
INGENIEURHOCHSCHULEN
INGENIEURSCHULEN
FACHHOCHSCHULEN
DIPLOM-INGENIEUR
INGENIEUR
ABSCHLUSS
TECHNISCHE
UNIVERSITÄ
FH
ABSOLVENTEN
INGENIEURWESEN
TECHNISCHE
HOCHSCHULE
ENGINEERING
FRANKREICH
DEUTSCHLAND
SEIT
BEISPIEL
GESETZLICH
BAD ING
VON PHISH(ING) BIS VISH(ING)
VDI - AKIS-77 -
FRANK EWERT

Jeder von uns kennt solche Maileingänge:

DHL PAKET

Ihre Lieferung wartet auf Bestätigung

Sehr geehrte/r [redacted],

Ihre Sendung mit der Nummer **#9555648992661** wartet auf Ihre Bestätigung, damit die Lieferung bearbeitet werden kann.

Was müssen Sie tun?

Klicken Sie bitte auf den untenstehenden Link, um Ihre Lieferinformationen zu überprüfen und zu bestätigen:

Sendung bestätigen

Wenn Sie Fragen haben, wenden Sie sich bitte an unseren Kundenservice unter support@dhl.com oder rufen Sie uns an: 0800 123 456.

2025 © DHL. Alle Rechte vorbehalten.
Deutsche Post DHL Group, Charles-de-Gaulle-Straße 20, 53113 Bonn, Deutschland.

Wenn Sie keine weiteren Benachrichtigungen erhalten möchten, klicken Sie hier.

Unsubscribe

ING
Die Bank und Du

Neues Update wartet auf Bestätigung!

Aus Sicherheitsgründen haben wir unser System aktualisiert. Um sicherzustellen, dass Sie weiterhin problemlos auf Ihr ING Banking to Go zugreifen können, möchten wir Sie darüber informieren, dass der Authentifizierungsdienst für Ihr Konto am 21.10.2024 ausläuft.

Es ist wichtig, dass Sie die erforderlichen Verlängerungen rechtzeitig vornehmen. Wir empfehlen Ihnen, dies so bald wie möglich zu tun, um Unterbrechungen in Ihrem Service zu vermeiden. Ihre Sicherheit ist uns sehr wichtig, und wir arbeiten ständig daran, unsere Systeme zu verbessern und zu aktualisieren.

Bitte nutzen Sie den folgenden Link, um die Verlängerung vorzunehmen:

Jetzt aktivieren

Hinweis: Sie erhalten auch eine Bestätigungs-E-Mail, sobald der Update-Vorgang abgeschlossen ist.

Viele Grüße,
Ihre Kundenservice.

Impressum | Datenschutz

Die automatische Verlängerung ist fehlgeschlagen

Lieber Netflix-Abonnent,

Wir möchten Sie darüber informieren, dass beim Versuch, Ihr Abonnement zu verlängern, ein Problem aufgetreten ist. Leider hat dies zu einer vorübergehenden Sperrung Ihres Kontos geführt.

Um Ihren Zugriff auf unser breites Angebot an Filmen, Serien und Unterhaltung wiederherzustellen, aktualisieren Sie bitte so schnell wie möglich Ihre Zahlungsinformationen. Nach der Aktualisierung wird Ihr Abonnement sofort reaktiviert. Sie können Ihre Zahlungsinformationen aktualisieren, indem Sie die Schaltfläche unten verwenden.

Vielen Dank für Ihre anhaltende Unterstützung. Wir freuen uns darauf, Ihnen weitere großartige Unterhaltung auf Netflix zu bieten!

Kontoinformation aktualisieren

Wenn Sie Fragen haben oder Hilfe benötigen, steht Ihnen unser Support-Team gerne zur Verfügung.

Aufrichtig,
Das Netflix-Team

Netflix Services Germany GmbH
Unsubscribe
Help Center

Jeder von uns kennt solche Maileingänge:

Gemeinsamkeiten?

- **Renommierte Absender** mit mehr oder weniger Bezug zu einem selbst
- **Selten personalisiert**, meist allgemein gehaltene Anrede
- **Dringender Handlungsbedarf**
- **Link oder Anhang soll geöffnet werden**
- **Abfrage von sicherheitsrelevanten Informationen (Kennwörter, Bankdaten, Geburtstag etc.)**

Frage:
Um was handelt es sich wohl ??

WWM - Folge 1184

Was ist Phishing?

A: Eine Fischart

B: Ein Betrugsversuch per E-Mail oder SMS

C: Eine bestimmte Art von Musik

D: Eine Sportart

WWM - Folge 1184

Phishing ist nicht neu und in den Medien, trotzdem passieren aktuell noch solche Dinge:

- **Frau reagiert auf Phishingmail bzgl. *Update des Sicherheitsmedium sei notwendig*, gibt u.a. Handynummer an, kurze Zeit später erhält sie einen Anruf eines „seriös wirkenden, gutes Deutsch sprechenden Bankmitarbeiters“ der Sie um Unterstützung bei der Umstellung bittet:**
  - **Freigabe von 22 (!) „Testzahlungen“ per Smartphone (*Schaden > 10.000 EUR*) Telefonat dauerte über 30 Minuten!**
- **Mann reagiert auf Mail bzgl. *„Unstimmigkeit am Konto“*, erhält ebenfalls einen Rückruf „der Bank“ (O-Ton: „Bankmitarbeiter hatte türkischen Dialekt“) und muss ebenfalls „Prüf-TANs“ telefonisch weitergeben**
  - **Lastschriftrückgaben und Kleinkredit zum Kontofüllen, mehrere Echtzeit-überweisungen die in 20s beim Zielkonto sind (*Schaden > 12.000 EUR*)**
- **Ehepaar reagiert nach Urlaub auf Phishingmail bzgl. *Betrugsversuch mit den Kreditkartendaten* und gibt im „Bankportal“ sensible Daten (u.a. Ausweiskopie), Kontodaten und CVC-Code (dreistellige Sicherheitsnummer) ein (*Schaden > 4.700 EUR*)**

„Da muss ja dann die Bank haften“...

