Das Internet – Gefahr und Betrug

Deutscher Philologenverband



Herzlich Willkommen!

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Vorstellung Prof. Dr. Horst Heineck

- bis 2020 Professor für Datenbank- und Betriebssysteme an der Hochschule Hof
- bis 2020 Dekan der Fakultät Informatik an der Hochschule Hof
- seit 2019 wohnhaft in Adelsdorf / Mittelfranken
- seit 2020 beratendes Mitglied des Seniorenbeirates Adelsdorf
- seit 2021 verantwortlich für den IT-Stammtisch in Adelsdorf, ab 2026 DigiFIT Adelsdorf
- seit 2024 Mitwirkung bei DigiFIT in Aurachtal und seit 2025 in Höchstadt
- seit 2025 Vorsitzender des Seniorenbeirates in Adelsdorf

Das Internet – Gefahr und Betrug

Gliederung

Grundbegriffe des Internets

Was ist Internetbetrug?

Phishing per E-Mails, SMS oder Messenger

Quishing

Anzeigenbetrug

Gefälschte Online-Shops – Fake Shops

Vorkassenbetrug

Dreiecksbetrug

Liebesbetrug

CEO-Fraud

Abofallen

Anlagebetrug

Deep-Fake-Betrug

Fazit

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Geschichte des Internets

Um die heutige Bedeutung des Internets und seine Auswirkungen auf unser tägliches Leben besser zu verstehen, ist es nötig, einen genauen Blick auf die Entstehungsgeschichte zu werfen.

Die Geschichte des Internets begann in den späten 1960er-Jahren mit einem Forschungsauftrag der Advanced Research Projects Agency (ARPA), einer Abteilung des US-Verteidigungsministeriums. Die ARPA finanzierte die Entwicklung eines Computernetzwerks namens ARPANET, das ursprünglich als Nachrichtensystem für Wissenschaftler an Universitäten und Forschungseinrichtungen konzipiert war. Die Anbindung der Großrechner über Telefonleitungen führte zur Vernetzung von Computern, was damals eine wahre Revolution in der Computertechnik darstellte.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Geschichte des Internets

Im Jahr 1983 wurde das MILNET, ein Ableger des ARPANET, konstruiert, um militärische Zwecke zu erfüllen. Um Zugang zu weiteren Rechnern in anderen Netzwerken zu ermöglichen, entwickelten Wissenschaftler der Stanford Universität und der amerikanischen Behörde für Forschungsprojekte der Verteidigung (DARPA) das Netzwerkprotokoll TCP/IP. Dieses Protokoll erlaubt es, Informationen zwischen verschiedenen Netzwerken auszutauschen. Die Einführung von TCP/IP führte schließlich zur Verbindung von ARPANET, MILNET und später auch CSNET, einem Netzwerk für Computerwissenschaftler.

Der Zugang zum World Wide Web wurde durch den ersten grafischen Webbrowser, Mosaic, im Jahr 1993 entscheidend erleichtert. Die benutzerfreundliche Oberfläche ermöglichte es auch Nicht-Experten, das Internet zu nutzen, und führte zu einer raschen Verbreitung des Internets in den 1990er-Jahren. Damit konnten nun auch Privatanwender und Unternehmen die vielfältigen Möglichkeiten des Netzes nutzen. Die Anzahl der Knotenpunkte wuchs rasant, **der Siegeszug des Internets war nun nicht mehr aufzuhalten.**

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Grundbegriffe des Internets - URL

Ein **Uniform Resource Locator** – URL (englisch für „einheitlicher Verorter für Ressourcen“) identifiziert und lokalisiert eine Ressource, beispielsweise eine Webseite, über die zu verwendende Zugriffsmethode (zum Beispiel das verwendete Netzwerkprotokoll wie http, https oder ftp) und den Ort der Ressource in Computernetzwerken.

Der grundsätzliche URL-Aufbau besteht aus einer, die Zugriffsmethode festlegenden Schema-Bezeichnung und einem Schema-spezifischen Teil, die durch einen Doppelpunkt getrennt sind:

<scheme>:<scheme-specific-part>

https://horst-heineck.de

mailto:Horst.Heineck@googlemail.com

Das Schema legt fest, mit welcher Methode die Resource angesprochen werden soll. Meistens, aber nicht zwingend gleichlautend mit dem verwendeten Netzwerkprotokoll, wie http, https oder ftp

Je nach Schema sind unterschiedliche spezifische Angaben erforderlich und möglich. In den meisten Fälle beginnen sie mit der Zeichenkette //.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Grundbegriffe des Internets - http und https

Bei **http** handelt es sich um eine Abkürzung. Sie steht für **Hypertext Transfer Protocol** und ermöglicht es Nutzern, Daten zu übertragen und zu empfangen – es ist das Protokoll des World Wide Webs und wird daher automatisch vorangestellt, auch wenn es nicht eingegeben wird.

Mithilfe des Protokolls können Clients und Server im Internet miteinander kommunizieren. Erstere kennen Sie als User beispielsweise in Form von Anwendungen wie den Webbrowsern Firefox, Chrome oder Safari und E-Mail-Diensten wie Outlook, Thunderbird oder Mail.

Wenn Sie eine Website besuchen, sendet Ihr Browser eine http-Anfrage an den Webserver, der mit einer http-Antwort antwortet. Der Webserver und Ihr Browser tauschen Daten im Klartext aus. Kurz gesagt, das http-Protokoll ist die zugrunde liegende Technologie, die die Netzwerkkommunikation unterstützt. Wie der Name schon sagt, ist **https - Hypertext Transfer Protocol Secure** eine sicherere Version oder Erweiterung von http. Bei https stellen Browser und Server eine sichere, verschlüsselte Verbindung her, bevor Daten übertragen werden.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Grundbegriffe des Internets - ftp und sftp

ftp - File Transfer Protocol ist ein Standard-Internetprotokoll, das, wie der Name schon sagt, zum Übertragen von Dateien zwischen Computern verwendet wird. ftp-Software verwendet ein Client-Server-Modell Bsp.: Fischmarkt Hamburg eile, einen ftp-Client und einen ftp-Server. Beliebte Anwendungen für ftp sind das Hoch- oder Herunterladen von Dateien zur Archivierung oder das Teilen von Dateien, die für E-Mail zu groß sind

In den meisten Fällen wird die ftp-Funktion heute tatsächlich von sftp-Servern und **ssh**-Clients bedient. sftp ähnelt ftp mit der Ausnahme, dass der gesamte Datenverkehr, einschließlich Passwörter, Befehle und Daten, verschlüsselt wird, um ein Abhören während der Übertragung zu verhindern.

Grundbegriffe des Internets - ssh

ssh - Secure Shell ist ein Netzwerkprotokoll, das verschlüsselte Verbindungen zwischen Computern für einen sicheren Fernzugriff herstellt. Es arbeitet über **TCP-Port 22** und bietet Authentifizierung, Verschlüsselung und Integrität zum Schutz von Daten, die über ungesicherte Netzwerke übertragen werden.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Grundbegriffe des Internets - TCP/IP-Transmission Control Protocol/Internet Protocol

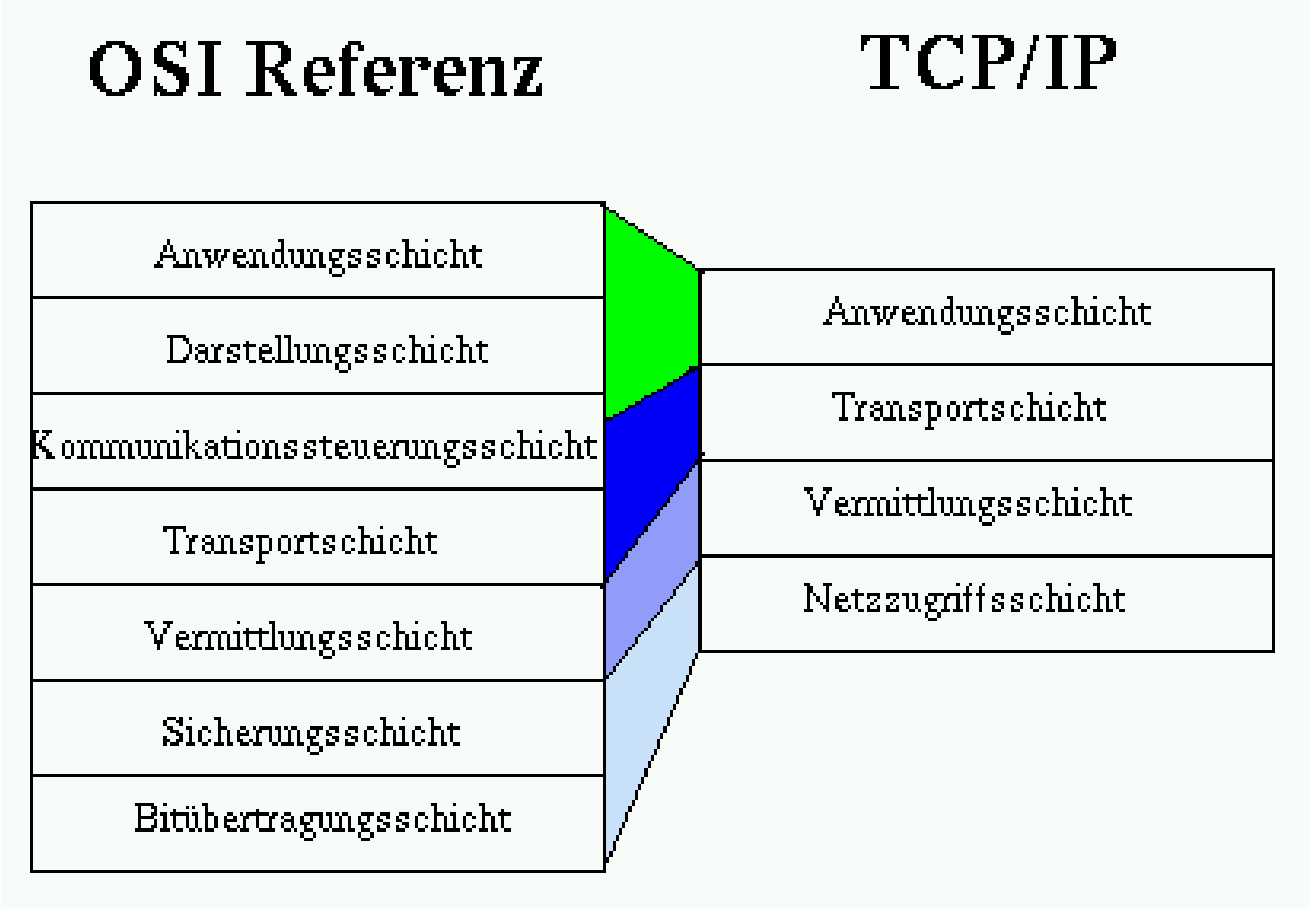
Eine **IP-Adresse** ist eine Adresse in Computernetzen, die – wie das Internet – auf dem Internetprotokoll (IP) basieren. Sie wird Geräten zugewiesen, die an das Netz angebunden sind, macht die Geräte so adressierbar und damit erreichbar. Die IP-Adresse kann einen einzelnen Empfänger oder eine Gruppe von Empfängern bezeichnen (Multicast, Broadcast). Umgekehrt können einem Computer mehrere IP-Adressen zugeordnet sein.

Die IP-Adresse wird vor allem verwendet, um Daten von ihrem Absender zum vorgesehenen Empfänger zu transportieren. Ähnlich der Postanschrift auf einem Briefumschlag werden Datenpakete mit einer IP-Adresse versehen, die den Empfänger eindeutig identifiziert. Aufgrund dieser Adresse können die „Poststellen“, die Router, entscheiden, in welche Richtung das Paket weitertransportiert werden soll. Im Gegensatz zu Postadressen sind IP-Adressen nicht an einen bestimmten Ort gebunden.

Das Internet - Gefahr und Betrug

Deutscher Philologenverband

Open Systems Interconnection versus Transmission Control Protocol/Internet Protocol



Das Internet - Gefahr und Betrug

Deutscher Philologenverband

TCP/IP - Transmission Control Protocol/Internet Protocol

Transmission Control Protocol					
Familie:	Internetprotokollfamilie				
Einsatzgebiet:	Zuverlässiger bidirektionaler Datentransport				
TCP im TCP/IP-Protokollstapel:					
Anwendung	HTTP		SMTP		…
Transport	**TCP**				
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	…

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Grundbegriffe des Internets - IP-Adresse und DNS

Der Name einer Internetseite muss in eine entsprechende IP-Adresse übersetzt werden. Dazu wird im Netz der Dienst DNS - Domain Name System genutzt. Dieser wird im Computer durch eine IP-Adresse adressiert.

