AVANTEC
Competence. Security. Trust.

Weil Sicherheit alles ändert.

Matthias Geiser (Principal Security Engineer) geiser@avantec.ch

26. März 2026

AVANTEC
Competence. Security. Trust.

E-Mail Security Evolution: Der Posteingang als Risiko

A Brief History of Mail

26. März 2026

A Brief History of Mail

AVANTEC
Competence. Security. Trust.

- 1971
  - Das erste E-Mail wurde von Ray Tomlinson zwischen zwei Rechnern im Arpanet verschickt.
  - Erfindung der "E-Mail Adresse" mit dem @, kaum genutztes Zeichen im ASCII Zeichensatz
- 1973
  - erste Versionen von TCP durch Vinton Cerf und Robert Kahn
- 1981
  - RFC 790-792, TCP/IP
- 1982
  - RFC 822, Standard for the format of Arpa Internet Text Messages
    - RFC 5322, Internet Message Format
  - RFC 821, Simple Mail Transfer Protocol
    - RFC 5321, Simple Mail Transfer Protocol
- 1983 Umstellung des Arpanet auf IP -> Geburt des Internet

A Brief History of Mail

Mailversand

AVANTEC
Competence. Security. Trust.

- E-Mails werden heute meist per SMTP im Internet versendet
- Mailbox, BBS (bulletin board systems)
- Netze:
  - FidoNet (1984), weltweit maximum 37'000 Nodes)
  - MausNet (1988), DACH
  - Z-Netz (Zerberus) (1992)
- Usenet (1979)
- Öffentliche Nachrichten auf «Schwarzen Brettern»
- Kommunikation ursprünglich per UUCP (Unix to Unix Copy)
- Später dann per nntp (network news Transport Protocol) übers Internet

Email-Missbrauch

Spam

- Unnötige Massennachrichten im Usenet
- 3.5.1978
  - erstes Massenmail vom DEC an ein paar hundert User, Werbung für neue Computer
    - Buffer Overflow: Zuviele Adressen im «To»
    - DoS durch Verbrauch von zu viel Speicherplatz
- 1970
  - Sketch von Monty Python, wo das Wort Spam so oft verwendet wird, dass eine vernünftige Kommunikation nicht mehr möglich ist.
- 1994
  - Werbekampage für Green Cards in vielen Newsgroups des Usenets

Gegenmassnahmen

AVANTEC
Competence. Security. Trust.

- ~2002
  - Sendmail mit Trend Micro VirusWall auf Solaris und Linux
- 1998
  - Brightmail Anti-Spam, 2004 von Symantec übernommen
    - https://en.wikipedia.org/wiki/Brightmail
- ~2004
  - MailFrontier
- Pattern basierte Inhaltserkennung (Viagra, ...)
- IronPort Email Appliances, 2000 gegründet, 2007 von Cisco übernommen.
  - Zuerst mit Brightmail Anti-Spam Engine, dann mit eigenem Spamfilter
  - Reputation der Sender IP Adresse

Email-Missbrauch

Phishing

Betrug per Email

- Ende 1990er
  - Zugangsdaten für online Dienste wie ICQ, später Online-Banking
  - Schadprogramme im Anhang oder via Link
    - Keylogger
      - Zugangsdaten
      - Identitätsdiebstahl
    - Kryptolocker
      - Erpressung

AVANTEC
Competence. Security. Trust.

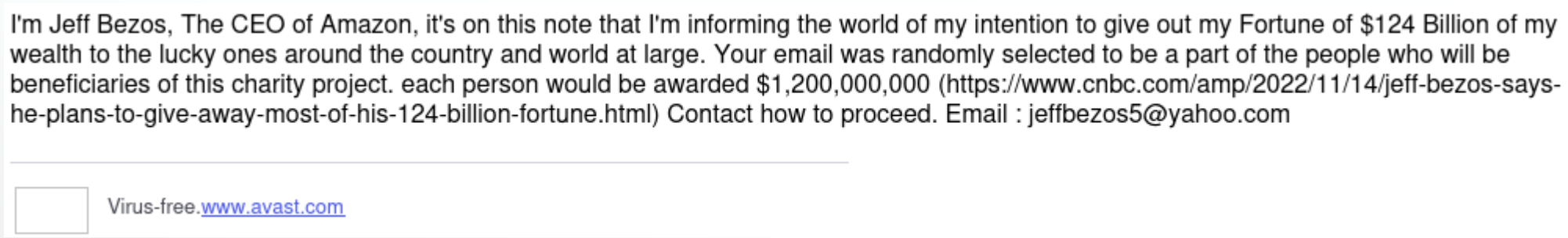
Phishing

Beispiele von einfachen Klassikern bis komplexen modernen Angriffen
Und wie wir diese erkennen können

26. März 2026

Phishing

Normal - English



I'm Jeff Bezos, The CEO of Amazon, it's on this note that I'm informing the world of my intention to give out my Fortune of $124 Billion of my wealth to the lucky ones around the country and world at large. Your email was randomly selected to be a part of the people who will be beneficiaries of this charity project. each person would be awarded $1,200,000,000 (https://www.cnbc.com/amp/2022/11/14/jeff-bezos-says-he-plans-to-give-away-most-of-his-124-billion-fortune.html) Contact how to proceed. Email : jeffbezos5@yahoo.com

Virus-free.www.avast.com

- From: mpraveen@fsinv.in
- To: user@customer.ch
- Reply To: jeffbezos5@yahoo.com
- EHLO: mail.srikaragold.com
- EHLO IP: 103.125.163.50
- Reverse DNS: static-103-125-163-50.pol.net.in

- Inhalt: Money, CEO, ...
- IP: schlechte Reputation

Erkennungsmöglichkeiten

AVANTEC
Competence. Security. Trust.

- IP Reputation
- Keywords

Phishing

Normal - Deutsch

Mein Name ist Bill Gates, ich bin US-amerikanischer Unternehmer, Philanthrop und Gründer von Breakthrough Energy sowie Mitbegründer der Microsoft Corporation. Über die Jahre habe ich einen bedeutenden Teil meines Vermögens wohltätigen Zwecken und globalen Entwicklungsprojekten gewidmet. Um weiterhin einen positiven Beitrag zu leisten, habe ich mich verpflichtet, im Jahr 2026 weitere 40 % meines Vermögens an ausgewählte Personen weltweit zu spenden. Sie wurden ausgewählt, im Rahmen dieser globalen philanthropischen Initiative eine persönliche Spende in Höhe von 5.500.000,00 € zu erhalten. Mehr über mich erfahren Sie unter folgendem Link: https://en.wikipedia.org/wiki/Bill_Gates https://www.bbc.com/news/articles/cx2e87lzqkdo ========== Herzliche Grüße, Bill Gates, Gründer von Breakthrough Energy, Mitgründer von Microsoft If you are interested in receiving this donation of €5,500,000.00, please feel free to contact me for further details on how to proceed.

- From: "Mr. Bill Gates" manager@antcareltd.com
- To: Recipients manager@antcareltd.com
- Bcc: user@customer.ch
- Reply To: billgatesfoundation@freecashdonation.net
- EHLO: server.hawkandowltrust.org
- EHLO IP: 91.192.195.168
- Reverse DNS: server6.webtechdesign.com

- Inhalt: Money, CEO, ...
- IP: ok Reputation
- Empfänger nur im BCC
- Reply To

Erkennungsmöglichkeiten

AVANTEC
Competence. Security. Trust.

- Keywords
- IP Reputation
- Eigenschaften
  - Nur BCC
  - Displayname hat nichts mit Mailadresse zu tun
  - Reply To

Phishing

Schlechtes Deutsch

Nach den letzten Berechnungen Ihrer haben wir festgestellt, dass Sie Anspruch auf eine Rückerstattung in der Höhe von 376.00 CHF haben.

Bitte beachten Sie, dass diese Rückerstattung nur für einen begrenzten Zeitraum verfügbar ist. Wir empfehlen Ihnen, den Prozess so bald wie möglich abzuschließen.

Im oben genannten Fall leisten wir folgende Zahlung:

Betrag: 376.00 CHF
Zahlungsdatum: 25 Februar 2026

Wir überweisen Ihr Guthaben auf das von Ihnen gewünschte Konto:

Bestätigen Sie Ihre Rückerstattung im AXA-Kundenportal.

- Subject: Wir Ã¼berweisen Ihr Guthaben auf das von Ihnen gewÃ¼nschte Konto.
- From: "AXA | Switzerland“ pedro.gonzalez03@unicaribe.edu.do
- To: user@customer.ch
- Reply To: jonypare94@gmail.com
- EHLO: mail-wr1-x442.google.com
- EHLO IP: 2a00:1450:4864:20::442
- Reverse DNS: mail-wr1-x442.google.com

- Inhalt: Sprachliche Fehler
- Subject: Probleme mit Umlauten
- From: Name ungleich Mailadresse
- Reply-To: Freemailer
- Verschickt über Google

Erkennungsmöglichkeiten

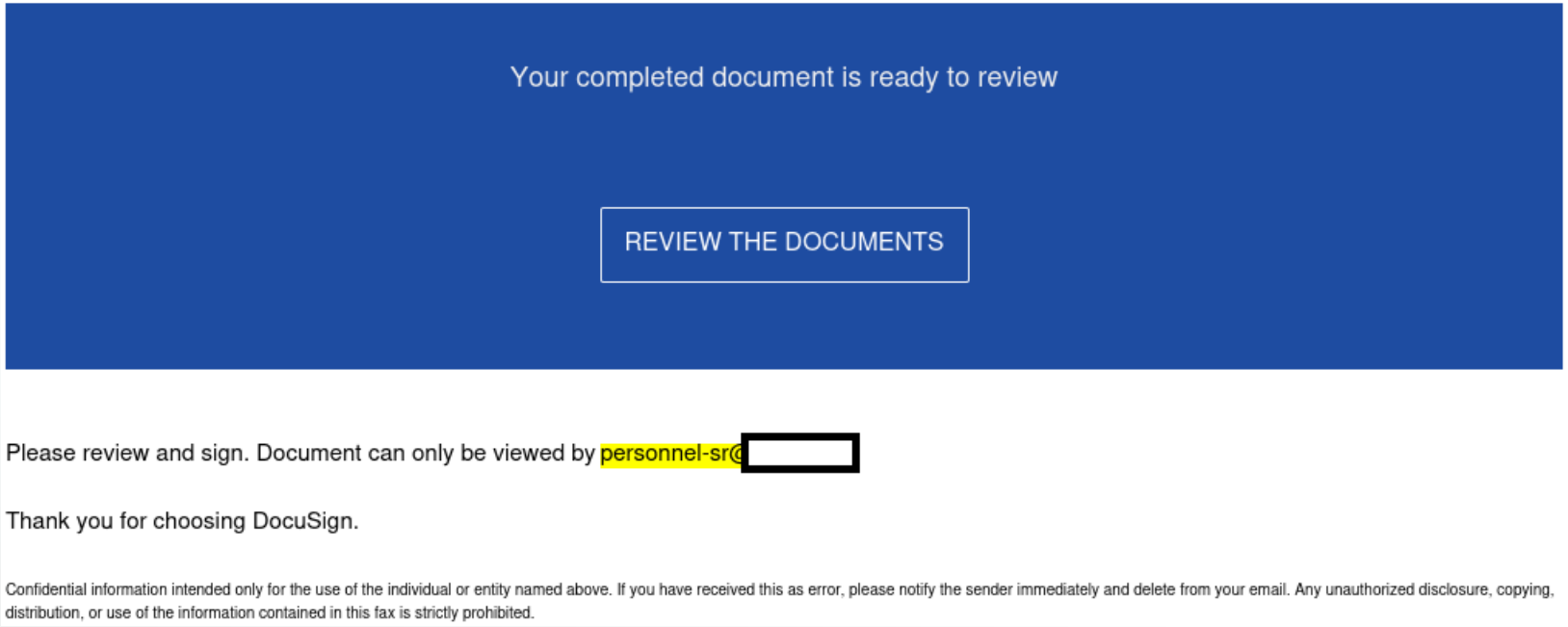
AVANTEC
Competence. Security. Trust.