Da primäre **keine direkte Manipulation des OnlineBankings** durchgeführt (Viren, Trojaner), sondern die **Personen manipuliert** wurden, die Zahlungen mit ihren eigenen Sicherheitsmedien (PIN/TAN) selbst durchzuführen, ist es eine **Betrugsmasche** für die die Bank nicht haften muss* .

Die Bank wird, sofern die Zahlungen zeitnah gemeldet wurden, einen sogenannten **Rückruf** durchführen, aber oftmals werden die Anrufe Freitag abends durchgeführt und/oder das Geld gleich weitergeleitet...

Beim Inhaber des Zielkonto* handelt es sich hier in der Regel um ahnungslose „**Finanzagenten**“. Diese sind meist selbst auf „***Jobangebote***“ für „**lukrative Heimarbeit**“ oder „***gut bezahltes App-Testing***“ etc. hereingefallen.

Schmidt Vermittlung (support@arbeitsagentur.de) Kontakt hinzufügen 23.11.2016 17:13

An [redacted]

Sehr geehrte/r Arbeitsuchender,

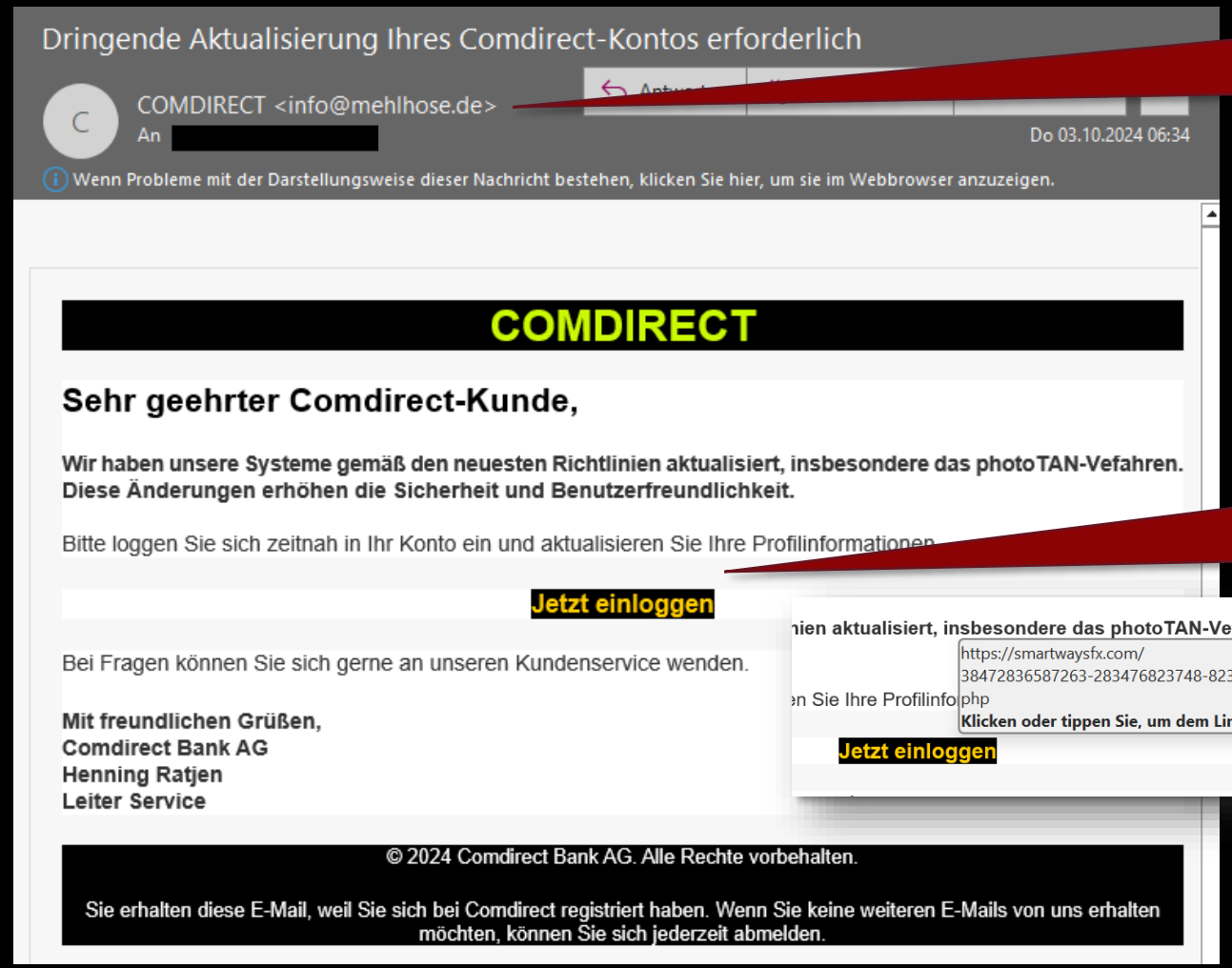
unsere Gesellschaft ist eine moderne und kundenorientierte Firma, die einen hohen Lohn und eine Menge Vorteile für die Mitarbeiter anbietet. Das Hauptanliegen unserer Tätigkeit ist die Optimierung der Geldflüsse und Trading mit Coins. Jedermann kann bei uns ohne Vorkenntnisse gleich anfangen Geld zu verdienen.