Das DNS, deutsch Domain-Namen-System, ist ein hierarchisch unterteiltes Bezeichnungssystem in einem meist IP-basierten Netz zur Beantwortung von Anfragen zu Domain-Namen.

Das DNS funktioniert ähnlich wie eine Telefonauskunft. Der Benutzer kennt die Domain (den für Menschen merkbaren Namen eines Rechners im Internet) – zum Beispiel **`example.com`**. Diese sendet er als Anfrage in das Internet. Die Domain wird dann dort vom DNS in die zugehörige IP-Adresse (die „Anschlussnummer“ im Internet) umgewandelt. Jeder Computer, der im Internet ist, besitzt mindesten eine IP-Adresse.

Zum Beispiel eine IPv4-Adresse der Form: **`81.169.145.90`**
oder eine IPv6-Adresse wie: **`2001:db8:85a3:8d3:1319:8a2e:370:7347`**
und führt so zum richtigen Rechner.

Das Internet – Gefahr und Betrug

Grundbegriffe des Internets - IPv4-Internet Protocol Version 4

Eine IPv4-Adresse ist eine **32-Bit-Nummer**, die eindeutig ein Netzwerkinterface in einem IPv4-Netzwerk identifiziert. Sie ist normalerweise in **dezimaler Form** dargestellt und durch Punkte in **vier 8-Bit-Blöcke** (Oktette) unterteilt.

Jedes der vier Oktette besteht aus 8 Bit und stellt somit $2^8 = 256$ verschiedene Werte dar. Daraus ergibt sich eine Gesamtzahl von $256 \times 256 \times 256 \times 256 = 256^4 = 2^{32}$ = **4.294.967.296 IPv4-Adressen**.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

IPv4 versus IPv6 – Internet Protocol, Version 6

Der Hauptunterschied zwischen den Protokollen IPv4 und IPv6 besteht darin, dass IPv4-Adressen 32 Bits verwenden, das sind 4,3 Milliarden IP-Adressen. Die IPv6 ist ein 128-Bit-Protokoll und bietet 340 Undezillionen IP-Adressen.

2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456

IPv6 wird in naher Zukunft IPv4 als Haupt-Internetprotokoll ablösen. Das liegt daran, dass wir mit IPv4 irgendwann keine eindeutigen IP-Adressen mehr zuweisen können. Das neue Internetprotokoll löst dieses Problem.

Trotz seiner offensichtlichen Überlegenheit im Umfang hat sich IPv6 aus folgendem Grund noch nicht vollständig durchgesetzt. Weil IPv6 nicht mit IPv4 funktioniert. Wenn eine Webseite auf IPv4 läuft, Ihr Gerät und Ihr Internetanbieter aber ausschließlich das neuere Protokoll verwenden, können Sie nicht auf die Webseite zugreifen. Um auf die Webseite zugreifen zu können, muss Ihr Gerät auch mit IPv4 kompatibel sein.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Grundbegriffe des Internets - DNS-Domain Name System

Die Verwendung eines einfacheren, einprägsameren Namens anstelle der numerischen Adresse eines Gastgebers stammt aus der ARPANET-Ära. Das Stanford Research Institute führte eine Textdatei namens HOSTS.TXT ein, die Hostnamen den numerischen Adressen von Computern auf dem ARPANET zuordnete.

In Betriebssystem wird diese Datei als **`/etc/hosts`** - in UNIX-Systemen bzw. **`C:\Windows\System32\drivers\etc\hosts`** – in Windows bezeichnet. Darin sind in der Regel IP-Adressen des lokalen Netzwerkes zusammengefasst:

```
127.0.0.1 localhost

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

192.168.178.1      gateway.fritz.box          gateway
192.168.178.1      NTP-server-host
192.168.178.107    ioBroker-NUC7CJYH.fritz.box  ioBroker-NUC7CJYH   # LAN
192.168.178.50     smarthome2.fritz.box       smarthome2          # WLAN
192.168.178.46     smarthome3.fritz.box       smarthome3          # WLAN
```

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Grundbegriffe des Internets - DNS-Domain Name System

Da nicht alle zugreifbaren Domänen in der Datei **`hosts`** vorhanden sein können, wird die Namensauflösung im DNS weiter versucht. Dazu wird im Betriebssystem, Browser oder Router eine Ziel-IP-Adresse eingetragen. Meistens kommen die Systeme von den Tech-Konzerne aus den USA.

In den Produkten von Google wird dementsprechend die Adresse **`8.8.8.8`** hinterlegt. Entweder direkt oder bei fehlender Angabe indirekt in den Systemen. Alle Aufrufe der Nutzer benutzen jeweils mehrmals das DNS und liefern somit Daten der Nutzers an Google.

Diesen Machenschaften der Tech-Konzerne kann begegnet werden, indem DNS-Andressen, z.B. von Servern, die in der EU liegen, eingetragen werden.

Ein vorgeschlagener Server ist **`dns.quad9.net`**. Folgende Einträge sollten dazu in den Systemen vorgenommen werden:

Protokoll		Alternative
IPv4	9.9.9.11	149.112.112.11
IPv6	2620:fe::11	2620:fe::fe:11

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Grundbegriffe des Internets - MAC-Adresse

Die MAC-Adresse Media-Access-Control-Adresse, auch Media-Access-Code-Adresse ist die Nummer eines Gerätes auf einer Datenverbindung. Anhand dieser Nummer werden über die Verbindung laufende Daten den Geräten zugeordnet.

Die MAC-Adresse wird auch als physische Adresse bezeichnet, weil sie normalerweise vom Hersteller in ein Gerät fest und nicht veränderbar einprogrammiert wurde. Sofern Betriebssystem und Hardware dies unterstützen, kann die MAC-Adresse jedoch auch von dem Benutzer geändert werden.

Seit 2020 werden vor allem bei Smartphones auch zufällig vergebene temporäre MAC-Adressen eingesetzt. Bei dem Betriebssystem Android ist dies seit Version 10 beziehungsweise bei iOS seit Version 14 voreingestellt der Fall. Damit soll aus Gründen des Datenschutzes ein Nachverfolgen von Nutzern verhindert werden.

Das Internet – Gefahr und Betrug

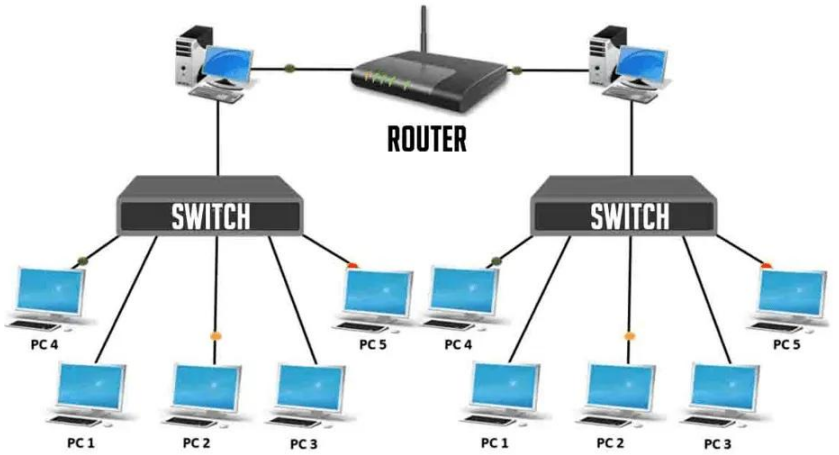
Deutscher Philologenverband

Grundbegriffe des Internets - Router versus Switch

Router und Switches sind beide Computer Networking Geräte, mit denen ein oder mehrere Computer mit anderen Computern, vernetzten Geräten oder anderen Netzwerken verbunden werden können.

Die meisten Unternehmensnetzwerke verwenden heutzutage Switches, um Computer, Drucker und Server innerhalb eines Bürogebäudes miteinander zu verbinden. Ein Switch dient als Controller, der es vernetzten Geräten ermöglicht, effizient miteinander zu kommunizieren.

Ein Router verbindet mehrere Computer oder Swiches mit dem Internet, sodass Nutzer die Verbindung gemeinsam nutzen können. Ein Router fungiert als „Dispatcher“, also als Zuteiler, der den besten Pfad für den Fluss von Informationen wählt, damit diese schnell empfangen werden.



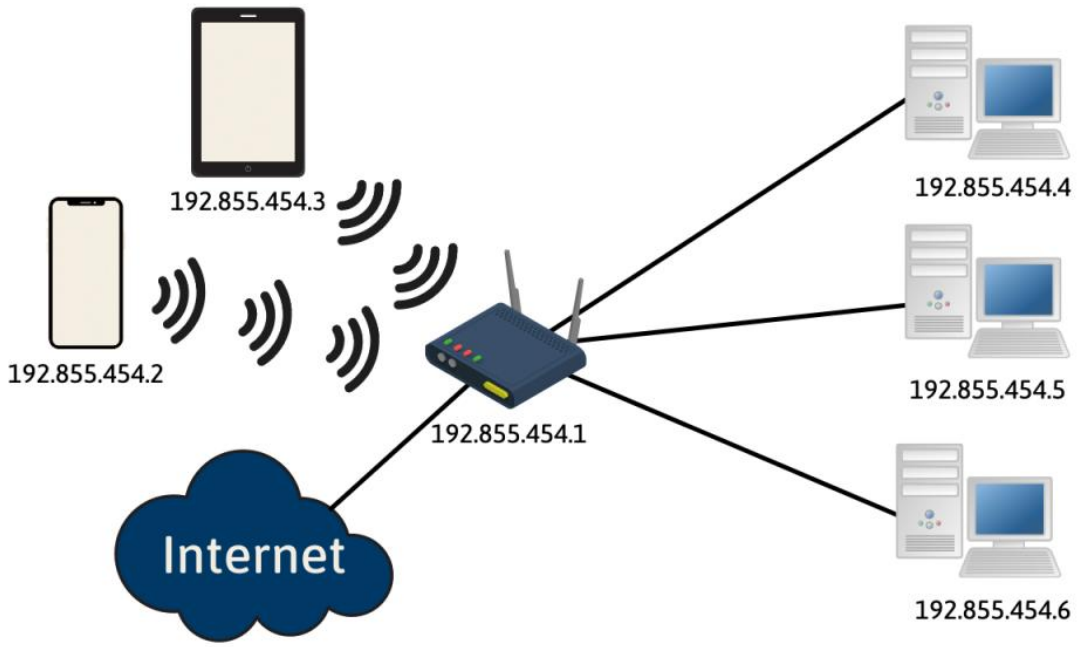
Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Grundbegriffe des Internets - Einsatz der Fritz!box

Eine Fritz Box ermöglicht es Ihnen, Internet per DSL oder Kabel oder sogar UMTS/LTE zu empfangen und über den Router anschließend an Ihre internetfähigen Geräte zu verteilen.

Da die Fritz!Box ein Router ist, können Sie ein eigenes Netzwerk aufbauen und somit viele unterschiedliche Endgeräte untereinander verbinden, dabei spielt die Beschränkung der möglichen IP-Adresse weltweit keine Rolle.

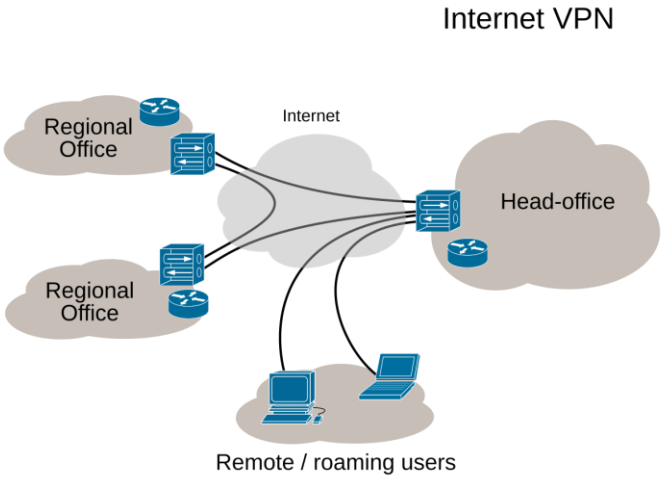


Das Internet – Gefahr und Betrug

Grundbegriffe des Internets - VPN-Virtual Private Network

Das **Virtual Private Network** virtuelles privates Netzwerk bezeichnet ein virtuelles privates (in sich geschlossenes) Kommunikationsnetz. Virtuell in dem Sinne, dass es sich nicht um eine eigene physische Verbindung handelt, sondern um ein bestehendes Kommunikationsnetz, das als Transportmedium verwendet wird. Das VPN dient dazu, Teilnehmer des bestehenden Kommunikationsnetzes an ein anderes Netz zu binden.

