Seniorentreff Grafrath 2021

Was sind Computerviren, Trojaner, Würmer, P(V)ishing und Spams ?

(unbedingt beachten, wollen Sie nicht der Nächste sein)

Computerviren, Trojaner und Würmer

Viren und Trojaner

Ein Virus benötigt immer ein Wirtsprogramm und verbreitet sich, indem es sich selbst in noch nicht infizierte Dateien kopiert und diese so anpasst, dass das Virus mit ausgeführt wird. Zu den infizierbaren Dateien zählen normale Programmdateien (erkennbar an der Erweiterung .exe, .com), Programmbibliotheken (.dll), Skripte (.vbs), sowie Bootsektoren. Diese beiden Typen wollen vorrangig zerstören bzw. das ordnungsgemäße Arbeiten z.B. von einer Erpressung abhängig machen.

Würmer

Würmer sind in Ihrer Wirkung den Viren sehr ähnlich, benötigen jedoch keinen "Wirt", z.B. Makros oder den Bootsektor, für Ihre Verbreitung. Im Gegensatz zu Viren warten Würmer nicht passiv darauf, von einem Anwender auf einem neuen System aufgerufen zu werden, sondern versuchen, aktiv (also selbständig) in neue Systeme einzudringen. Sie nutzen dazu Sicherheitsprobleme auf dem Zielsystem aus, wie zum Beispiel: mangelhafte Standardpasswörter, fehlerhafte Software (Adobe Flashplayer). Ein Wurm kann sich dann wie ein Virus in eine andere Programmdatei einfügen, da sie sich selbst kopieren und die Kommunikationsplattformen von verschiedenen Computern nutzen um sich wie vor zu verteilen.

Trojaner

Der Überlieferung nach war der Auslöser des Trojanischen Krieges in der griechischen Sage die Entführung der Helena, der Ehefrau des Menelaos, durch Paris, dem Sohn des trojanischen Königs Priamos . Daraufhin zogen die vereinten Griechen gegen Troja, um sich zu rächen. Trotz zehnjähriger Belagerung gelang es jedoch nicht, die stark befestigte Stadt zu erobern. Auf Rat des Odysseus bauten die Griechen endlich ein großes hölzernes Pferd, in dem sich die tapfersten Krieger versteckten, und täuschten die Abfahrt ihrer Schiffe vor. Die Trojaner holten entgegen den Warnungen der Kassandra und des Priesters Laokoon das Pferd in die Stadt. In der Nacht kletterten die Griechen aus ihrem Versteck, öffneten die Tore und konnten so die Trojaner überwältigen.

„Trojaner“ in der EDV verhalten sich ähnlich.

Einmal eingefangen, lauern sie im Hintergrund, speichern z.B. Passwörter, Bankverbindungen, Kontonummern, Adressen u.ä. und werden bei Sammlung genügender Daten aktiv. Diese sogenannten **Backdoor-Trojaner** haben bis dahin nichts zerstört.

Stellen Sie sich einmal vor, ein solcher Trojaner hat Ihr Zugangspasswort zu Ihrem Rechner oder Ihrer Bank geändert. Sie sind damit vom **Einloggvorgang** ausgeschlossen (da Sie ja jetzt nicht mehr „berechtigt“ sind) und die „Arbeit“ kann von dem Trojaner in aller Ruhe aufgenommen werden. Ihr Konto wird abgeräumt, persönliche Daten werden für weiteres Übel ausgelesen und übertragen, usw..

Auch fehlerhaft programmierte Software lädt zum Direktangriff (Wurm) ein

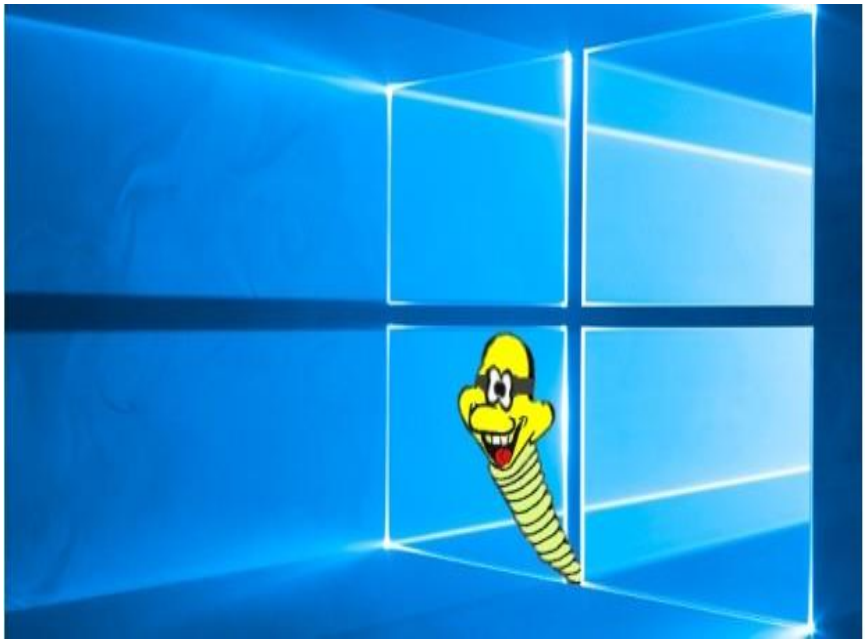
Zero-Day-Lücke

Eine Zero-Day-Lücke ist eine Schwachstelle im IT-System einer Firma. (Adobe FlashPlayer) Die betroffene Software, Hardware oder Firmware lässt sich zunächst **nicht dagegen** schützen. Ein potentieller Angriff (Zero-Day-Exploit) erfolgt **am selben** Tag, an dem die Security-Lücke entdeckt wurde. Die Schwachstelle wird daher Zero-Day-Lücke genannt, da zwischen der Entdeckung des ersten Angriffs und der Sicherheitslücke **null Tage** liegen

Auslöser einer Zero-Day-Lücke ist sehr oft ein fehleranfälliger Code. Leider werden Informationen über solche Security-Lücken immer häufiger im sogenannten Darknet verkauft. Um diese Sicherheitslücken zu schließen, müssen Entwickler einen Patch oder ein Update erstellen und veröffentlichen. Sie und die Unternehmen sollten dieses **Update** dann unmittelbar einspielen. Firmen haben aber auch die Möglichkeit, sich gegen Zero-Day-Lücke zu schützen. S. auch nachfolgende Meldung.

Wurm-taugliche Windows-Lücke entdeckt

09.05.2017 | 09:32 Uhr | Frank Ziemann



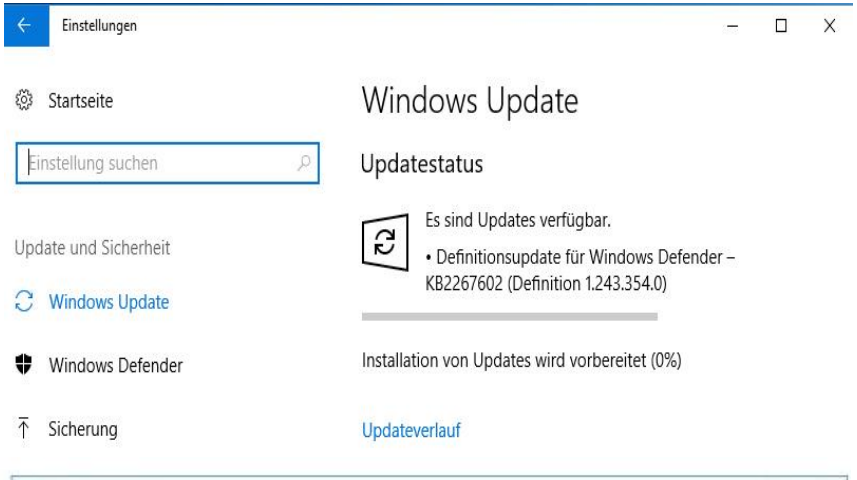
Google-Forscher haben eine kritische Sicherheitslücke in Windows entdeckt. Sie soll wurmtauglich und in allen Standardinstallationen vorhanden und ausnutzbar sein.

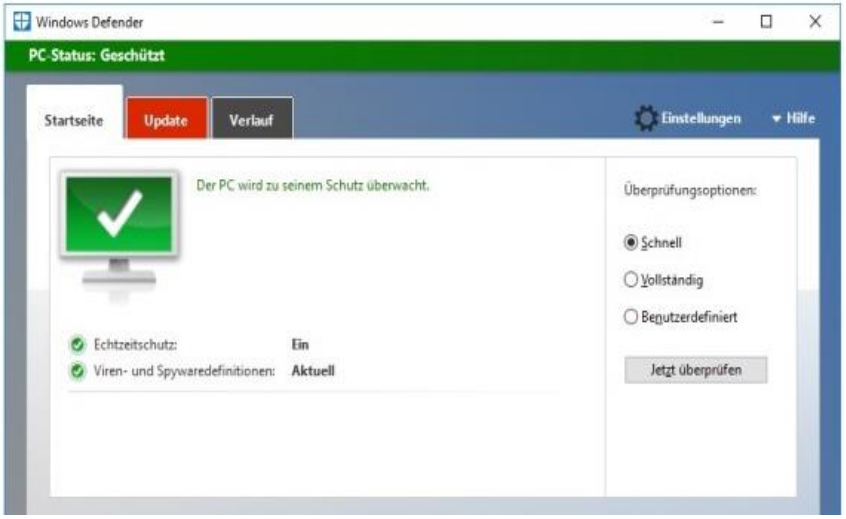
In Windows soll sie eine der schlimmsten dieser Art sein, die in letzter Zeit entdeckt worden sei. Sie soll ferner geeignet sein, um damit einen Wurm zu konstruieren – also Malware, die sich selbsttätig von PC zu PC verbreiten kann.

Ein Angriff, der die Schwachstelle ausnutze, würde bei jeder Standardinstallation von Windows funktionieren. Viel mehr Details hat Ormandy, der für Googles Project Zero arbeitet, bislang nicht verlauten lassen.

Sicherheits-Update für Windows Defender

09.05.2017 | 10:02 Uhr | Frank Ziemann





In praktisch allen Antivirus-Produkten aus dem Hause Microsoft steckt eine gravierende Sicherheitslücke. Sie kann ausgenutzt werden, um beliebigen Code auszuführen. Verwundbar ist das Scan-Modul, das Microsoft als „Malware Protection Engine“ bezeichnet. Es ist der Kern der Schutzlösungen von Windows Defender über Security Essentials bis System Center Endpoint Protection. Microsoft hat am 8. Mai, einen Tag vor dem regulären Update-Dienstag eine Sicherheitsmeldung (Security Advisory 4022344) veröffentlicht. Demnach weist die Microsoft Malware Protection Engine eine als kritisch eingestufte Sicherheitslücke auf. Beim Scannen einer speziell präparierten Datei kann es zu Speicherfehlern kommen. Ein Angreifer kann dies ausnutzen, um eingeschleuste Codes mit den Berechtigungen des lokalen Systemkontos auszuführen.

+++Sicherheits-Update für Firefox 52+++

Erst vor kurzem hatte Firefox das Update auf die Version 52 angeboten. Neben mehr Sicherheit gibt es auch neue Funktionen. Unter anderem warnt nun Firefox vor **unsicherer Anmeldung** auf Webseiten.

Das BSI empfiehlt das Update unmittelbar zu installieren. Mit dem Update wird eine schwere Sicherheitslücke geschlossen. Zum Updaten im Firefox-Menü (Button ganz links neben dem Eingabefeld) klicken Sie auf "Einstellungen".

Unter "Erweitert"-"Update automatisch installieren„ klicken. So bleibt der Browser immer auf dem neuesten Stand.

Vorsicht, Sicherheitslücke

Firefox-Browser sofort updaten

20.03.2017, 21:57 Uhr | hd

Im Firefox-Browser klafft eine Sicherheitslücke (Quelle: imago)

Teilen Twittern Drucken Mailen Redaktion

Firefox-Nutzer sollten ihren Browser sofort auf die aktuelle Version 53.0.2 aktualisieren. Das Update schließt eine schwere Sicherheitslücke, so das Bundesamt für Sicherheit in der Informationstechnik. Betroffen ist nur die Windows-Version.

Your PC is now Stoned, legalize Marijuana!
(Nun ist Ihr PC versteinert, legalisieren Sie Marijuana)

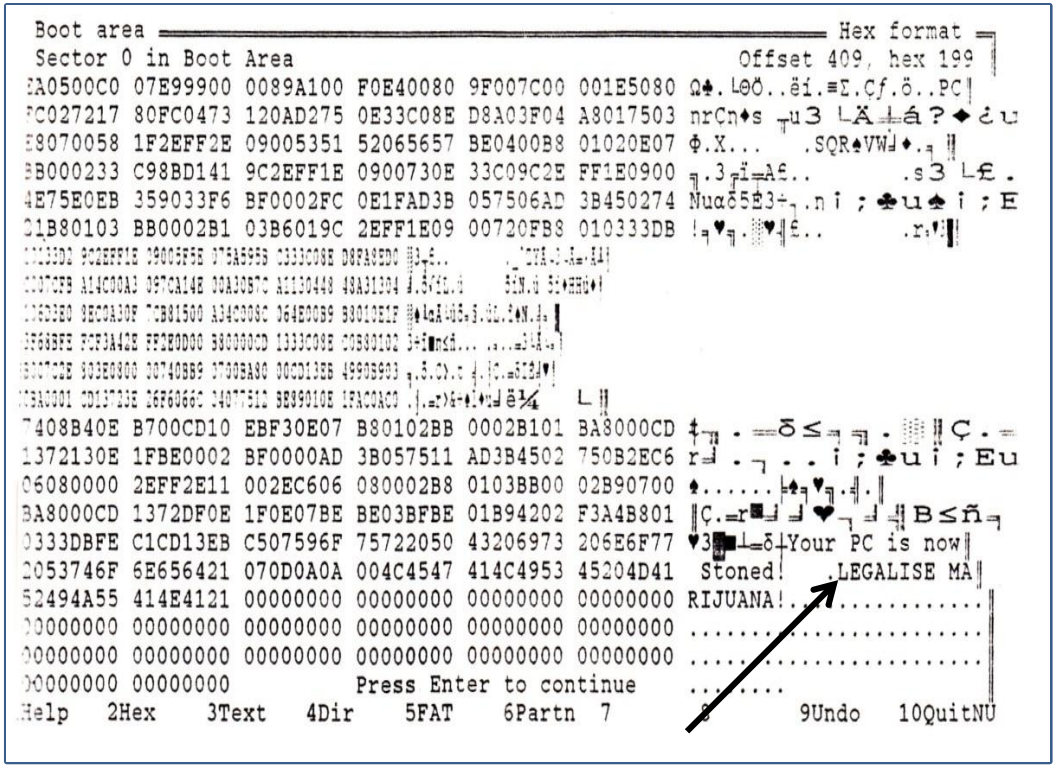
Dieser Virus tauchte erstmalig 1986 bei der DB auf.

Er setzte sich in der Partitions-tabelle fest und ließ den Rechner zwar starten, dann aber wurde der Bildschirm grün und es erschien lediglich die Meldung, dass der PC „einge-froren ist“.