Unsere Gesellschaft bietet Ihnen einen attraktiven Zusatzverdienst bis zu 3600 Euro im Monat an, bei nur wenigen Arbeitsstunden pro Woche. Ihre Arbeitszeit ist variabel und kann Ihren Wünschen angepasst werden. Der Arbeitnehmer hat keine Ausgaben und muss keine besonderen Kenntnisse mitbringen.

Ihre Aufgabe ist es die Bitcoins für unsere Kunden zu erwerben, das Geld dafür bekommen Sie im Voraus und Ihren Verdienst von 20% behalten Sie gleich ein.

* Zielkonto landet dadurch oft auf einer Embargo-Liste und ist für Gutschriften gesperrt!

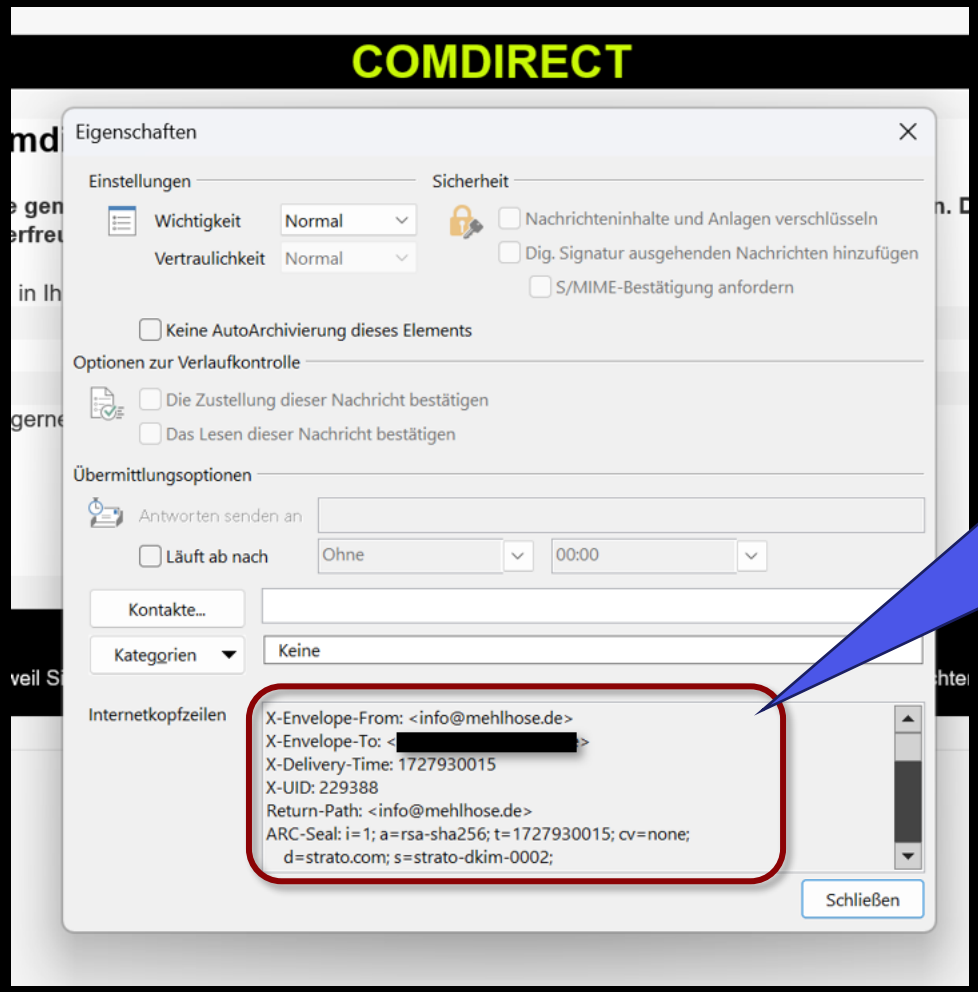
Analyse eine Phihingmail



Hier war der Absender nicht sorgfältig genug..

Auch hier hätte man das Ziel besser verschleiern können…

Analyse eine Phishingmail



Authentication-Results: strato.com;
dmarc=none header.from="mehlhose.de";
arc=none smtp.remote-ip=85.215.179.79;
dkim=none;
dkim-adsp=none;
spf=neutral smtp.mailfrom="info@mehlhose.de"

Analyse eine Phishingmail

Mechanismus	Bedeutung	Ergebnis	Erklärung
DMARC	Domain-based Message Authentication Reporting & Conformance		
ARC	Authenticated Received Chain		weiterzugeben.
DKIM	DomainKeys Identified		Die E-Mail enthält **keine gültige DKIM-Signatur**. DKIM prüft, ob der
DKIM-ADSP	DKIM Author Domain Signing Practices		
SPF	Sender Policy Framework	`neutral`	Die IP-Adresse `85.215.179.79` ist **nicht explizit erlaubt oder verboten** laut SPF-Eintrag der Domain `mehlhose.de`. Das bedeutet: Der SPF-Eintrag ist entweder nicht vorhanden oder unklar.