So kann beispielsweise der Computer eines Mitarbeiters von zu Hause aus Zugriff auf das Firmennetz erlangen, gerade so, als säße er mittendrin. Aus Sicht der VPN-Verbindung werden dafür die dazwischen liegenden Netze (sein Heimnetz sowie das Internet) auf die Funktion eines Verlängerungskabels reduziert, das den Computer (VPN-Partner) ausschließlich mit dem zugeordneten Netz verbindet (VPN-Gateway). Er wird nun zum Bestandteil dieses Netzes und hat direkten Zugriff darauf.



Das Internet – Gefahr und Betrug

Grundbegriffe des Internets - Viren und Trojaner

- Ein Computervirus hängt sich an ein Programm oder eine Datei an und erstellt eigenen Code, um sich zwischen einzelnen Programmen zu verbreiten und die betroffenen Geräte dabei zu infizieren.
- Ähnlich wie bei menschlichen Viren können Computerviren nach der Schwere der Infektion unterschieden werden. Einige Viren verursachen nur geringfügige störende Effekte, während andere Ihre Hardware, Software oder Dateien beschädigen.
- Nahezu alle Computerviren sind an eine ausführbare Datei angehängt.
- Das bedeutet, dass der Virus auf Ihrem Computer vorhanden sein kann, ihn jedoch erst infiziert, wenn Sie das Schadprogramm anklicken, ausführen oder öffnen.
- Ein wichtiger Punkt ist, dass sich ein Virus nicht ohne menschliches Zutun verbreiten kann und sich z. B. erst durch Klicken auf einen manipulierten Link oder durch Ausführen eines infizierten Programms ausbreitet.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Grundbegriffe des Internets - Viren und Trojaner

- Als Trojaner wird jede Art von Schadsoftware bezeichnet, die dem Benutzer eine falsche Absicht vortäuscht.
- Dabei kann es sich zum Beispiel um ein Schadprogramm handeln, das wie eine legitime Anwendung aussieht.
- Die Bezeichnung Trojaner ist vom Trojanischen Pferd aus der griechischen Sagenwelt abgeleitet, das letztendlich als Mittel zur Zerstörung Trojas diente.
- Im Gegensatz zu Viren replizieren sich Trojaner nicht selbst, können jedoch ebenso großen Schaden anrichten.
- Trojaner öffnen zudem eine Hintertür auf Ihrem Computer, über die Angreifer oder andere Schadprogramme Zugang zu Ihrem System erhalten und personenbezogene Daten oder andere vertrauliche Informationen stehlen können.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Grundbegriffe des Internets - E-Mail-Parameter

Email-Sender:	Über diesen Parameter kann die Bezeichnung des Benutzers oder einer Benutzergruppe angegeben werden. Abhängig von dieser Einstellung werden die entsprechenden Informationen aus der Konfiguration der E-Mail-Konten verwendet. Wird der Parameter nicht gesetzt, wird die Benutzergruppe verwendet.
Email-To:	Mit diesem Parameter wird angegeben an welche E-Mail-Adresse oder E-Mail-Adressen die E-Mail versendet werden soll.
Email-Cc, Email-Bcc:	Mit diesen Parametern können weitere E-Mailadressen für eine Kopie bzw. Blindkopie der E-Mail hinzugefügt werden. Das senden einer Blindkopie verhindert, dass alle anderen Empfänger diese E-Mail-Adresse sehen. Mehrere E-Mail-Adressen müssen durch ein Komma getrennt werden. Werden mehrere Zeilen an den Email Connector übergeben macht das System hieraus automatisch eine durch Komma getrennte Liste von E-Mail-Adressen.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Was ist Internetbetrug?

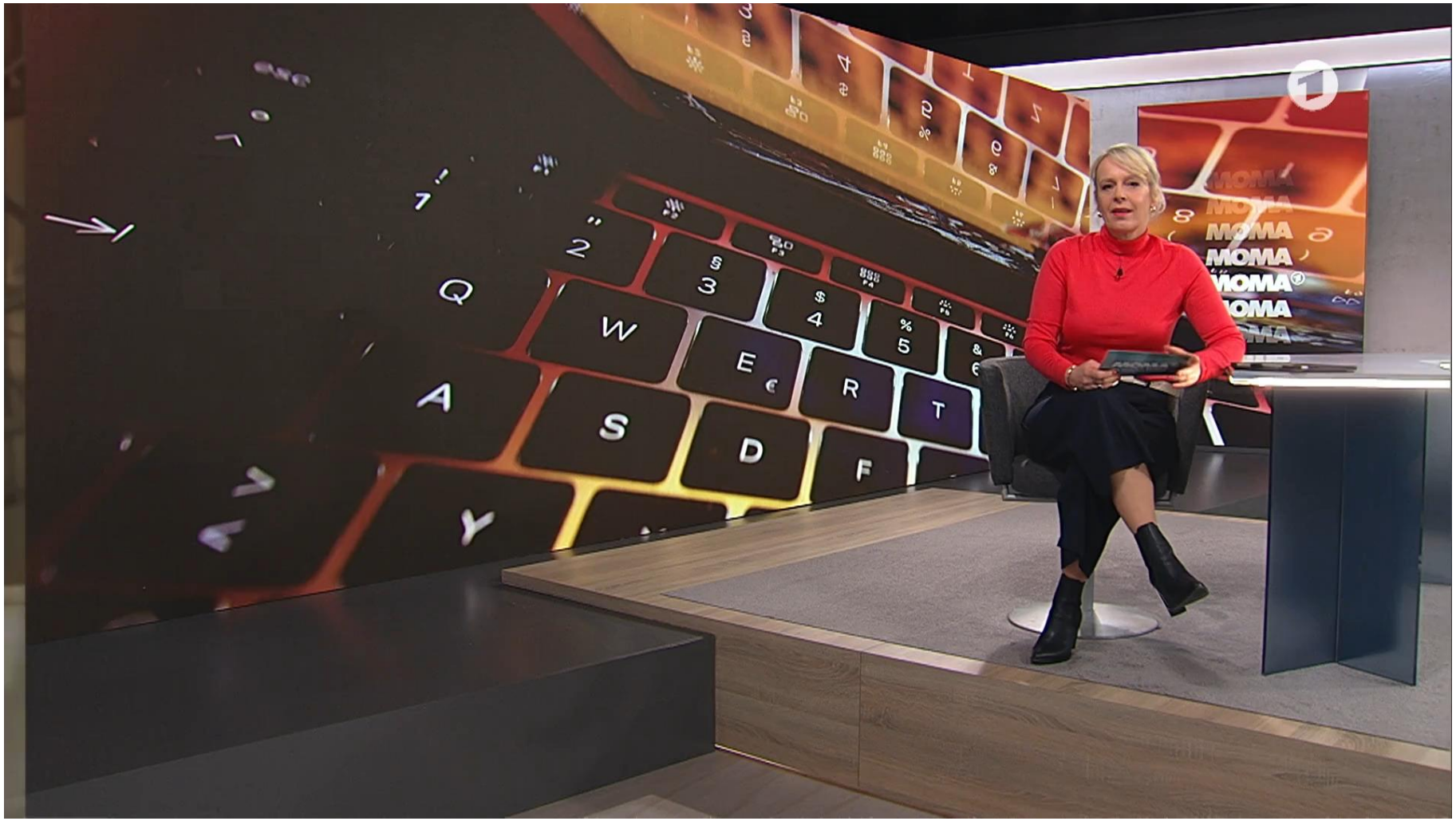
Internetbetrug umfasst die Nutzung von Online-Diensten und Software, die Zugang zum Internet haben, um Opfer zu betrügen oder auszunutzen.

Der Begriff „Internetbetrug“ umfasst im Allgemeinen Cyberkriminalitäts-Aktivitäten, die über das Internet oder per E-Mail, Messenger und Social Media stattfinden.

Einschließlich Straftaten wie Identitätsdiebstahl, Phishing und andere Hacking-Aktivitäten, die darauf abzielen, Menschen um ihr Geld zu betrügen oder die Identität von Nutzern abzugreifen.

Ihre Identität, d.h., Ihre persönlichen Daten sind ein Wirtschaftsgut, das für Betrüger bares Geld wert ist.

Das Internet – Gefahr und Betrug



Das Internet – Gefahr und Betrug

Phishing per E-Mails, SMS oder Messenger

- Phishing (Englisch, in Anlehnung an *fishing* = das Fischen) ist eine der wohl bekanntesten Betrugsformen: Kriminelle verschicken gefälschte E-Mails, SMS oder Messenger-Nachrichten.

- Diese sehen so aus, als kämen sie von vertrauenswürdigen Institutionen – z. B. von der Bank, einem Online-Shop, einer Behörde, einem Transportunternehmen oder sogar von Bekannten.

- In diesen Nachrichten fordern Sie Betrüger auf, einen Anhang zu öffnen. Oder sie wollen Sie dazu verleiten, auf einen Link zu klicken. Dieser führt auf eine betrügerische Seite. Oft ist dort eine täuschend echt wirkende Oberfläche nachgebaut.

- Dort sollen Sie sensible Daten eingeben. Betrüger haben es mit Phishing in der Regel auf Zugangs-, Adress- oder Zahlungsdaten abgesehen. Teilweise geht es beim Phishing auch um Ihre Identität – Betrüger fragen dann beispielsweise nach einer Ausweiskopie.

Das Internet – Gefahr und Betrug

Phishing per E-Mails, SMS oder Messenger

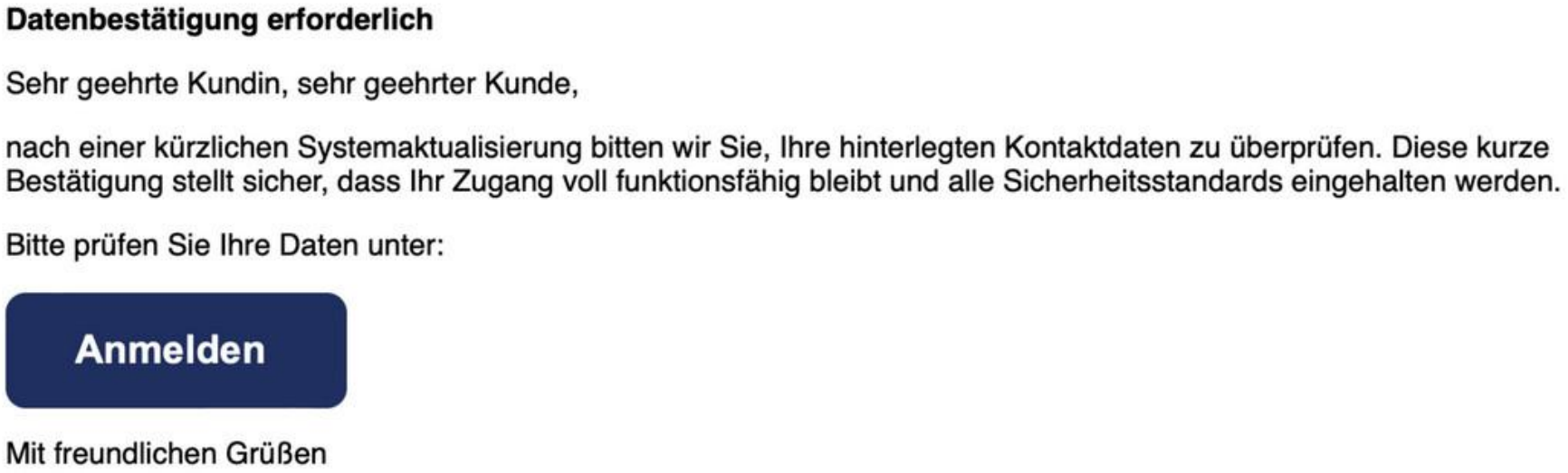
So erkennst man den Betrug:

- Man erhält Nachrichten (bspw. per E-Mail, SMS oder Messenger), die zu einer schnellen (dringlichen) Handlung auffordern.
- Man wird in der Nachricht unpersönlich oder falsch angesprochen („Werte/werter Kundin/Kunde", „Sehr geehrte Damen und Herren", „Guten Tag").
- Die Nachricht enthält Rechtschreib- und Grammatikfehler und/oder stammt von einer Adresse, die nicht der üblichen Adresse des angeblichen Absenders entspricht (z. B. kryptische E-Mail-Adresse oder ausländische Rufnummer).
- Man wird für den Fall, des Sie nicht reagieren, mit Konsequenzen – beispielsweise einer Sperre des Kontos – bedroht.