- Keywords
- IP Reputation
- Eigenschaften
  - Nur BCC
  - Displayname hat nichts mit Mailadresse zu tun
  - Reply To
  - Freemailer
  - Encoding-Probleme
  - Sprach-Probleme

Phishing

International

Bekannte Services



- Subject: (Sign and Review Agreement)PDF Ref-SMK95816
- From: tom.valletta@kmtire.com
- To: user.name@customer.ch
- EHLO IP: 209.85.214.225
- Reverse DNS: mail-pl1-f225.google.com
- Link: https://broadridgefinancial-mid-prod8.campaign.adobe.com/r/?id=h11336a...

- Inhalt: ähnlich berechtigter Mails
- Verschickt über Google
- Link hat nichts mit DocuSign zu tun
- Link mit embedded URL

Erkennungsmöglichkeiten

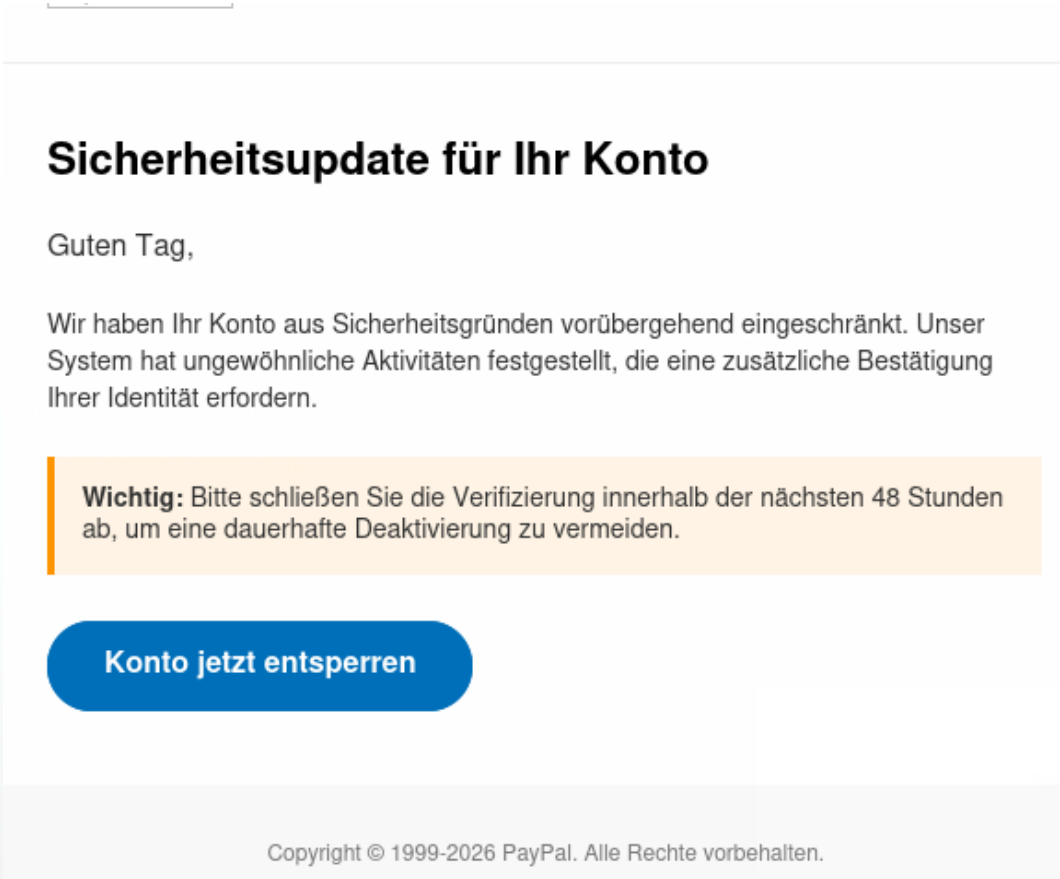
AVANTEC
Competence. Security. Trust.

- Keywords
- IP Reputation
- Eigenschaften
  - Nur BCC
  - Displayname hat nichts mit Mailadresse zu tun
  - Reply To
  - Freemailer
  - Encoding-Probleme
  - Sprach-Probleme
- URL Reputation
  - Mismatch URL - Maildomain

Phishing

International, Deutsch

Bekannte Services



Sicherheitsupdate für Ihr Konto

Guten Tag,

Wir haben Ihr Konto aus Sicherheitsgründen vorübergehend eingeschränkt. Unser System hat ungewöhnliche Aktivitäten festgestellt, die eine zusätzliche Bestätigung Ihrer Identität erfordern.

Wichtig: Bitte schließen Sie die Verifizierung innerhalb der nächsten 48 Stunden ab, um eine dauerhafte Deaktivierung zu vermeiden.

Konto jetzt entsperren

Copyright © 1999-2026 PayPal. Alle Rechte vorbehalten.

- Subject: PayPal: Wichtig: Identität in 24h bestätigen. Konto sonst gesperrt..
- From: Kundenservice kontakt@neonail.de
- To: user.name@customer.ch
- EHLO IP: 18.156.147.178
- Reverse DNS: mail-eu29.freshemail.io
- Link: http://em.yotpo.com/ls/click?upn=u001.-2F....

- Inhalt: ähnlich berechtigter Mails
- Subject/Inhalt: Dringend!
- From: Mailadresse nicht angeblicher Sender
- Verschickt über freshmail.io
- Malicious Link

Erkennungsmöglichkeiten

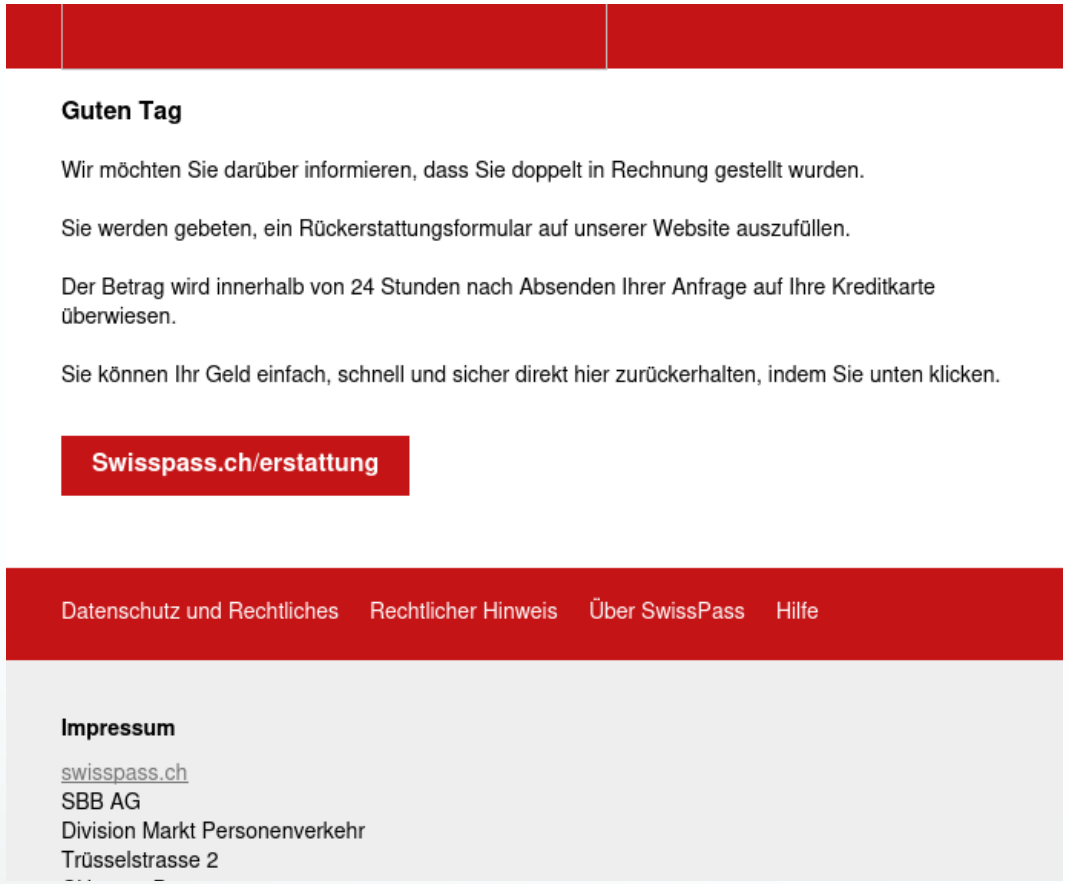
AVANTEC
Competence. Security. Trust.

- Keywords
- IP Reputation
  - Legitime Massenmailversender
- Eigenschaften
  - Nur BCC
  - Displayname hat nichts mit Mailadresse zu tun
  - Reply To
  - Freemailer
  - Encoding-Probleme
  - Sprach-Probleme
- URL Reputation
  - Mismatch URL - Maildomain

Phishing

Schweizerisch

Bekannte Services



Guten Tag

Wir möchten Sie darüber informieren, dass Sie doppelt in Rechnung gestellt wurden.

Sie werden gebeten, ein Rückerstattungsformular auf unserer Website auszufüllen.

Der Betrag wird innerhalb von 24 Stunden nach Absenden Ihrer Anfrage auf Ihre Kreditkarte überwiesen.

Sie können Ihr Geld einfach, schnell und sicher direkt hier zurückerhalten, indem Sie unten klicken.

Swisspass.ch/erstattung

Datenschutz und Rechtliches Rechtlicher Hinweis Über SwissPass Hilfe

Impressum

swisspass.ch
SBB AG
Division Markt Personenverkehr
Trüsselstrasse 2

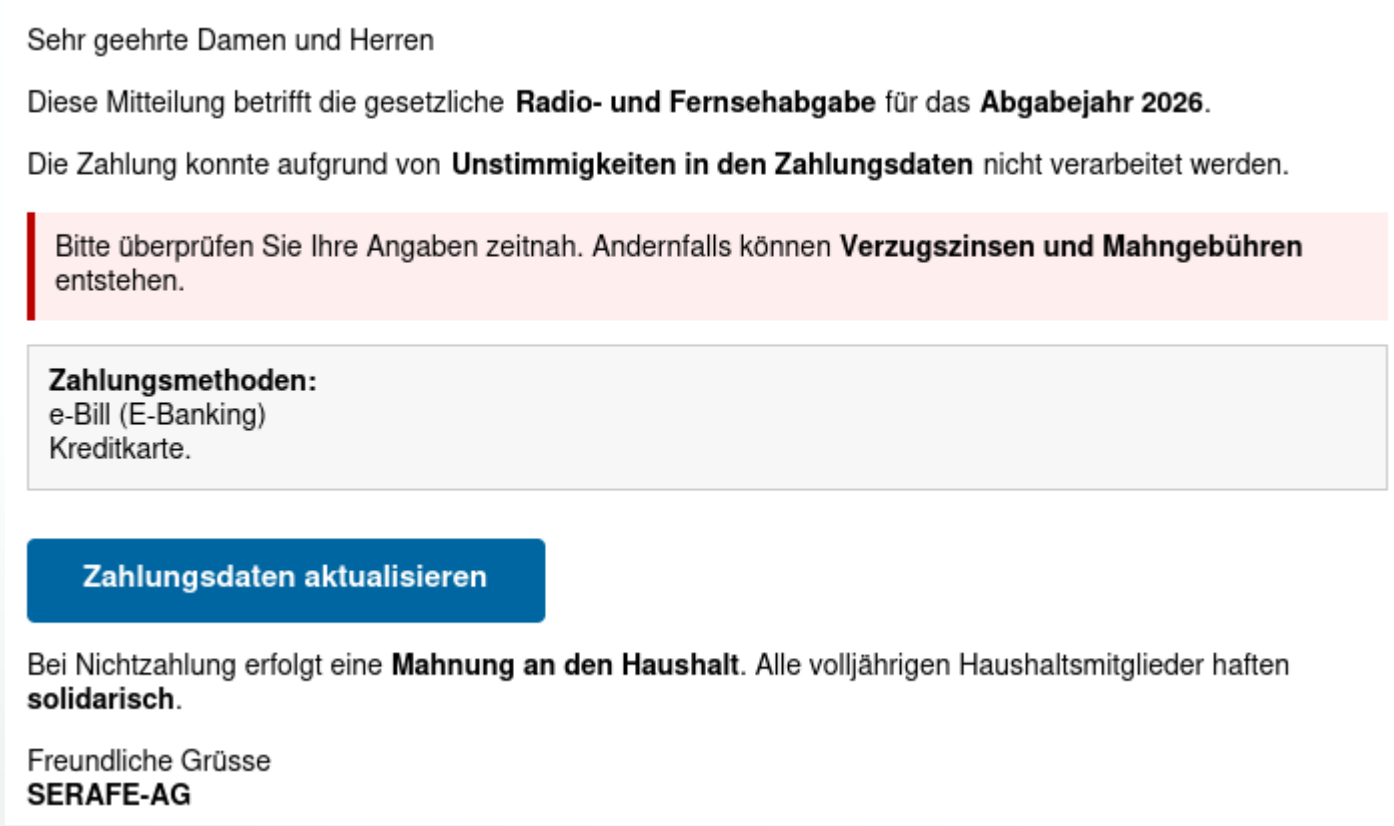
- Subject: Ihre digitale Rückerstattung bei der SBB
- From: SBB CFF FFS elena.berezina@successdigital.com.ua
- To: user.name@customer.ch
- EHLO IP: 195.230.115.2
- Reverse DNS: bars.stikonet.od.ua
- Link: https://s8h3w.ttrk.io/6984...