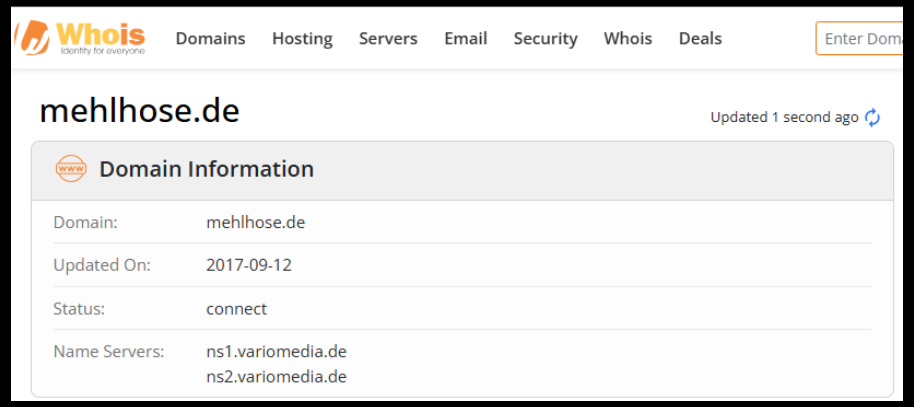
DMARC legt fest, wie mit nicht authetifizierbaren Mails verfahren wird:

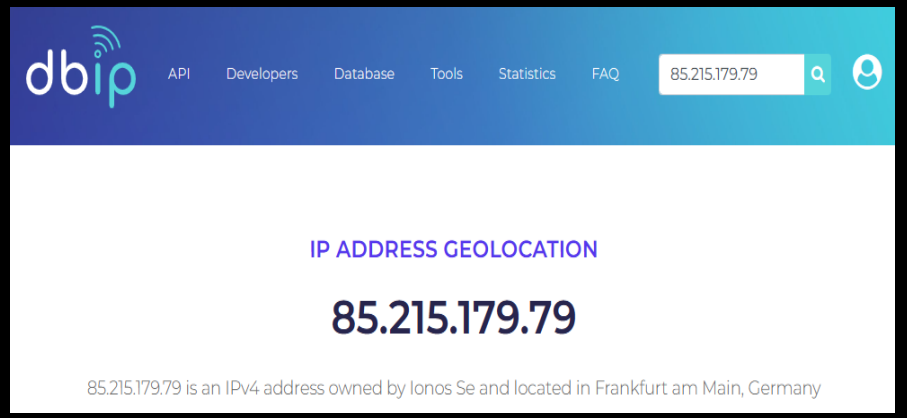
none, quarantine, reject

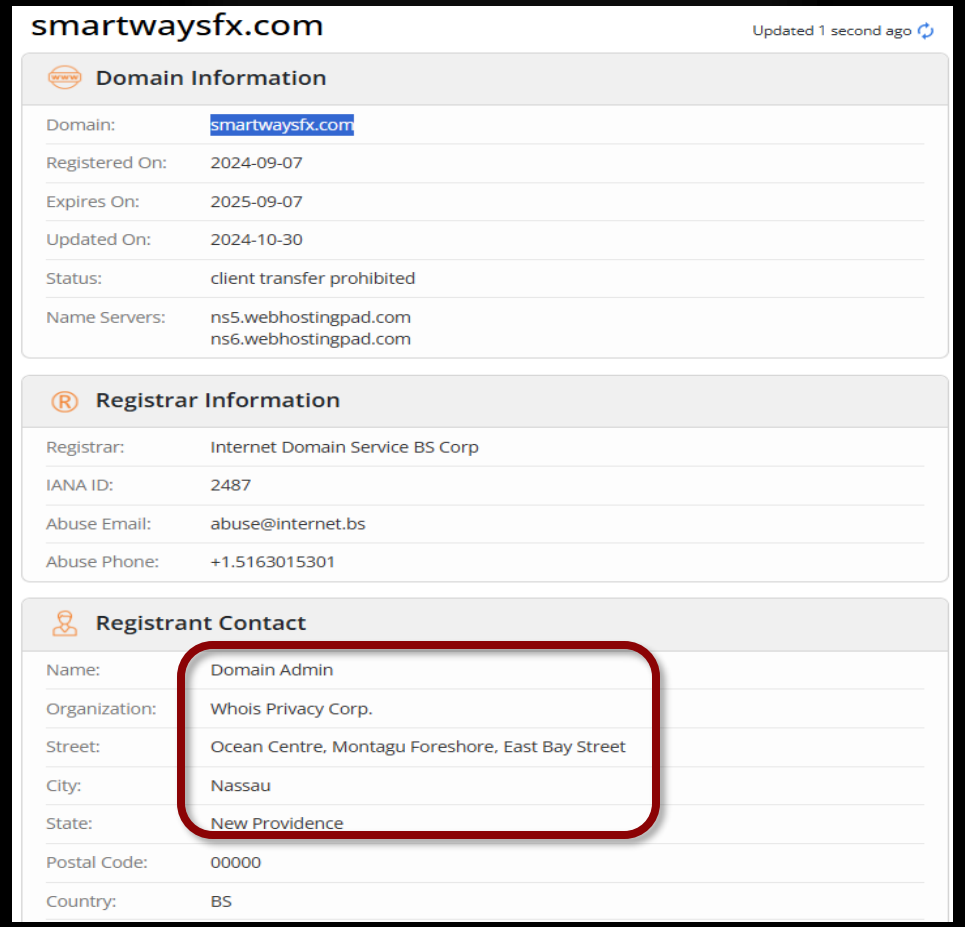
DKIM fügt eine Signatur des Absenders bei um dessen Authentität zu gewährleisten

ion-Results: strato.com;
e header.from="mehlhose.de";
mtp.remote-ip=85.215.179.79;
=none;
-adsp=none;
neutral smtp.mailfrom="info@mehlhose.de"

dmarc=none header.from="mehlhose.de";
arc=none smtp.remote-ip=85.215.179.79;







ACHTUNG – aktuelle Gefahr!

