon an. Oder sie befinden sich gerade online im Internet und es erscheinen Warnhinweise von Microsoft. In dem Fall wird ihnen schnelle Hilfe per Rufnummer angeboten.



- Sobald sie mit den Betrügern telefonieren, werden sie so sehr beeinflusst, dass sie am Ende einen Code eingeben. Plötzlich öffnen sich unendlich viele Ereignisanzeigen oder andere Protokolle von Microsoft, welche keine Viren oder Schadsoftware sind. Nun bekommen sie Angst, dass doch der Computer infiziert wurde. Die schnelle Hilfe wird angenommen.
- Die Betrüger senden eine Datei oder geben ihnen einen Link oder bitten Sie auf eine Webseite etwas herunterzuladen. Jetzt haben die Betrüger absolute Kontrolle über ihren Computer und Zugriff auf alle Dateien.
- Oftmals werden Sie gebeten das Mobiltelefon abzuschalten. So können die Täter unbemerkt PayPal und andere gehackte Konten nutzen. Sie erhalten keine Push-Up-Benachrichtigungen mehr auf dem Mobiltelefon.

„JA“ UND SCHON BETROGEN ?

BETRÜGER RUFEN MIT UNTERDRÜCKTER RUFNUMMER. OFTMALS WIRKEN DIE GESPRÄCHE ANFANGS SERIÖS. ES WIRD GEFRAGT, OB MAN SCHON VON DEN NEUEN SOLARMODULEN KENNTNIS HAT ODER AN UMFRAGEN TEILNEHMEN WILL.

Der Betrüger will lediglich ein deutlich ausgesprochenes „JA“ hören. Dies wird aufgezeichnet. Damit schließt der Betrüger Verträge bei LOTTO24 oder anderen Firmen auf ihren Namen ab.

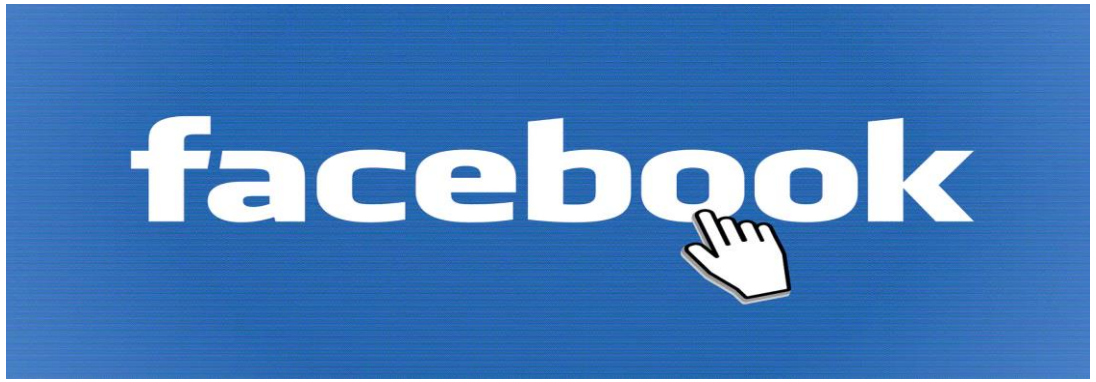
Nach europäischen Recht sind diese Verträge rechtsgültig. Sie müssen tätig werden und per Einwurfeinschreiben dem Vertrag während der Widerspruchsfrist von 14 Tagen widersprechen.

LAS UNS DOCH MAL ÜBER DIE ARBEIT SPRECHEN

EINE NEUE MASCHE DER BETRÜGER IST DAS FREUNDLICHE GESPRÄCH ÜBER DIE ARBEIT. MITTELS EINER AUSLÄNDISCHEN RUFNUMMER WERDEN SIE GEBETEN SICH PER WHATSAPP ZU MELDEN.

Sobald Sie Kontakt aufgenommen haben, versuchen die Betrüger

1. Daten von Ihnen zu erlangen (Phishing)
2. Sie als Warenagent oder Finanzagent anzuwerben
3. Den Abbruch des Gespräches vorzutäuschen, damit Sie kostenpflichtig zurückrufen. Solche PING ANRUFE werden nach Gebührenverordnungen des Auslands über die Handyrechnung sehr teuer vergütet (Kostenfalle).



Soziale Medien

Copyright ist kein deutsches Gesetz !

In Bezug auf **personenbezogene Daten und Persönlichkeitsrechte** finden in Deutschland folgende Gesetze Anwendung:

1. Recht am eigenen Bild

Grundsätzlich darf von keinem Menschen ohne dessen Zustimmung ein Bild oder Video angefertigt werden. Bei Verletzung der Persönlichkeitsrechte können zivilrechtliche Verfahren eingeleitet werden

2. Verbreitung von Bildern und Videos

Werden Bilder oder Videos über Soziale Medien – auch WhatsApp – ohne Zustimmung der Person weiterverbreitet, begeht dieser eine Ordnungswidrigkeit gemäß Kunsturheberrechtsgesetz.