Die einzige Möglichkeit ihn wieder zu reaktivieren, bestand in einer Neuformatierung mit dem Befehl

Format/s,

dabei gingen alle gespei-cherten Daten verloren

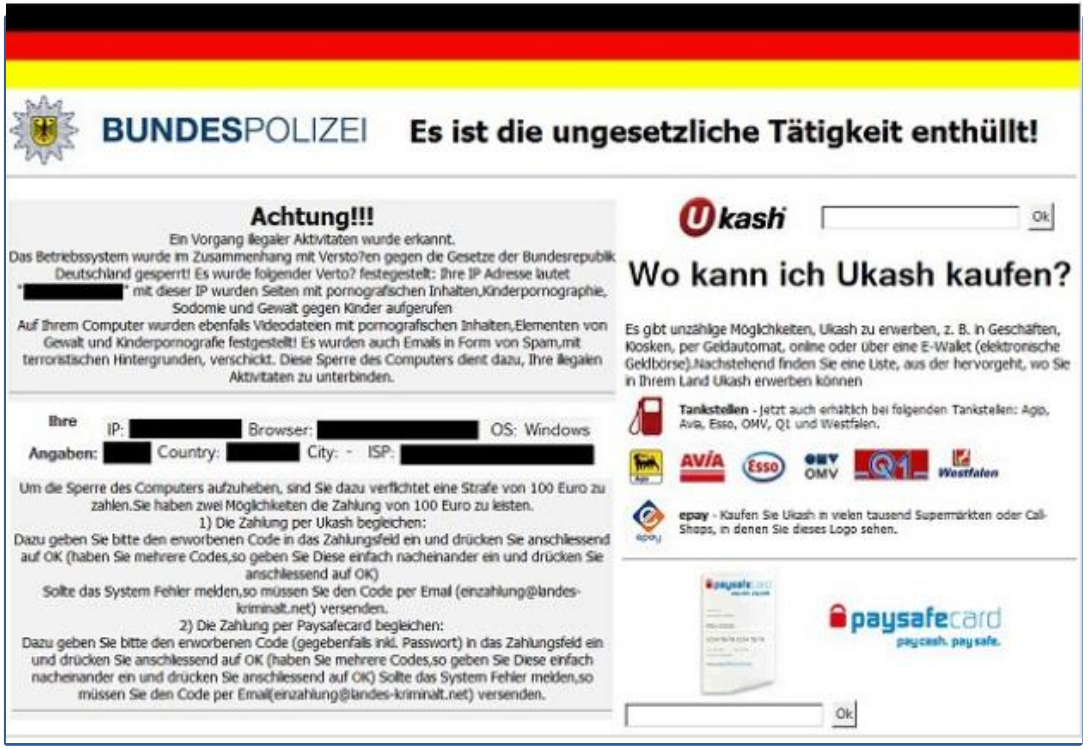


Der Bundestrojaner

Mit diesem Trojaner versuchte man Ihnen einzusuggerieren, dass Sie Bilder bzw. Programme pornografischen Inhalts im Internet heruntergeladen hätten und dabei „erwischt“ worden wären. Ihr Rechner „fror“ bei dieser Anzeige ein. Sie wurden aufgefordert zur Verhinderung einer Strafverfolgung einen Geldbetrag über **Western Union** zu zahlen. Der Ukash kann z.B. an Tankstellen oder in Grafrath auch bei Edeka erworben werden – **nur** der Überweisungsweg zum Empfänger kann nicht mehr nachverfolgt werden.

Dies alleine dürfte Sie schon misstrauisch machen. Weiterhin müssten Sie noch Ihre IP, Browser, Windows-Version usw. angeben.

Hatten Sie gezahlt, stand es in den Sternen, ob Sie Ihren Rechner wieder freigeschaltet bekamen. Außerdem war Ihr PC durch Ihre persönlichen Angaben weiterhin extrem gefährdet.



Eine andere Darstellung des Bundestrojaners

Microsoft certified

Man kann selbst erstellte Programme durch Microsoft prüfen und gegen Rechnung zertifizieren lassen.

Eigenartigerweise werden derartig zertifizierte Programme vielfach von einigen Virenprogrammen nicht erkannt und da sie von „Microsoft certified“ sind, wohl auch übergangen (bprotector).

Was ist also einfacher als das: Man eigne sich widerrechtlich ein Zertifikat von einer vertrauenswürdigen Stelle an und alles weitere ist ein Kinderspiel

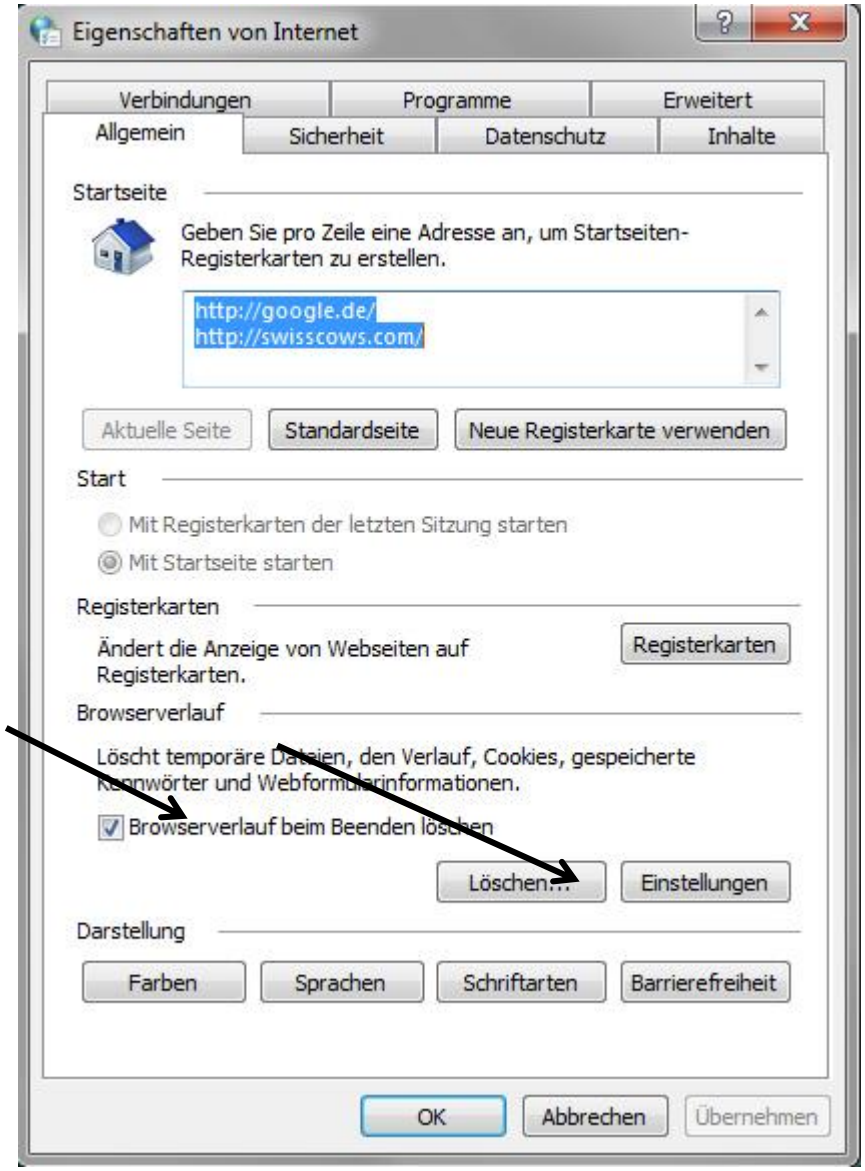
Gefälschte E-Mail-Absenderadressen – die technische Basis

Findige Würmer

Computer-Würmer verbreiten sich, indem sie E-Mail-Adressen missbrauchen. Einerseits versenden sie sich selbst an jede Adresse weiter, die sie in Adress-Verzeichnissen auf einem infizierten PC entdecken. Andererseits benutzen sie auch gefälschte Absenderadressen oder durchfilzen Ihren Cache nach verwert-baren Daten.

Die meisten Browser sind so eingestellt, dass sie besuchte Websites für eine gewisse Zeit im Cache abspeichern. Aus diesen HTML-Seiten lassen sich eben-falls die ggf. darin enthaltenen E-Mail-Adressen bei unerlaubten Zugriff leicht herausfinden. **Daher sollte der Browser-Verlauf** bei längerer Benutzungsdauer des PC's **öfter gelöscht werden**. Sie finden ihn in der Systemsteuerung unter der Einstellung **INTERNETOPTIONEN.**

S.a. nachfolgende Bankwarnung



Warnungen durch Ihre Online-Banken

Banken weisen diesbezüglich nach Beendigung Ihrer Online-Banking Aktionen darauf hin, nicht wie Sie es gewohnt sein mögen, den Vorgang über Windows - **x** zu beenden, sondern über die vorgegebene **LOGOUT**-Taste mit nachfolgender Löschung des Browserverlaufs (Cache)

Eine typische Viren-eMail.

Der Virus steckt im Anhang - angeblich in einem Bild und stammt vermutlich aus Russland

Eine Viren-eMail:

1.)Hier wird simuliert, dass die eMail von **Teome Buck** aus **Frankreich** über die eMail-Adresse von christianmartin44@wanadoo.**fr** versandt wurde

2.) Im weiteren Verlauf erscheinen kyrillische Schriftzeichen:

Ich bin eine **schцne** und einfache Frau: (Russisch **ц** . Deutsch **z,** also **„schzne“**)

Ich **heiЯe** Teom**a**! (Russich **Я** Deutsch **ja,** also **„heijae“**)

Mit freundlichen **GгьЯen**

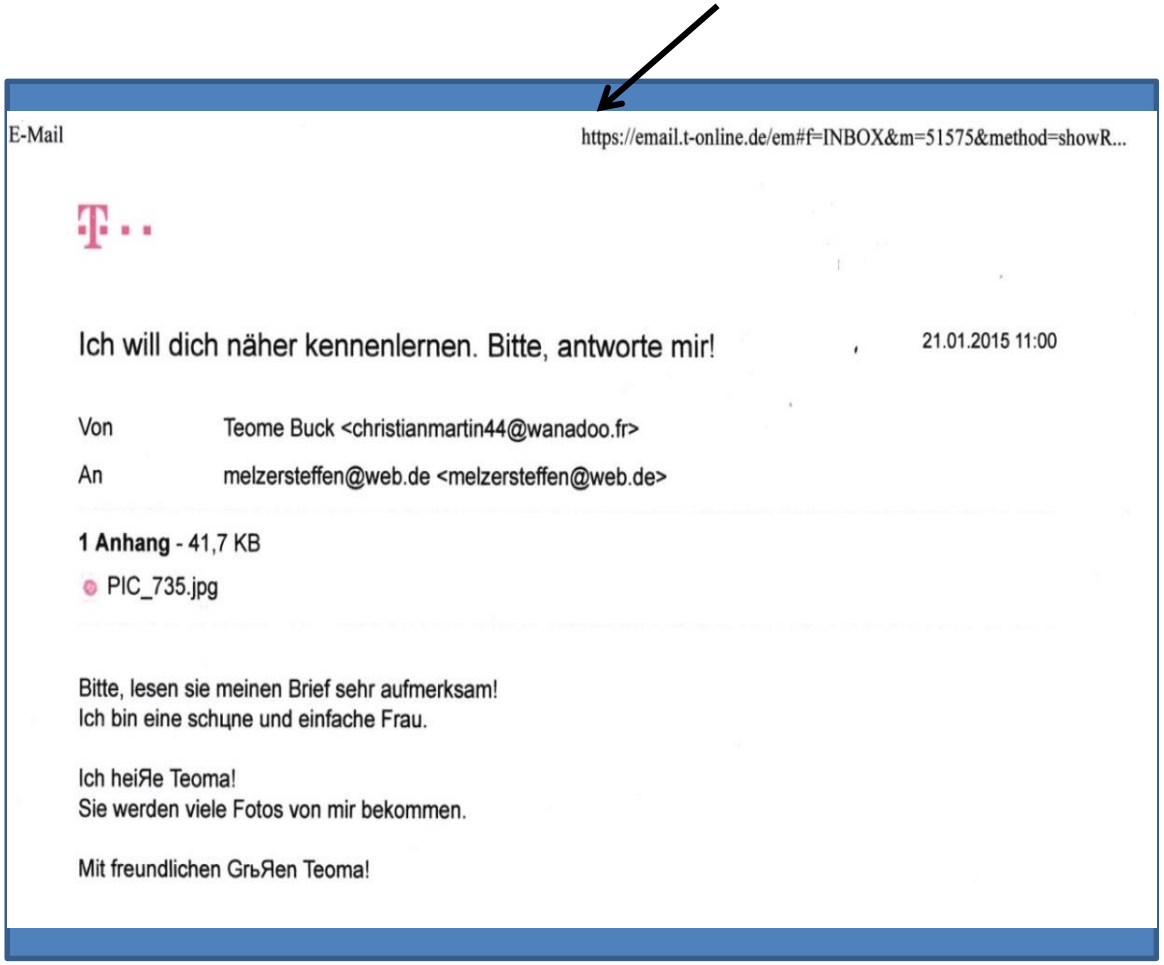
(Russisch „**гь**“ weich „g“ gesprochen und **ja,** also **Ggjaen“**)

Teom**e** heisst auf einmal Teom**a**

3.) Und……. **Ich** bin nicht Melzersteffen@web.de !!!!!

Diese Adresse ist entweder gestohlen oder existiert gar nicht.

Hauptsache: Neugier geweckt !!!



Eine weitere eMail
ähnlich wie vorhergehendes Bild

Was schreibt Mi Yuliya an Brocken-bullis?