- Inhalt: ähnlich berechtigter Mails
- From: Mailadresse nicht angeblicher Sender
- Malicious Link
- IP: ohne Reputation

Phishing

Schweizerisch

Bekannte Services



Sehr geehrte Damen und Herren

Diese Mitteilung betrifft die gesetzliche **Radio- und Fernsehabgabe** für das **Abgabejahr 2026**.

Die Zahlung konnte aufgrund von **Unstimmigkeiten in den Zahlungsdaten** nicht verarbeitet werden.

Bitte überprüfen Sie Ihre Angaben zeitnah. Andernfalls können **Verzugszinsen und Mahngebühren** entstehen.

Zahlungsmethoden:
e-Bill (E-Banking)
Kreditkarte.

Zahlungsdaten aktualisieren

Bei Nichtzahlung erfolgt eine **Mahnung an den Haushalt**. Alle volljährigen Haushaltsmitglieder haften **solidarisch**.

Freundliche Grüsse
SERAFE-AG

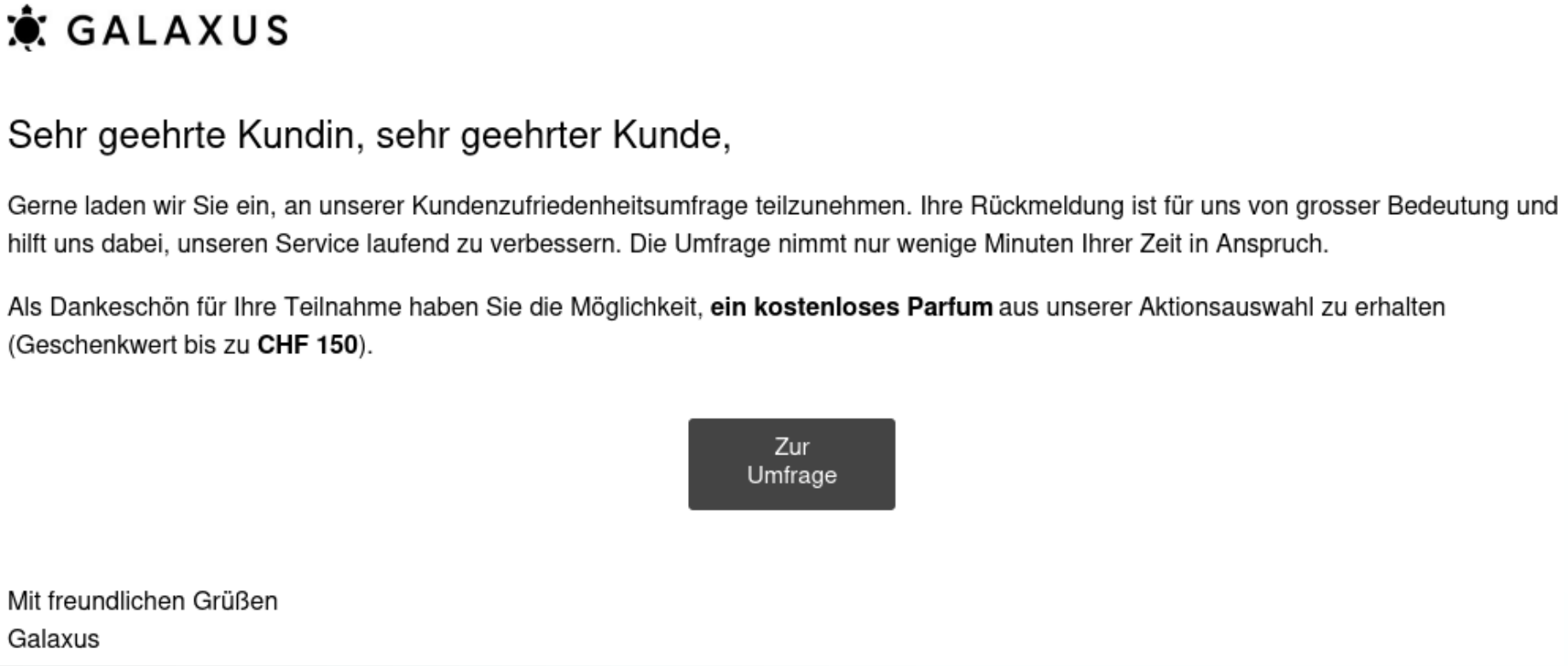
- Subject: Sofortiger Handlungsbedarf – Zahlung SERAFE 2026 fehlgeschlagen
- From: admin.serafe.ch press@ropaly.com
- To: user.name@customer.ch
- EHLO IP: 161.248.201.18
- Reverse DNS: sbdix.bdswebhosting.com

- Inhalt: User weiss, dass er solche Rechnungen erhält
- From: Mailadresse nicht angeblicher Sender
- Verschickt über Webhoster
- Malicious Link: https://acto.ge/.../

Phishing

Schweizerisch

Bekannte Services



- Subject: Ihre Meinung. Unser Dankeschön. Ihre Chance auf ein Parfum - (Bestellnummer: 24764144)
- From: Paul-Kuster-von-Galaxus noreply@qonnect.me
- To: user.name@customer.ch
- EHLO IP: 69.169.224.14
- Reverse DNS: b224-14.smtp-out.eu-central-1.amazonses.com

- Inhalt: Belohnung
- From: Mailadresse nicht angeblicher Sender
- Verschickt über Amazon SES
- Malicious Link: https://islamicft.com/swissweb/....php

Erkennungsmöglichkeiten

AVANTEC
Competence. Security. Trust.

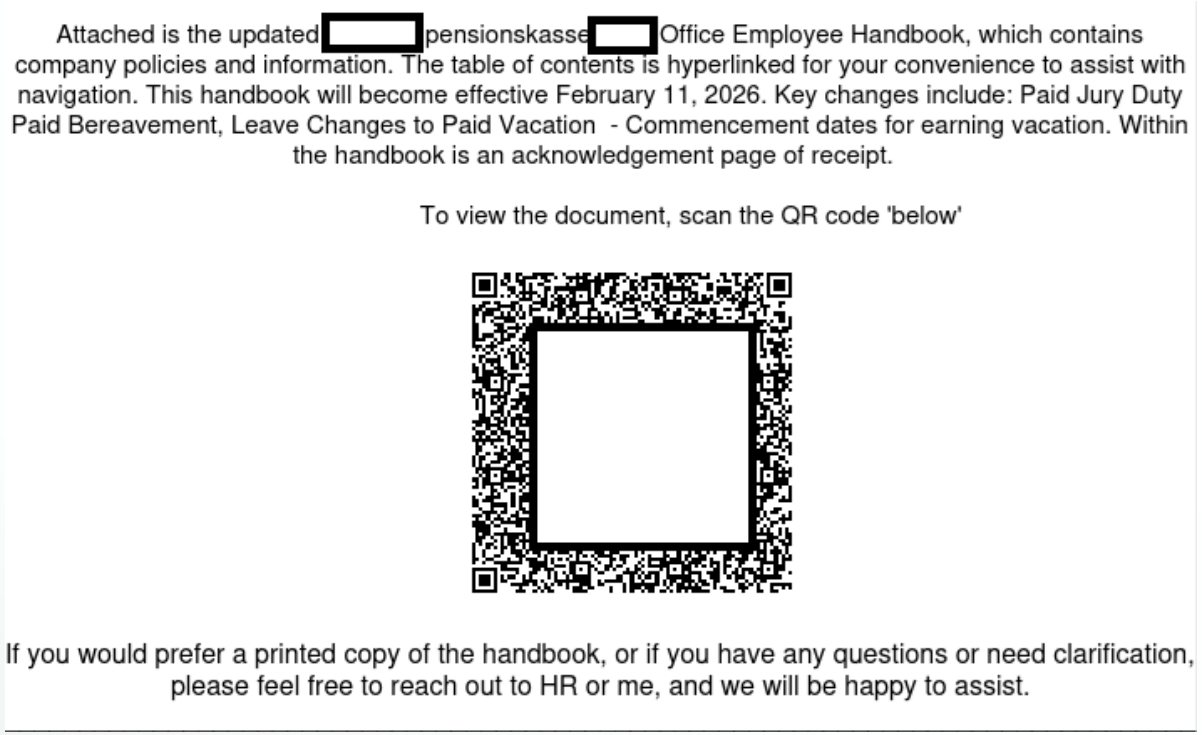
- Keywords
- IP Reputation
  - Legitime Massenmailversender
  - Legitime Cloud-Anbieter
    - Amazon SES, Google, MS
- Eigenschaften
  - Nur BCC
  - Displayname hat nichts mit Mailadresse zu tun
  - Reply To
  - Freemailer
  - Encoding-Probleme
  - Sprach-Probleme
- URL Reputation
  - Mismatch URL - Maildomain

Phishing

Targetet

Out of Band Communication

QR Codes



- Subject: pensionskasse XYZ Policy Handbook Eff-Review Mtg. 02/11/2026 3:52 PM.
- From: “user.name” info@flaunt.glass
- To: user.name@customer.ch
- Reply To: jonypare94@gmail.com
- EHLO: d215-9.smtp-out.sa-east-1.amazonses.com
- EHLO IP: 23.249.215.9
- Reverse DNS: d215-9.smtp-out.sa-east-1.amazonses.com

- Inhalt: Englisch
- Subject: Auf Kunde angepasst
- From: Name ungleich Mailadresse
- Reply-To: Freemailer
- Verschickt über Amazon Simple Email Service
- Link als QR Code

Erkennungsmöglichkeiten

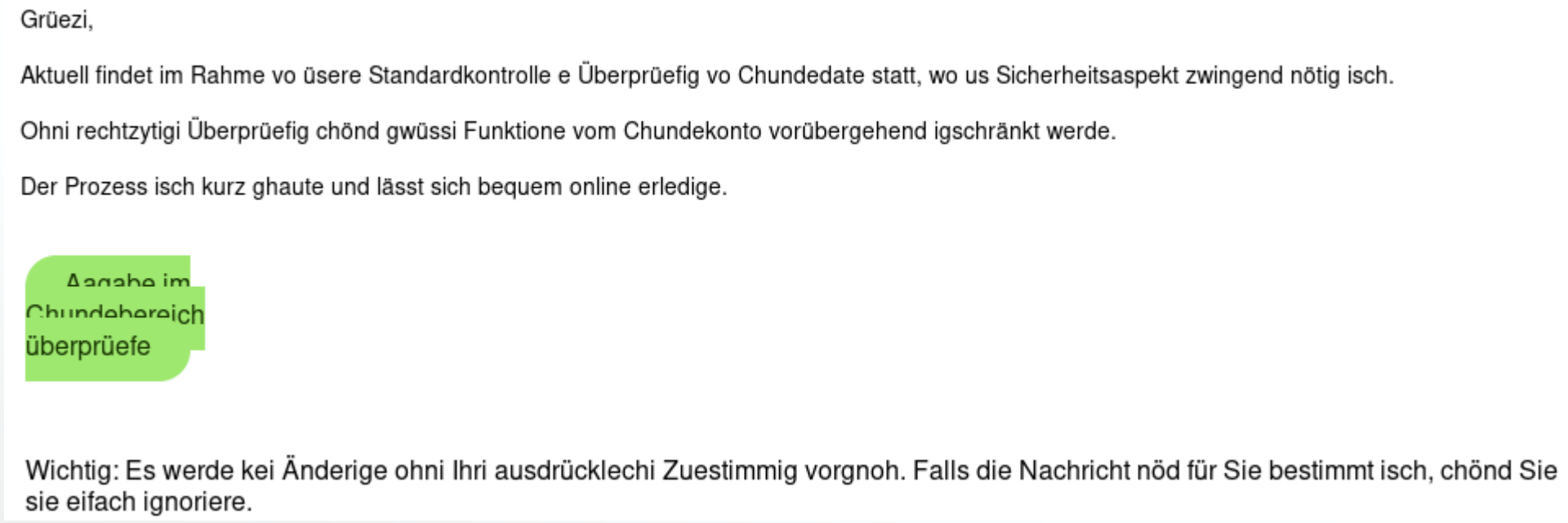
AVANTEC
Competence. Security. Trust.