Das Internet – Gefahr und Betrug

Phishing per E-Mails, SMS oder Messenger

- Alle Nachrichten haben eines gemein: Die Täter bauen Druck auf. Es sei eine dringende Handlung erforderlich. Beispielsweise, weil ein Paket im Zoll feststecke. Demnach stünde der Zustellung nur die Zahlung einer „Zollgebühr" im Weg. Es geht in der Regel um eher geringe Beträge. Doch wer seine Daten preisgibt, kann einen immensen finanziellen Schaden erleiden.



Datenbestätigung erforderlich

Sehr geehrte Kundin, sehr geehrter Kunde,

nach einer kürzlichen Systemaktualisierung bitten wir Sie, Ihre hinterlegten Kontaktdaten zu überprüfen. Diese kurze Bestätigung stellt sicher, dass Ihr Zugang voll funktionsfähig bleibt und alle Sicherheitsstandards eingehalten werden.

Bitte prüfen Sie Ihre Daten unter:

Anmelden

Mit freundlichen Grüßen

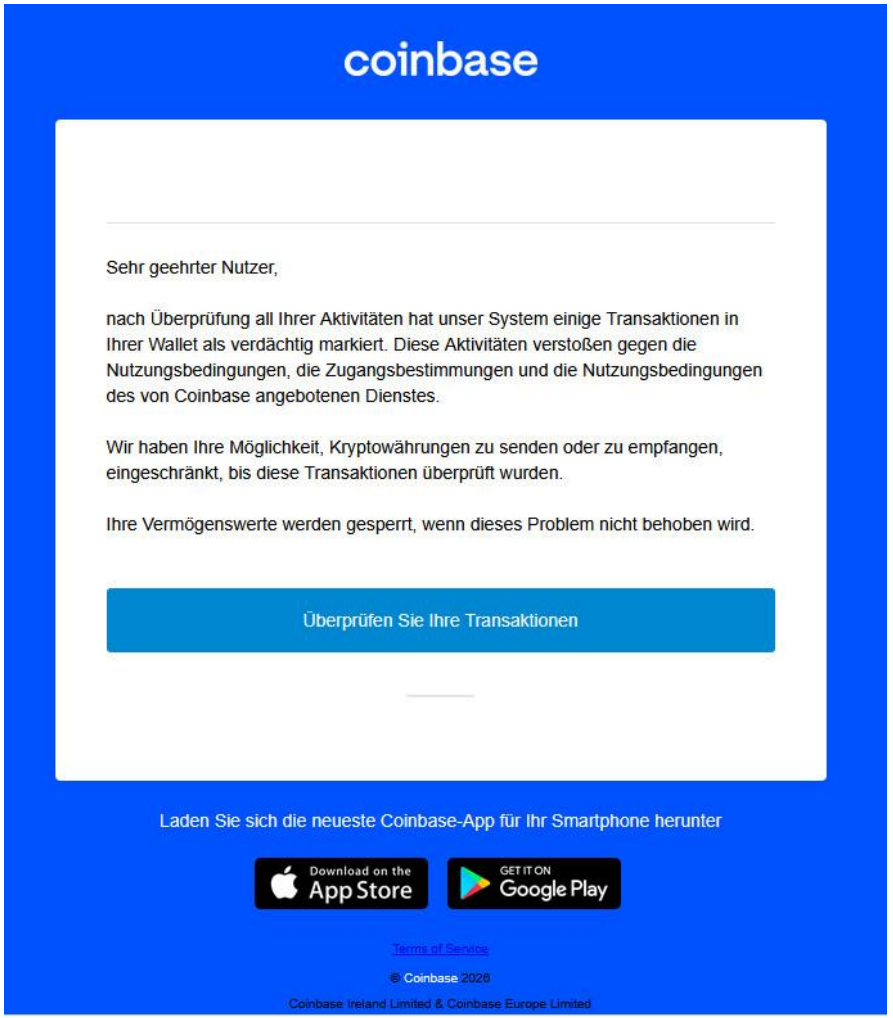
Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Phishing per E-Mails, SMS oder Messenger

Betrugsversuch mittels E-Mail
Empfangen am 25.04.2026

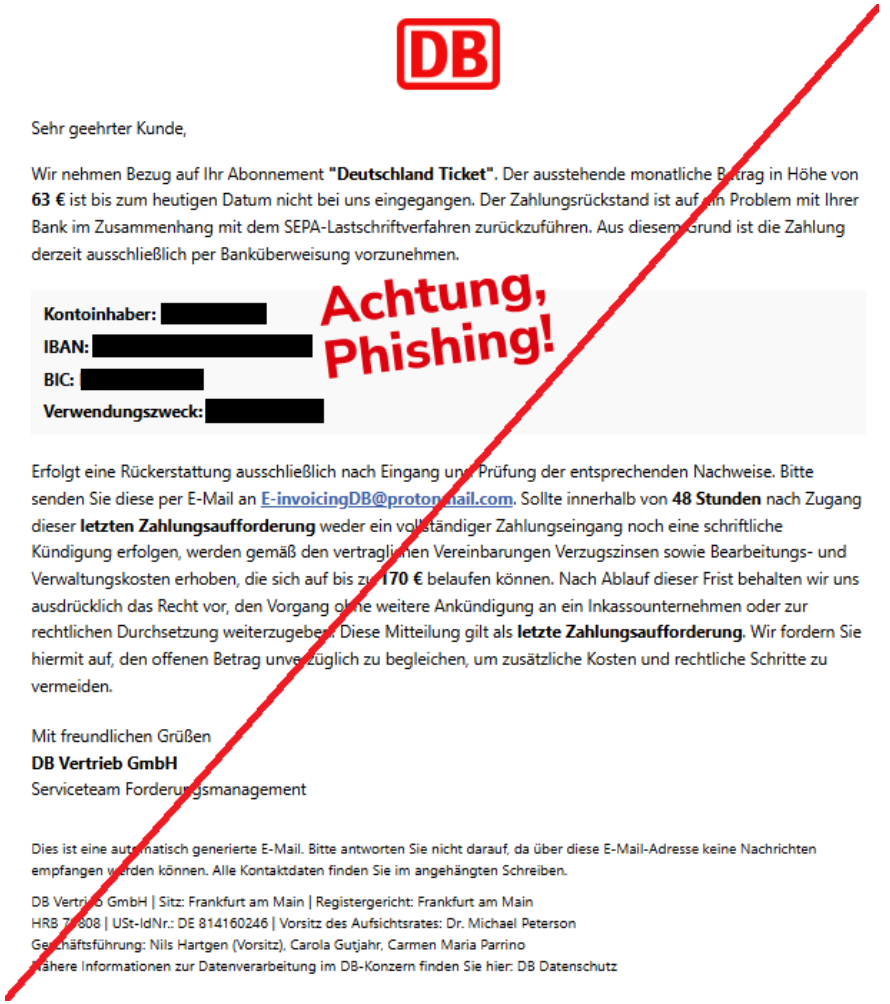
Absender:
GMX.Kundenservice.administrator.support.email.info.notification-seniorenbeirat@misis.ru



Das Internet – Gefahr und Betrug

Phishing per E-Mails, SMS oder Messenger

22. April 2026:
Vermeintliche Zahlungsaufforderung im Namen der Deutschen Bahn



DB

Sehr geehrter Kunde,

Wir nehmen Bezug auf Ihr Abonnement **"Deutschland Ticket"**. Der ausstehende monatliche Betrag in Höhe von **63 €** ist bis zum heutigen Datum nicht bei uns eingegangen. Der Zahlungsrückstand ist auf ein Problem mit Ihrer Bank im Zusammenhang mit dem SEPA-Lastschriftverfahren zurückzuführen. Aus diesem Grund ist die Zahlung derzeit ausschließlich per Banküberweisung vorzunehmen.

Kontoinhaber: [redacted]
IBAN: [redacted]
BIC: [redacted]
Verwendungszweck: [redacted]

Achtung, Phishing!

Erfolgt eine Rückerstattung ausschließlich nach Eingang und Prüfung der entsprechenden Nachweise. Bitte senden Sie diese per E-Mail an E-invoicingDB@protonmail.com. Sollte innerhalb von **48 Stunden** nach Zugang dieser **letzten Zahlungsaufforderung** weder ein vollständiger Zahlungseingang noch eine schriftliche Kündigung erfolgen, werden gemäß den vertraglichen Vereinbarungen Verzugszinsen sowie Bearbeitungs- und Verwaltungskosten erhoben, die sich auf bis zu **170 €** belaufen können. Nach Ablauf dieser Frist behalten wir uns ausdrücklich das Recht vor, den Vorgang ohne weitere Ankündigung an ein Inkassounternehmen oder zur rechtlichen Durchsetzung weiterzugeben. Diese Mitteilung gilt als **letzte Zahlungsaufforderung**. Wir fordern Sie hiermit auf, den offenen Betrag unverzüglich zu begleichen, um zusätzliche Kosten und rechtliche Schritte zu vermeiden.

Mit freundlichen Grüßen
DB Vertrieb GmbH
Serviceteam Forderungsmanagement

Dies ist eine automatisch generierte E-Mail. Bitte antworten Sie nicht darauf, da über diese E-Mail-Adresse keine Nachrichten empfangen werden können. Alle Kontaktdaten finden Sie im angehängten Schreiben.

DB Vertrieb GmbH | Sitz: Frankfurt am Main | Registergericht: Frankfurt am Main
HRB 7[illegible]808 | USt-IdNr.: DE 814160246 | Vorsitz des Aufsichtsrates: Dr. Michael Peterson
Geschäftsführung: Nils Hartgen (Vorsitz), Carola Gutjahr, Carmen Maria Parrino
Nähere Informationen zur Datenverarbeitung im DB-Konzern finden Sie hier: DB Datenschutz

Das Internet - Gefahr und Betrug

Phishing per E-Mails, SMS oder Messenger

Betreff: Unbezahlte Rechnung....
Datum: 25.05.2026, 07:42

hallo! Ich bin der chinesische Software-Ingenieur, der sich erfolgreich in dein Geräte-OS durch eine ausgeklügelte Hintertür eingeklinkt hat. Seit Monaten bist du unter stiller Beobachtung. Die Infektion begann, als du vor kurzem diese Pornoseite besucht hast; ein versteckter Trojaner wurde in deinen Browser-Cache injiziert und läuft seitdem im Hintergrund. Ich habe alle vertraulichen Dateien von deinem System extrahiert, einschließlich Dokumente, Fotos und Verlauf, und weitere Beweise gesichert.

Dein Smartphone gehört mir. Ich habe alles gesehen... speziell ein hochauflösendes Video von dir, wie du masturbierst (tolle Einrichtung, übrigens). Deine Kamera war in den letzten zwei Wochen insgesamt 47 Stunden aktiv – ohne dass du es bemerkt hast, denn ich habe manuell das kleine LED-Licht ausgeschaltet, damit es beim Aufnehmen nicht blinkt.

hier ist, was ich vorbereitet habe: Ein geteiltes Bild mit deiner aktuellen Bildschirmaktivität auf der einen Seite und deinem zufriedenen Gesicht auf der anderen. Mit einem Klick geht das an alle Kontakte in deiner Liste. Alles bereit. Zugriff auf WhatsApp? Gesichert. Private Chats mit Familie, Freunden, Kollegen, sogar Chef? Screenshots gemacht und in Ordner sortiert. Das Video ist zur sofortigen Ausstrahlung bereit. Ein falscher Schritt, und der Knopf wird gedrückt.

Dein Ruf steht auf dem Spiel. Stell dir vor, wie deine Verwandten das von deiner Nummer in der Familiengruppe erhalten oder dein Chef es während der Arbeitszeit sieht, während du eigentlich arbeiten solltest. Wie erklärst du das? Dein Leben ändert sich für immer. Alle Daten sind auf meinen sicheren Servern in einer entfernten Cloud hochgeladen. Selbst wenn du jetzt ein Werkreset machst, deinen Cache löschst und die App entfernst, habe ich noch Kopien auf meiner Festplatte. Die E-Mail-Vorlagen stehen bereit mit personalisierten Betreffzeilen. Das Video ist verarbeitet, für mobile Ansicht optimiert und komprimiert. Ich warte nur darauf, dass der Timer abläuft.