Auch hier scheint der Virus bzw. Trojaner in der „Bilddatei PCX_086.jpg“ zu stecken. Durch Anklicken würde er aktiviert. Dabei können z.B. Ihre Zugangsdaten gestohlen und im Darknet dem „interessierten„ Publikum zum Kauf angeboten werden. Das BKA ist erst kürzlich im Darknet auf eine „Verkaufsebene“ gestoßen in der **500 Millionen Zugangsdaten** verramscht werden konnten. Bei British Airways wurden erst neulich **380.000 Kundendaten** mit allen Bank- und Kontenverbindungen gestohlen

-Mail https://email.t-online.de/em

Hey. 17.01.2015 15:18

Von Mi Yuliya <noemie.rannou@orange.fr>

An brocken-bullis@gmx.de <brocken-bullis@gmx.de>

1 Anhang - 28,6 KB

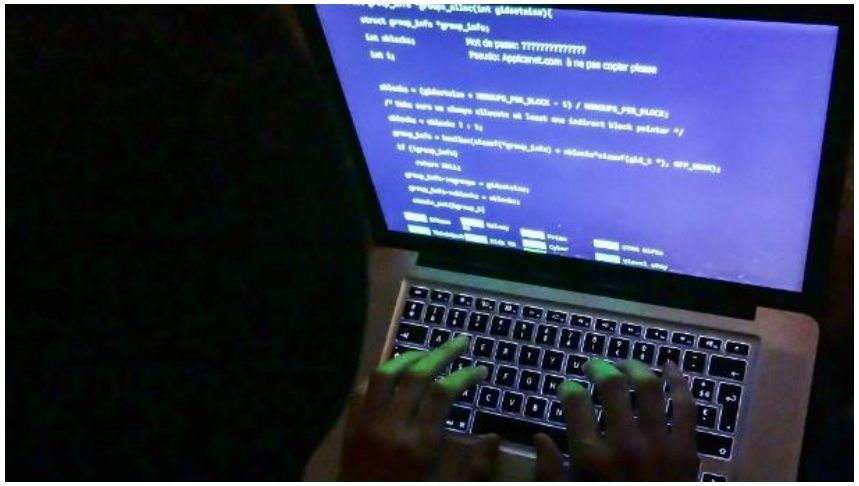
PCX_086.jpg

Tag!
Ich hatte nie gedacht, dass das schicksal mich mit dem Net zu bringen,
fur die Suche nach meinem zweiten Teil.
Ich sah dein Profil auf einer DatingWebseite und beschlossen, Ihnen zu schreiben.
Ich habe mich entschieden, das Internet zu verwenden, um kennenzulernen, da sich im realen
Leben mir die schlechten Manner treffen, die mich verraten mich nicht schatzen.
Ich bin 31 jahre alt, lebe in Russland in der provinz weit von gro?en Stadten und all diese Eitelkeit.
Ich war verheiratet niemals und ich habe keine Kinder.
Es ist ein wunsch, den guten mann fur die ernsten beziehungen treffen.
Ich hoffe, dass sie mein Foto war angenehm. Schreiben sie mir, wenn sie sich fur mich interessieren.
Sehr wichtig! Ich freue mich nur ernsthafte Beziehung! Ich brauche keine Spiele und virtuellen Sex!
Ich werde euch noch mehr Foto senden ...

Antworten Sie bitte nur meine privaten email: krohayulka83@gmail.com

Ich hoffe, dass Sie ehrlich zu mir sein.
Schreiben Sie mir den gegenwartigen Namen.
Goodbye...

BKA findet 500 Milionen gestohlene Zugangsdaten



Mehr als 500 Millionen kopierte Zugangsdaten für Online-Dienste haben Ermittler auf einer Hacker-Plattform im "Darknet" gefunden. Darunter sind offenbar auch viele Daten von deutschen Nutzern. Ein Selbsttest zeigt Ihnen, ob Ihre Daten auch betroffen sind. Die Datenbank des Hasso-Plattner-Instituts (HPI) erlaubt den Abgleich der eigenen Daten über den **Identity-leak-checker**

Passwörter ändern, falls Sie betroffen sind

Achtung: Nur wer betroffen ist, bekommt eine Nachricht und sollte dann aber sofort alle betroffenen Passwörter ändern. Außerdem sollten Nutzer überlegen, wo sie die betroffenen Zugangsdaten eventuell noch benutzen und sie dort auch ändern. Generell gilt: Für unterschiedliche Dienste immer unterschiedliche Passwörter nutzen, die nicht zu erraten sind und Ziffern und Sonderzeichen enthalten

British Airwaiys:

07.09.2018 | 16:18 Uhr |

Hacker konnten 380.000 Kundendaten bei British Airways entwenden, darunter auch Kreditkartennummern.

Ein Leck in der Datenbank des On-line-Buchungssystems von British Airways wurde von Hackern ausgenutzt, um Kundendaten im großen Stil zu stehlen. Die Datensätze umfassen laut Anbieter Name, Adresse, E-Mail sowie Kreditkartendaten und Bankverbindungen. Die Details zur Reise oder aus dem Reisepass seien hingegen nicht gestohlen worden. British Airways wurde erst im Juli ein unvorsichtiger Umgang mit den Kundendaten vorgeworfen. Diese seien mutmaßlich an Werbeunternehmen verkauft worden. Entdeckt wurde diese Schwachstelle bereits am Mittwoch. Sie sei mittlerweile überarbeitet und geschlossen worden.

Wie aber kamen die Hacker an diese Kundendaten

Zwischen dem 21. August und 5. September griffen die Hacker die Kundendaten sowohl von der Website als auch aus der App ab. Dem Sicherheitsforscher fiel auf, dass nur Kundendaten gestohlen wurden, die bei **Buchung eines Tickets in das Bezahlformular** eingegeben wurden. Laut dem Sicherheitsexperten nutzt Magecart so genannte Kreditkarten-Skimmer zum Abgreifen von Zahlungsdaten in digitaler Form. Eine solche Skimmer-Software wurde laut Klijnsma auch in die Website von British Airways injiziert. Da die App auf das Grundgerüst der Website zurückgreift, wurde der Diebstahl auch hier möglich. Die Malware wurde wahrscheinlich schon am 21. August 2018 unbemerkt installiert. Kam nun ein Nutzer auf die Website und buchte Tickets, wurden seine Daten über die Bezahlseite von der Malware abgegriffen und an eine Fake-Website weitergeleitet, die auf einem **privaten Server in Rumänien** gehostet wurde.

E-Mail-Header: Der Weg zum Absender

Beim Fälschen einer E-Mail-Absenderadresse wird der **E-Mail-Header** (die Kopfzeilen einer Nachricht) manipuliert. Dieser enthält unter anderem Informationen rund um den Zustellungsweg der E-Mail. Den Header können Sie sich in Ihrem E-Mail-Programm anzeigen lassen.

(ALT und linke Maustaste)

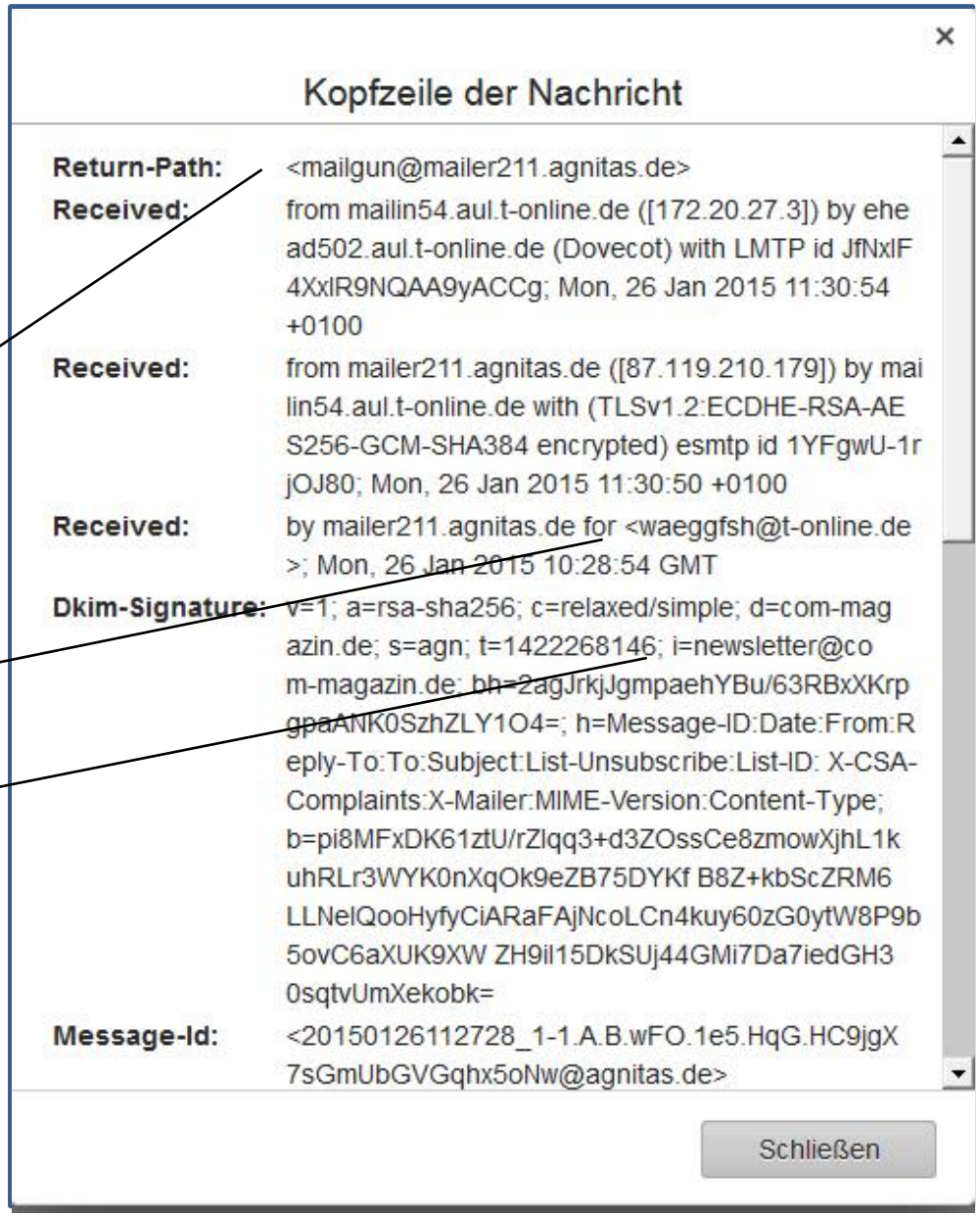
Über **mailgun** versandtes eMail

An: waeggfsh@t-online.de

Domain**K**eys **I**dentified **M**ail-Signature**:**

Newsletter des COM-Magazins

Ursprünglich sollte das Verfahren **D**omain**K**eys **I**dentified **M**ail nur die Spam-Flut eindämmen. Doch da es gefälschte Absenderadressen entdeckt, hilft es besser gegen **Phishing** und zusammen mit der Reputation des Absenders senkt es auch die Spam-Flut.

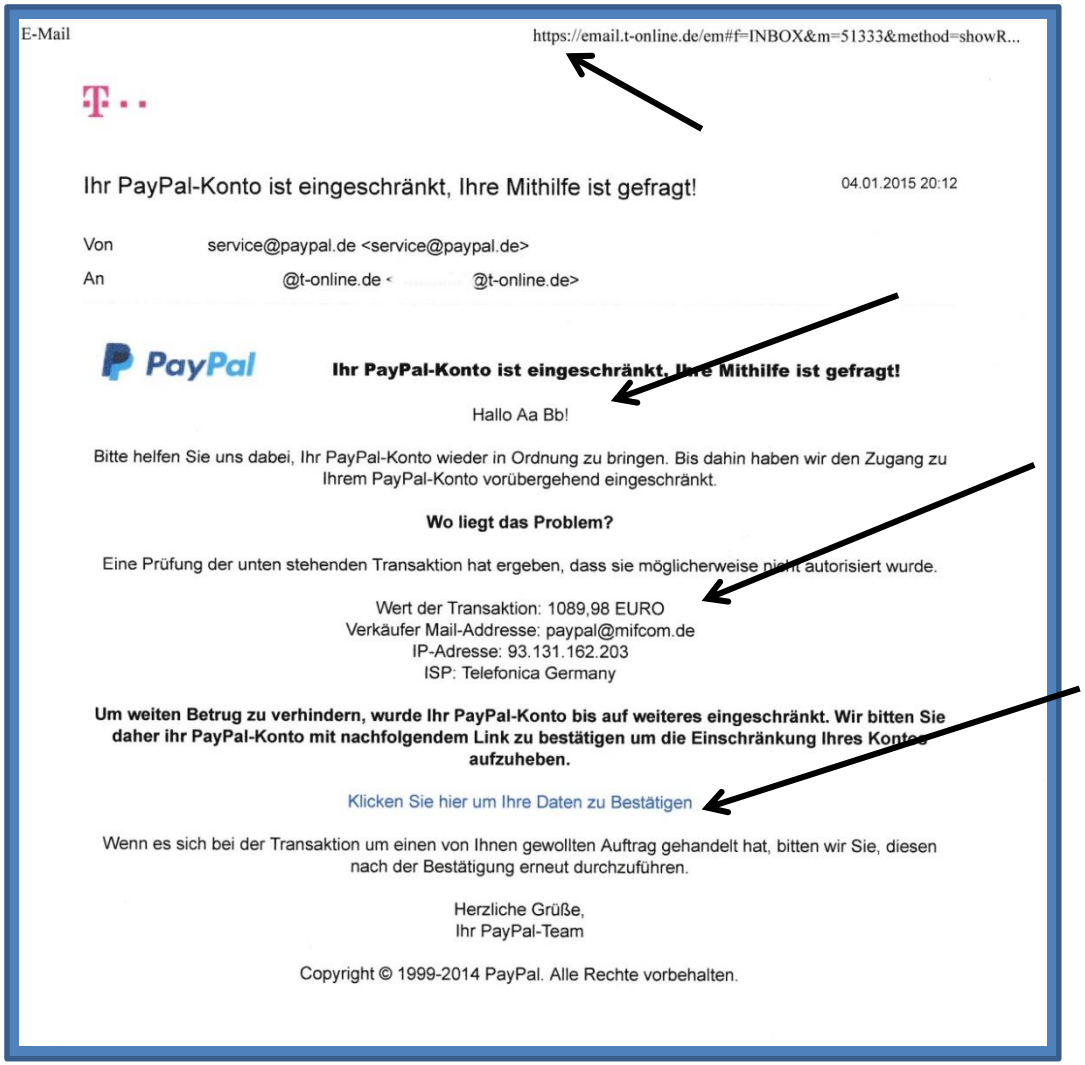


Computer-Viren ähneln in ihrer Funktion und ihrem Aufbau sehr biologischen Viren.

Biologische Viren	Computerviren
Greifen spezielle Körperzellen an.	Greifen auf bestimmte Dateien zu, nämlich Programme (*.exe, *.com, usw. …)
Die Erbinformation einer Zelle wird verändert.	Das infizierte Programm wird verändert.
In der befallenen Zelle wachsen neue Viren heran.	Das befallene Programm befällt weitere Programme.
Eine infizierte Zelle wird nicht mehrfach vom gleichen Virus befallen.	Fast alle Computer-Viren befallen nur einmal das Programm.
Ein befallener Organismus zeigt unter Umständen lange Zeit keine Krankheitserscheinungen.	Ein befallenes Programm kann auch unter Anderem lange Zeit fehlerfrei weiterarbeiten.
Viren können mutieren und somit nicht immer eindeutig erkennbar sein.	Manche Computer-Viren können sich verändern und versuchen damit Suchroutinen auszuweichen.

„PayPal-Konto ist eingeschränkt“

Hier empfehle ich die verseuchte Datei **direkt an PayPal senden** und anschließend gleich löschen. Ihre „Anrede“ wird übrigens aus Ihrer eMail-Adresse generiert



E-Mail https://email.t-online.de/em#f=INBOX&m=51333&method=showR...

Ihr PayPal-Konto ist eingeschränkt, Ihre Mithilfe ist gefragt! 04.01.2015 20:12

Von service@paypal.de <service@paypal.de>

An @t-online.de < @t-online.de>

PayPal **Ihr PayPal-Konto ist eingeschränkt, Ihre Mithilfe ist gefragt!**

Hallo Aa Bb!