3. Bilder in Notsituation oder höchstpersönlichen Lebensbereich

Werden Bilder an einer Unfallstelle gefertigt oder Personen im Badezimmer ohne Zustimmung fotografiert, stellt dies eine Straftat nach dem Strafgesetzbuch dar.

Bei FACEBOOK gilt Copyright nach amerikanischen Recht und auch deren allgemeinen Geschäftsbedingungen. Mit der Erstellung des Accounts willigt man ein, dass alle Persönlichkeitsrechte aufgegeben werden. Bilder dürfen ohne Zustimmung vom Betreiber der Webseite überall verkauft und verbreitet werden !!!

Auch für Drohnen mit Kamera gelten die gleichen Vorschriften bezüglich der Persönlichkeitsrechte !!!

Laut Drohnengesetz vom 01.01.2024 dürfen:

1. Drohnen ab 16 Jahren in SICHTWEITE geführt werden
2. Drohnen benötigen eine Haftpflichtversicherung
3. Für Bestandsdrohnen über 250 Gramm Gewicht (auch Bestandsdrohnen) benötigt man einen Drohnenführerschein (online gegen Gebühr beim Luftfahrtbundesamt
4. Drohnen müssen mit Piloten – ID sichtbar für Jedermann gekennzeichnet sein

Laut Manöverklasse A1 darf man Drohnen bis 900 Gramm Gewicht nah an unbeteiligte Personen vorbeifliegen lassen, aber auf keinen Fall Bilder anfertigen oder Videos aufzeichnen.

DROHNEN VERSICHERUNG

KREDITVERMITTLUNGSBETRUG

In den sozialen Medien werden unter Anderem auch Waren und andere Dienstleistungen angeboten.

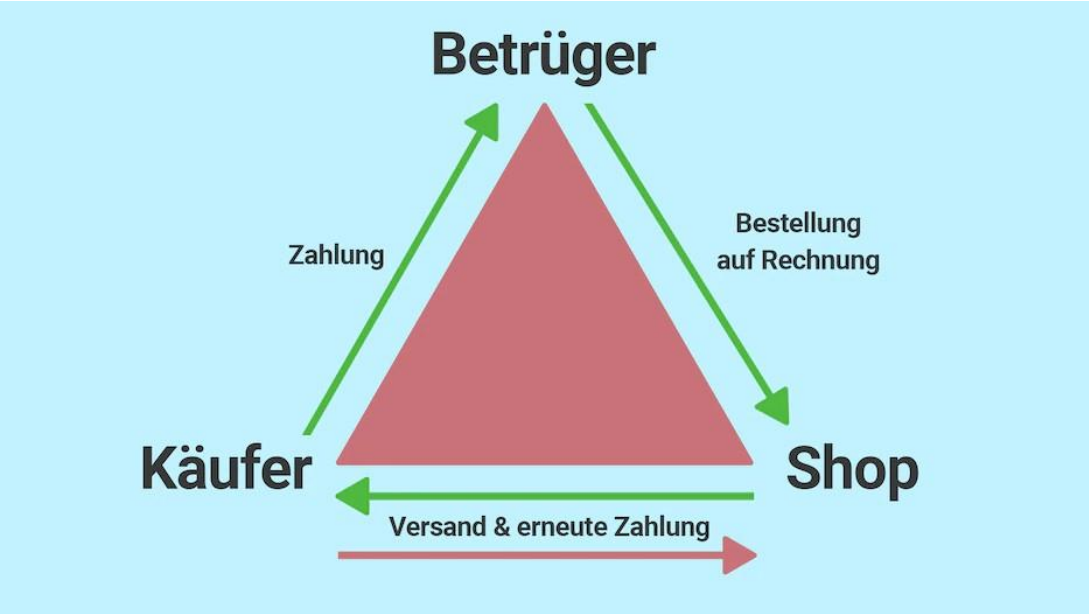
Meistens finde diese Geschäfte in Gruppen statt, denen man beitreten muss.

„Geld leihen und Freunde helfen“ (Kreditvermittlung)
„Gebrauchtes zu Schleuderpreisen“ (Warenbetrug)

In der Gruppe verleihen angeblich seriöse Menschen Geld zu unfassbar günstigen Konditionen oder sogar ohne Gegenleistung. Es werden augenscheinlich echte Verträge zugesendet. Sobald die Daten in den Formularen eingefügt sind und diese unterschrieben eingescannt zurückgesandt werden, fordern die Betrüger eine Gebühr nach der Anderen. Von der Kontoeröffnungsgebühr, Kontoführungsgebühr, Abschlussgebühr, Verzögerungsgebühr und Rückerstattungsgebühr der bereits gezahlten Beträge summiert sich das Ganze schnell auf mehrere hundert Euro, so dass das Opfer immer noch hofft das Geld zu erhalten.