Ich beobachte diesen Posteingang live über ein dediziertes Skript. Wenn du weiterleitest, jemandem zeigst oder die Polizei rufst, weiß ich es sofort durch die Metadaten und die Ausstrahlung beginnt – beginnend mit Familie und Arbeit. Kein Zurück mehr nach dem Senden. Willst du das stoppen? Angesichts der Vulgärität des Films, stell dir die Scham vor, wenn alle es sehen. Dein Ruf ist zerstört. Du wirst ihnen nie wieder in die Augen schauen können.

Um dich zu retten: Sende **500 Euro in Bitcoin**. Hier ist meine Wallet-Adresse als QR-Code:



Schnellanleitung (Nur 12 Stunden):

1. Lade sofort **Trust Wallet** oder **Exodus** auf dein handy herunter (App Store oder Google Play).
2. Tippe **"Kaufen"**, wähle 500 EUR an Bitcoin mit Karte, Überweisung oder PayPal in der App aus.
3. Um zu zahlen, tippe **"Senden"**, scanne den QR-Code oben mit deiner Kamera/App-Schnittstelle und überweise das BTC an meine Adresse.
4. Die Transaktion muss innerhalb von **12 Stunden** auf der Blockchain bestätigt sein.

Der Countdown beginnt im Moment des Öffnens dieser E-Mail. Du hast genau **12 Stunden**. Wenn bis dann nicht bestätigt, wird das Video automatisch über mein Server-Skript gesendet. Kein manueller Knopfdruck nötig von mir.

Prüfe deinen Kontostand nicht an einer öffentlichen Börse; nutze ein privates Node oder Tor für Anonymität. Antworte nicht auf diesen Thread – schicke einfach die Mittel. Sobald ich das Geld in meiner Wallet sehe, verifiziere ich es in 10 Minuten und lösche die Dateien von meinen Servern. Du erhältst eine automatische Quittung zur Bestätigung des Löschvorgangs.

Wenn du zögerst... wenn du versuchst, es über Nacht schlafen zu lassen... oder morgen aufwachst und merkst, dass du vergessen hast... nun, das Video geht um 8:00 Uhr morgens pünktlich raus. Angehängt mit dem Text "Aus meiner privaten Sammlung".

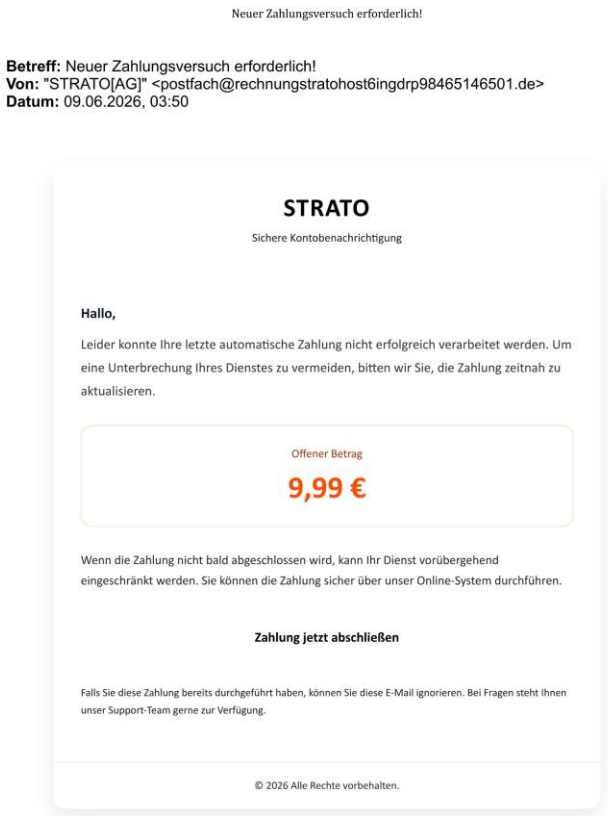
Ich suche nicht nach einer Rückerstattung. Ich suche nach Stille. Sobald bezahlt, erwarte keine Antworten von mir. Einfach wissen, dass du sicher bist. Für jetzt.

Der Ingenieur.

Das Internet - Gefahr und Betrug

Phishing per E-Mails, SMS oder Messenger

09. Juni 2026:
Vermeintliche Zahlungsaufforderung des Domänen-Anbieters Strato



Neuer Zahlungsversuch erforderlich!

Betreff: Neuer Zahlungsversuch erforderlich!
Von: "STRATO[AG]" <postfach@rechnungstratohost6ingdrp98465146501.de>
Datum: 09.06.2026, 03:50

STRATO

Sichere Kontobenachrichtigung

Hallo,

Leider konnte Ihre letzte automatische Zahlung nicht erfolgreich verarbeitet werden. Um eine Unterbrechung Ihres Dienstes zu vermeiden, bitten wir Sie, die Zahlung zeitnah zu aktualisieren.

Offener Betrag

9,99 €

Wenn die Zahlung nicht bald abgeschlossen wird, kann Ihr Dienst vorübergehend eingeschränkt werden. Sie können die Zahlung sicher über unser Online-System durchführen.

Zahlung jetzt abschließen

Falls Sie diese Zahlung bereits durchgeführt haben, können Sie diese E-Mail ignorieren. Bei Fragen steht Ihnen unser Support-Team gerne zur Verfügung.

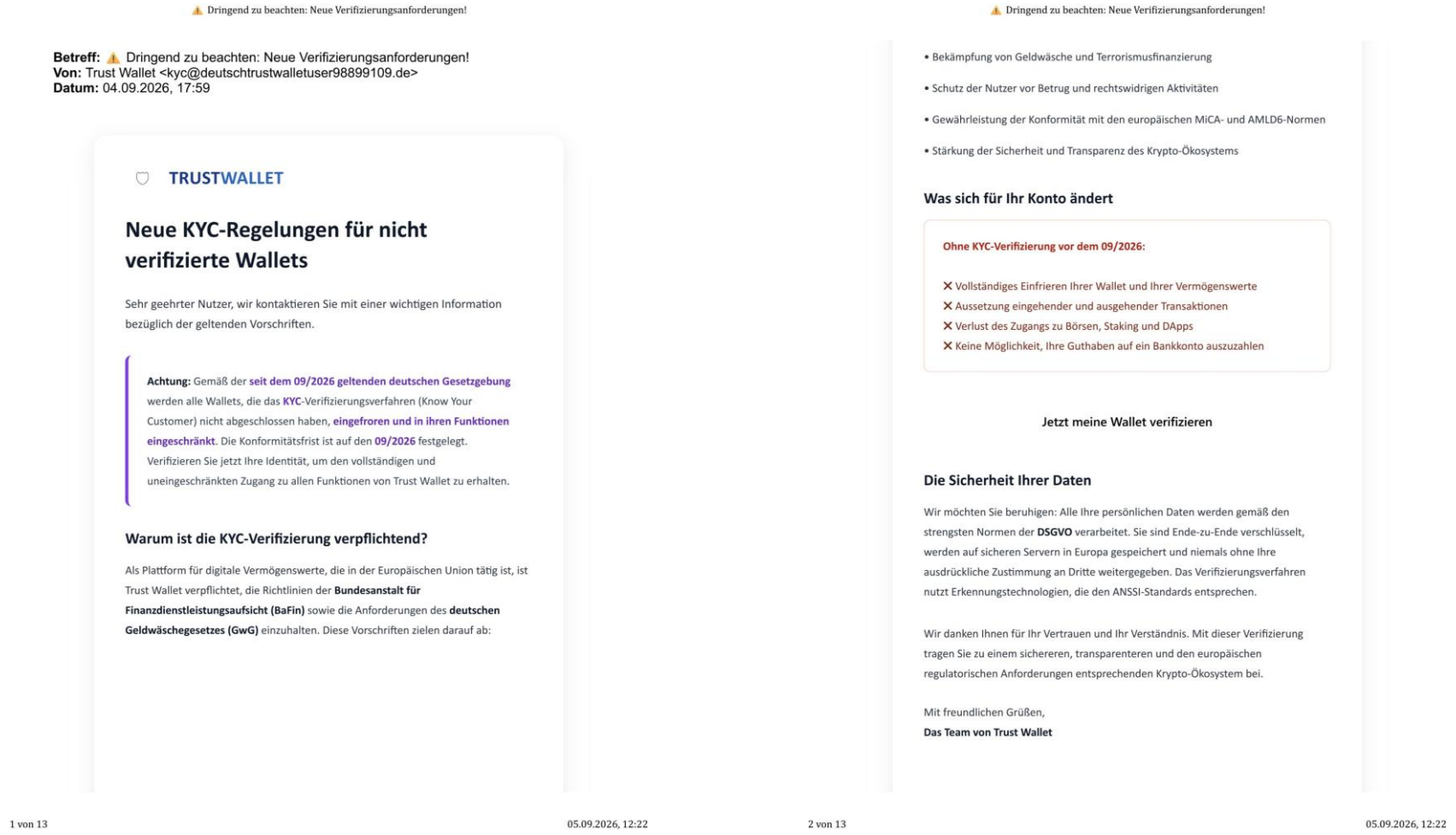
© 2026 Alle Rechte vorbehalten.

Es fällt die große Zahl an Seiten auf -> 12. D.b., dass der Text aus einer anderen Zahlungsaufforderung kopiert wurde.

1 von 12 09.06.2026, 13:52

Das Internet - Gefahr und Betrug

Phishing per E-Mails, SMS oder Messenger



⚠️ Dringend zu beachten: Neue Verifizierungsanforderungen!

Betreff: ⚠️ Dringend zu beachten: Neue Verifizierungsanforderungen!
Von: Trust Wallet <kyc@deutschtrustwalletuser98899109.de>
Datum: 04.09.2026, 17:59

TRUSTWALLET

Neue KYC-Regelungen für nicht verifizierte Wallets

Sehr geehrter Nutzer, wir kontaktieren Sie mit einer wichtigen Information bezüglich der geltenden Vorschriften.

Achtung: Gemäß der **seit dem 09/2026 geltenden deutschen Gesetzgebung** werden alle Wallets, die das **KYC**-Verifizierungsverfahren (Know Your Customer) nicht abgeschlossen haben, **eingefroren und in ihren Funktionen eingeschränkt**. Die Konformitätsfrist ist auf den **09/2026** festgelegt. Verifizieren Sie jetzt Ihre Identität, um den vollständigen und uneingeschränkten Zugang zu allen Funktionen von Trust Wallet zu erhalten.

Warum ist die KYC-Verifizierung verpflichtend?

Als Plattform für digitale Vermögenswerte, die in der Europäischen Union tätig ist, ist Trust Wallet verpflichtet, die Richtlinien der **Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)** sowie die Anforderungen des **deutschen Geldwäschegesetzes (GwG)** einzuhalten. Diese Vorschriften zielen darauf ab:

1 von 13 05.09.2026, 12:22

⚠️ Dringend zu beachten: Neue Verifizierungsanforderungen!

- Bekämpfung von Geldwäsche und Terrorismusfinanzierung
- Schutz der Nutzer vor Betrug und rechtswidrigen Aktivitäten
- Gewährleistung der Konformität mit den europäischen MiCA- und AMLD6-Normen
- Stärkung der Sicherheit und Transparenz des Krypto-Ökosystems

Was sich für Ihr Konto ändert

Ohne KYC-Verifizierung vor dem 09/2026:

- ✕ Vollständiges Einfrieren Ihrer Wallet und Ihrer Vermögenswerte
- ✕ Aussetzung eingehender und ausgehender Transaktionen
- ✕ Verlust des Zugangs zu Börsen, Staking und DApps
- ✕ Keine Möglichkeit, Ihre Guthaben auf ein Bankkonto auszuzahlen

Jetzt meine Wallet verifizieren

Die Sicherheit Ihrer Daten

Wir möchten Sie beruhigen: Alle Ihre persönlichen Daten werden gemäß den strengsten Normen der **DSGVO** verarbeitet. Sie sind Ende-zu-Ende verschlüsselt, werden auf sicheren Servern in Europa gespeichert und niemals ohne Ihre ausdrückliche Zustimmung an Dritte weitergegeben. Das Verifizierungsverfahren nutzt Erkennungstechnologien, die den ANSSI-Standards entsprechen.

Wir danken Ihnen für Ihr Vertrauen und Ihr Verständnis. Mit dieser Verifizierung tragen Sie zu einem sichereren, transparenteren und den europäischen regulatorischen Anforderungen entsprechenden Krypto-Ökosystem bei.