Bitte helfen Sie uns dabei, Ihr PayPal-Konto wieder in Ordnung zu bringen. Bis dahin haben wir den Zugang zu Ihrem PayPal-Konto vorübergehend eingeschränkt.

Wo liegt das Problem?

Eine Prüfung der unten stehenden Transaktion hat ergeben, dass sie möglicherweise nicht autorisiert wurde.

Wert der Transaktion: 1089,98 EURO
Verkäufer Mail-Addresse: paypal@mifcom.de
IP-Adresse: 93.131.162.203
ISP: Telefonica Germany

Um weiten Betrug zu verhindern, wurde Ihr PayPal-Konto bis auf weiteres eingeschränkt. Wir bitten Sie daher ihr PayPal-Konto mit nachfolgendem Link zu bestätigen um die Einschränkung Ihres Kontos aufzuheben.

Klicken Sie hier um Ihre Daten zu Bestätigen

Wenn es sich bei der Transaktion um einen von Ihnen gewollten Auftrag gehandelt hat, bitten wir Sie, diesen nach der Bestätigung erneut durchzuführen.

Herzliche Grüße,
Ihr PayPal-Team

Copyright © 1999-2014 PayPal. Alle Rechte vorbehalten.

https: wird bestimmt nicht bei normalen eMails eingesetzt.

Hypertext **T**ransport **P**rotocol **S**ecure

Hallo **Aa Bb**

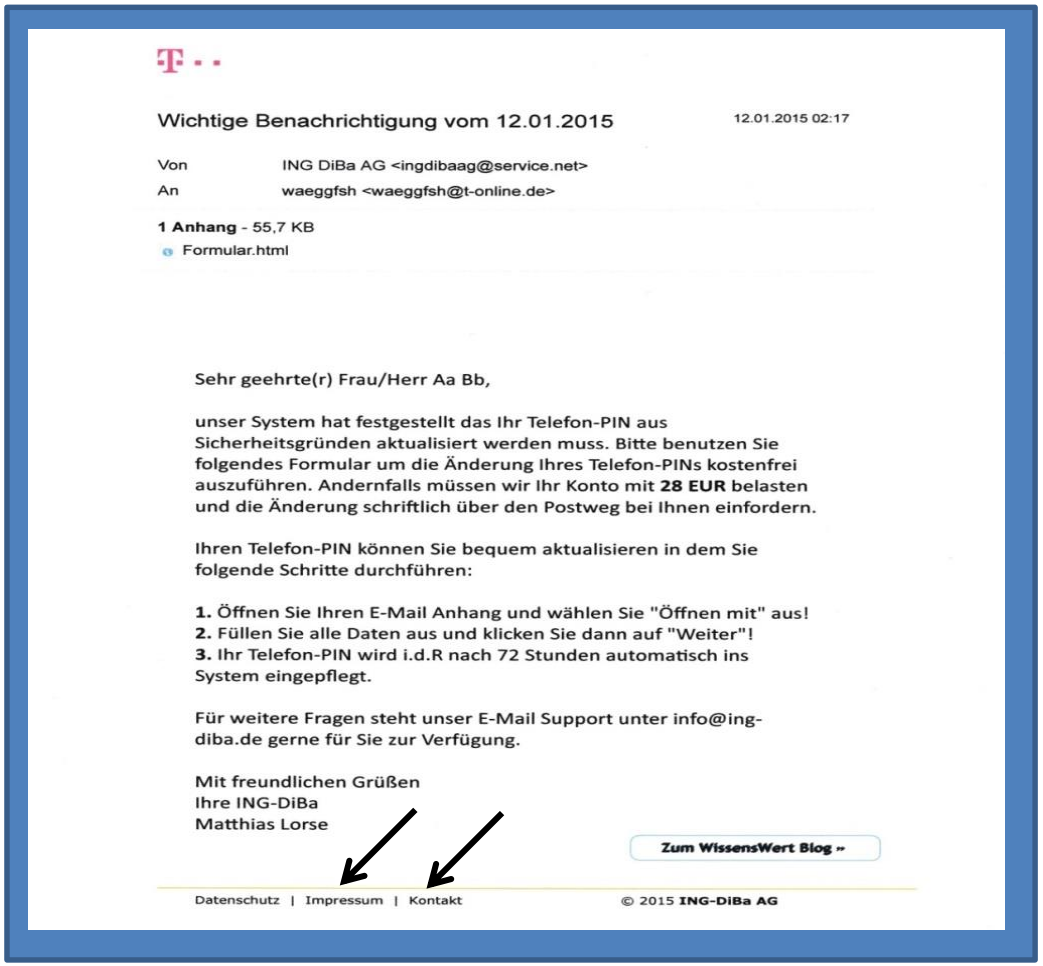
sind Platzhalter für aus eMails generierte Anreden. Daher in eMail-Adressen **keine** Vor- und Zunamen verwenden.

Mit der Angabe der Höhe der Transaktion von **1089,89 €** will man Sie unter Stress setzen, um Sie zu unüberlegten Handlungen zu verleiten. Damit aber installieren Sie zielgerichtet einen Virus!

„Klicken Sie hier um Ihre Daten zu Bestätigen“

Deshalb Ruhe bewahren, überlegen und anschließend einfach ***LÖSCHEN***

Pishing-Versuch
Ergaunern Ihrer Bankdaten



Wichtige Benachrichtigung vom 12.01.2015 12.01.2015 02:17

Von ING DiBa AG <ingdibaag@service.net>
An waeggfsh <waeggfsh@t-online.de>

1 Anhang - 55,7 KB
Formular.html

Sehr geehrte(r) Frau/Herr Aa Bb,

unser System hat festgestellt das Ihr Telefon-PIN aus Sicherheitsgründen aktualisiert werden muss. Bitte benutzen Sie folgendes Formular um die Änderung Ihres Telefon-PINs kostenfrei auszuführen. Andernfalls müssen wir Ihr Konto mit **28 EUR** belasten und die Änderung schriftlich über den Postweg bei Ihnen einfordern.

Ihren Telefon-PIN können Sie bequem aktualisieren in dem Sie folgende Schritte durchführen:

1. Öffnen Sie Ihren E-Mail Anhang und wählen Sie "Öffnen mit" aus!
2. Füllen Sie alle Daten aus und klicken Sie dann auf "Weiter"!
3. Ihr Telefon-PIN wird i.d.R nach 72 Stunden automatisch ins System eingepflegt.

Für weitere Fragen steht unser E-Mail Support unter info@ing-diba.de gerne für Sie zur Verfügung.

Mit freundlichen Grüßen
Ihre ING-DiBa
Matthias Lorse

Zum WissensWert Blog »

Datenschutz | Impressum | Kontakt © 2015 **ING-DiBa AG**

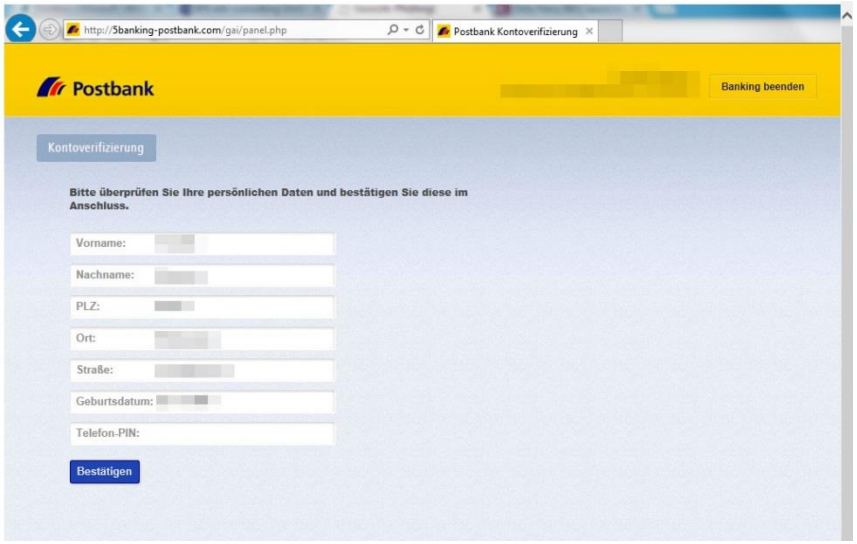
Google stoppt Phishing-Angriff

Google hat einen sich rasch ausbreitenden Phishing-Angriff gestoppt. Die Attacke sei binnen einer Stunde unterbunden worden, sagte ein Sprecher des US-Internetriesen am Donnerstag. Weniger als 0,1 Prozent der eine Milliarde Gmail-Nutzer weltweit seien betroffen gewesen. Die Nutzer bekamen eine gefälschte E-Mail von einer bekannten Adresse mit der Einladung zur Online-Bürosoftware Google Docs. Wer auf den Link klickte, öffnete einer Schadsoftware den Zugang zu seinem Gmail-Konto, die sich dann über die Kontakte weiter verbreitete.

MM 05.05.17

Trügerische Links und Webseiten

Der Empfänger wird für die Dateneingabe über einen Link auf eine Internetseite geführt, die zum Beispiel der Banken-Homepage ähnlich sieht. Auf den ersten Blick scheint alles ganz normal, selbst die Eingabeformulare sehen gleich aus. Die Phishing-Betrüger nutzen darüber hinaus entweder Internetadressen, die sich nur geringfügig von denen der renommierten Firmen unterscheiden.



Oder aber sie fälschen die Adressleiste des Browsers mit einem JavaScript. Man glaubt also, man sei auf einer seriösen Seite, ist es aber nicht. Wer einer solchen Seite seine EC-Geheimnummer, Passwörter oder andere Daten anvertraut, der beschert dem Angler fette Beute und kann sich selbst jede Menge Ärger einhandeln.

Im Nachfolgenden wird sogar nach einer Telefon-Pin gefragt, Wenn Sie nach dem Ausfüllen diese „Formulars“ noch **BESTÄTIGEN** drücken, haben Sie den Ärger.

HTTPS („Hypertext Transport Protocol Secure“) Bankverbindung “ohne” Secure?

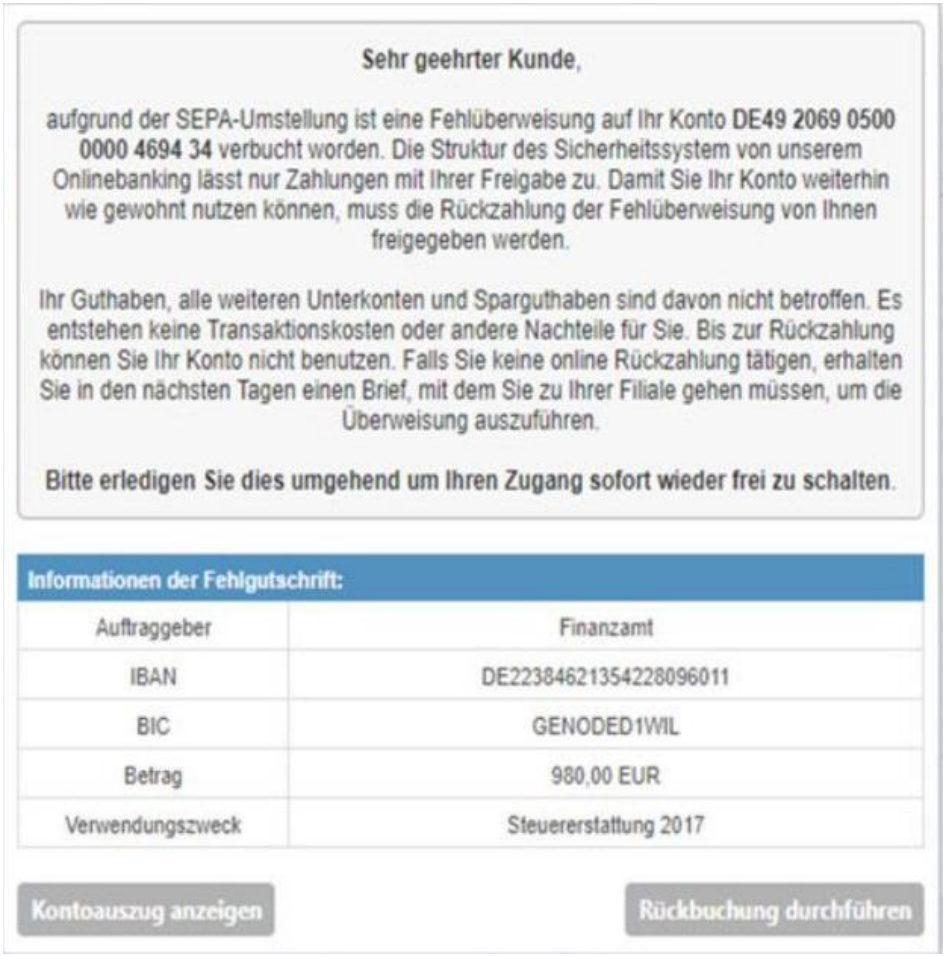
Trojaner täuschen unberechtigte Gutschrift vor

Online-Banker – Vorsicht !! Online-Banking sollte eigentlich sicher sein **(https**). Doch die Gauner haben hier wieder eine Lücke gefunden. Das BKA warnt dazu aktuell vor neuen Schadprogrammen. Kunden des Online-Bankings werden z.B. aufgefordert, eine fehlgeleitete Gutschrift mit einer TAN zurück zu überweisen.
Der entsprechende Beleg könne online abgerufen werden. Wer dieser Aufforderung folgt, lädt sich einen **Spion** auf den PC.

"Sie haben eine Eilüberweisung an die Empfänger-IBAN GB31 LOYD 3157 1915 5021 31 in Höhe von 1.191,31 EUR erfasst", heißt es in der Mail. Am Ende der sehr kurzen Mitteilung findet der Empfänger einen Link, der zur angeblichen Artikelfreigabe führen soll.

Dahinter verbirgt sich jedoch in aller Regel eine Zip-Datei, die – heruntergeladen und ausgeführt – den Computer mit Schadsoftware verseuchen kann. Getarnt werden die Spam-Mails als eine Benachrichtigung von Ihrer Bank und/oder anderen Finanzdienstleistern. "Dabei gehen Cyberkriminelle immer raffinierter vor und bestücken ihre E-Mails mit zahlreichen echten Links auf Dienstleistungen der Institute". Damit erhöhen sie deren Glaubwürdigkeit. Der Empfänger fällt so leichter auf den einzigen schadhaften Link in der E-Mail herein."

Auf das „Finanzamt“ fällt hoffentlich keiner herein



Sehr geehrter Kunde,

aufgrund der SEPA-Umstellung ist eine Fehlüberweisung auf Ihr Konto **DE49 2069 0500 0000 4694 34** verbucht worden. Die Struktur des Sicherheitssystem von unserem Onlinebanking lässt nur Zahlungen mit Ihrer Freigabe zu. Damit Sie Ihr Konto weiterhin wie gewohnt nutzen können, muss die Rückzahlung der Fehlüberweisung von Ihnen freigegeben werden.