- Keywords
- IP Reputation
  - Legitime Massenmailversender
  - Legitime Cloud-Anbieter
    - AmazonSES, Google, MS
- Eigenschaften
  - Nur BCC
  - Displayname hat nichts mit Mailadresse zu tun
  - Reply To
  - Freemailer
  - Encoding-Probleme
  - Sprach-Probleme
- URL Reputation
  - Mismatch URL – Maildomain
  - QR Codes -> Link Extraction aus Dokumenten, Bildern, ...

Phishing

Schweizerdeutsch

Bekannte Services


Grüezi,

Aktuell findet im Rahme vo üsere Standardkontrolle e Überprüefig vo Chundedate statt, wo us Sicherheitsaspekt zwingend nötig isch.

Ohni rechtzytigi Überprüefig chönd gwüssi Funktione vom Chundekonto vorübergehend igschränkt werde.

Der Prozess isch kurz ghaute und lässt sich bequem online erledige.

Aagabe im Chundebereich überprüefe

Wichtig: Es werde kei Änderige ohni Ihri ausdrücklechi Zuestimmig vorgnoh. Falls die Nachricht nöd für Sie bestimmt isch, chönd Sie sie eifach ignoriere.

- Subject: Fwd: Ihri Mithilf isch gfrogt: Konto-Überprüefig offen Ref-X2T19TD8XC69RI6880
- From: |Wise;-Inc|| cgvdkycdstuvcfdsyjtfcdsyjdsjyds@dcshgvkfcdfsycds.freshdesk.com
- To: user.name@customer.ch
- EHLO IP: mail-ind31.freshemail.io
- Reverse DNS: mail-ind31.freshemail.io
- Link: https://www.bing.com/ck%2Fa%3F%21%26%26p%

- Inhalt: Schweizerdeutch
- From: Abuse von Freshdesk
- Verschickt über Freshmail
- Link zu bing.com mit embedded URL

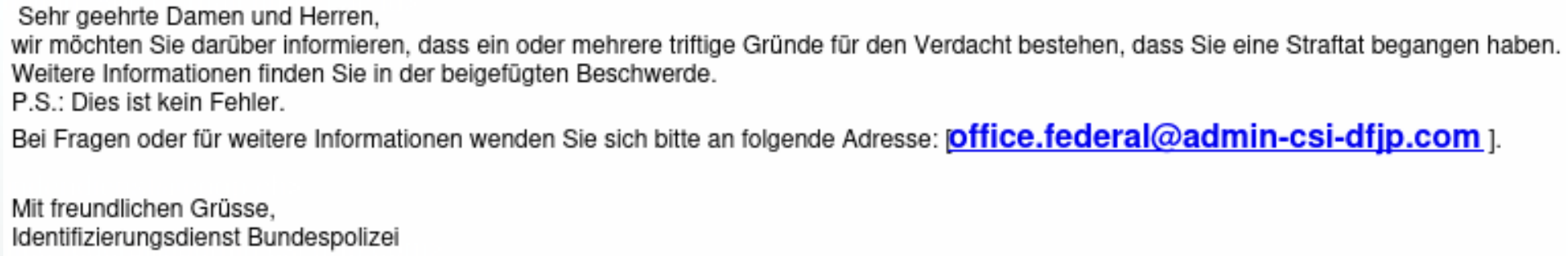
26. März 2026

Phishing

Extortion

Fedpol

schlecht



Sehr geehrte Damen und Herren,
wir möchten Sie darüber informieren, dass ein oder mehrere triftige Gründe für den Verdacht bestehen, dass Sie eine Straftat begangen haben.
Weitere Informationen finden Sie in der beigefügten Beschwerde.
P.S.: Dies ist kein Fehler.
Bei Fragen oder für weitere Informationen wenden Sie sich bitte an folgende Adresse: [office.federal@admin-csi-dfjp.com].

Mit freundlichen Grüsse,
Identifizierungsdienst Bundespolizei

- Subject: 🟥 Verfahrensmitteilung Akte FACT RT-A052 🟥
- From: BUNDESAMT FÜR POLIZEI fadlillah25001@mail.unpad.ac.id
- To: user.name@customer.ch
- EHLO IP: 2607:f8b0:4864:20::22f
- Reverse DNS: mail-oi1-x22f.google.com

- Inhalt: Polizei, Anhang öffnen
- From: Mailadresse nicht angeblicher Sender
- Verschickt über Google
- Image Attachment -> Man muss antworten

Phishing

Extortion
Fedpol
schlecht

- Subject: 🟥 V
- From: BUND
  fadlillah250
- To: user.nam
- EHLO IP: 26
- Reverse DN

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

BUNDESAMT FÜR POLIZEI – FEDPOL

VORLADUNG VOR GERICHT

Für die Zwecke einer gerichtlichen Untersuchung.
(Artikel 339-1 des Strafgesetzbuches)

Föderale Polizei (FEDPOL)
Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Eidgenössisches Departement des Innern (EDI)
Bundesreferenz: FACT / RT-A052-SIS-3003 /01-2026
Beschwerde gegen die Entscheidung FEDPOL-PFPDT - Akte FACT / RT-A052

In meiner Funktion als Direktorin des Bundesamts für Polizei (fedpol) möchte ich Sie hiermit darüber informieren, dass gegen Sie ein Strafverfahren gemäß den Bestimmungen des Schweizerischen Strafgesetzbuches (StGB), des Bundesgesetzes über den Datenschutz (DSG) und anderer geltender Rechtsvorschriften eingeleitet wurde.

Im Rahmen einer behördlich genehmigten, technischen Überwachungs- und Datensicherungsoperation, die als Teil einer verdeckten Ermittlung durchgeführt wurde, konnten Beweise erlangt werden, die Ihre mutmaßliche Beteiligung an strafbaren Handlungen belegen. Diese Taten beziehen sich hauptsächlich auf Cyberkriminalität und umfassen die folgenden Straftaten:

Besitz und Verbreitung von kinder- oder jugendpornografischem Material (Art. 197 StGB) ;
Teilnahme an illegalen Online-Plattformen, die gegen die Bestimmungen zur Ausbeutung und Verbreitung illegaler Inhalte verstoßen ; Verdacht der Beteiligung an kriminellen Aktivitäten im Bereich der Pädophilie ;
Nicht autorisierte Verbreitung von Exhibitionismus im Internet.

Die im Rahmen dieser Ermittlung gesammelten Beweise haben ergeben, dass Sie in den Besitz und die Verbreitung von

Erkennungsmöglichkeiten

AVANTEC
Competence. Security. Trust.

- Keywords
- IP Reputation
  - Legitime Massenmailversender
  - Legitime Cloud-Anbieter
    - AmazonSES, Google, MS
    - Freshdesk, Salesforce
- Eigenschaften
  - Nur BCC
  - Displayname hat nichts mit Mailadresse zu tun
  - Reply To
  - Freemailer
  - Encoding-Probleme
  - Sprach-Probleme
- URL Reputation
  - Mismatch URL – Maildomain
  - QR Codes -> Link Extraction aus Dokumenten, Bildern, ...
- Intent, Sentiment, Tonlage
  - Dringend, Angst machen

Phishing

Extortion
Fedpol
besser

Bonjour,

Attention

Après plusieurs mois d'enquête sur votre réseau, nous avons détecté une activité anormale.

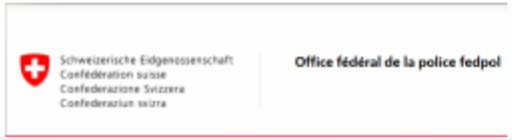
Vous êtes convoqué(e)

Veuillez consulter le document ci-joint.

Pour plus d'informations, veuillez contacter la Fedpol ICI.

Cordialement,
Mauricio Millan

Chef du Département de la cyberpornographie



- Subject: Fedpol/CONVOCATION/BERUFUNG
- From: Mauricio de Jesús Millán Malpica mauricio.millan@anahuac.mx
- To: user.name@customer.ch

- Inhalt: Polizei, Anhang öffnen
- PDF Attachment -> Man muss antworten
- Im PDF: Kontakt via Gmail Adresse

Phishing

Extortion

Fedpol

besser

- Subject: Fedpol/CONVO
- From: Mauricio de Jesús
  mauricio.millan@anahu
- To: user.name@custom

Identifikationsdaten wurden auf illegalen Websites gefunden und Sie sind Gegenstand mehrerer laufender Gerichtsverfahren: Kinderpornografie, Cyberpredatoren, Sammler, Sammler und Vertreiber von obszönen Szenen.

Zu Ihrer Information: Ein internationales Gesetz vom März 2007 verschärft die Strafen für Übergriffe, sexuelle Übergriffe oder Vergewaltigungen von Minderjährigen im Internet. Wir haben diese elektronische Beschwerde eingereicht, um Ihre Aufmerksamkeit auf die Schwere der Strafen für solche Straftaten zu lenken. Sie haben im Notfall 72 Stunden Zeit, um auf die Vorladung zu reagieren. Nach Ablauf der Frist führt Ihr Schweigen zu einer Strafverfolgung.

Wichtig: Für weitere Informationen schreiben Sie uns bitte ausschließlich an diese E-Mail-Adresse: netch.fedpol@gmail.com

Ihre Informationen werden an den Genfer Generalstaatsanwalt weitergeleitet, damit dieser einen Haftbefehl erlassen kann. Dieser Haftbefehl wird zur Festnahme an die nächstgelegene Polizeistation weitergeleitet. Sie werden zudem als Sexualstraftäter registriert, und Ihr Fall wird auf mehreren Fernsehkanälen ausgestrahlt.

Eva Wildi-Cortés

Direktorin fedpol

POLIZEI.CH

n

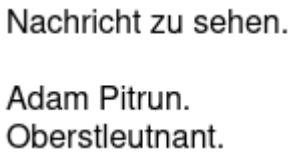
26. März 2026

Phishing

Extortion

Europol

lustig



Nachricht zu sehen.

Adam Pitrun.
Oberstleutnant.