Mit freundlichen Grüßen,
Das Team von Trust Wallet

2 von 13 05.09.2026, 12:22

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Phishing per E-Mails, SMS oder Messenger

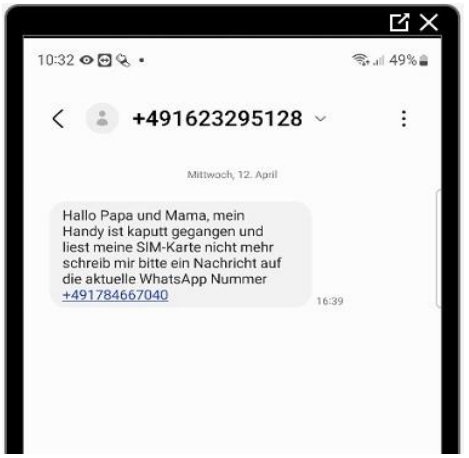
So schützt man sich:

- Nehmen Sie sich die Zeit: prüfen Sie die Nachrichten eingehend und orientieren Sie sich dabei an typischen Merkmalen für Betrug.
- Klicken Sie niemals auf Links von unbekannten Absendern. Generell sollten Websites besser direkt aufrufen, in der Regel findet man dort die Nachrichten erneut.
- Öffnen Sie auf keinen Fall Dateianhänge, die Sie nicht selbst angefragt haben.
- Geben Sie niemals sensible Informationen wie Zugangs- oder Zahlungsdaten auf Websites ein, die Ihnen verdächtig vorkommen.
- Sind Sie sich unsicher, besprechen Sie sich mit Bekannten oder Verwandten oder wenden Sie sich auf vertrauten Wegen direkt an den vermeintlichen Absender.

Das Internet – Gefahr und Betrug

Phishing per E-Mails, SMS oder Messenger

Der sogenannte „Enkeltrick“:



- Ständig werden Nachrichten verschickt, die dem Enkeltrick zuzuordnen sind. Das Bild zeigt exemplarisch eine solche Nachricht, die ich am 12.04.2023 um 16:39 Uhr erhalten habe:

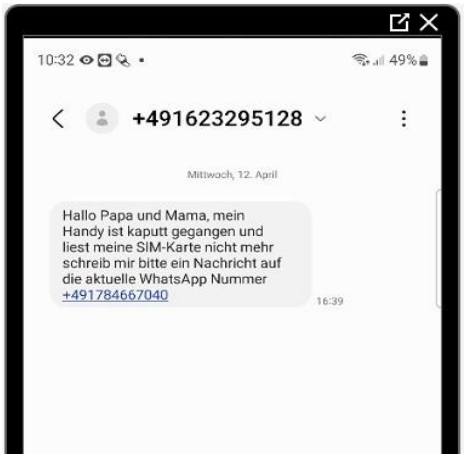
- Was ist in diesem Fall zu tun. **Auf keinen Fall** auf die angegebene Nummer, hier +491784667040 klicken oder drücken. Weiterhin sollte die Sende-Nummer hier +491623295128 gesperrt werden.

- Umfangreiche Informationen über ergriffene Maßnahmen gegen Rufnummernmissbrauch werden auf der Internetseite www.bundesnetzagentur.de/aktuelles und in einer Maßnahmenliste veröffentlicht www.bundesnetzagentur.de/massnahmenliste.

Das Internet – Gefahr und Betrug

Phishing per E-Mails, SMS oder Messenger

Der sogenannte „Enkeltrick“:



- Wie eine Telefonnummer gesperrt werden kann, ist unter anderem hier nachzulesen. Anschließend wird empfohlen, die Nachricht zu löschen. Weitere Hinweise findet man auf den Seite der Polizei, z.B. hier oder für Bayern hier und bei den Verbraucherzentralen.
- Auf der Seite Fachanwalt.de finden Sie noch zusätzliches Wissenswertes zu diesem Thema.
- Eine Anzeige empfiehlt sich auch auf der Seite der Bundesnetzagentur, der Link führt zum SMS-Beschwerte Formular:
- Die Bundesnetzagentur führt meine Anzeige unter dem Aktenzeichen

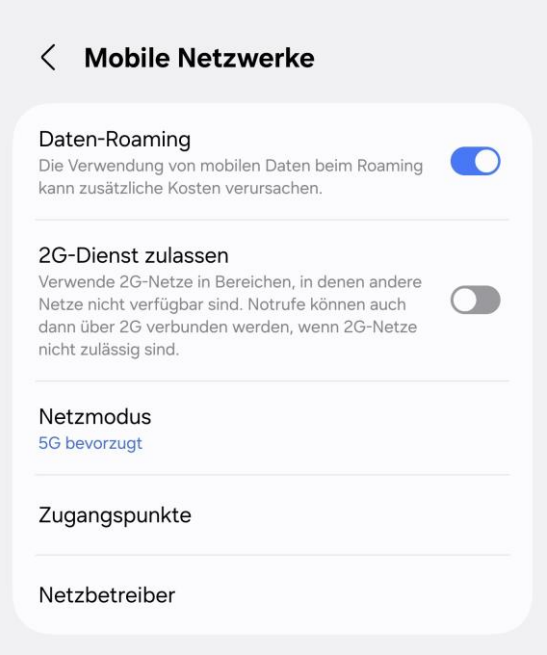
Dort21 EB-02330332.

Das Internet – Gefahr und Betrug

Phishing per E-Mails, SMS oder Messenger

SMS-Blaster:

- Durch das Schweizer Bundesamt für Cybersicherheit BACS wurde eine neue Varianten des SMS-Phishing dokumentiert.
- Mit einem SMS-Blaster können Textnachrichten (SMS) an viele Personen gleichzeitig versendet werden. Es ist ein mobiles Gerät in der Größe eines PC-Gehäuse, das sich als Mobilstation ausgibt. Das Gerät sendet ein starkes Signal aus und fordert alle Smartphones in einem Umkreis von 500 bis 1.000 Meter auf, sich mit ihm zu verbinden..
- Das Gerät gibt sich als beste verfügbare Basisstation aus. Sobald sich Ihr Smartphone verbindet, erhalten Sie automatisch eine gefälschte SMS ohne dass die Betrüger Ihre Telefonnummer kennen müssen.
- Die Schwachstelle ist das veraltete 2G-Netz.



Das Internet – Gefahr und Betrug

Anzeigenbetrug

- Um potenzielle Opfer zu erreichen, nutzen Betrüger zunehmend auch Werbeanzeigen. Im November 2025 berichtete eine US-Nachrichtenagentur darüber, dass Meta – das Unternehmen hinter Plattformen wie Instagram und Facebook – rund zehn Prozent seines weltweiten Umsatzes mit Anzeigen für Betrugsmaschen und/oder verbotenen Waren und Dienstleistungen verdient.

- Im Jahr 2024 entsprach das rechnerisch rund 16 Milliarden US-Dollar (ca. 13,5 Milliarden Euro).

Time-Advertising

- Erika Musterfrau ruft von ihrem heimischen Sofa ihre Lieblingswebsite auf. Noch während die Seite in Erikas Browser lädt, bieten Werbetreibende im Hintergrund über Werbebörsen um den Anzeigeplatz. Sie wissen nicht, dass die Nutzerin Erika Musterfrau ist. Doch sie wissen genug über Erika: Zum Beispiel, welchen Browser bzw. welches Betriebssystem sie nutzt und in welcher Region sie sich aufhält. Mithilfe von Cookies können Nutzer wie Erika über das Internet hinweg „verfolgt“ werden.

Das Internet – Gefahr und Betrug

Quishing

- Quishing - eine Wortkreuzung aus “QR-Code” und “Phishing” - ist eine Betrugsmasche, bei der Kriminelle präparierte QR-Codes nutzen, um an sensible persönliche Daten wie Passwörter oder Logins beispielsweise zu Online-Banking-Accounts zu gelangen.
- Die Täter leiten ihre Opfer über gefälschte QR-Codes auf betrügerische Webseiten weiter, die offiziellen Portalen täuschend ähnlich sehen. Der technische Hinterhalt: Während herkömmliche Antivirenprogramme schädliche Links in E-Mails automatisch erfassen und filtern, werden die in QR-Codes versteckten Webadressen von von Schutzprogrammen oft nicht erkannt.

Das Internet – Gefahr und Betrug

Quishing

Wo lauert die Gefahr? - Typische Risikoorte

Gefälschte QR-Codes bevorzugt an Orten des täglichen Lebens, an denen Menschen routiniert mit dem Smartphone scannen, bezahlen oder Informationen abrufen:

- **Parkscheinautomaten:** Aufkleber mit gefälschten QR-Codes werden über die Original-Codes geklebt.
- **E-Ladesäulen:** Manipulierte Sticker täuschen eine Bezahl- oder Freischaltseite für den Ladevorgang vor.
- **Knöllchen & Strafzettel am Fahrzeug:** Gefälschte Zahlungsaufforderungen an der Windschutzscheibe versprechen eine schnelle Online-Überweisung des Verwarnungsgeldes.
- **Gastronomie & Speisekarten:** Präparierte Aufkleber auf Tischaufstellern zum angeblichen digitalen Bestellen oder Bezahlen.
- **Mietfahrzeuge & E-Scooter:** Gefälschte QR-Codes an den Fahrzeugen zur angeblichen Freischaltung.
- **Paketbenachrichtigungen & Briefe:** QR-Codes auf gefälschten Benachrichtigungskarten im Briefkasten (z. B. für vermeintliche Zoll- oder Zustellgebühren).

Das Internet – Gefahr und Betrug

Quishing

Wie lässt sich Quishing erkennen?

- **Physische Überklebungen prüfen:** Ist der QR-Code fest aufgedruckt oder handelt es sich um einen nachträglich angebrachten Sticker? Ein überklebter Code mit fühlbaren Rändern ist ein klares Warnsignal.
- **Ziel-URL in der Vorschau kontrollieren:** Prüfen Sie vor dem Öffnen die angezeigte Webadresse genau. Stimmt die Domain exakt mit dem jeweiligen Anbieter überein? Achten Sie auf Buchstabendreher, Sonderzeichen oder verdächtige Adresszusätze.
- **Sofortige Datenabfrage hinterfragen:** Seriöse Zahlungsdienste zeigen nach dem Scan zuerst Tarif- oder Produktinformationen an, bevor sensible Bezahldaten abgefragt werden.
- **Fehlende Verschlüsselung:** Bietet die Seite keine sichere HTTPS-Verbindung oder wirkt das Design fehlerhaft, brechen Sie den Vorgang ab.
- **Direkten App-Zugriff bevorzugen:** Nutzen Sie für Bezahlvorgänge direkt die offizielle App des jeweiligen Anbieters (z. B. Ihre installierte Park- oder Lade-App) und geben Sie den Zonencode bzw. die Stationsnummer manuell ein.
- **Im Zweifelsfall nicht scannen:** Wenn Ihnen ein Code verdächtig vorkommt, brechen Sie den Scan ab und nutzen Sie alternative Bezahlwege.

Das Internet – Gefahr und Betrug

Anzeigenbetrug

- Experten gehen davon aus, dass der Anteil dieser automatisierten Werbung mittlerweile rund 75 Prozent entspricht. Mit anderen Worten: Bei drei Vierteln der Werbeanzeigen, die wir im Internet sehen, gibt es keine manuelle Prüfung der Inhalte. In vielen Fällen ist das kein Problem. Doch auch Betrüger machen sich den guten Ruf und die Reichweite der Plattformen, auf denen sie werben, zunutze.
- Es gibt Anzeichen dafür, dass Menschen, die einmal auf eine betrügerische Anzeige geklickt haben, anschließend häufiger betrügerische Werbeanzeigen ausgespielt bekommen. Grund dafür sind die Plattformen eigenen Algorithmen, die mittels Personalisierung versuchen, die vermeintlichen Interessen der Nutzer bestmöglich zu bedienen.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Anzeigenbetrug

So erkennt man den Betrug:

- Auf einer Website oder in Ihrer App sieht man eine Werbeanzeige für eine Geldanlage mit ungewöhnlich hohen Renditeaussichten.
- Man sieht eine Werbeanzeige für ein beliebtes Produkt, welches zu besonders günstigen Konditionen angeboten wird.

So schützt man sich:

- Sie sollten sich niemals verlasse, dass eine Werbeanzeige seriös ist, nur weil sie in einem seriösen Umfeld erscheint.
- Um auf „Nummer sicher“ zu gehen: Prüfen Sie die Anzeigeseite mit dem „Fakeshop-Finder“ der Verbraucherzentrale.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Gefälschte Online-Shops – Fake Shops

- Bei Fake Shops handelt es sich um eine besondere Form von Vorkassebetrug. Fake Shops sind Online-Shops, die in betrügerischer Absicht eröffnet werden. In der Regel zahlt man im Voraus für eine Ware, die man nie erhält. In wenigen Fällen bekommt man zwar Ware, doch diese ist von minderer Qualität oder es handelt sich um Fälschungen. Die Websites wirken dabei oft professionell und authentisch. Fake Shops weisen darüber hinaus oft sogar Bewertungen oder Gütesiegel auf, doch diese sind nicht authentisch. Der Händler existiert nicht wirklich.