Ihr Guthaben, alle weiteren Unterkonten und Sparguthaben sind davon nicht betroffen. Es entstehen keine Transaktionskosten oder andere Nachteile für Sie. Bis zur Rückzahlung können Sie Ihr Konto nicht benutzen. Falls Sie keine online Rückzahlung tätigen, erhalten Sie in den nächsten Tagen einen Brief, mit dem Sie zu Ihrer Filiale gehen müssen, um die Überweisung auszuführen.

Bitte erledigen Sie dies umgehend um Ihren Zugang sofort wieder frei zu schalten.

Informationen der Fehlgutschrift:	
Auftraggeber	Finanzamt
IBAN	DE22384621354228096011
BIC	GENODED1WIL
Betrag	980,00 EUR
Verwendungszweck	Steuererstattung 2017

Kontoauszug anzeigen

Rückbuchung durchführen

Warnung vor „Microsoft-Mitarbeitern“

Betrug durch falsche Microsoft-Mitarbeiter

In letzter Zeit häufen sich erneut Anrufe von **Betrügern, die sich als Mitarbeiter von Microsoft** ausgeben, um an sensible Daten zu gelangen. Ziel dieser Anrufe ist, die Angerufenen dazu zu bewegen, entweder Programme aus dem Internet herunterzuladen, infizierte Webseiten zu besuchen oder über die Anpassung der Registry in Windows Zugriff auf ihren Computer zu gewähren. Dies geschieht unter dem Vorwand, es handle sich um eine Support-Aktion von Microsoft zur Lösung der Computerprobleme.

Es sind Fälle bekannt, in denen die Angerufenen **zur Zahlung genötigt** werden sollten, mit der Behauptung, andernfalls funktioniere der Computer nicht mehr einwandfrei. Es sollen Zertifikate oder Sicherheitspakete erworben werden, welche per Netbanking, Überweisung oder Kreditkartenzahlung gekauft werden können.

Die Anrufer suchen sich die Opfer offensichtlich über öffentlich zugängliche Verzeichnisse aus. Die Gespräche werden oftmals auf Englisch geführt.

Verhaltenstipps:

- Gehen Sie nicht auf die Forderungen der Anrufer ein und beenden Sie das Gespräch.
- Unterbrechen Sie die Internetverbindung um Computer.
- Führen Sie keine Installation bzw. Downloads aus und tätigen sie keine Zahlungen.

Eine eMail der neuen und gemeinen Art

Stellen Sie sich einmal vor, Sie erhalten eine Nachricht, dass in Outlook eine eMail eingegangen sei. Der Absender scheint real zu existieren. In der eMail werden Sie aufgefordert eine Eingangsbestätigung zu senden – obwohl dies eine „no-replay“ – Nachricht ist. Letzteres sollte wohl „**NO REPLY**“ für keine Rückantwort lauten. Also schon ein 1.Hinweis auf ein Fake (Betrug).

Sie sind also nicht interessiert und wollen die eMail löschen da Ihr Virenprogramm diese eMail bereits als Spam identifiziert hat. Außerdem sind Fehler erkennbar an der Länderkennung [no-replay@csis.dik]. Das soll „Dänemark“ sein! Im Outlook-Fenster erscheint aber kontakt@csis.dk mit der richtigen Länderkennung. Warum soll auf eine eMail mit dem Index „**no-replay“** eine Lesebestätigung gesendet werden.

Und jetzt geht der Ärger los. Die Mail lässt sich nun **weder schließen noch verschieben** und **bleibt resistent** auf dem Desktop geöffnet. Lediglich im Outlook-Fenster entdecken Sie die zwei Button mit folgendem Hinweis.

Wollen Sie eine Bestätigung senden?

Das Feld NEIN ist grau unterlegt, was nun….

Abhilfe über den Taskmanager

Eine Nebentätigkeit als eine Teilarbeit!

Schönen guten Tag,
Ich erhalte mehr Geld mit Hilfe von meinem Konto in einer jeglichen deutschen oder österreichischen Bank und will diesen Weg mit Ihnen teilen.

Die kurze Beschreibung dieser Arbeit:

Auf meinem Konto in einer Bank trifft das Geld von der Finanzabteilung ein, mit der ich zusammenarbeite. **Meine Vergütung macht 18 % von dem auf meinem Konto eingegangenen Geld aus!** 82% von dem auf meinem Konto eingetroffenen Geld soll ich in der Bank bar abheben und es einem Vertreter der Firma versenden. **Die Summe der Banküberweisungen variieren und mein Einkommen für jede Operation macht durchschnittlich 700 EUR aus.**
Für die Bearbeitung von einer Transaktion ist mein Zeitaufwand nicht mehr als 2 Stunden. Dieser Job lenkt mich von meiner Hauptarbeit gar nicht ab und bringt mir zusätzliches Nebeneinkommen. **Im vorigen Monat hab ich mehr als 4.000 EUR bekommen.**
Jetzt wirbt diese Firma um neue Angestellte! Um in unserem Unternehmen eine Stelle zu bekommen, sollen Sie Staatsangehörigkeit in Deutschland oder Österreich und ein Konto in einer deutschen oder österreichischen Bank haben.

Um in unserer Firma mit der Arbeit zu starten, beantworten Sie diese Email.

Auch für „Dumpfbacken“ ist etwas dabei

- Der Betrogene sind Sie, denn Sie haben wie aus der Anweisung ersichtlich 82% der annullierten Überweisung aus eigener Tasche bezahlt.
- Sollte der Betrogene zur Polizei gehen um Anzeige zu erstatten, so kann ihm selbst zusätzlich noch eine Anzeige nach dem **Geldwäschegesetz** blühen.

Vishing

Vishing leitet sich ab von Voice Phishing, also telefonischem Trickbetrug. Hierbei wird mit Telefonanrufen versucht, Sie als Empfänger in die Irre zu führen und zur Herausgabe von Zugangsdaten, Passwörtern, Finanzdaten etc… zu bewegen.
Meist wird ein automatisiertes Sprachsystem (Band) eingesetzt. Hierbei wird ihnen eine hohe Dringlichkeit vermittelt um Sie unter Druck zu setzen, und dadurch zu Fehler zu verleiten, die verlangten Daten herauszurücken. Gerade in Stresssituationen passiert das dann eher, als wenn Sie cool und in Ruhe telefonieren. Natürlich ist die Identität des Anrufers keinesfalls echt! So sind bei diesen „Gangstern“ folgende Rufnummern sehr beliebt z.B. „08141 **110**“ oder „089 **118**“. Wenn Sie nicht wissen, dass derartige Rufnummern **niemals** **„abgehend“** sein können, schnappt die Falle schon zu. **Die Polizei ruft niemals über die Notrufnummer „110“ an**, sondern ganz normal über eine örtliche, in jedem Telefonbuch nachzulesende Rufnummer.
Unverschämt sind folgende Versuche: Der Anrufer fragt, ob Sie ihn verstehen können. Wenn Sie diese Frage mit **JA** beantworten, erhalten Sie umgehend eine Rechnung über nicht bestellte Ware, da Ihr **JA** in eine vorgefertigte Bandaufnahme eingefügt wird und somit der Eindruck entstehen kann, Sie hätten einen Artikel telefonisch bestellt, in der Regel ein 2-Jahres Abonnement. In derartigen Fällen antworten Sie statt dessen besser mit Gegenfragen, z.B. **WER SIND SIE, WAS WOLLEN SIE, WARUM** usw.

Blockieren eines Vishing-Versuchs

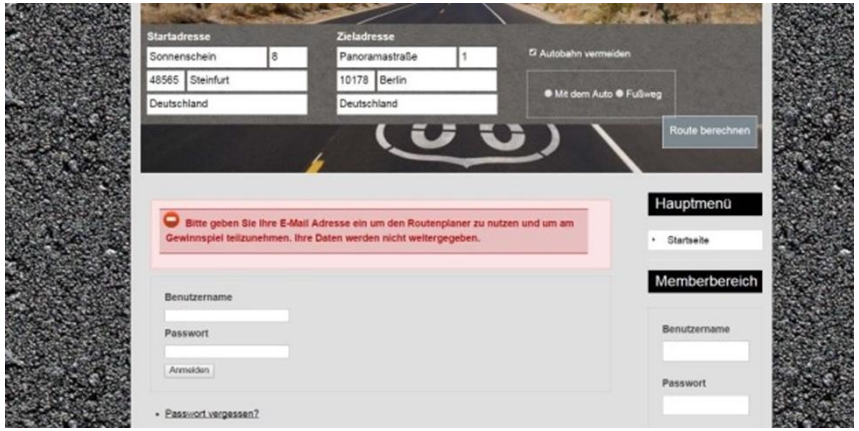
Sie werden ständig über eine gefakte Rufnummer **0211 66783**, die selbstverständlich nicht geschaltet ist, per Bandansage mit täglichen Gewinnversprechen überhäuft. Sie werden dabei aufgefordert durch Drücken der Tasten „1“, „2“ oder „3“ auf dem Ziffernblock Ihres Telefons Ihren Gewinn abzurufen. Sie würden angeblich umgehend mit einem Sachbearbeiter, der die Gewinnausschüttung vornimmt, verbunden. Wenn Sie dies aber tun, können Sie mit großer Sicherheit davon ausgehen z.B. in eine Warteschleife mit einer 0900er-Nummer zu landen. – Und das kann sehr teuer und auch sehr nervig werden. Leider kann diese Rufnummer nicht über Ihre Fritz-Box gesperrt werden, da sie ja nicht vorhanden ist. Doch nach einer Beratung durch die Telekom scheint hier Abhilfe möglich, für die angeblich jeder Bürger selbst sorgen kann.

Geben Sie nun in Ihr Telefon folgenden Auftrag ein:

Heben Sie dazu Ihren Telefonhörer ab und geben folgende Kombination ein. ***934***1611**#021166783.** Anschließend legen Sie den Hörer nach einer kurzen Wartezeit wieder auf. Zwischen dem 2.Stern und der Raute muss eine 4 stellige Pin-Nummer eingegeben werden, die Sie selbst bestimmen. **Die Zahlen nach der Raute sind die der zu sperrenden Rufnummer incl. Vorwahl.**

Ab sofort sollten Sie nach Auskunft der Telekom Ruhe vor dieser Rufnummer haben, da sie in der Zentrale für Ihren Anschluss damit gesperrt wird.

Totgesagte leben länger: Eine neue „alte“ Betrugsmasche mit Online-Routenplanern (kein Virus)