DREI-ECKS-BETRUG – RAFFINIERTE BETRÜGER

Übersichtsskizze



Funktionsweise

- Käufer findet Webseite (Fake-Shop) des Betrügers
- Er bestellt seine Ware und bezahlt den Kaufpreis
- Täter erhält das Geld und bestellt bei einem echten Online – Shop exakt diese Ware mit den Daten des Käufers
- Käufer erhält die Ware
- Danach erhält der Käufer eine Zahlungserinnerung und muss die erhaltene Ware erneut bezahlen

Immer wenn der Betrüger die Daten des Geschädigten für Geschäftsverträge einsetzt, begeht er eine weitere Straftat wegen Fälschung beweiserheblicher Daten.

FONTS

Fonts sind normalerweise kostenlose Schriftarten. Wenn man diese lokal auf seinem Rechner herunterlädt sind diese auch zulässig.

Wenn man diese Fonts auf eigene Webseiten als Firmeninhaber oder auch als Privatperson verwendet, ist dies auch grundsätzlich zulässig, aber es gibt einige Anwälte, welche für die Betrüger arbeiten und Abmahnungen über hunderte von Euro an Webseiten – Betreiber senden.

Deren Begründung beruht darauf, dass die Besucher der Webseiten die Schriftarten nur nutzen können, da sie von der Webseite zur Verfügung gestellt werden und nicht auf deren heimischen Rechner installiert sind.

Es wird auch mit Inkasso – Büros zusammengearbeitet und mit Pfändungen gedroht.

Private Sammelklagen gegen Betrügerische Institutionen und Einzelpersonen laufen bereits. Diesen sollte man sich bei Erhalt eines amtlichen Schreibens von solchen Anwälten zeitnah anschließen.

SKIMMING – PHISHING DER DATEN AN GELDAUTOMATEN (VORGEHENSWEISE ÜBERWIEGEND IM AUSLAND)

Kartenleser wird mit Aufsatz manipuliert oder eine täuschend echt aussehende Tastatur wird angebracht.

Kartendaten werden ausgelesen, im Dark Web verkauft oder Dupletten der Karte (Daten werden auf einer leeren Karte transferiert) erstellt

In Deutschland wurden 99% aller Geldautomaten ausgetauscht. Ausnahme: BERLIN

WERBEBANNER AUF WEBSEITEN ODER SOZIALE MEDIEN (FACEBOOK) MIT BEKANNTEN PERSONEN

Gewinnversprechen mit einer Einmal-Wallet-Einlage

Mittels Künstlicher Intelligenz (KI) werden bekannte Personen (Millionäre oder Politiker oder erfolgreiche Schauspieler und Musiker) in den Werbe-Videos gezeigt, welche für die Investitionen in Kryptowährungen Werbung machen.

Diese Werbebanner sind IMMER Weiterleitungen zu den Betrügern !!!

Oftmals schreiben Täter Sie direkt in sozialen Medien an, damit Sie Interesse an Verkäufe digitaler Werke oder Käufe von Kryptowährungen bekommen.

Bekanntesten Kryptowährungen

1. Bitcoin
2. Ethereum
3. Tether
4. Binance
5. U.S. Dollar

Wie kann ich mich als Opfer schützen, wenn der Täter sogar Server wie bei T-Online oder Facebook „hacken“ kann ?

Der Täter arbeitet mit Programmen wie Viren, Malware, Trojaner, Würmer und auch Fernsteuerungssoftware,

Eine hunderprozentige Sicherheit gibt es zwar nicht, aber wenn man aufmerksam ist, kann vieles vermieden werden.