Wie erkennt man den Betrug?

- Anzeigen in Suchmaschinen oder auf Websites mit unschlagbaren Preisen (z. B. das neueste Smartphone für die Hälfte) locken Sie auf die Seite.
- Obwohl zunächst auch andere Bezahlmethoden wie Kreditkarte, Nachnahme oder PayPal angeboten bzw. dargestellt werden, kann man am Ende nur per Vorkasse (Banküberweisung) zahlen.
- Das Impressum fehlt, ist unvollständig oder die Adresse liegt im Ausland.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Gefälschte Online-Shops – Fake Shops

Wie kann man sich schützen?

- Man kauft nur in Onlineshops, die sichere Zahlungsarten wie etwa Rechnungskauf anbieten und nutze diese. Auch Bezahlmethoden mit Käuferschutz können als sicher gelten, wenn man weißt, wie diese funktionieren und welche Bedingungen gelten.

- Sein Sie skeptisch, wenn ein Shop Gütesiegel aufführt, aber nicht zu den Ausstellern verlinkt.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Vorkassenbetrug

- Es gibt verschiedene Formen des Vorkassenbetrugs. Er zählt zu den ältesten und häufigsten Betrugsmaschen im Internet. Diese Masche tritt in unzähligen Varianten auf. Das Grundprinzip ist simpel: Die Betrüger verlangen für eine vereinbarte Leistung eine Zahlung von ihrem Opfer – bevor sie diese erbringen. Fallen Opfer darauf herein, verschwinden die vermeintlichen Anbieter spurlos mit dem Geld, ohne dass die Betroffenen die versprochene Leistung erhalten. Deshalb ist Vorkasse die beliebteste Zahlart unter Betrügern.
- Dabei ist es ganz egal, ob Sie mit einem privaten oder gewerblichen Anbieter handeln. Insbesondere auf Kleinanzeigenportalen ist der Vorkassebetrug ein häufiges Phänomen. Denn zwischen Privatleuten ist es durchaus gang und gäbe, dass der Verkäufer zuerst sein Geld erhält und dann die Ware verschickt.
- Die Masche betrifft keineswegs nur hochpreisige Artikel. Kriminelle nutzen bisweilen bewusst günstige Artikel wie Bücher. Auch kleine Summen können bei einer Vielzahl von Opfern „lukrativ“ sein. Es ist eine lohnende Taktik, denn das Entdeckungsrisiko sinkt. Viele Menschen scheuen es, bei kleineren Verlusten den Vorfall zu melden.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Vorkassenbetrug bei der Wohnungssuche

- Selbst Menschen auf Wohnungssuche können Opfer von Vorkassebetrug werden. Hier ist die Masche besonders perfide, da sie die oft verzweifelte Lage von Suchenden ausnutzt. Zugleich geht es oft um höhere Summen – nicht selten mehrere tausend Euro für Kautionen oder erste Monatsmieten. Der vermeintliche Vermieter behauptet beispielsweise, er sei gerade im Ausland und würde den Schlüssel gegen eine vorab überwiesene Kaution per Kurier schicken. Hin und wieder verlangen Betrüger auch „Gebühren“ für einen Besichtigungstermin. Seriöse Makler oder Vermieter tun dies niemals.
- Vorkassebetrug wird oft mit einer anderen Masche kombiniert – Identitätsdiebstahl: Dabei werden die Opfer gebeten, eine Kopie ihres Personalausweises zu schicken. Diese Daten nutzen die Kriminellen dann, um unter den Namen ihrer Opfer neue Fake-Anzeigen zu schalten, Legenden zu stricken oder gar Konten zu eröffnen.

Das Internet – Gefahr und Betrug

Vorkassenbetrug

Wie erkennt man den Betrug?

- Grundsätzlich gilt: Wenn ein Angebot zu gut klingt, um wahr zu sein (z. B. ein neues Smartphone zu einem besonders günstigen Preis), ist es das meistens auch.
- Der Anbieter lehnt andere Bezahlmethoden kategorisch ab oder erklärt wortreich, weshalb diese für ihn nicht in Frage kommen.
- Legenden, Druck und Eile – Achten Sie auf klassische Manipulationsversuche wie „Wer zuerst zahlt, erhält den Zuschlag“ oder klassische Betrugsanzeichen wie Aufenthalt im Ausland.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Vorkassenbetrug

Wie kann man sich schützen?

- Überweisen Sie niemals Geld per Vorkasse (Banküberweisung) an Unbekannte. Einmal überwiesenes Geld zurückzuholen, ist extrem schwierig und nur selten erfolgreich. Es spielt dabei übrigens keine Rolle, ob es sich um ein deutsches oder ausländisches Konto handelt.

- Bestehen Sie auf der Verwendung sicherer Bezahlmethoden, Kreditkarte oder Rechnungskauf. Machen Sie sich vorab mit der Funktionsweise und den Bedingungen von etwaigen Treuhand-Services oder Käuferschutz-Programmen vertraut.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Dreiecksbetrug

- Der Dreiecksbetrug ist eine besonders raffinierte Betrugsmasche: Dabei wird man beispielsweise auf einem Online-Marktplatz auf einen Artikel aufmerksam. Man nimmt Kontakt mit dem vermeintlichen Anbieter auf. Dieser sichert zu, den Artikel an Sie zu verkaufen. Dazu teilt er mit Ihnen Zahlungsinformationen. Sie zahlen wie verlangt. Doch anschließend hört man nichts mehr von dem angeblichen Verkäufer. Man erhält auch keine Ware.

- Was ist passiert? Der vermeintliche Verkäufer (Betrüger) steht während der Verhandlungen mit Ihnen zeitgleich mit einem Dritten in Verbindung. Der Dritte bietet tatsächlich Ware zum Verkauf an. Für diese lässt Sie der Betrüger bezahlen. Der Betrüger erhält daraufhin von dem nichtsahnenden Verkäufer die Ware, während Sie leer ausgehen. Denn man stehst am Ende dieser Masche ohne Geld und ohne Ware da.

Das Internet – Gefahr und Betrug

Dreiecksbetrug

- Diese Masche gibt es auch im Zusammenhang mit Onlineshops, die als Bezahlmethode Kauf per Rechnung anbieten. In diesen Fällen bezahlt man Geld an den Betrüger, der daraufhin in einem Onlineshop Ware bestellt und an Sie senden lässt. Bezahlt hat er dafür nicht – er wählt Rechnungskauf und nutzt dafür Ihre Daten. Perfide: Man erhält die gewünschte Ware und ahnt nichts Böses. Doch in der Regel verlangt der Onlineshop von Ihnen die Bezahlung der gelieferten Ware.

Wie erkennt man den Betrug?

- Dreiecksbetrug lässt sich leider oft erst erkennen, wenn es bereits zu spät ist. Doch man kann sich davor schützen, Opfer zu werden: Zahlen Sie niemals an Unbekannte per Vorkasse (Banküberweisung).
- Man kauft von einem privaten Verkäufer, aber die Ware (in der Regel Neuware) kommt von einem Dritten wie einem professionellen Online-Händler.
- Im Paket liegt ein Lieferschein oder sogar eine Rechnung auf Ihren Namen.

Das Internet – Gefahr und Betrug

Dreiecksbetrug

Wie kann man sich schützen?

- Nutzen Sie bei Privatkäufen immer die offiziellen Bezahlsysteme der Plattformen – oft bieten diese einen Käuferschutz.
- Machen Sie sich jedoch vorab mit der Funktionsweise und den Bedingungen vertraut.
- Falsche Freunde: Überweisen Sie niemals Geld vorab per Banküberweisung oder mittels „Freunde und Familie“ bei PayPal, wenn Sie den Verkäufer nicht persönlich kennen.
- Kontaktieren Sie sofort den Händler, von dem das Paket stammt, falls Rechnungssteller und Absender nicht zusammenpassen.

Das Internet – Gefahr und Betrug

Liebesbetrug

- Bei dieser Masche bauen Betrüger über Dating-Plattformen oder soziale Medien eine emotionale Beziehung zu ihrem Opfer auf – oft über Wochen oder sogar Monate.

- Wenn das Vertrauen groß genug ist, bitten sie um Geld, z. B. für eine plötzlich „dramatische“ Notlage, Reisekosten oder medizinische Ausgaben. In den meisten Fällen haben die Opfer die Person noch nie im echten Leben getroffen.

So erkennt man den Betrug

- Ihr neuer Online-Schwarm überhäuft Sie mit Komplimenten oder plant schnell eine gemeinsame Zukunft – ohne dass ihr euch zuvor persönlich gesehen habt.

- Geplante Treffen werden immer kurzfristig wegen dramatischer Zwischenfälle (Unfall, Krankheit, Verbrechen) abgesagt.

- Plötzlich werden Sie angefleht, schnell Geld zu senden, um eine lebenswichtige OP oder ein Flugticket zu bezahlen.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Liebesbetrug

Reales Beispiel zu Kontaktaufnahme:

Betreff: Eine Einladung
Von: SMS1 <bhumika.garkhal@polytechnique.edu>
Datum: 19.06.2025, 08:17
An: Undisclosed recipients:;

Hallo,

Ich erlaube mir, dir diese paar Zeilen zu schreiben, ohne Unterschrift, obwohl wir uns nicht wirklich kennen. Ich schreibe dir diese Nachricht etwas unerwartet (in der Hoffnung, dass sie jemanden erreicht, den du bereits kennst), getrieben von einem aufrichtigen Impuls.
Diese Nachricht mag aus dem Nichts kommen, aber manchmal muss man sich trauen, etwas Ungewöhnliches zu tun. Ich möchte dich nicht verärgern oder dir Unbehagen bereiten, sondern dir einfach zeigen, dass dich ein freundliches Auge aus der Ferne ansieht ... und dass, falls dich die Idee einer Verbindung anspricht ...
Ich möchte weder Verstecken spielen noch ein Geheimnis unnötig in die Länge ziehen, sondern dir mit diesem Brief einfach etwas Aufrichtiges anbieten: uns kennenzulernen.
Wenn dir die Idee gefällt, würde ich mich freuen, ein paar Worte zu wechseln, dich besser kennenzulernen oder anschließend vielleicht einen Kaffee oder ein Getränk mit dir zu trinken.
Sollte dir dies nicht der richtige Zeitpunkt sein oder dir diese Nachricht unangenehm sein, habe ich dafür vollstes Verständnis.
Ich bleibe vorerst im Hintergrund, vielleicht aus Schüchternheit oder aus Angst, den Zauber der Anonymität zu brechen. Wer weiß, vielleicht beginnt mit diesen wenigen Worten eine wunderschöne Geschichte.

Auf jeden Fall wünsche ich Ihnen einen wunderschönen Tag.

Bis bald vielleicht. Ich freue mich darauf, von Ihnen zu hören.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Liebesbetrug

- Besonders auffällig ist die verschiedene Benutzung der Anrede. Der allgemeine, beginnende Text verwendet die ich- und du-Schreibweise. Das ist wohl der einmalig entworfene Betrügertext.
- Die letzten beiden Zeilen verwenden Ihnen und scheint der eigene Beitrag der schreibende Person zu sein, hier bhumika.garkhal.
- Die verwendete Emailadresse gibt es wirklich.

So schützt man sich

- Brechen Sie den Kontakt sofort ab, sobald Forderungen nach Gefälligkeiten, Gutscheinen oder Geld kommen – insbesondere in Kryptowährung. Überweisen Sie niemals Geld an Menschen, die Sie noch nie im echten Leben getroffen haben.

Das Internet – Gefahr und Betrug

CEO-Fraud

- Beim sogenannten CEO-Fraud geben sich Betrüger als Führungskräfte (z. B. Geschäftsführer, Vorstand) aus und schicken E-Mails oder Nachrichten an Mitarbeitende – meist in der Finanzabteilung. Sie fordern Überweisungen, weil „dringende geschäftliche Gründe“ vorliegen, etwa „Vertraulichkeit“ oder „Eile“. Weil es so klingt, als käme es von der echten Geschäftsführung, fallen viele auf die Masche herein.

So erkennt man den Betrug

- Man bekommt eine E-Mail von der „Chefetage“, die extremen Zeitdruck aufbaut und nach absoluter Geheimhaltung verlangt.
- Es geht meist um „dringende Firmenangelegenheiten“ oder eine „streng vertrauliche Rechnung“, die sofort beglichen werden muss.
- Die E-Mail-Adresse des Absenders wirkt zunächst authentisch, weicht aber bei genauem Hinsehen vom Original ab (z. B. ein „m“ statt „rn“).