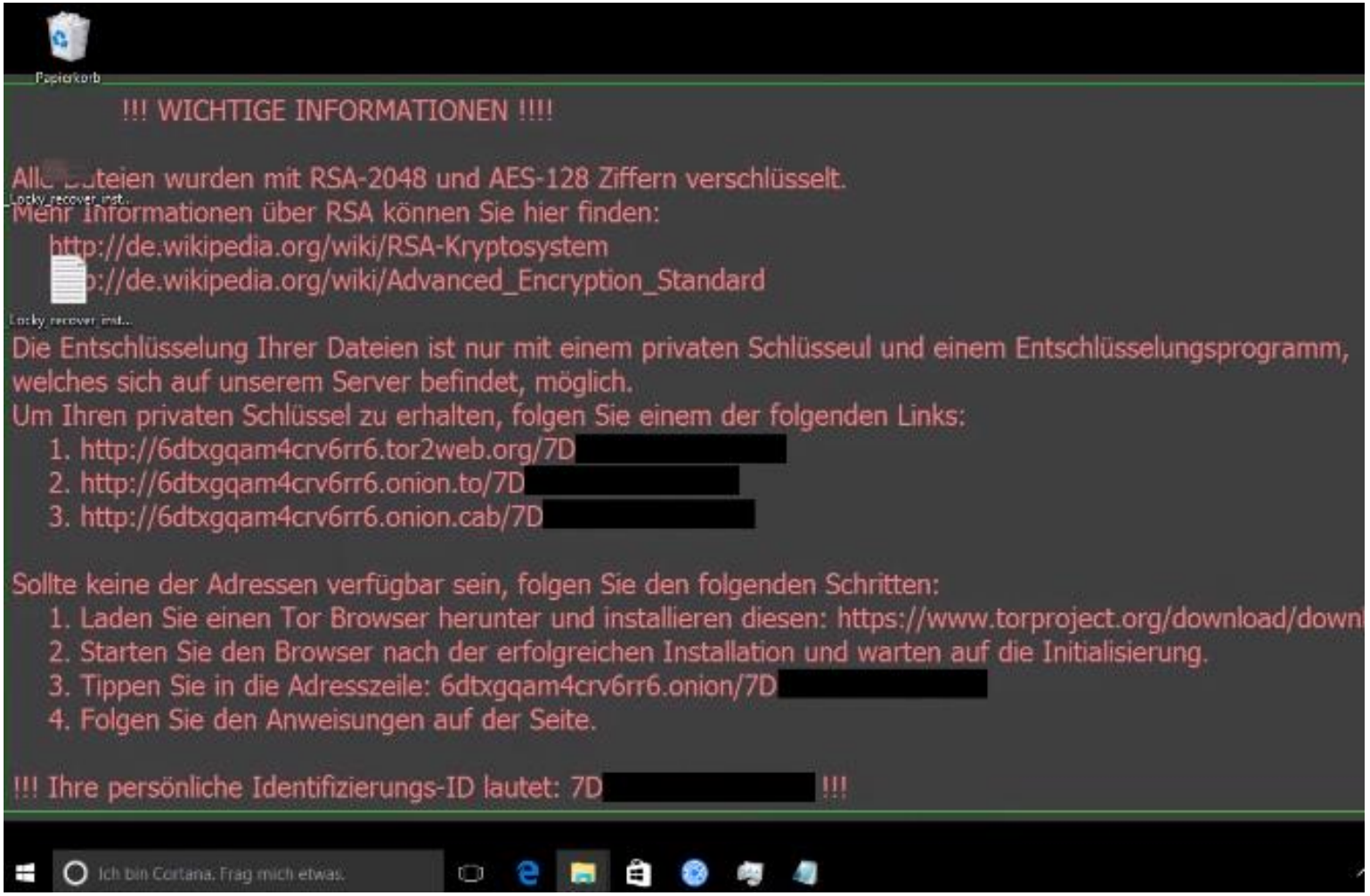


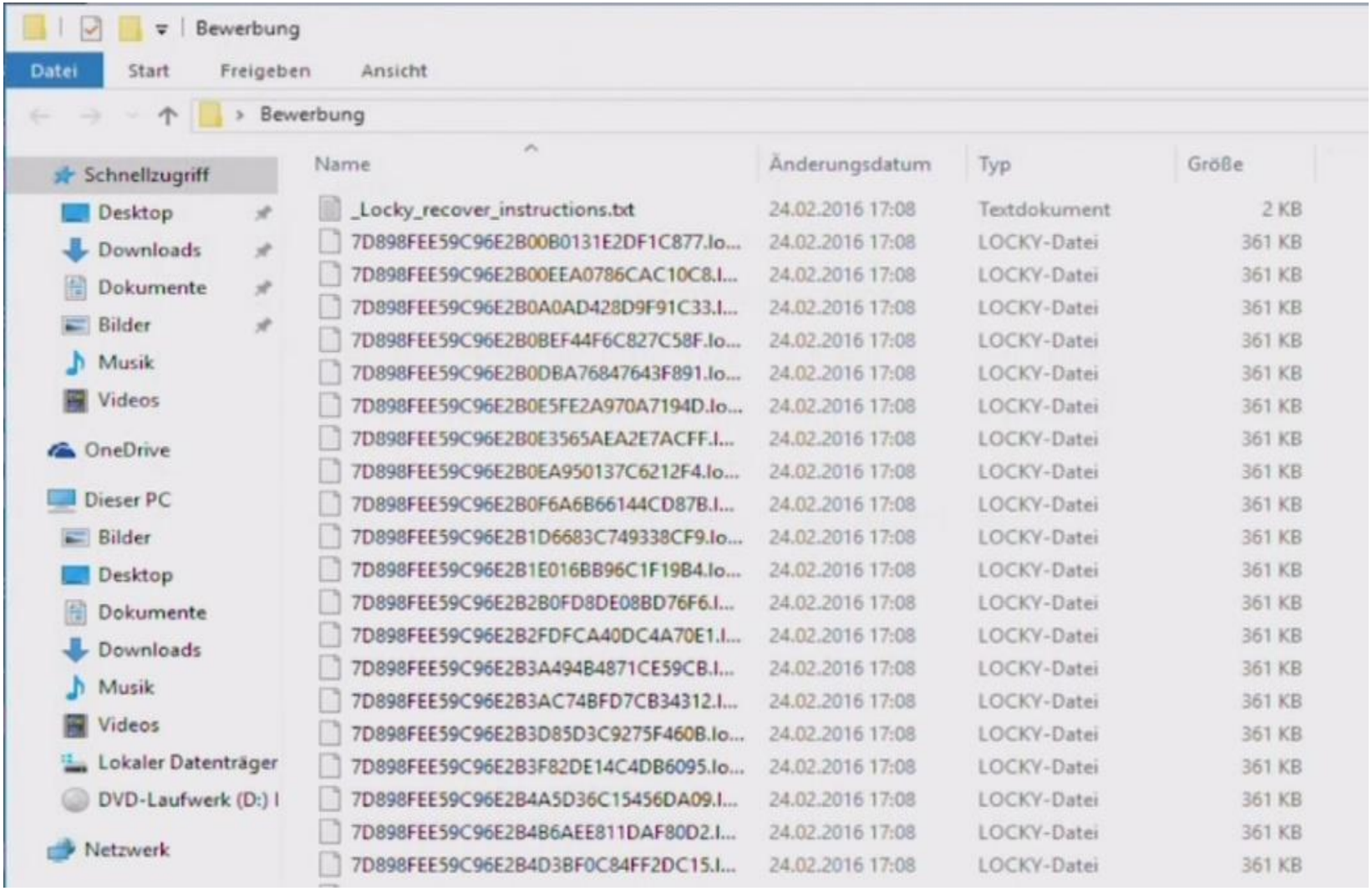
Abzockvariante mit Routenplaner-maps.website von Digital Media GmbH seit Februar 2017. Doch diese Firma existiert nicht.

Diese Betrugsmasche mit maps-routenplaner.info und Web24 GmbH Internetportale ist nicht neu. Sie kursierte schon vor 4 Jahren im Internet und lockt Internetnutzer mit der Aussicht auf ein Gewinnspiel an. Versucht dabei ihnen stattdessen einen kostenpflichtigen Nutzungsvertrag für einen Online-Routenplaner unterzujubeln. Wenn die überraschten Nutzer die Zahlung verweigern, dann schicken die Betrüger Mahnungen, Inkasso-Forderungen und drohen sogar mit Pfändung. „Auf die ‚Erinnerung‘ folgte direkt die ‚Letzte Mahnung‘, nicht mit Inkassodrohung, sondern direkt Gerichtsvollzieher. Die Mail und die darin gemachte Drohung mit der Pfändung sind völliger Unsinn. Betroffene sollten die angebliche Rechnung keinesfalls bezahlen, es liegt entgegen der Behauptung kein gerichtlicher Vollstreckungstitel vor und die Betrüger wissen anscheinend nicht einmal Namen und Adresse der angeblichen Kunden, sondern beziehen sich immer nur auf eine gespeicherte IP-Adresse. **Media Solution GmbH** und **Content Solution GmbH** haben ihren angeblichen Sitz in Frankfurt, doch beide Unternehmen existieren dort ganz offensichtlich nicht. Die entsprechenden Impressumangaben auf der Webseite des besagten Online-Routenplaners sind falsch.

Fazit: Zahlen Sie nicht!

Erpressungs-Trojaner Locky spricht Deutsch





So sieht Ihre Festplatte nach der Verschlüsselung mit Locky aus

Wie kann diese Ransomware einen Computer befallen.

Der '.locky – Infektions-Prozess ist leicht zu verstehen. Zuerst wird die '.locky Dateierweiterung'-Ransomware mit Hilfe von üblichen Bedrohungsmethoden geliefert, in den meisten Fällen über eine schädliche **E-Mail-Anlage**, die in einer **Phishing-E-Mail**-Nachricht enthalten ist. Wenn das Opfer diese E-Mail-Anlage öffnet, ist die '.locky Ransomware schon auf dem PC des Opfers installiert. Die '.locky' Ransomware führt einen Scan des Opfercomputers durch und sucht nach Dateien, die mit dem AES-Verschlüsselungsalgorithmus verschlüsselt werden können. Der .locky 'Ransomware Trojaner infiziert Dateien mit den folgenden Erweiterungen:

.7z**; **.rar**; .m4a; **.wma**; **.avi**; **.wmv**; .csv; .d3dbsp; .sc2save; .sie; .sum; .ibank; .t13; .t12; .qdf; .gdb; .tax; .pkpass; .bc6; .bc7; .bkp; .qic; .bkf; .sidn; .sidd; .mddata; .itl; .itdb; .icxs; .hvpl; .hplg; .hkdb; .mdbackup; .syncdb; .gho; .cas; .svg; **.map;** .wmo; .itm; .sb; .fos; .mcgame; .vdf; .ztmp; .sis; .sid; .ncf; .menu; .layout; .dmp; .blob; .esm; **.001**; .vtf; .dazip; .fpk; .mlx; .kf; .iwd; .vpk; .tor; .psk; .rim; .w3x; .fsh; .ntl; .arch00; .lvl; .snx; .cfr; .ff; .vpp_pc; .lrf; .m2; .mcmeta; .vfs0; .mpqge; .kdb; .db0; .DayZProfile; .rofl; .hkx; .bar; .upk; .das; .iwi; .litemod; .asset; .forge; .ltx; .bsa; .apk; .re4; .sav; .lbf; .slm; .bik; .epk; .rgss3a; .pak; .big; .unity3d; .wotreplay; .xxx; .desc; .py; .m3u; .flv; **.js**; .css; .rb; .png; **.jpeg; .txt**; .p7c; .p7b; .p12; .pfx; .pem; .crt; .cer; .der; .x3f; .srw; .pef; .ptx; .r3d; .rw2; .rwl; **.raw**; .raf; .orf; .nrw; .mrwref; .mef; .erf; .kdc; .dcr; .cr2; .crw; .bay; .sr2; .srf; .arw; .3fr; .dng; **.jpeg**; **.jpg**; .cdr; .indd; .ai; .eps; **.pdf**; .pdd; .psd; .dbfv; .mdf; .wb2; .rtf; .wpd; .dxg; .xf; .dwg; .pst; **.accdb**; **.mdb**; **.pptm; .pptx; .ppt; .xlk; .xlsb; .xlsm; .xlsx; .xls; .wps; .docm; .docx; .doc; .odb; .odc; .odm; .odp; .ods; .odt

Ein neuer Erpresser: „Ransomware Petya“

Wird diese Datei geöffnet, also ausgeführt, stürzt der PC mit einem Bluescreen ab und startet neu. Doch zuvor hat der Schädling noch den Bootsektor der Festplatte (MBR, Master Boot Record) manipuliert. Der Master Boot Record ist der Bereich eines Datenträgers, der unter anderem den Boot-Loader und wesentliche andere Informationen enthält, dazu zählen:

Partitionstabelle
Größenangaben der Festplatte
Programmcode
Hilfsprogramme

Ransomware: Petya-Schlüssel veröffentlicht

Für Nutzer, deren Daten von Petya, Mischa oder Goldeneye verschlüsselt wurden, gibt es Hoffnung.

Der Entwickler Janus veröffentlicht den Schlüssel für neuere Petya-Versionen.

Am Wochenende hat Janus, der Entwickler der Ransomware Petya, seinen privaten Schlüssel für die Verschlüsselungssoftware veröffentlicht. **Seine ursprüngliche Malware wurde von Hackern gestohlen und modifiziert.** Janus hat daraufhin das Petya-Projekt geschlossen und will nun betroffenen Nutzern helfen

Wanna Cry (Ich könnte heulen)

Eine weltweite Welle von Cyber-Attacken hat am 12. Mai zehntausende Computer von Unternehmen, Behörden und Verbrauchern getroffen.

Ungeachtet der Warnungen sind einige Opfer der weltweiten Cyberattacke offenbar auf die Lösegeld-forderungen der Angreifer eingegangen. Der Anti-Virenprogramm-Hersteller Symantec sprach von 81 Transak-tionen im Umfang von 28.600 Dollar bis Samstag Mittag.

Die erpresserische Schadsoftware mit dem Namen "WannaCry" hatte sich über das Wochenende auf mehr als 200.000 Ziele in über 150 Ländern verbreitet. Experten und Behörden gehen davon aus, dass die Zahl der infizierten Computer steigt, wenn am Montag zahlreiche Rechner erstmals nach dem Wochenende wieder hochgefahren werden.

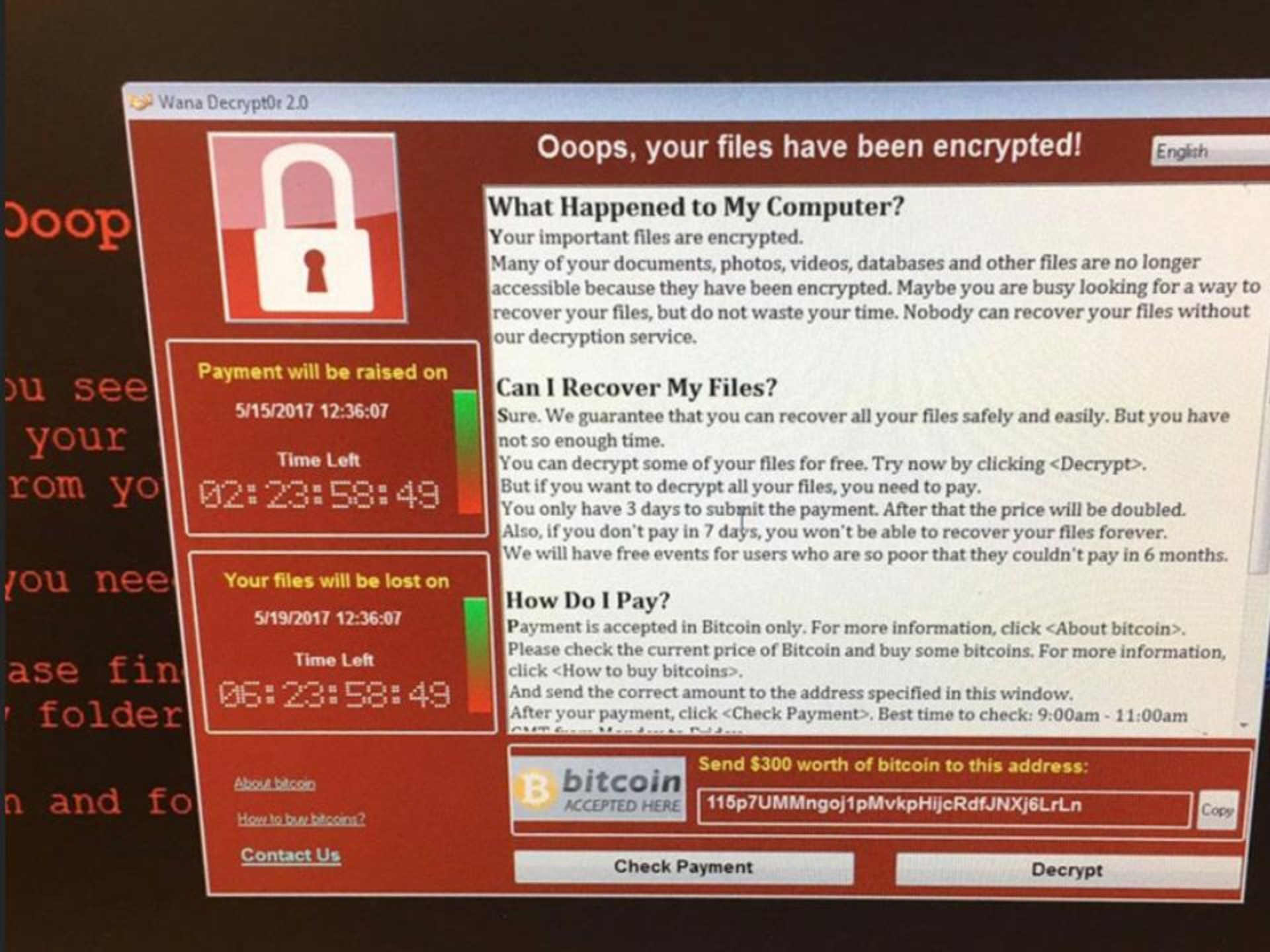
Cyberangriff trifft Computer der Deutschen Bahn

(13. Mai 2017, 4:53 Uhr Aktualisiert am 13. Mai 2017, 6:25 Uhr)

Auch die DB war an diesem Tag Ziel eines Trojaner-Hacks geworden. Der Ransomware-Angriff hat in fast 100 Ländern stattgefunden. In Deutschland ist die Bahn betroffen. Es gebe Systemausfälle, teilte das Unternehmen mit.

Die weltweite Cyberattacke hat auch die Deutsche Bahn getroffen. Wie die Bahn auf ihrer Website bekannt gab, gebe es wegen "eines Trojanerangriffs im Bereich der DB Netz AG" Systemausfälle in verschiedenen Bereichen. Die Cyber-Attacke hat aber auch die Technik der Deutschen Bahn zur Videoüberwachung angegriffen. Die Bahn stellt diese Technik für die Bundespolizei bereit. Für die Bundesregierung und andere Bundesbehörden sei dies zum gegenwärtigen Zeitpunkt auszuschließen.

Und warum nur die DB? **Weil sie immer noch mit XP arbeitet**.