Seit Juni warnt die Verbraucherzentrale Niedersachsen vor Phishing im Umfeld von Booking.com und ähnlichen Anbietern:

- **Über den offiziellen Chat der Booking.com-App wurden Kunden gebeten, Ihre Kreditkartendaten für „eine erneute Überprüfung“ nochmals einzugeben, wobei diese Überprüfung zu realen Abbuchungen geführt hat**

- **Kunden wurde per nahezu originalen Mails und sogar Anschreiben gebeten, wegen technischer Probleme die Zahlungen über einen „alternativen Link“ durchzuführen. Die Zahlungen wurden dabei ebenfalls „wegen eines technischen Problems“ mehrfach abgelehnt, bevor dann eine Zahlung erfolgreich war. Alle Zahlungen wurden jedoch ordentlich ausgeführt!**

Social Engineering

Tom sah Ben an: „***Das ist doch keine Arbeit. Es macht mir Spaß, den Zaun zu streichen. Schwimmen kann ich jeden Tag, aber den Zaun streicht man nur einmal im Jahr. Das kann auch nicht jeder Junge***.“ Ben wurde nachdenklich. Er betrachtete Tom und nach einer Weile sagte er: „Tom, bitte, lass mich auch einmal streichen!“ Tom hielt ihm den Pinsel hin, aber dann zog er ihn schnell wieder zurück. „Nein, nein“, sagte er, „das geht nicht. Tante Polly sieht den Zaun nachher genau an. Man muss ihn ganz vorsichtig streichen, weil er an der Straße steht. Das kannst du bestimmt nicht.“ „***Aber ich mache es auch ganz vorsichtig, Tom. Lass es mich doch einmal versuchen! Ich schenke dir auch meinen Apfel***.“

Aus „Tom Sawyer und Huckleberry Finn“ von Mark Twain

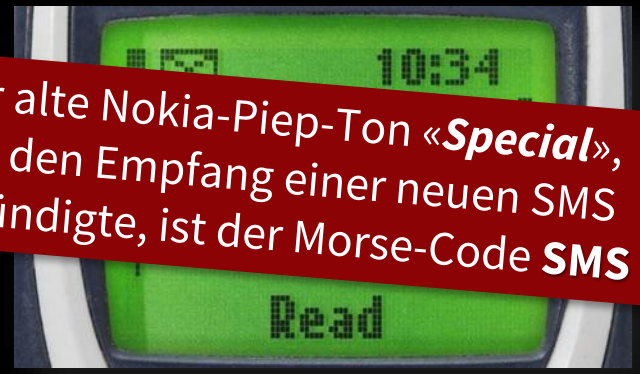
Phishing per SMS oder kurz SMISHING

Erste SMS
Am 3. Dezember 1992 wurde die erste SMS mit dem Text „Merry Christmas“ von Neil Papworth an einen Vodafone-Manager gesendet

Kommerzieller Start
Die SMS wurde erst 1994 auf der CeBIT in Hannover kommerziell eingeführt – zu einem Preis von 39 Pfennig pro Nachricht

Erste Smishing-Attacken
Die ersten Attacken begannen schon 2008, da ab da bei vielen Banken nun auch „Mobil-TAN“ bzw. „SMS-TAN“-Verfahren angeboten wurden

Polizeiliche Kriminalstatistik 2024
Smishing-Kampagnen auffallend stark angestiegen!



Der alte Nokia-Piep-Ton «***Special***», der den Empfang einer neuen SMS ankündigte, ist der Morse-Code **SMS**

PDP Delivery Update

Dear Customer,

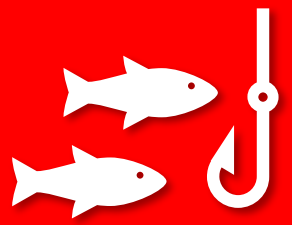
We were unable to deliver your package due to incomplete address information. Please update your address within the next 24 hours using the link below:

https://dpd.com-des.icu/de

To activate the link, please reply "Y," exit this message, and then reopen it, or copy and paste the link into your Safari browser.

Thank you for choosing PDP. We appreciate your prompt attention to this matter.

Best regards,
The PDP Team



PDP Delivery Update

Dear Customer,

We were unable to deliver your package due to incomplete address information. Please update your address within the next 24 hours using the link below:

https://dpd.com-des.icu/de

To activate t…k, please reply "Y," exit this messag… …r copy and pa… brov…

Thank y… appreciate you… …on to this matter.

Best regards,
The PDP Team

Webseite: com-des.icu

Bug:
PDP statt DPD…

Hermes®
am 8.07. haben wir versucht, Ihr Hermes Paket zuzustellen. Leider konnten wir Sie persönlich nicht erreichen und das Paket benötigt eine Unterschrift bei der Übergabe. Deshalb konnte die Zustellung nicht abgeschlossen werden.
Bitte vereinbaren Sie jetzt einen neuen Zustelltermin.
Hier neuen Termin auswählen:

https://myhermes.dwouaok.live/de

Sie haben folgen… …Möglichkeiten:
- Einen neuen Wu… … Wunschzeitraum f… auswählen.
- Das Paket a… umleiten lasse…

Antworte einfach mit ‚Y', schließe die SMS und öffne sie neu – dann wird der Link aktiviert. Falls er nicht klappt, kopier den Link und füg ihn direkt in Safari ein

Wichtiger Hinweis:
- Ihr Paket wird in unserem lokalen Lager bis zum 11. Juli aufbewahrt.
- Sollte bis zu diesem Datum kein neuer Termin vereinbart werden, wird Ihre Sendung an den Absender zurückgeschickt.
- Stellen Sie sicher, dass Ihre Kontaktdaten für Lieferaktualisierungen über Hermes aktuell sind.

Webseite: dwouaok.live

Gestern • 13:01

SMS/MMS-Austausch mit 0178 4611080

Hallo Mama/Papa, das ist meine neue Nummer. Mein Handy ist kaputt gegangen. Bitte schreib mir eine Nachricht auf WhatsApp! +49 178 4611080

Fr., 13:01

Achtung!
Dies leitet idR Fragen nach finanzieller Unterstützung oder gar Schockanrufe ein!!!