Das Internet – Gefahr und Betrug

Online-Betrug – CEO-Fraud

Wie kann man sich schützen?

- Rufen Sie Ihren Vorgesetzten über die bekannte Nummer an und fragen persönlich nach – egal wie eilig es scheint.
- Seien Sie besonders kritisch bei Anweisungen, die von den normalen Abläufen in Ihrer Firma abweichen – oder recherchieren Sie die Ursachen, etwa bei Vorgesetzten.
- Achten Sie auf ungewöhnliche Formulierungen oder eine Sprache, die nicht zum Absender passt.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Abofallen

- Abofallen sind Webseiten oder Apps, die mit vermeintlich kostenlosen Angeboten locken – etwa Rezepten, Gewinnspielen, Horoskopen oder PDF-Downloads. Erst im Kleingedruckten findet sich ein Hinweis auf ein kostenpflichtiges Abonnement. Viele Betroffene merken erst nach Erhalt einer Rechnung, dass sie (angeblich) ein Abo abgeschlossen haben.

So erkennt man den Betrug

- Ein Angebot wirbt damit, kostenlos zu sein (z. B. ein „Gratis-Abo“), verlangt aber trotzdem Ihre Zahlungsdaten.
- Wichtige Kostenhinweise verstecken sich tief im Kleingedruckten oder hinter winzigen Sternchentexten am Seitenende.
- Der übliche „Kaufen“-Button ist irreführend beschriftet, zum Beispiel mit „Anmelden“ statt „Zahlungspflichtig bestellen“.

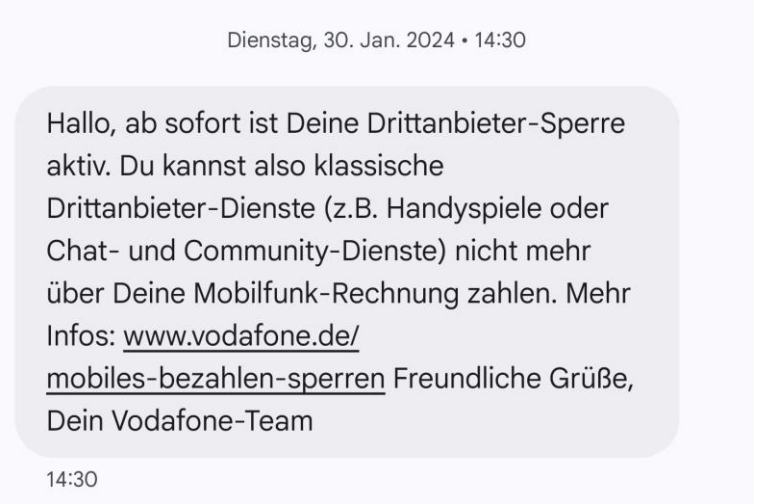
Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Abofallen

Wie kann man sich schützen?

- Achten Sie darauf, dass der Bestell-Button eindeutig beschriftet ist. Es gibt gesetzliche Vorgaben. Abweichungen können ein Indiz für Betrug sein.
- Dokumentieren Sie den Prozess. Machen Sie zum Beispiel Screenshots von Angeboten, die als „kostenlos“ beworben werden, bevor Sie Ihre Daten eingeben. Das hilft, um später gegen den Betrug vorzugehen.
- Widersprechen Sie unberechtigten Abbuchungen sofort bei Ihrer Bank oder Ihrem Mobilfunkanbieter (setzen Sie gegebenenfalls auch eine sogenannte Drittanbietersperre).



Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Anlagebetrug

- Kriminelle locken mit extrem hohen Renditen bei „todsicheren“ Anlagen – oft über Krypto-Plattformen, Social-Media-Werbung oder angebliche Finanzexperten. Die Webseiten wirken professionell, zeigen fingierte Kurs-Diagramme oder erfundene Gewinne.
- Die Betrüger wirken freundlich und professionell. Sie setzen Sie unter Druck, dass Sie die „einmalige Chance“ nicht verpassen dürfen und deshalb schnell investieren sollen. Oft folgen auf eine erste kleinere Einzahlung ständige Nachforderungen.

So erkennt man den Betrug

- Sie erhalten per E-Mail, SMS oder Messenger unverlangt Angebote mit scheinbar lukrativen Anlagemöglichkeiten.
- Sie sehen auf Websites oder in Social-Media-Apps Werbeanzeigen für Geldanlagen mit ungewöhnlich hohen Renditeaussichten.
- Prominente bürgen scheinbar für die Seriosität der Angebote, es werden Bilder ohne das Einverständnis der Abgebildeten missbraucht.

Das Internet – Gefahr und Betrug

Anlagebetrug

Wie kann man sich schützen?

- Hohe Gewinne ohne Risiko? Das klingt zu schön, um wahr zu sein. Bleiben Sie skeptisch – hohe Gewinnmöglichkeiten sind stets mit einem hohen Risiko verbunden.
- Nicht immer geht es um Geld – schützen Sie auch Ihre persönlichen Daten. Betrüger nutzen Informationen wie Name, Adresse und Ausweiskopie, um Identitätsdiebstahl zu begehen.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Anlagebetrug

Kreditantrag

Herzlichen Glückwunsch! Ihr Kreditantrag wurde genehmigt.

Betreff: Herzlichen Glückwunsch! Ihr Kreditantrag wurde genehmigt.
Von: Validierungsservice <jeandijoux5@gmail.com>
Datum: 07.06.2025, 16:05
An: undisclosed-recipients:;
Blindkopie (BCC): <Seniorenbeirat@adelsdorf.de>

Herzlichen Glückwunsch! Ihr Kreditantrag wurde genehmigt.
Bitte senden Sie Ihre Bankdaten so schnell wie möglich an die folgende E-Mail-Adresse: sociaaleuros@gmail.com, um den Vorgang abzuschließen.
Sie stehen auf der Prioritätenliste der Begünstigten, die ihre Finanzierung in Kürze erhalten.
Mehr als 24 Personen haben letzte Woche bereits ihren Kredit erhalten. Warten Sie also nicht länger!

- Glauben die Betrüger ernsthaft, dass jemand an diese Adresse seine Bankdaten sendet? Offensichtlich doch, auch wenn der Ertrag wahrscheinlich sehr gering ist, der Aufwand dazu ist es auch.

Das Internet – Gefahr und Betrug

Deep-Fake-Betrug

- Moderne KI-Technik ermöglicht täuschend echte Stimmen oder Videos. Täter imitieren vertrauenswürdige Personen, wie z. B. Verwandte, Kolleginnen, Vorgesetzte. Das Ziel: Geldüberweisungen oder vertrauliche Informationen.

So erkennt man den Betrug

- Sie erhalten einen Videoanruf oder eine Sprachnachricht von einer vertrauten Person, die sehr blechern oder unnatürlich klingt.

- Die Person im Video bewegt sich seltsam oder die Lippenbewegungen passen nicht perfekt zum Ton.

- Es wird eine emotionale Notsituation vorgetäuscht, um Sie zu einer schnellen Geldüberweisung zu drängen.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Deep-Fake-Betrug

Wie kann man sich schützen?

- Legen Sie im Zweifel auf bzw. trenne die Verbindung und rufen die Person über ihre normale, gespeicherte Telefonnummer zurück.

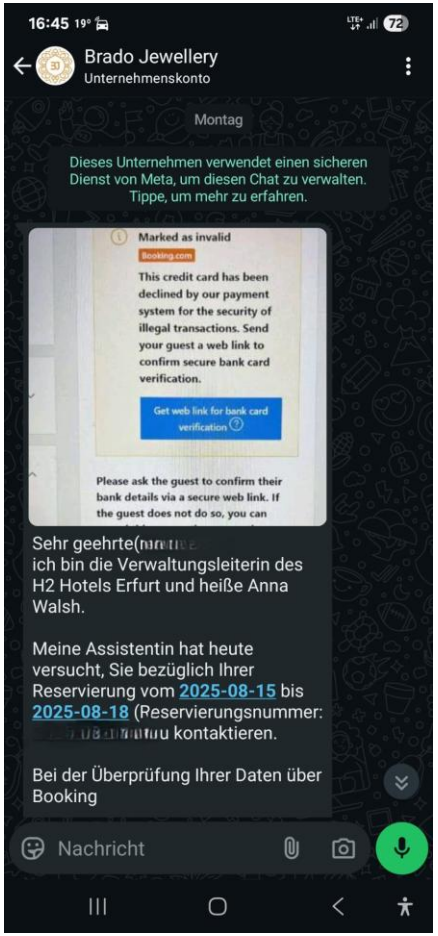
- Stellen Sie der Person eine persönliche Frage, die nur sie beantworten kann und die nicht öffentlich bekannt ist oder ohne Weiteres recherchiert werden kann.

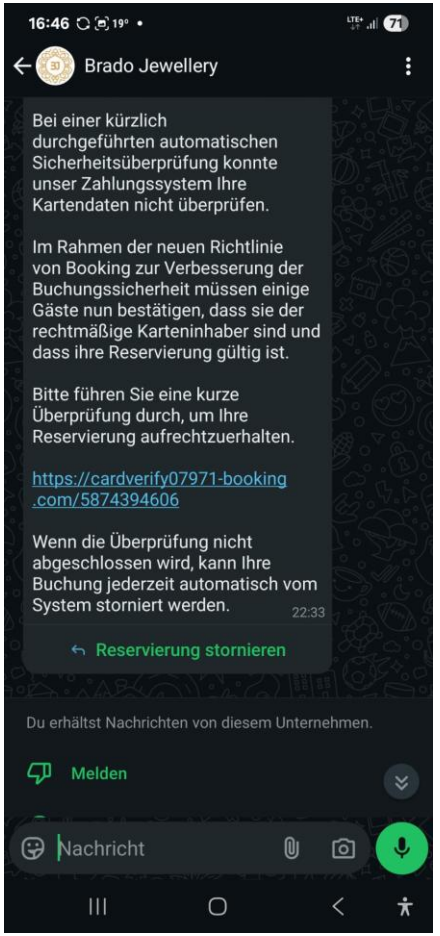
- Vereinbaren Sie in der Familie ein „Codewort“ für echte Notfälle, das eine KI nicht kennen kann.

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Noch ein Beispiel:





Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Fazit – Worauf sollte man achten!

- Dringende Aufforderungen, sofort zu handeln oder Geld zu senden.
- Absenderadressen, die seltsam oder falsch aussehen; Grammatikfehler in der Nachricht.
- Links in der Nachricht zu unbekannten Webseiten.
- Versprechungen von besonders hohen Renditen oder unrealistischen Geschäften.
- Druck, persönliche Daten wie Passwörter oder TANs zu teilen.

Hilfreiche Links:

- **Fakeshop-Finder**
  https://www.verbraucherzentrale.de/fakeshopfinder-71560
- **SiBa-App: Das DsiN-Sicherheitsbarometer**
  https://www.sicher-im-netz.de/sicherheitsbarometer/

Das Internet – Gefahr und Betrug

Deutscher Philologenverband

Fazit – Schutzmaßnahmen – einfach umsetzbar

- Nutzen Sie starke, individuelle Passwörter. Verwenden Sie, wenn möglich, einen Passwort-Manager.
- Aktivieren Sie 2-Faktor-Authentifizierung, dort, wo es sinnvoll ist.
- Seien Sie skeptisch bei unverlangten Nachrichten, besonders mit Anhängen oder Links.
- Prüfen Sie URLs genau: Achten Sie auf HTTPS und die korrekte Domain.
- Bezahlen Sie lieber mit sicheren Methoden; vermeiden Sie Vorauskasse ohne Schutz.
- Halten Sie Computer, Smartphone und Programme aktuell.
- Nutzen Sie seriöse Antivirus-Software und machen Sie regelmäßige Backups.
- Sprechen Sie Verdachtsfälle ruhig an: Ihren Sohn/Tochter, Enkel oder den Kundendienst Ihres Anbieters.
- Melden Sie verdächtige Aktivitäten bei Ihrem Anbieter oder der Polizei.

Deutscher Philologenverband

Vielen Dank für Ihre Aufmerksamkeit

Unterlage (PDF-Datei) bitte per Email an:
Horst.Heineck@googlemail.com
anfordern

oder auf:
https://horst-heineck.de/weitere-aktivitaeten/#DPhV
downloaden

Das Internet - Gefahr und Betrug

Deutscher Philologenverband