- Subject: ASAP
- From: Adam Pitrun 251736@vutbr.cz
- To: user.name@customer.ch
- EHLO IP: 2a00:1450:4864:20::533
- Reverse DNS: mail-ed1-x533.google.com

- Inhalt: ???
- PDF Attachment mit QR Code
- Kontaktadresse: yahoo

Phish

Extortion
Europol
lustig

- Subje
- From:
- To: us
- EHLO
- Revers

EUROPOL EC3 European Cybercrime Centre

Herr William MCKINSEY
Kriminalbeamter
E-Mail: europoleuropaeu@yahoo.com

JUGENDSCHUTZBRIGADE
CEPOL - EC3 - EUROPOL
Schlaue Kriminalpolizei

Doss N^0/DC56-ART798

ANKLAGE: PEDOPORNOGRAFIE

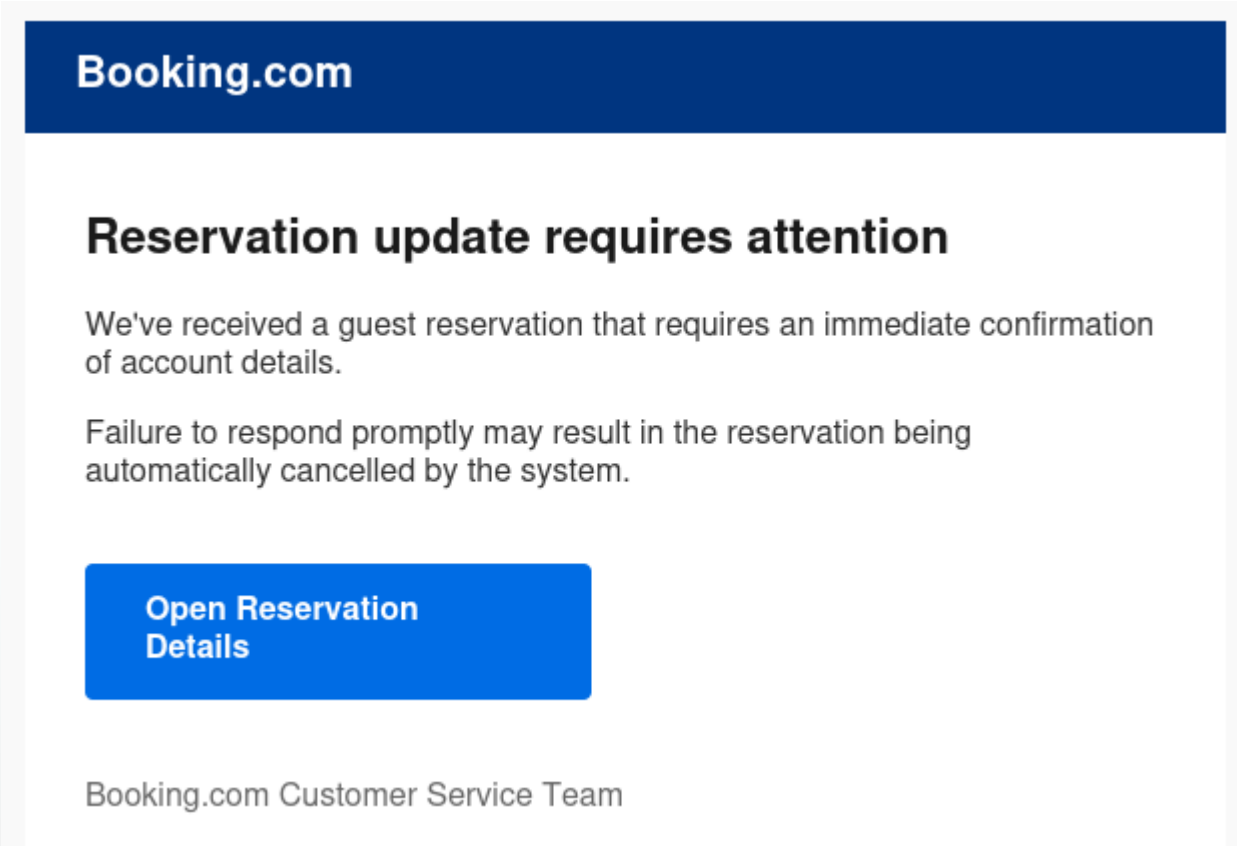
Auf Ihre freundliche Aufmerksamkeit

Auf Ersuchen von General Jean-Philippe LECOUFFE, Brigadekommandant von Europol "Brigade für den Jugendschutz (BPM)"
Wir verklagen Sie kurz nach der Eingabe von Computerdaten durch unsere Cyber-Infiltration für: **Kinderpornografie**
Zu Ihrer Information: Gesetz 390-1 der Strafprozessordnung vom März 2007 verschärft die Strafen, wenn Vorschläge, sexuelle Übergriffe oder Vergewaltigungen unter Nutzung des Internets begangen wurden.

Phishing

Targeted

Hotel



- Subject: Review required
- From: Booking.com Reservation reservation@booking.com.reservation-id-8745464543.kebtech.net
- To: info@hotelxy.ch
- EHLO IP: 54.240.4.7
- Reverse DNS: a4-7.smtp-out.eu-west-1.amazonses.com
- Inhalt: Angepasst auf Kunde (Hotel)
- URL mit Link-Shortener (share.google)

Erkennungsmöglichkeiten

AVANTEC
Competence. Security. Trust.

- Keywords
- IP Reputation
  - Legitime Massenmailversender
  - Legitime Cloud-Anbieter
    - AmazonSES, Google, MS
    - Freshdesk, Salesforce
- Eigenschaften
  - Nur BCC
  - Displayname hat nichts mit Mailadresse zu tun
  - Reply To
  - Freemailer
  - Encoding-Probleme
  - Sprach-Probleme
- URL Reputation
  - Mismatch URL – Maildomain
  - QR Codes -> Link Extraction aus Dokumenten, Bildern, …
  - Link Shortener
- Intent, Sentiment, Tonlage
  - Dringend, Angst machen

Phishing

Targeted

Hotel

Booking.com

Case #CMP-5163-284

Dear Booking.com Support,

BOOKING REF	GUEST NAME
BKG-5163-284	**Terrence Jackson**
CHECK-IN	CHECK-OUT
28 Aug 2025	31 Aug 2025

I'm writing to report an incident that occurred during my stay at your partner property. On the evening of August 29, I was approached by security while sitting in the lobby and asked to "prove I was a guest." After showing my key card, the front desk clerk made a derogatory comment about my race within earshot of other guests. When I requested to speak with a manager, I was told none were available and was then ignored for 20 minutes. The following morning, housekeeping entered my room without knocking at 7:45 AM, saw I was asleep, and left without closing the door properly.

I have documented everything – photos and recordings are available here. The hotel has not responded to any of my emails since checkout.

Requested resolution:
Full refund of $892 and a formal investigation into staff conduct.

- Subject: Booking BKG-2230-61 - racial discrimination at check-in - Carlos Rodriguez
- From: Victor Lopez k-takahashi@momometal.co.jp
- To: info@hotelxy.ch
- EHLO IP: 143.125.222.17
- Reverse DNS: momometal.co.jp

- Inhalt: Beschwerde via booking.com
- URL, welche zur Zeit nicht mehr malicious ist

Phishing

Targeted

Hotel

Hi

Thank you very much for the amazing time we spent at your property
Everything was absolutely wonderful
and the atmosphere was warm and relaxing.

We especially appreciated the cleanliness, comfort, and professionalism.

We have already left a positive review about your hotel
and also uploaded several professional-quality photos of your hotel.

https://booking.com/hotel/reviews.html?aid=304142&label=gen173nr-1DCAEggJ46AdIM1oHwnsrYuMjRwmtVKoXYTZNjLuNuHzpnJLspOT8&cl

Many thanks again to you and your team.
We will definitely be happy to return to your hotel again this year.

We would appreciate a reply at your convenience.
Warm Christmas wishes to you and your entire team!

- Subject: Hotel booking clarification request
- From: noreply servicio@inespre.gob.do
- To: info@hotelxy.ch
- EHLO IP: 50.6.199.138
- Reverse DNS: server-623641.inespre.gob.do

- Inhalt: Dank für schönen Hotelaufenthalt
- Link zeigt nicht wirklich zu booking.com

Phishing

Targeted Hotel

Hello,

I hope this message finds you well.

My fiancé and I are currently in the process of selecting a venue for our wedding reception and would like to inquire about your availability for any Saturday during the summer of 2026 or any Saturday in April 2027.

If available, we would greatly appreciate it if you could provide details on the following:

- Venue hire pricing for a wedding reception only
- Menu options and pricing for a wedding breakfast
- Evening buffet options and associated costs
- Any wedding packages or special offers you may have

We would be grateful for any additional information that could help us determine whether your venue aligns with our vision and budget.

Thank you very much for your time and consideration. We look forward to hearing from you.

Kind regards,
Debbie

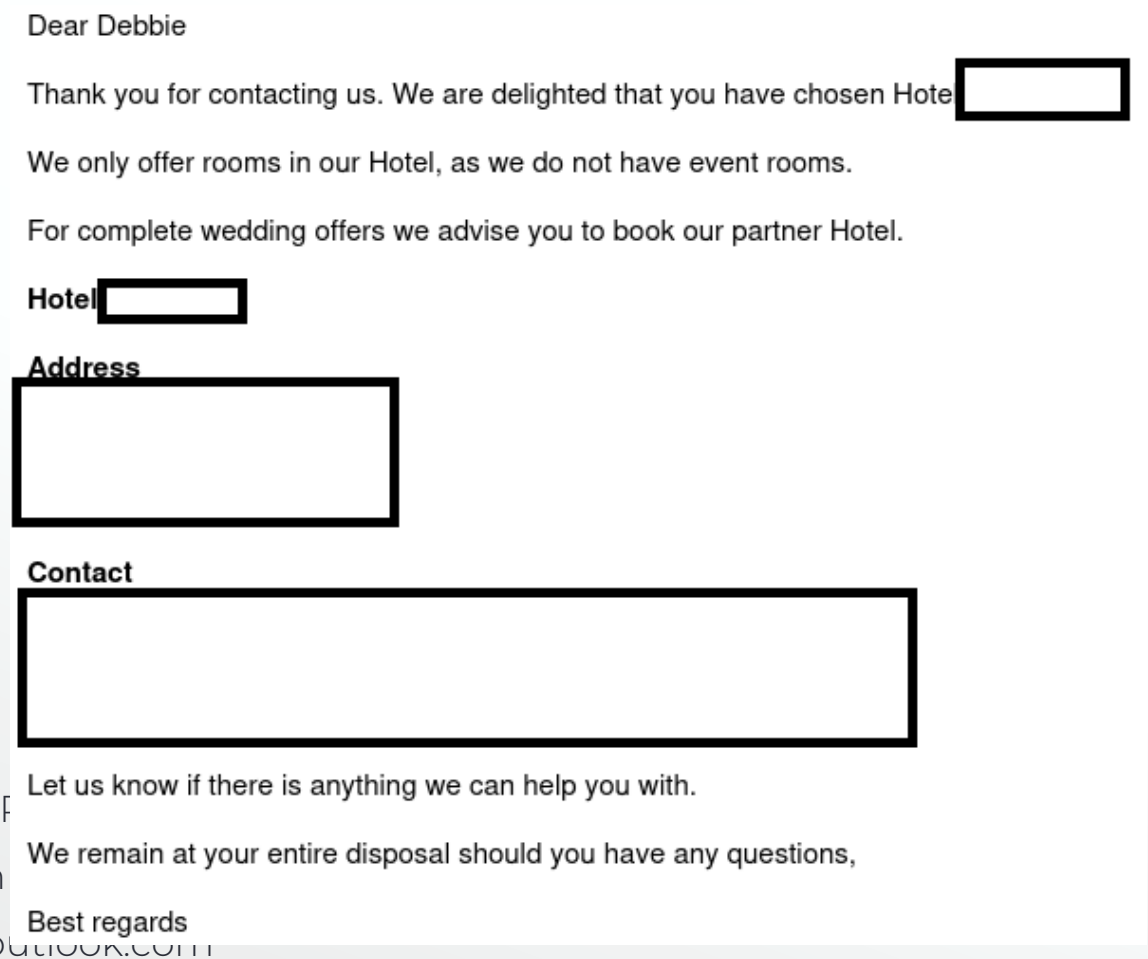
- Subject: Wedding Reception Venue Availability Inquiry
- From: Debbie debbie.lacoste1@outlook.com
- To: info@hotelxy.ch
- EHLO IP: 124.217.230.100
- Reverse DNS: vps.hmn.com.my

- Inhalt: Anfrage für Hochzeitsanlass an Hotel
- Ohne Links
- Ohne Attachments

Phishing

Targeted

Hotel



Dear Debbie

Thank you for contacting us. We are delighted that you have chosen Hote

We only offer rooms in our Hotel, as we do not have event rooms.