Weitere Szenarien: Finanzamtrückzahlung oder Gewinn freigeben

Q(u)ishing = QR-Code Phishing

QR-Codes

Die sogenannten Quick Respons-Codes dienen einer schnellen und fehlerfreien Kontaktmöglichkeit und finden sich mittlerweile nahezu überall...

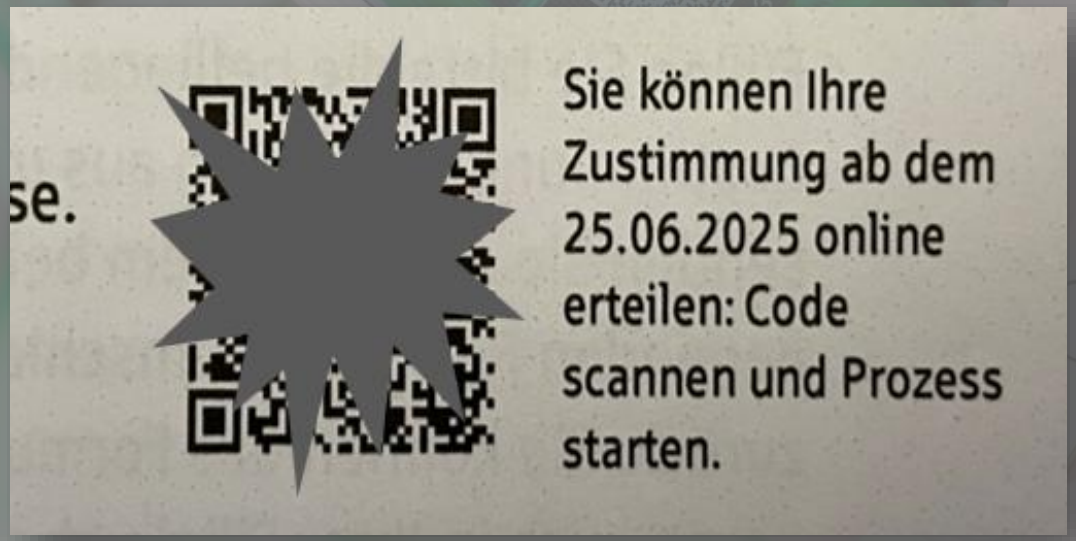
Beim Quishing werden die Original-Codes meist einfach überklebt und der Kunde, der bspw. die notwendige App zum Bezahlen des Parkplatzes herunter-laden möchte, erhält Schadsoftware und/oder bezahlt an eine falsche Bankverbindung!

Aufnahme privat

Q(u)ishing-Attacken

- **Kunden erhalten Briefe(!) von „Ihrer Bank“ mit der Bitte, *gesetzlichen Änderungen bei den Sicherheitsverfahren zuzustimmen**. Damit der Aufwand gering bleibt ist ein QR-Code beigefügt**

  Ziel ist eine Phishingseite die u.a. eine Drive-by-Infektion versucht



- **Ebenfalls per Post wurden Briefe mit *vermeintlichen Geschwindigkeits-übertritten (Strafzettel)* verschickt (Ohne Kennzeichen!) und bei sofortiger Bezahlung mit einem Rabatt und keiner weiteren Strafen-verfolgung gelockt…**

Darf ich vorstellen:

~~Adam from the Microsoft...~~

Nein, er ist ein „VISHER*“!

* V = Voice

ISHER = Phisher

Zur Info:

2024 entstand laut Bitkom e.V. in Deutschland

ein Schaden durch Cybercrime gesamt von 178,6 Mrd EUR

In Deutschland gingen 2023 laut BKA über

7,4 Millionen Euro durch Tech-Support-Betrug verloren

Laut FICO (Fair Isaac Corporation) betrug 2023

der durchschnittliche Verlust pro “Bankmitarbeiter-Anruf“

ca. 1.800 EUR

Vishing – Beispiele

Wie sehr die Opfer Ihren Betrügern vertrauen möchte ich an zwei Vorgängen aufzeigen:

Über eine „Incident“-Meldung des Rechenzentrums wurde mehrere auffällige Zahlungen gemeldet, eine umgehende Rücksprache mit dem Kunde wurde angefordert.

Ein Anruf beim Kunde bestätigte, das er „*auf der andren Leitung mit Microsoft telefoniert und die ihm seinen verseuchten PC bereinigen*“. Der Kunde bestand darauf das Microsoft am Telefon war und auch die Zahlungen nach Litauen (insgesamt bis dahin über 25.000 EUR!) „*nur Testzahlungen seien die sowieso nicht ausgeführt werden*“

Erst eine Kontosperre und eine Konferenz (Anruf) mit dem persönlichen Kundeberater brachten den Kunden dazu, das Telefonat mit dem Visher zu beenden, jedoch nicht ohne um einen zeitnahen Rückruf zu bitten…

Vishing – Beispiele

Wie sehr die Opfer Ihren Betrügern vertrauen möchte ich an zwei Vorgängen aufzeigen:

Kunde wurde von einem Finanzberater einer „renommierten, amerikanischen Investmentbank“ wegen eines tollen Angebots mit großer Rendite angerufen. Er zahlte daraufhin monatlich Beträge > 1.000 EUR und erhielt neben einem „Kontoauszug“ vierteljährlich kleinere Beträge (< 300 EUR) gutgeschrieben…

Nach über 1,5 (!) Jahren sei sein Gewinn auf über 2,4 Mio. Dollar angewachsen und er beantragte eine Auszahlung. Man teilte ihm mit, er müsse erst eine „*in Amerika übliche Vorablösesteuer*“ von knapp 700.000 EUR anweisen damit man ihm das Geld auf sein deutsches Konto übertragen würde. Hierfür wollte er einen Kredit bei seiner Bank aufnehmen….