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 12:36:07
Time Left
02:23:58:49
Your files will be lost on
5/19/2017 12:36:07
Time Left
06:23:58:49
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt

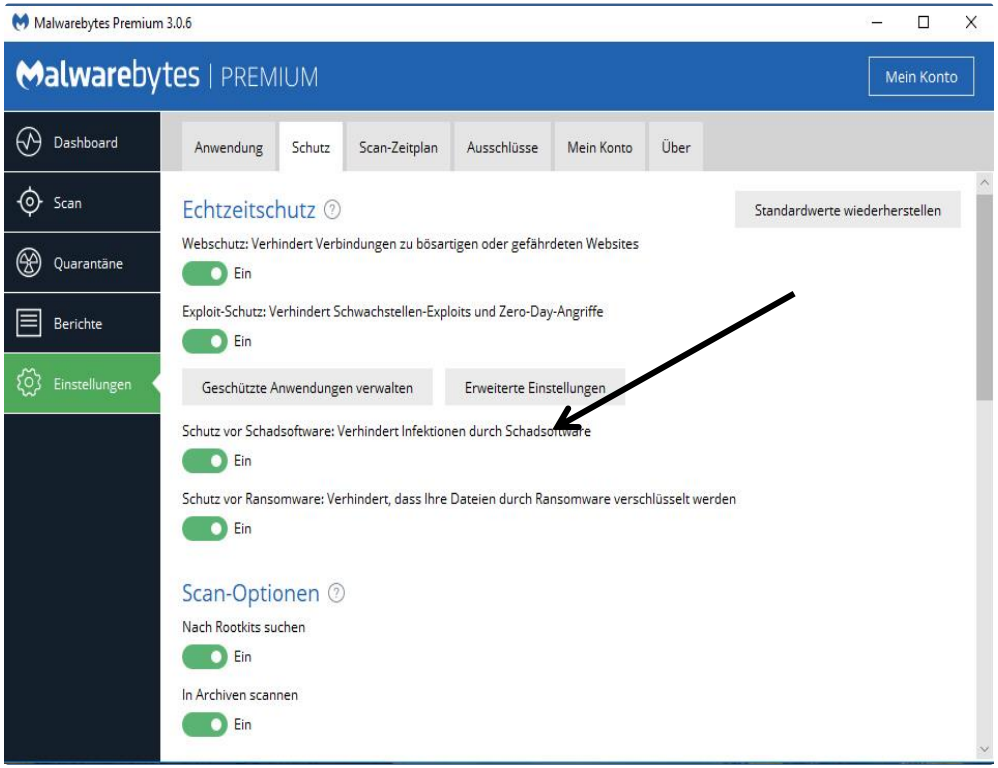
Australien: WannaCry stellt 8.000 falsche Strafzettel aus

Verkehrssünder und Raser in der australischen Stadt Victoria können vorerst aufatmen. Die Polizei erklärte in dieser Woche bei einer Pressekonferenz, dass rund 8.000 Strafzettel eventuell für ungültig erklärt werden. Der Grund: 280 Blitzer-Kameras in der Stadt und im Umland waren mit der Erpresser-Software WannaCry infiziert. Die Kameras haben aber keinen eigenen Internet-Zugang.

Ursache:

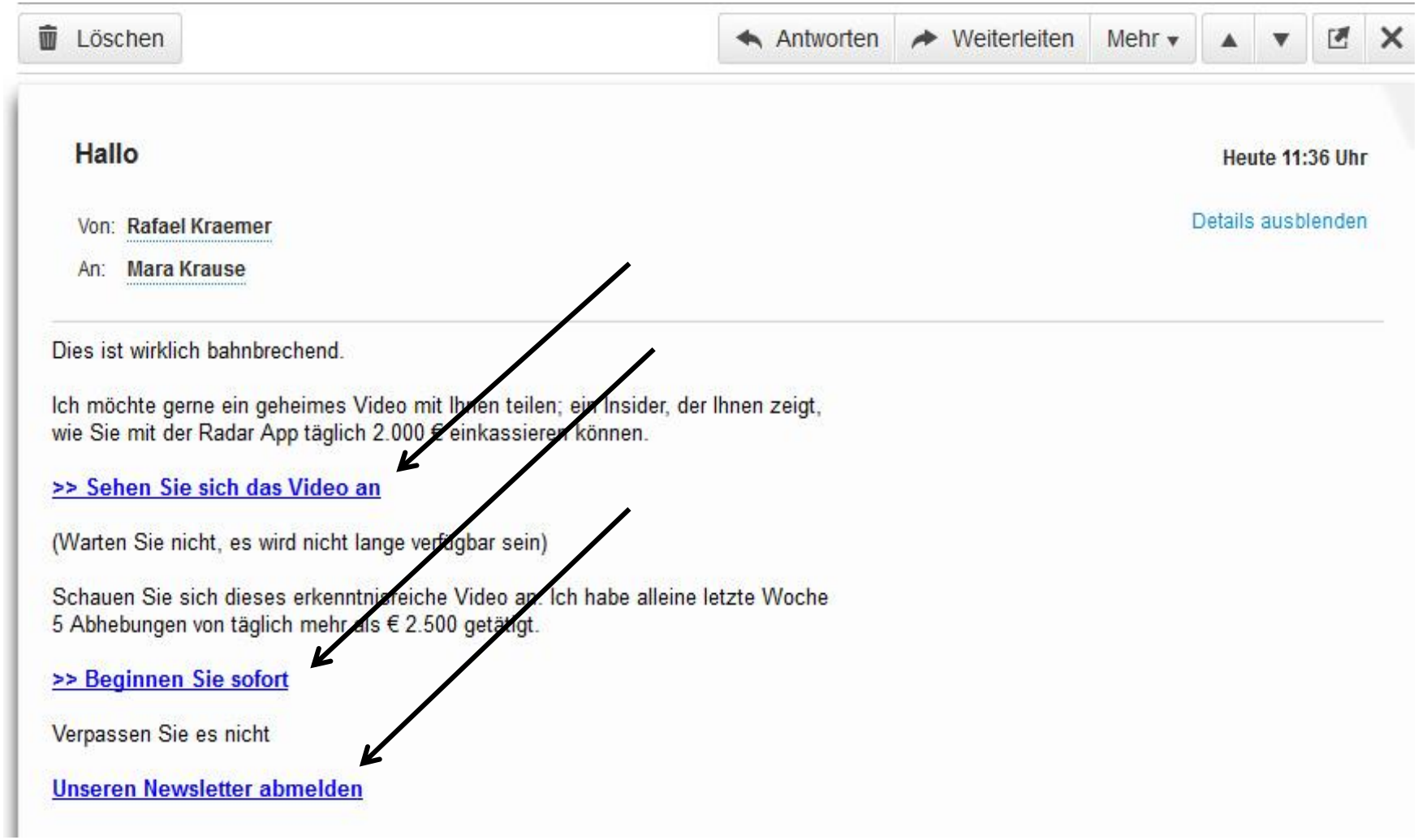
Bei Wartungsarbeiten am 6. Juni 2017 soll die Malware versehentlich per USB-Stick auf die Geräte aufgespielt worden sein.

Hilfe mit Malwarebytes Anti-Ransomware



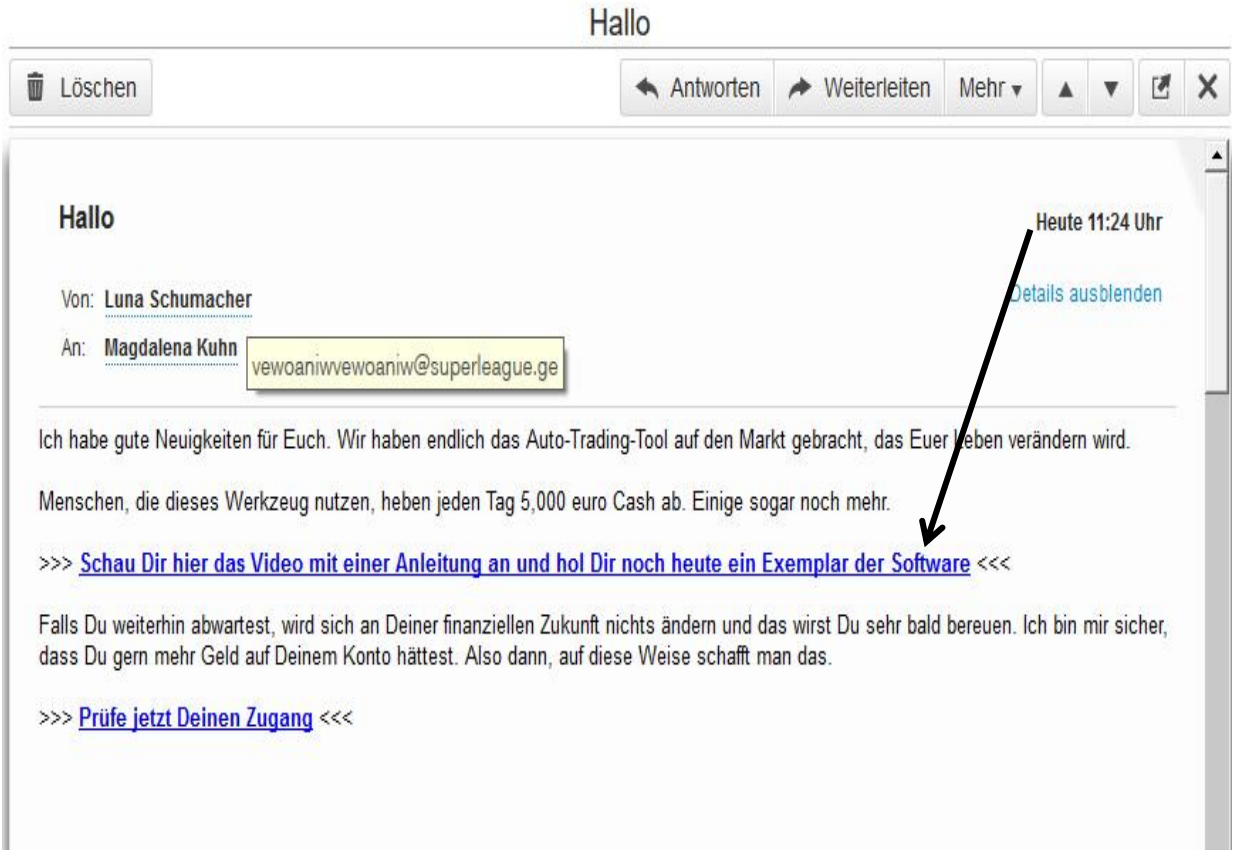
- Um zu untersuchen, ob das Schutzprogramm hält, was es verspricht, hat PC-Welt ein Testsystem bewusst mit Locky infiziert. Tatsächlich konnte Anti-Ransomware den Trojaner stoppen – allerdings erst, nachdem er bereits 20 Dateien verschlüsselt hatte. Angesichts des Umstands, dass die aktuelle Beta 5 des Tools veröffentlicht wurde, **bevor** die erste Locky-Variante in den Umlauf kam, ist das jedoch eine beachtliche Leistung.

Geld verdienen ohne Mühe ????



Hier können Sie sich sogar 3-fach mit einem Virus „infizieren“ (man achte auf die Links)… **und was interessiert mich die eMail von Rafael Kraemer an Mara Krause**

Neueste „Videowerbung“



Täglich bis zu 4 „Benachrichtigungen“
…
…und alle wollen nur das Eine…
…Ihr Geld!

…Hol Dir noch heute ein Exemplar der Software …..

besser lade Dir die MalWare herunter

„**Drohbrief**“ eines dümmlichen Schreiberlings, der sich so gar nicht mit der Textverarbeitung **WORD** auskennt, da er jede Zeile mit **ENTER** schließt. Im Übrigen „strotz“ diese „**Mahnung**“ vor Rechtschreib- und Grammatikfehlern

[redacted]¶

Von:·Beaufuagter·RechtsanwaltAmazon·AG·[inkasso@ebay.de]¶
Gesendet:·Freitag,·10.·Februar·2017·11:02¶
[redacted]·Ihre·Rechnung·zur·Bestellung·Nr.·364075360¶
Anlagen:·10.02.2017·Klaus_peter·[redacted].zip¶

Sehr·geehrte/r·Klaus'·peter·[redacted]

zu·unserem·Bedauern·haben·wir·festgestellt,·dass·die·Aufforderung·Nummer·364075360· bisher·erfolglos¶
blieb.·.letzt·bieten·wir·Ihnen·hiermit·letztmalig·die·Chance.·den·ausstehenden· Betrag·unseren·Mandanten¶
Amazon·AG·zu·begleichen.¶

Aufgrund·des·andauernden·Zahlungsverzug· sind·Sie·gezwungen·zusätzlich,·die·durch·unsere·Beauftragung¶
entstandene·Gebähren·von82.72·Euro·zu·tragen.·Bei·Rückfragen·oder·Anregungen·erwarten·wir·eine¶
Kontaktaufnahme· innerhalb·von·48·Stunden.·Um·zusätzliche·Mahnkosten· auszuschließen.·bitten·wir·Sie¶
den·fiilligen·Betrag·auf·unser·Bankkonto·zu·überweisen.·Berücksichtigt·wurden·alle·Buchungen·bis·zum¶
08.02.20·r·7.¶

Verbindliche·Personalien:¶

Klaus'·peter·[redacted]¶
[redacted]¶
[redacted]¶

AdWare

"Adware" ist **keine** Viren-Software. Sie wird zu Werbezwecken eingesetzt. Meist gelangt Adware über heruntergeladene Programme auf Ihren Rechner. Wenn Sie beispielsweise ein Programm installieren und bei der Installation **alle** Komponenten zulassen, kann auch Adware mitinstalliert werden.

Häufig verändert die Adware Ihre Suchmaschine im Browser (z.B. durch weitere Toolbars etc.) oder fügt Desktop-Symbole zu diversen Internetseiten hinzu. Ihr PC wird also regelrecht zugemüllt. Adware ist **meist eher lästig als ernsthaft schädlich**, verlangsamt aber auch Ihre Rechnergeschwindigkeit. Adware kann aber ebenso in Form von Viren oder anderer Schadsoftware auftreten.

Besonders bei kostenlosen Programmen sollten Sie aufmerksam sein, da sich diese vereinzelt durch Adware refinanzieren. Achten Sie daher bei der Installation unbedingt darauf, dass **keine zusätzlichen Komponenten** installiert werden.

AdwCleaner von Malwarebytes entfernt risikolos diesen „Werbe-Müll“

0900 Rufnummern mit Topvergütung

0900-9: Die Dialer-Nummer

Bei Sonderrufnummern sollte man aufmerksam sein und sich vor einem Anruf über die anfallenden Kosten informieren. Die 0900 etwa steht für Mehrwertdienste, deren Leistungen über das Telefonat abgerechnet werden

Wenn Transparenz bei der Installation und Kostenhöhe gegeben ist, können Dialer dem Nutzer eine komfortable Art der Bezahlung bieten. Allerdings fehlte es in der Vergangenheit oft genau an dieser notwendigen Transparenz. Daher wurden Dialer als eine der größten - und teuersten - Plagen im Internet bekannt, indem sie sich teilweise unbemerkt vom Benutzer installierten und anschließend mittels teurer **0190-** oder eben **0900-9**-Nummern ins Internet einwählten. Dabei konnten Gebühren bis zu **900,-€/min** entstehen.