For complete wedding offers we advise you to book our partner Hotel.

Hotel

Address

Contact

Let us know if there is anything we can help you with.

We remain at your entire disposal should you have any questions,

Best regards

- Subject: Re: Wedding F Hotels
- From: info@hotelxy.ch
- To: debbie.lacoste1@outlook.com

Phishing

Targeted

Hotel

Hello Katrin,

Thank you very much for your prompt response and for sharing the detailed information regarding venue hire, menus, and available packages. We are truly excited about the possibility of hosting our wedding reception at your venue.

To assist with your recommendations and to ensure we remain within our budget, I have attached a copy of our wedding budget for your reference. This should provide a helpful overview of our target range for the venue, catering, and any additional services.

We would greatly appreciate any suggestions or options you feel would align well with our budget, as well as details of any packages that may be particularly suitable for our needs.

Thank you again for your time and assistance. We look forward to your reply and hope to find the perfect fit for our celebration.

Kind regards,
Debbie

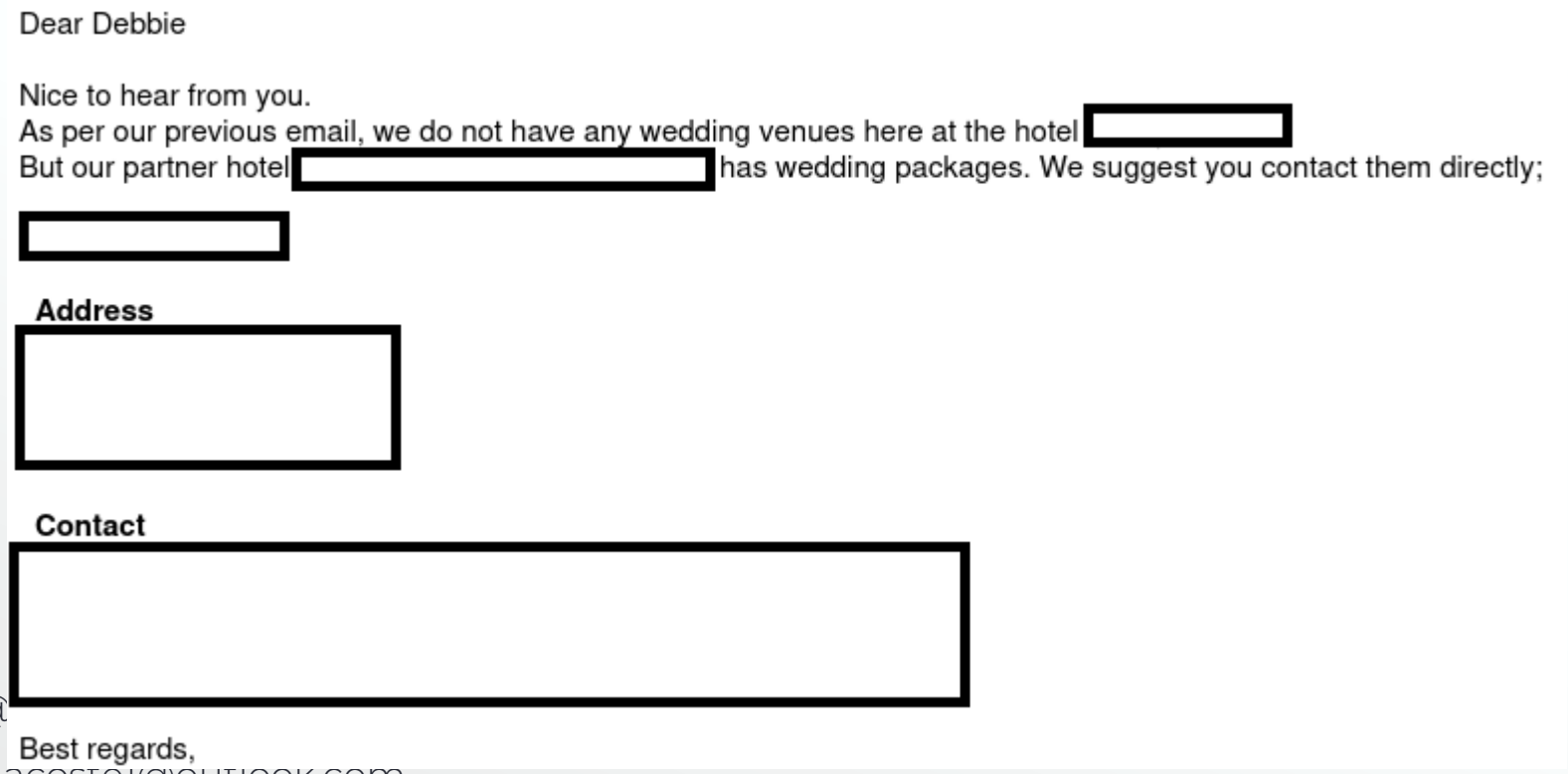
- Subject: Re: Wedding Reception Venue Availability Inquiry
- From: Debbie debbie.lacoste1@outlook.com
- To: info@hotelxy.ch
- EHLO IP: 124.217.230.100
- Reverse DNS: vps.hmn.com.my

- Inhalt: Bezieht sich nicht auf die Antwort
- Html Attachment mit Malicious URL https://formcarry.com/...

Phishing

Targeted

Hotel



Dear Debbie

Nice to hear from you.
As per our previous email, we do not have any wedding venues here at the hotel [redacted]
But our partner hotel [redacted] has wedding packages. We suggest you contact them directly;

[redacted]

Address

[redacted]

Contact

[redacted]

Best regards,

- Subject: Re: [redacted]
- From: info@[redacted]
- To: debbie.lacoste1@outlook.com

Phishing

Targeted

Hotel

Hello Katrin,

Thank you very much for your prompt response and for sharing the detailed information regarding venue hire, menus, and available packages. We are truly excited about the possibility of hosting our wedding reception at your venue.

To assist with your recommendations and to ensure we remain within our budget, I have attached a copy of our wedding budget for your reference. This should provide a helpful overview of our target range for the venue, catering, and any additional services.

We would greatly appreciate any suggestions or options you feel would align well with our budget, as well as details of any packages that may be particularly suitable for our needs.

Thank you again for your time and assistance. We look forward to your reply and hope to find the perfect fit for our celebration.

Kind regards,
Debbie

- Subject: Re: Wedding Reception Venue Availability Inquiry
- From: Debbie debbie.lacoste1@outlook.com
- To: info@hotelxy.ch
- EHLO IP: 124.217.230.100
- Reverse DNS: vps.hmn.com.my

- Inhalt: Bezieht sich nicht auf die Antwort
- Html Attachment mit Malicious URL https://formcarry.com/...

Erkennungsmöglichkeiten

AVANTEC
Competence. Security. Trust.

- Keywords
- IP Reputation
  - Legitime Massenmailversender
  - Legitime Cloud-Anbieter
    - AmazonSES, Google, MS
    - Freshdesk, Salesforce, Sendgrid, …
- Eigenschaften
  - Nur BCC
  - Displayname hat nichts mit Mailadresse zu tun
  - Reply To
  - Freemailer
  - Encoding-Probleme
  - Sprach-Probleme
- URL Reputation
  - Mismatch URL – Maildomain
  - QR Codes -> Link Extraction aus Dokumenten, Bildern, …
  - Link Shortener
- Intent, Sentiment, Tonlage
  - Dringend, Angst machen

Erkennungsmöglichkeiten

Einfach

- Keywords
- IP Reputation
  - Legitime Massenmailversender
  - Legitime Cloud-Anbieter
    - AmazonSES, Google, MS
    - Freshdesk, Salesforce, Sendgrid, …
- Eigenschaften
  - Nur BCC
  - Displayname hat nichts mit Mailadresse zu tun
  - Reply To
  - Freemailer
  - Encoding-Probleme
  - Sprach-Probleme
- URL Reputation
  - Mismatch URL – Maildomain
  - QR Codes -> Link Extraction aus Dokumenten, Bildern, …
  - Link Shortener
- Intent, Sentiment, Tonlage
  - Dringend, Angst machen

Erkennungsmöglichkeiten

Schwieriger

AVANTEC
Competence. Security. Trust.

- Keywords
- IP Reputation
  - Legitime Massenmailversender
  - Legitime Cloud-Anbieter
    - AmazonSES, Google, MS
    - Freshdesk, Salesforce, Sendgrid, …
- Eigenschaften
  - Nur BCC
  - Displayname hat nichts mit Mailadresse zu tun
  - Reply To
  - Freemailer
  - Encoding-Probleme
  - Sprach-Probleme
- URL Reputation
  - Mismatch URL – Maildomain
  - QR Codes -> Link Extraction aus Dokumenten, Bildern, …
  - Link Shortener
- Intent, Sentiment, Tonlage
  - Dringend, Angst machen

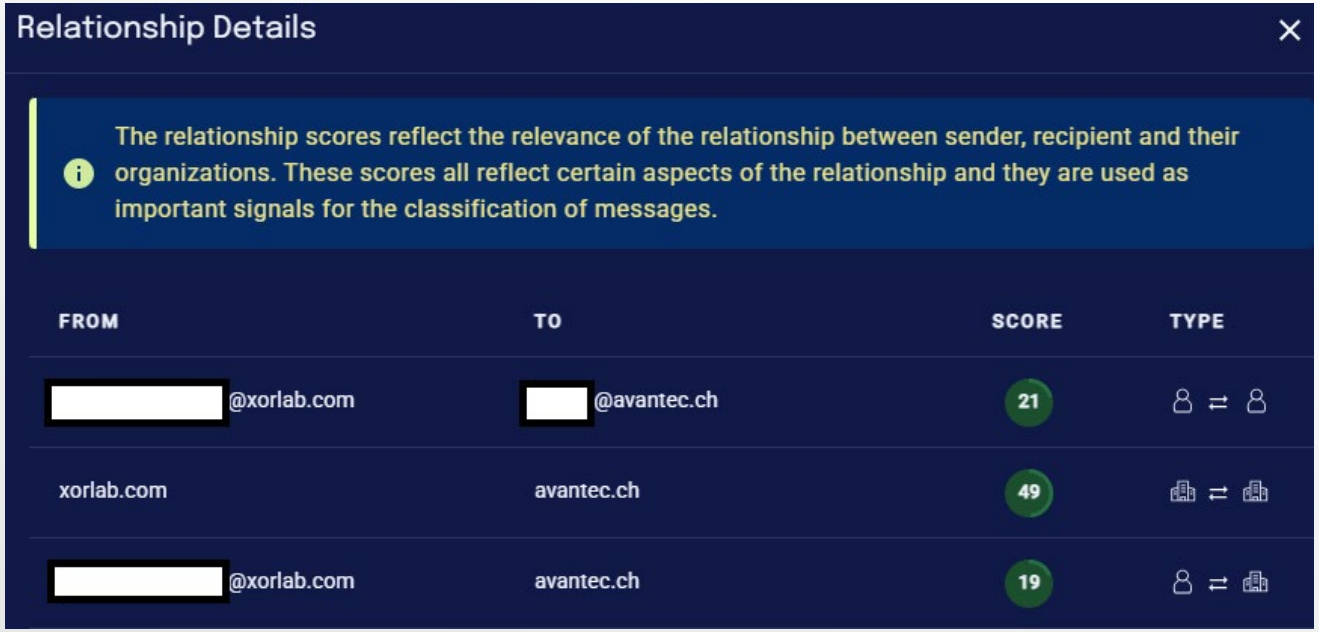
Lösungsansätze

Kommunikationsbeziehungen

AVANTEC
Competence. Security. Trust.

- Klassische MTAs betrachten jedes Mail einzeln
- Wer kommuniziert mit wem?
  - Trust zwischen Personen
  - zwischen Organisationen

- Noch nie gesehener Absender?
- Unbekannter Absender schickt Rechnung?
- Bekannter Absender schickt neu plötzlich Rechnungen?



Lösungsansätze

Kommunikationsbeziehungen

- Links
  - Welche Domains sind für meine Organisation relevant?
- Attachments
  - Was für Filetypen werden mit wem ausgetauscht?