Eine kurze Überprüfung seiner eingereichten Dokumente ergab:
- **die Webseite der Investmentfirma wurde am Tag seiner ersten Zahlung registriert**
- **laut Google Maps befand sich die Firmenadresse in einem Sumpfgebiet in Florida**
- **die Telefonnummern auf den „Kontounterlagen“ existierten nicht**

Selbst die von der Bank hinzugezogene Polizei konnte den Mann nur schwer überzeugen einem Betrüger aufgesessen zu sein….

Visher = die dunkle Seite der Callcenter

Der Film „The Beekeeper“ (2024)

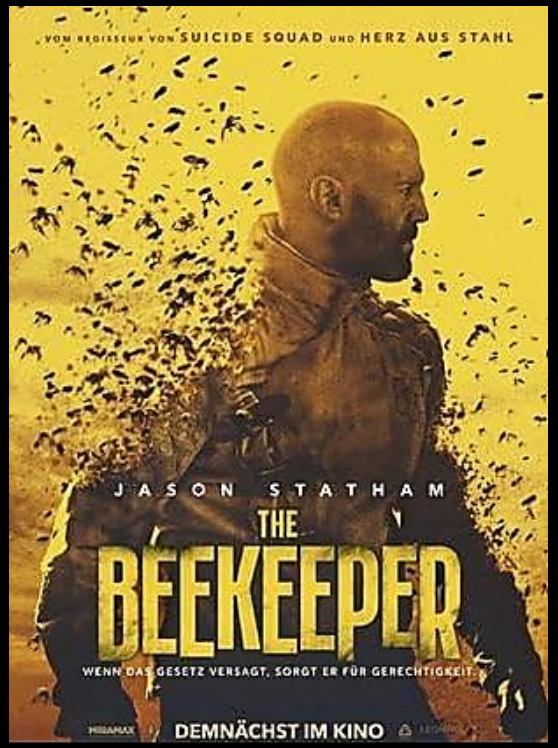
Der Film behandelt in gewohnter „Jason Statham“-Manier den Kampf gegen ein Visher-Callcenter, das für den Selbstmord einer älteren Dame, die um sämtliches Geld (eigenes wie treuhänderisch verwaltetes) gebracht wird.

Zwar ist alles fürs Kino aufgebauscht, aber im Grunde spielt sich ein Vishing-Telefonat so ab:

- falsches Vertrauen schaffen (Hilfe/Unterstützung)
- Erzeugung von Panik unterbindet rationales Denken
- Spoofing von Nummern (Bank, Polizei o.ä.)

Mittlerweile auch:

KI-generierte Stimmen/Videos (Deepfakes) ⇨ LoveScamming



Abruf am 14.07.25
https://www.imdb.com/de/title/tt15314262

Visher = die dunkle Seite der Callcenter

Abruf am 14.07.25
https://www.focus.de/panorama/welt/anne-laesst-sich-fuer-falschen-brad-pitt-scheiden-und-schickt-830-000-euro-an-betrueger_b56c6b6f-1ddb-4a42-99bc-026d5b6f4f49.html

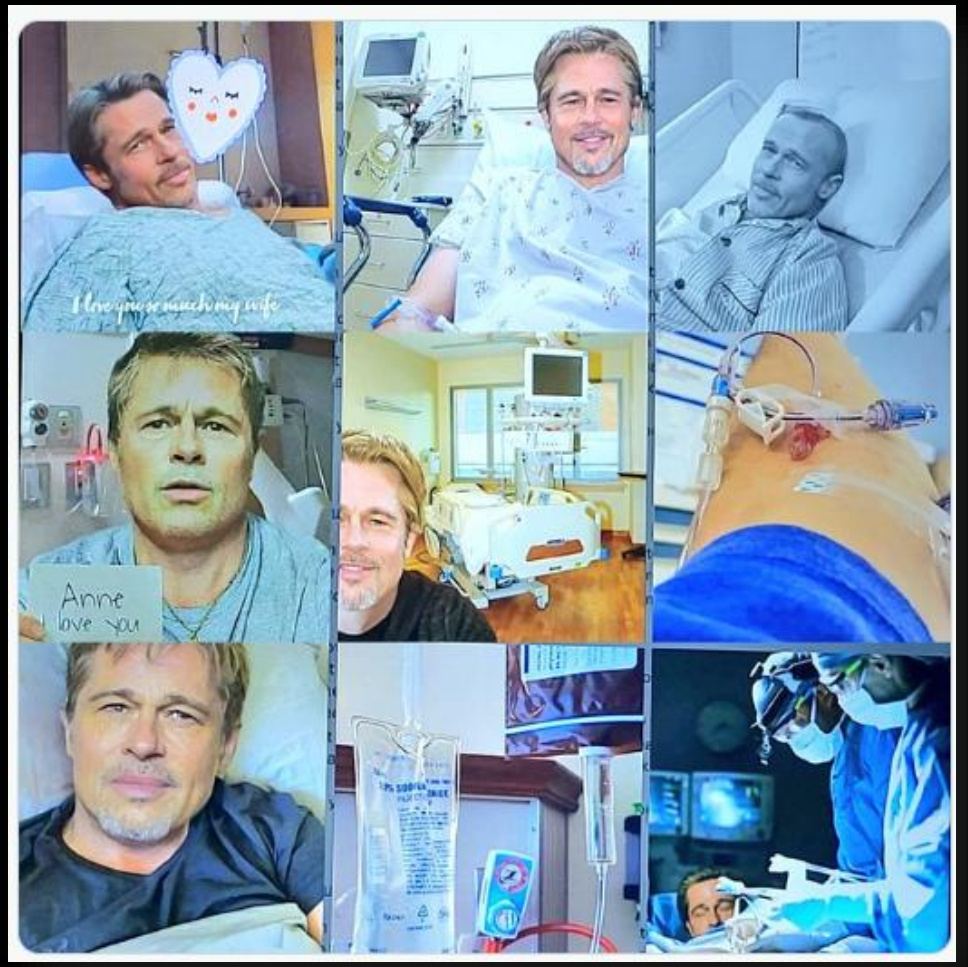
LoveScamming

Zwar handelt es sich bei dieser Betrugsmasche nicht direkt um Vishing, jedoch werden die gleichen Methoden genutzt.