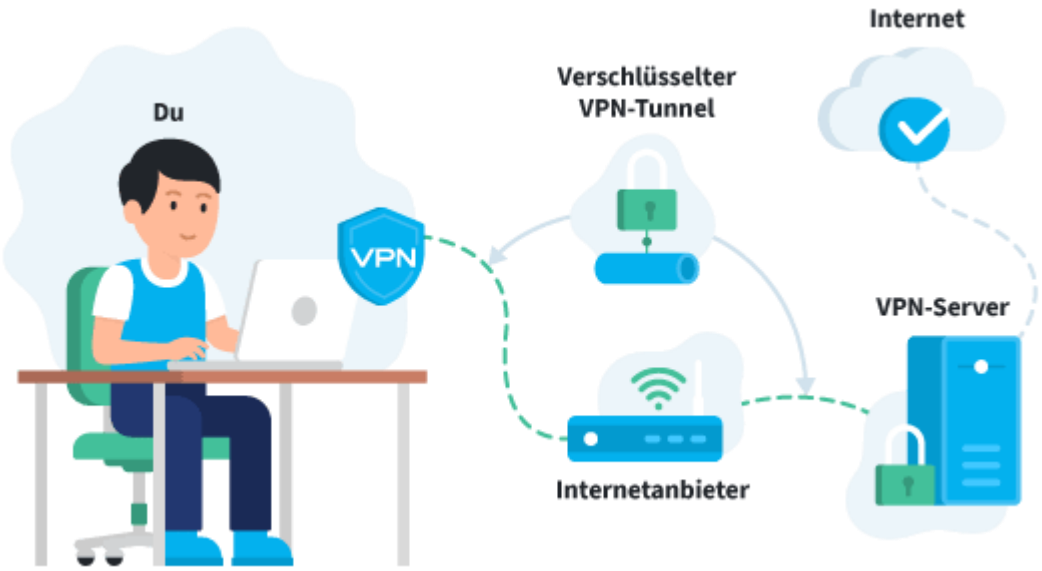
Man sollte drei E-Mail-Adressen besitzen. Eine als Kontakt-E-Mail-Adresse. Die zweite E-Mail-Adresse für die Registrierung und Bestellung bei Online-Shops und eine dritte E-Mail-Adresse ausschließlich für Bezahldienste wie Paypal. Kennwort mindestens 8 Zeichen und ein Sonderzeichen um den Standard einer SSL – Verschlüsselung zu entsprechen. Am Besten drei verschiedene Anbietern (T-Online, Web, GMX, mail, gmail, etc)

Zum Bezahlen nur Bezahldienste mit Käuferschutz nutzen.

Nutzen Sie die zwei-Faktor-Authentisierung. Man benötigt Zugangsdaten und ein Endgerät.

Bei Verdacht auf Betrug, erkundigen Sie sich bei der Polizei. Man kann nicht alles wissen, aber jeder kann nachfragen.

OFFENES WLAN UND VPN - TUNNEL



Wer von Ihnen eine FRITZ BOX zuhause hat, kann diese weltweit kostenlos als VPN – SERVER nutzen !!!

Wenn Sie am Flughafen, im Cafe oder Hotel ein FREE WIFI oder auch das Bayern WLAN vor Ort kostenlos nutzen, kann absolut jeder im gleichen Netzwerk ihre Daten abfangen und im schlimmsten Fall unbemerkt Schadsoftware bei Ihnen installieren.

Deshalb sollten Sie in solchen Netzwerken niemals E-Mail abrufen und schon gar nicht Online Banking nutzen. Andere Zugangsdaten auch nicht.

Sie können sich durch Nutzung eines VPN-Tunnels schützen. Daten werden verschlüsselt ins World Wide Web gesendet.

VIRTUAL PRIVATE NETWORK

CyberGhost

NordVPN

WIE KANN ICH MEIN KIND SCHÜTZEN, DASS BEREITS EIN SMARTPHONE BESITZT ?

EINE ÜBERWACHUNGSSOFTWARE BIETET DEN ELTERN EINEN GUTEN ÜBERBLICK, WAS IHR KIND IM INTERNET MACHT ODER MIT WEM ES KONTAKT HAT. AUCH EINE TRACKING-SOFTWARE IST EINE GUTE OPTION FÜR DEN STANDORT-ABRUF. ABER GRUNDREGELN SIND AUCH WICHTIG:

- Grundsätzlich sollten nur die Eltern Kontakte in das Telefonbuch eintragen. Ruft eine Person an, welche namentlich nicht angezeigt wird, weil sie nicht als Kontakt eingetragen ist, sollte Ihr Kind das Telefonat niemals annehmen, sondern Ihnen zeigen.
- Erhält Ihr Kind Nachrichten per SMS oder WhatsApp oder per E-Mail mit einem Button oder meistens blau hinterlegtem Link, soll es zu Ihnen kommen.
-- Hat Ihr Kind auf YouTube oder anderen sozialen Medien Informationen von Influencern oder anderen politisch oder sozial motivierten Leuten erhalten, sollten Sie mit ihrem Kind über das Thema reden. Nicht alles was im Internet erzählt oder gezeigt wird, entspricht der Wahrheit (manipuliert mit KI)
- Merken Sie, dass ihr Kind nach Verwendung des Mobiltelefons unüblich reagiert (schlecht gelaunt oder traurig) oder sich sichtbar „schlecht“ fühlt, sollten Sie mit dem Kind in Bezug auf Cybermobbing (Beleidigungen) oder Erpressung (Geldforderungen) reden.
- Sie kennen Ihr Kind am Besten und sollten auch deren Gefühlswelt im Blickfeld haben.

Digitale Helden fragen – Polizei antwortet