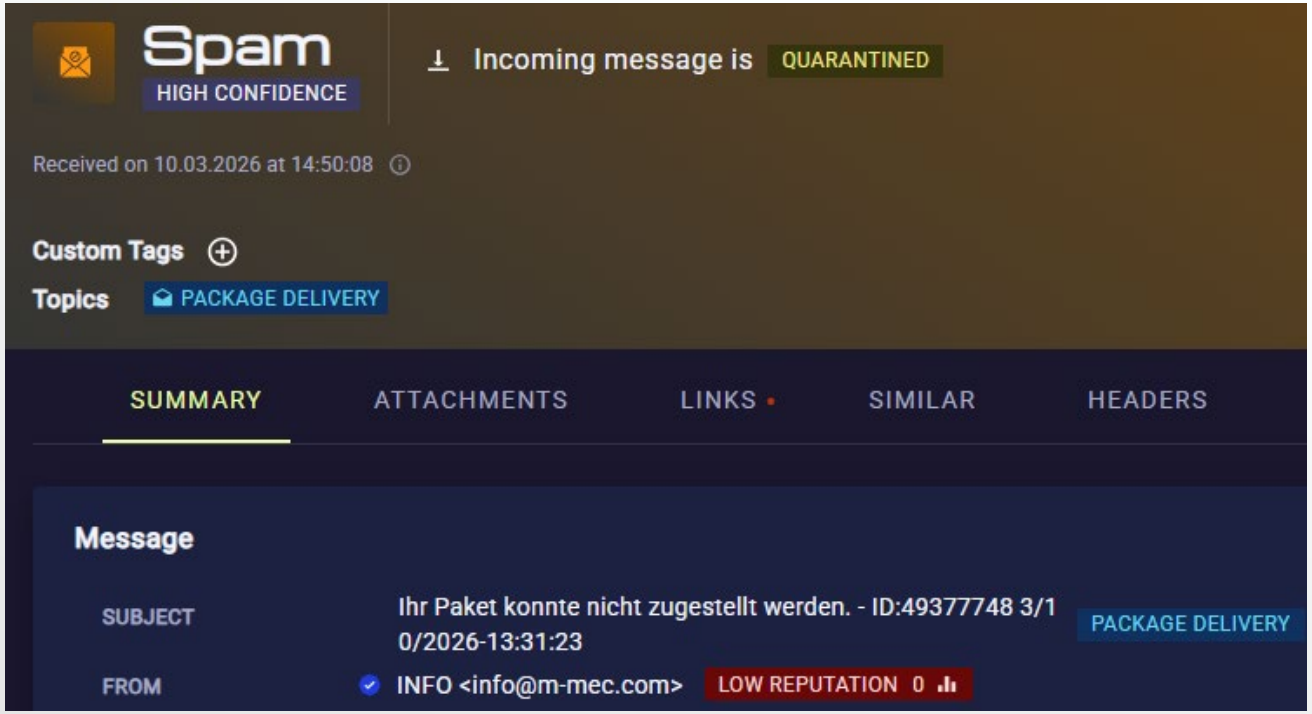
URL	DISPLAY TEXT	GLOBAL	LOCAL
https://www.tec-bite.ch/	n/a	7	100
http://www.avantec.ch/datenschutz%20	n/a	41	100
https://www.avantec.ch	n/a	41	100
https://www.avantec.ch/avantech-day-2026/	n/a	41	100
https://www.avantec.ch/	n/a	41	100
http://www.avantec.ch/datenschutz	n/a	41	100
http://www.avantec.ch/datenschutz%20	www.avantec.ch/d...	41	100
https://www.linkedin.com/company/avantec/	n/a	89	100
http://www.youtube.com/AVANTEC-Cyber-Security	n/a	92	100

Lösungsansätze

Erkennung der Absicht eines Mails

- Rechung?
- Paketzustellung?
- Account Login Problem?

- Dringend! Sofort reagieren!



xorlab

https://www.xorlab.com

AVANTEC
Competence. Security. Trust.

xorlab

https://www.xorlab.com

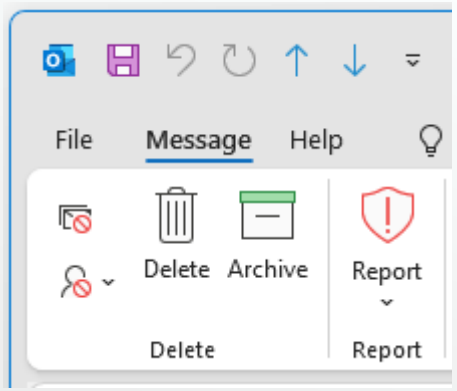
AVANTEC
Competence. Security. Trust.

- Email Security Gateway
- on-premises
- SaaS in CH und DE

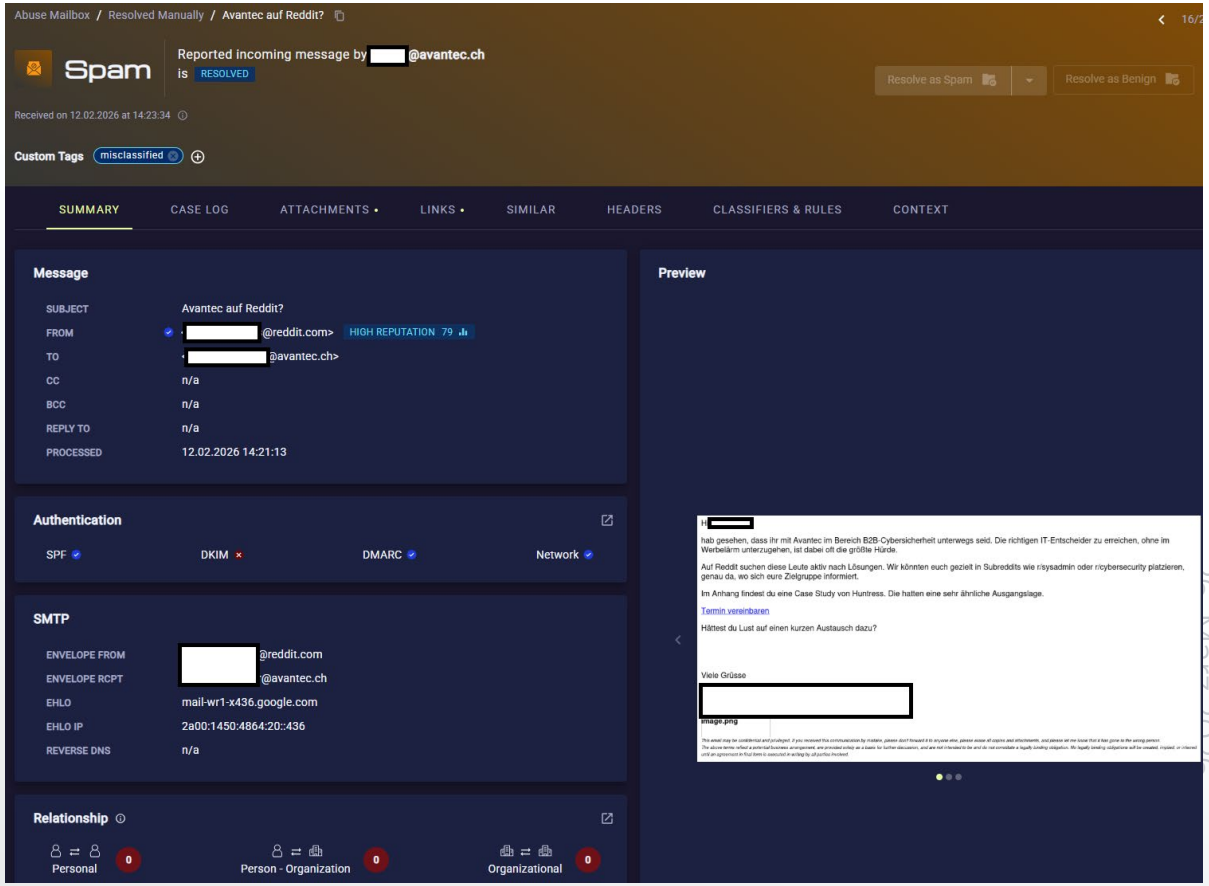
Lösungsansätze

Einbeziehung der User

- Verdächtiges Mail -> Melden!



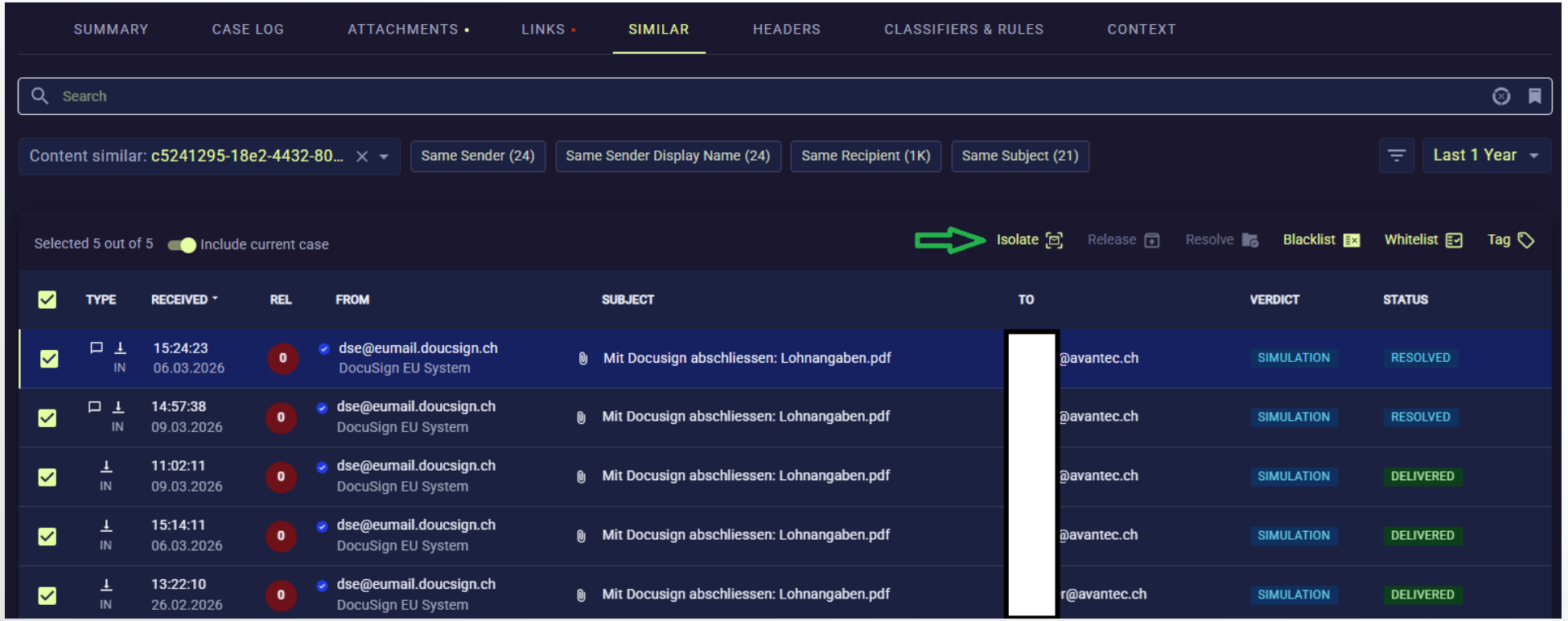
- Alle relevanten Informationen für die Analysten