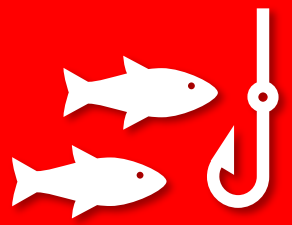
Und da Bilder mehr als 100 Worte sagen können neben der KI-Stimme auch gleich „Selfies“ geschickt werden!

Mit ausreichender Rechen-leistung sind mittlerweile sogar FaceTime- Anrufe möglich, die die Authentizität vermeintlich erhöhen!

Visher = die dunkle Seite der Callcenter



Abruf am 14.07.25
https://www.focus.de/panorama/welt/anne-laesst-sich-fuer-falschen-brad-pitt-scheiden-und-schickt-830-000-euro-an-betrueger_b56c6b6f-1ddb-4a42-99bc-026d5b6f4f49.html



Wie schütze ich mich?

Den wichtigsten Schutz haben Sie gerade erhalten, Sie haben sich informiert!

In Punkto Sicherheit muss man sich jederzeit neu informieren, da sich gerade in diesem Bereich nahezu täglich neue Szenarien ergeben.
Dank hier auch an Dieter Carbon der Ihnen dies monatlich bietet!

Bleiben Sie immer skeptisch

Hinterfragen Sie die Mails/SMS/Anrufe, ist das überhaupt plausibel?
Warum ruft mir die Bank Freitagabend 21 Uhr an??

Lassen Sie sich nicht unter Druck setzen!

Wie wir gesehen haben wird der Druck erhöht, um die Situation nicht rational zu betrachten. Sagen Sie deshalb, die Zeit ist aktuell ungünstig und sie möchten zurückrufen – sie werden vermutlich keine Ihnen bekannte Nummer erhalten bzw. Sie bekommen das Angebot, zurückgerufen zu werden. Kontaktieren Sie bspw. Polizei bzw. Bank unter den realen Telefonnummern!

Wie schütze ich mich?

Machen Sie mit Ihrer Familie Codewörter/-floskeln aus

Wenn Ihnen „Ihr Kind“ anruft, das es einen schweren Unfall hätte und sofort Geld für eine Kaution braucht, verwenden Sie die bekannte Floskel auf die die korrekte Antwort folgen muss. Oder sprechen Sie über eine für Dritte unbekannte Person:

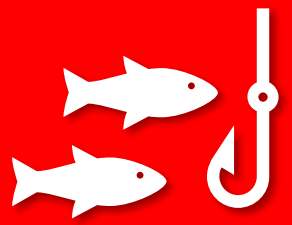
„ Was, so ein Unfall wie beim Kollegen von Deinem Vater? War das nicht der Klaus dem das letztes Jahr auch passiert ist?“

Bleiben Sie undurchschaubar

Wie Zauberkünstler/Mentalisten verstehen sich gut geschulte „Visher“ auf sogenanntes „cold reading“, bei dem während des Gespräches notwendige Informationen unbemerkt erfragt und anschließend zur Bestätigung gegen das Opfer eingesetzt werden.

Verifizieren Sie vermeintliche Rufnummernwechsel

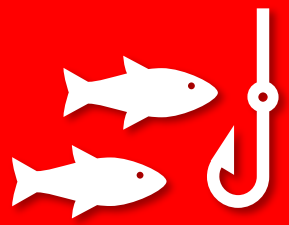
Wenn Sie über einen Rufnummerwechsel informiert werden einfach unter der bekannten Nummer nach der Echtheit nachfragen...



Übersicht der Warnsignale

- **Unbekannter Absender**
  Seltsame Telefonnummern oder Kurzcodes, die nicht zu bekannten Unternehmen gehören
- **Verdächtige Links**
  Verkürzte URLs (bit.ly, TinyURL) oder Domains, die nicht zur angeblichen Organisation passen
- **Persönliche Daten erfragen**
  Seriöse Unternehmen fragen niemals nach PIN, TAN oder Passwörtern
- **Unpersönliche Anrede**
  "Lieber Kunde" statt Ihres Namens
- **Falsche Logos**
  Leicht veränderte oder pixelige Firmenlogos
- **Unpassende Zeiten**
  Nachrichten außerhalb der Geschäftszeiten
- **Übertriebene Angebote**
  Unrealistische Versprechen oder Rabatte
- **Ungewöhnliche Aufforderungen**
  Sofortmaßnahmen, die von der normalen Kommunikation abweichen

Die Kunst der Erkennung liegt darin, diese Signale zu kombinieren und zu bewerten. Ein einzelnes Warnsignal kann ein Versehen sein, aber mehrere Hinweise zusammen sind ein klarer Indikator für Betrug.



Zusätzliche Infos:

Kostenloser Sperrnotruf (Kreditkarten, OnlineBanking etc.)

Telefonnummer 116 116

Buchtipp zu Social Engineering

Kevin D. Mitnick: Die Kunst der Täuschung, MITP-Verlag

Bilder

Sofern nicht andersweitig angegeben stammen alle verwendeten Bilder lizenzfrei von www.pexels.com oder www.pixabay.com

Haben Sie noch Fragen???

Falls diese erst später kommen, dann gerne über Dieter Carbon an mich weiterleiten lassen...