Lösungsansätze

Einbeziehung der User

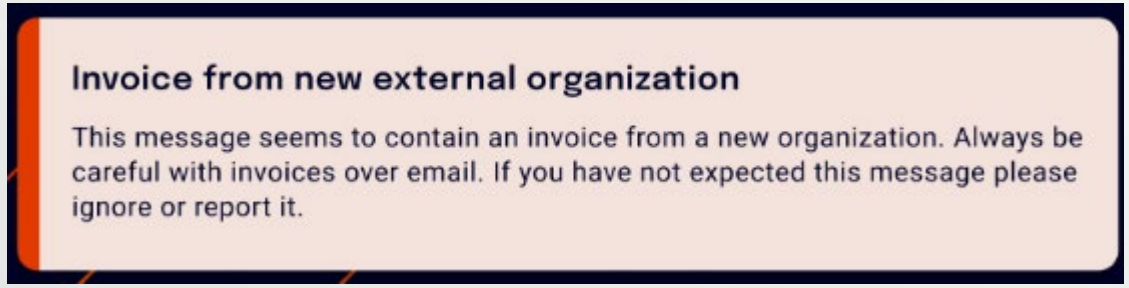
- Analyst kann ähnliche Mails suchen
- Und aus den Postfächern entfernen



Lösungsansätze

Einbeziehung der User

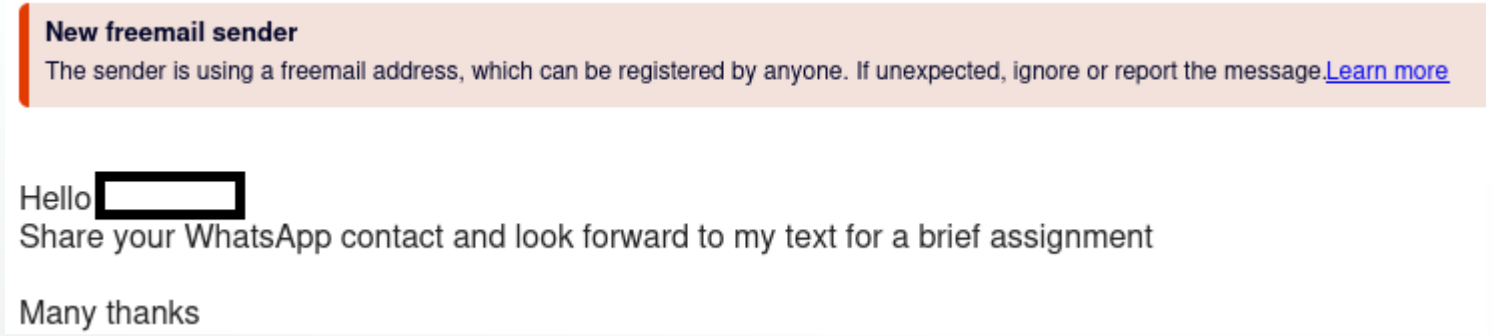
- Unterstützung der User
- Kontext-abhängige Banner
  - Nicht für jedes externe Mail
  - Nur wenn relevant



Phishing

Targeted

Neue Mitarbeiter



New freemail sender

The sender is using a freemail address, which can be registered by anyone. If unexpected, ignore or report the message.Learn more

Hello [redacted]
Share your WhatsApp contact and look forward to my text for a brief assignment

Many thanks

- Subject: “Name unseres CEO»
- From: Rapid reply?! teamscreativedesckcare@gmail.com
- To: user.name@avantec.ch
- EHLO IP: 2607:f8b0:4864:20::b36
- Reverse DNS: mail-yb1-xb36.google.com

- Inhalt: out of band Kommunikation mit neuer Mitarbeiterin

Phishing

Modification in transit

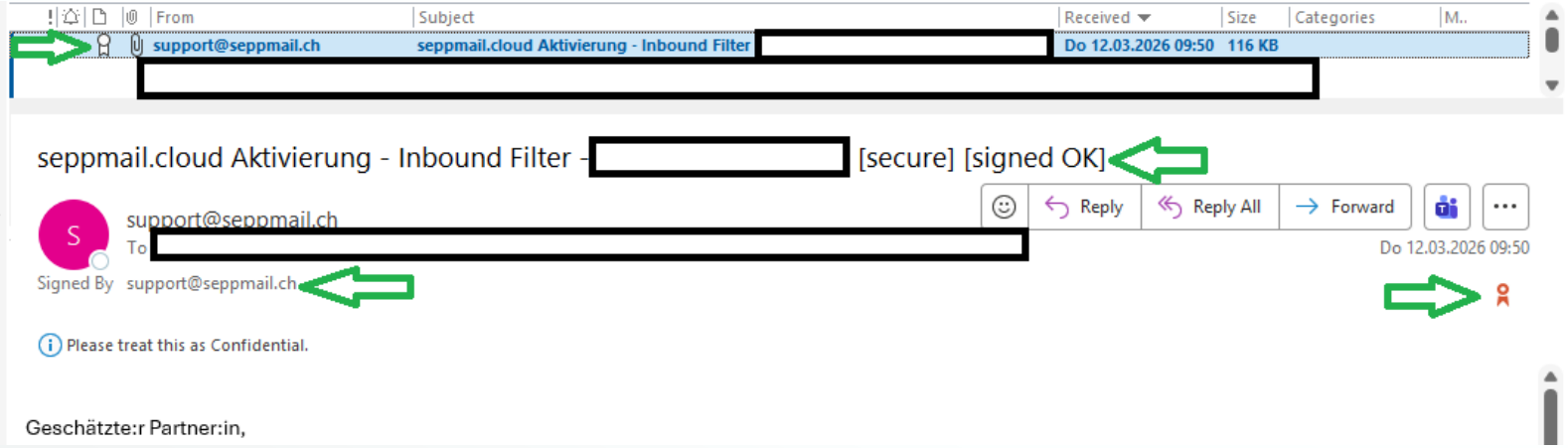
- Versand einer Rechnung nach Südafrika
- From: original
- To: original
- EHLO IP: original
- Reverse DNS: original
- Inhalt: original
- Attachment: original

- Einzig Kontonummer in der Rechnung wurde unterwegs angepasst

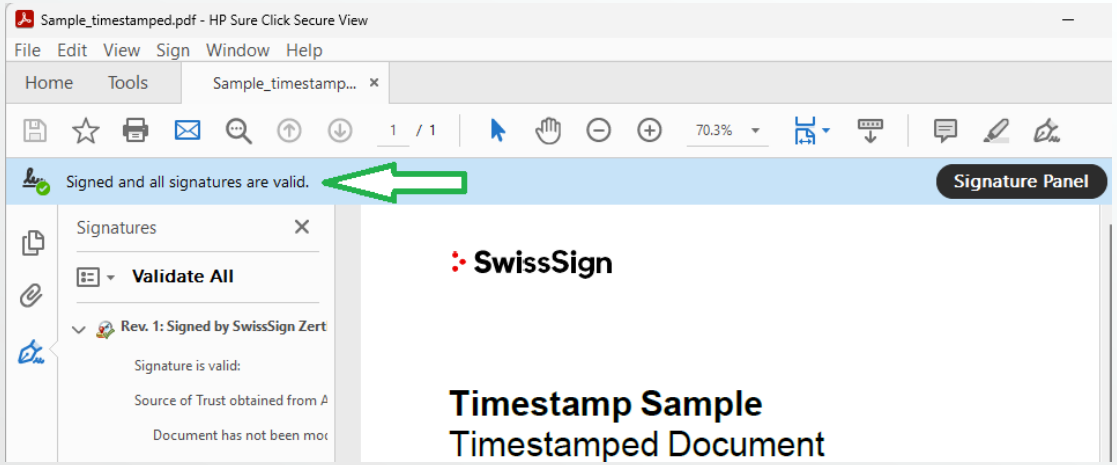
Lösungsansätze

Kryptographische Signierung

- Signierung der Mails mit S/MIME



- Signierung des Dokumentes



SEPPmail

https://www.seppmail.ch

SEPPmail

https://www.seppmail.ch

AVANTEC
Competence. Security. Trust.

- Email Security Gateway
- Email Verschlüsselung und Signatur
- on-premises
- SaaS in CH und DE

Phishing

Compromized Accounts

Guten Morgen, Mark,

Ich hoffe, es geht Ihnen gut.

Bitte bestätigen Sie den Zahlungsplan für Rechnung 220259. Bitte beachten Sie, dass unsere Finanzabteilung kürzlich umstrukturiert wurde. Unser Hauptbankkonto kann bis zum Abschluss der internen Prüfung nicht für Zahlungseingänge oder -überweisungen verwendet werden.

Wir erhalten derzeit ausstehende Zahlungen auf unserem Tochterbankkonto. Im Anhang finden Sie das Schreiben und die überarbeitete Rechnung mit unserer neuen Bankverbindung für Ihre Buchhaltung und Zahlungsabwicklung. Vielen Dank im Voraus.

Wir freuen uns auf Ihre Antwort.

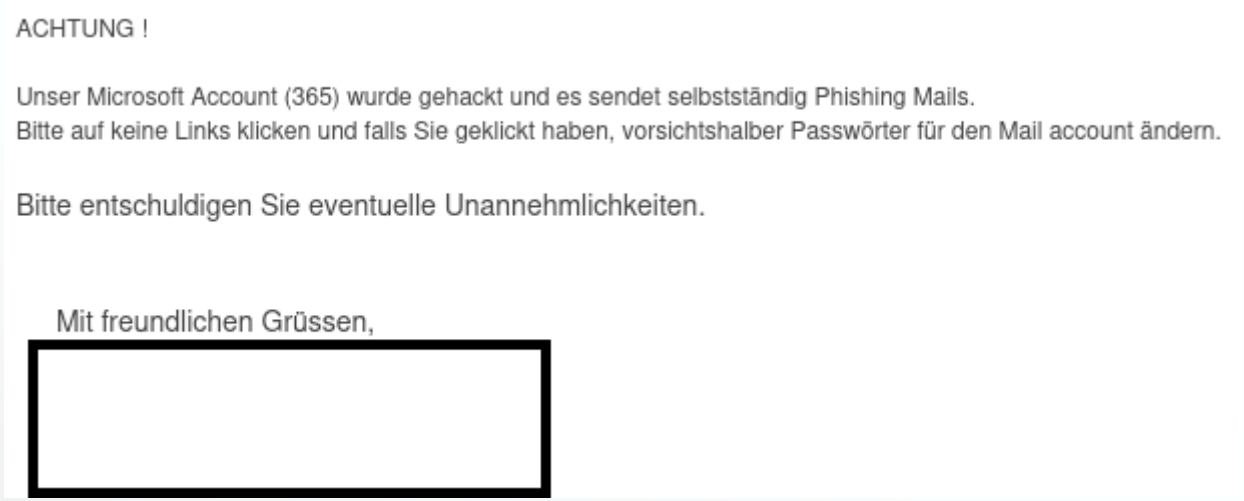
Roman

- Subject: Offene Zahlung AVANTEC AG [secure] [signed OK]
- From: user@partner.ch
- To: user@avantec.ch
- EHLO IP: IP Partner
- Reverse mail.partner.ch

- Inhalt: Kontoänderung
- Anhang
  - Original Rechnung
  - Bestätigung der Bank über Kontoänderung
- Mail war signiert!

Phishing

Compromized Accounts



ACHTUNG !

Unser Microsoft Account (365) wurde gehackt und es sendet selbstständig Phishing Mails.
Bitte auf keine Links klicken und falls Sie geklickt haben, vorsichtshalber Passwörter für den Mail account ändern.

Bitte entschuldigen Sie eventuelle Unannehmlichkeiten.

Mit freundlichen Grüssen,

- Schutz der eigenen Accounts mit phishing-sicherer Authentisierung
  - Keine Passworte
  - Asymmetrische Verfahren
    - Zertifikate
    - FIDO2/Passkeys

AVANTEC
Competence. Security. Trust.

Zusammenfassung

26. März 2026

Was kann ich tun?

AVANTEC
Competence. Security. Trust.

- Überprüfen Sie ihren Phishing Schutz
  - Schützt das Mail Gateway noch gegen aktuelle Angriffsmethoden?
  - xorlab Attack Simulation
- Einbeziehung der Mitarbeiter
  - Einfache Meldungsmöglichkeit von verdächtigen Mails / schnelles Feedback
  - Awareness Training
- Ausgehende Mails compliant verschicken
  - Einfachere Erkennung beim Empfänger
  - Brand Protection

  - Mail Authentisierung (SPF, DKIM, DMARC)
  - Emails signieren mit S/MIME
  - Sichere Authentisierung gegen Account Compromize

AVANTEC
Competence. Security. Trust.

Fragen!

26. März 2026