Missbräuchliche Anrufe mit Auslands-rufnummern

In den letzten Monaten haben Verbraucher im Display ihres Telefons **Auslandsrufnummern** oder Rufnummern für **Globale mobile Satellitensysteme** vorgefunden. Derzeit treten diese Rufnummern insbesondere im Zusammenhang mit sog. **Ping-Anrufen** in Erscheinung. Damit soll ein kostenpflichtiger Rückruf provoziert werden. Ein Rückruf dieser Nummern ist aber oft mit sehr hohen Kosten verbunden, teilweise in Höhe von mehreren Euro pro Minute. Für die Vorwahl **003750 (Weissrussland)** (03750 Zwickau) wurde bereits ein Verbot der Rechnungslegung und Inkassierung durch die BNA verfügt. Neu ist die Vorwahl 008515 (Hongkong – 90 €/min). Ähnlichkeit besteht mit der Vorwahl für Passau (08515). Deshalb: **Neugier unterdrücken, der Anrufer wird wieder anrufen, wenn er etwas will**.

SPAMS

Mittels **gefälschter** Absenderadressen wird nicht erlaubte Werbung versandt

Spammer wollen normalerweise unerkannt bleiben, um so den inzwischen horrenden Geldstrafen zu entgehen, die ihnen in den USA und auch in Deutschland drohen. Daher versenden Sie diesen **Mail-Müll** meist mit falschen Absender-adressen. **Phisher**, die arglose Nutzer auf gefälschte Internet-Seiten locken wollen, um ihnen Passwörter, PINs und TANs abzuluchsen, senden **grundsätzlich** unter falscher Flagge – schließlich müssen ihre Nachrichten ja wie die von einer Bank wirken, damit der Trick funktioniert.

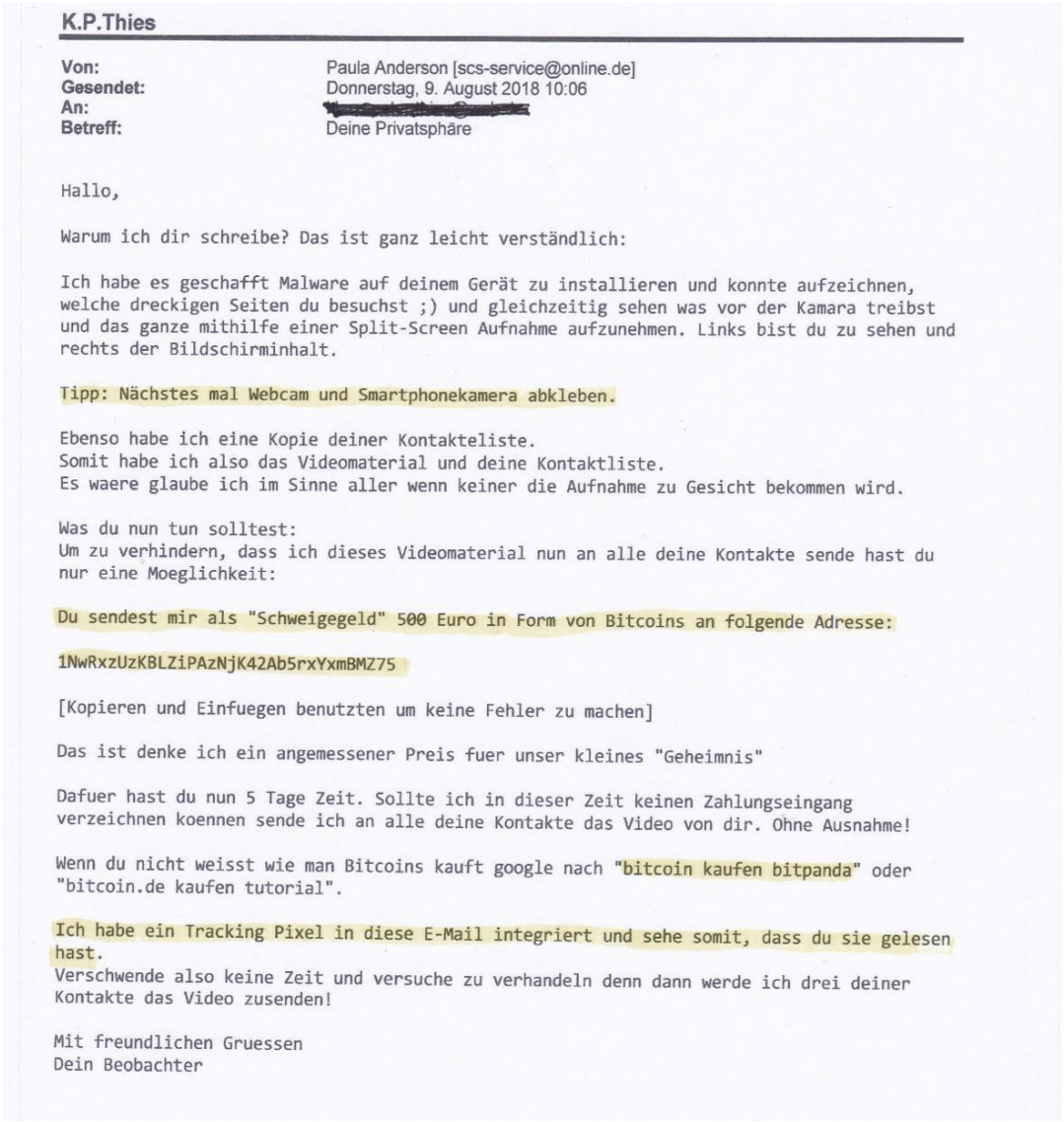
Windows kann heimlich Mikrofone belauschen

Microsoft bietet seit Windows 7 einen Audiorecorder in seinem Betriebssystem an, der Sprache und Geräusche per Mikro aufzeichnet. Die praktische Funktion lässt sich aber auch von Hackern missbrauchen. Eine simple Befehlseingabe startet **soundrecorder.exe** unbemerkt im Hintergrund und belauscht den Nutzer. Über den Autostart könnte die Aufnahme sogar direkt nach dem Einschalten beginnen. Unter Windows 10 greift dieser Tricks ins Leere, da Microsoft dort die entsprechende Exe-Datei nicht mehr mitliefert.

Erkennbar ist das Aufzeichnen des Audiorecorders nur durch ein Mikrofon-Symbol in der Taskleiste. Wird der Infobereich jedoch nur minimiert dargestellt, kann das Icon auch fehlen.

Sie werden über die in Ihrem PC eingebaute WebCam „beobachtet“

In letzter Zeit werden Erpresser-Emails versandt , nach denen Sie im Internet „dreckige Seiten“ besucht hätten und dabei über Ihre eingebaute WebCam aufgenommen worden seien. Ihre Reaktion: Anzeige wegen Erpressung bei der Polizei – und wenn sie der Meinung sind, dass das möglich sein könnte, zu Ihrer eigenen Sicherung:*Webcam abkleben*



K.P.Thies

Von: Paula Anderson [scs-service@online.de]
Gesendet: Donnerstag, 9. August 2018 10:06
An: [redacted]
Betreff: Deine Privatsphäre

Hallo,

Warum ich dir schreibe? Das ist ganz leicht verständlich:

Ich habe es geschafft Malware auf deinem Gerät zu installieren und konnte aufzeichnen, welche dreckigen Seiten du besuchst ;) und gleichzeitig sehen was vor der Kamara treibst und das ganze mithilfe einer Split-Screen Aufnahme aufzunehmen. Links bist du zu sehen und rechts der Bildschirminhalt.

Tipp: Nächstes mal Webcam und Smartphonekamera abkleben.

Ebenso habe ich eine Kopie deiner Kontakteliste.
Somit habe ich also das Videomaterial und deine Kontaktliste.
Es waere glaube ich im Sinne aller wenn keiner die Aufnahme zu Gesicht bekommen wird.

Was du nun tun solltest:
Um zu verhindern, dass ich dieses Videomaterial nun an alle deine Kontakte sende hast du nur eine Moeglichkeit:

Du sendest mir als "Schweigegeld" 500 Euro in Form von Bitcoins an folgende Adresse:

1NwRxzUzKBLZiPAzNjK42Ab5rxYxmBMZ75

[Kopieren und Einfuegen benutzten um keine Fehler zu machen]

Das ist denke ich ein angemessener Preis fuer unser kleines "Geheimnis"

Dafuer hast du nun 5 Tage Zeit. Sollte ich in dieser Zeit keinen Zahlungseingang verzeichnen koennen sende ich an alle deine Kontakte das Video von dir. Ohne Ausnahme!

Wenn du nicht weisst wie man Bitcoins kauft google nach "bitcoin kaufen bitpanda" oder "bitcoin.de kaufen tutorial".

Ich habe ein Tracking Pixel in diese E-Mail integriert und sehe somit, dass du sie gelesen hast.
Verschwende also keine Zeit und versuche zu verhandeln denn dann werde ich drei deiner Kontakte das Video zusenden!

Mit freundlichen Gruessen
Dein Beobachter

Das war noch ein „höflicher“ Erpresserversuch. Auch der nachfolgende muss zur Anzeige gebracht werden

K.P.Thies

Von: Franzi [laura.stier@online.de]
Gesendet: Donnerstag, 11. Oktober 2018 21:22
An:
Betreff:

Hallo du Sau,

SAGMAL findest du es eigentlich gut, dass du deiner besseren Hälfte fremdgehst!?
Als ich es rausgefunden habe wollte ich es ihr sofort verraten. Ich bin kurz davor es zu tun aber habe eine bessere Lösung.
Ich denke ich habe aber einen guten Kompromiss für uns beide gefunden. Ich gebe dir nun diese eine Chance, wenn du das verhindern willst.
Du brauchst auch garnicht versuchen rauszufinden wer ich bin, die E-Mail Adresse ist fake.

Sende mir 0.10 Bitcoins an diese Adresse:
1CLWEMQw7aER8v6EQ6ss78QPXNStrQfCan

Das ist ein fairer Preis und keiner erfährt dann etwas davon.

Du hast nun 96 Stunden Zeit mir die Bitcoins zuzusenden!

Wenn du nicht weisst wie man Bitcoins kauft google nach "bitcoins kaufen tutorial" oder "bitcoins kaufen bitpanda".

„Geld eintreiben“ und Virus lancieren

In beiliegender Mahnung (auf Rechtschreibfehler achten) werden Sie unter Drohungen zur Zahlung einer angeblich offenen Rechnung aufgefordert.

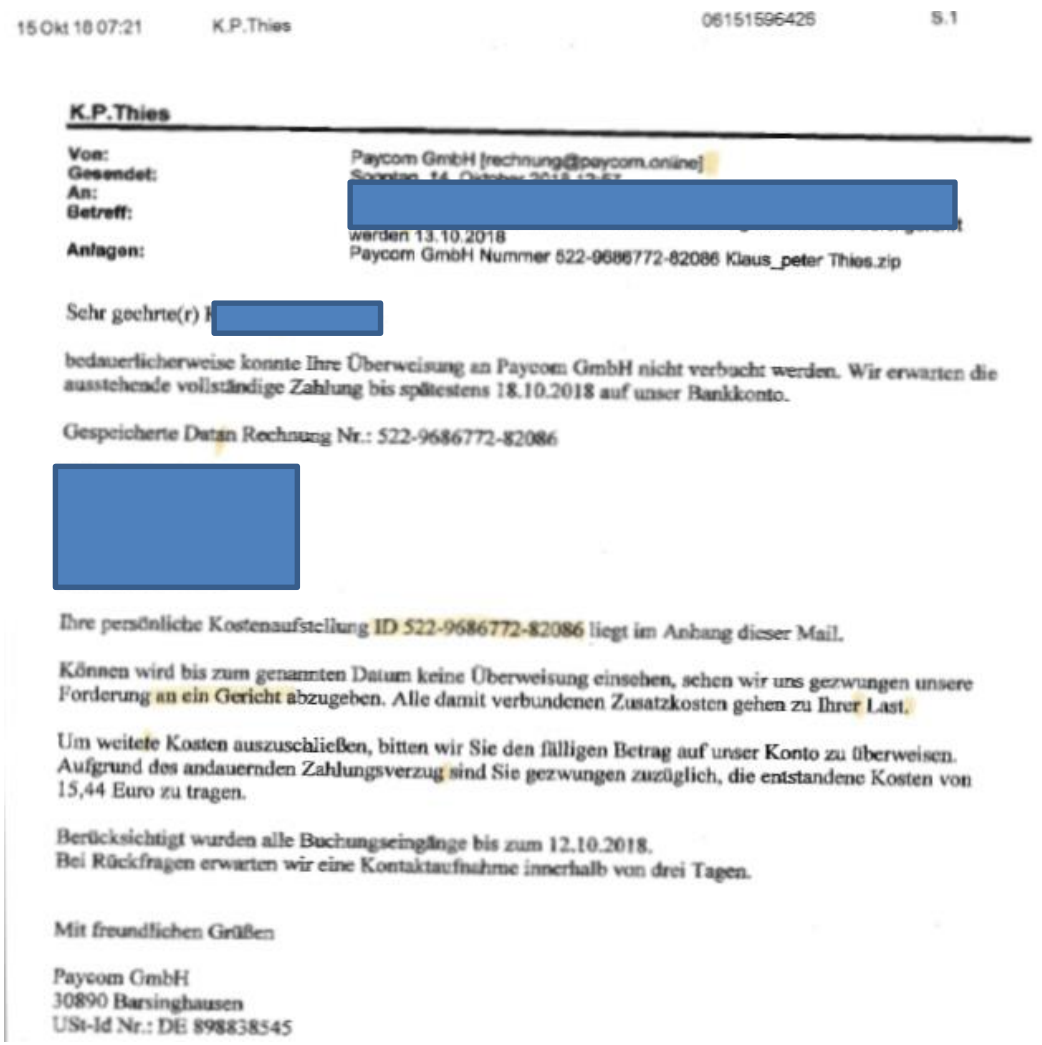
Doch wenn Sie den Anhang zur Einsicht öffnen, fangen Sie sich folgende Viren ein:

Win32:Trojan-gen

Trojan.Nymalm.226

GenericRXGM-TLIDGE710AA9011

Bscope.Troja.Downloader



15 Okt 18 07:21 K.P.Thies 06151596426 S.1

K.P.Thies

Von: Paycom GmbH [rechnung@paycom.online]
Gesendet:
An: [redacted]
Betreff: werden 13.10.2018
Anlagen: Paycom GmbH Nummer 522-9686772-82086 Klaus_peter Thies.zip

Sehr geehrte(r) [redacted]

bedauerlicherweise konnte Ihre Überweisung an Paycom GmbH nicht verbucht werden. Wir erwarten die ausstehende vollständige Zahlung bis spätestens 18.10.2018 auf unser Bankkonto.

Gespeicherte Daten Rechnung Nr.: 522-9686772-82086

[redacted]

Ihre persönliche Kostenaufstellung ID 522-9686772-82086 liegt im Anhang dieser Mail.

Können wird bis zum genannten Datum keine Überweisung einsehen, sehen wir uns gezwungen unsere Forderung an ein Gericht abzugeben. Alle damit verbundenen Zusatzkosten gehen zu Ihrer Last.

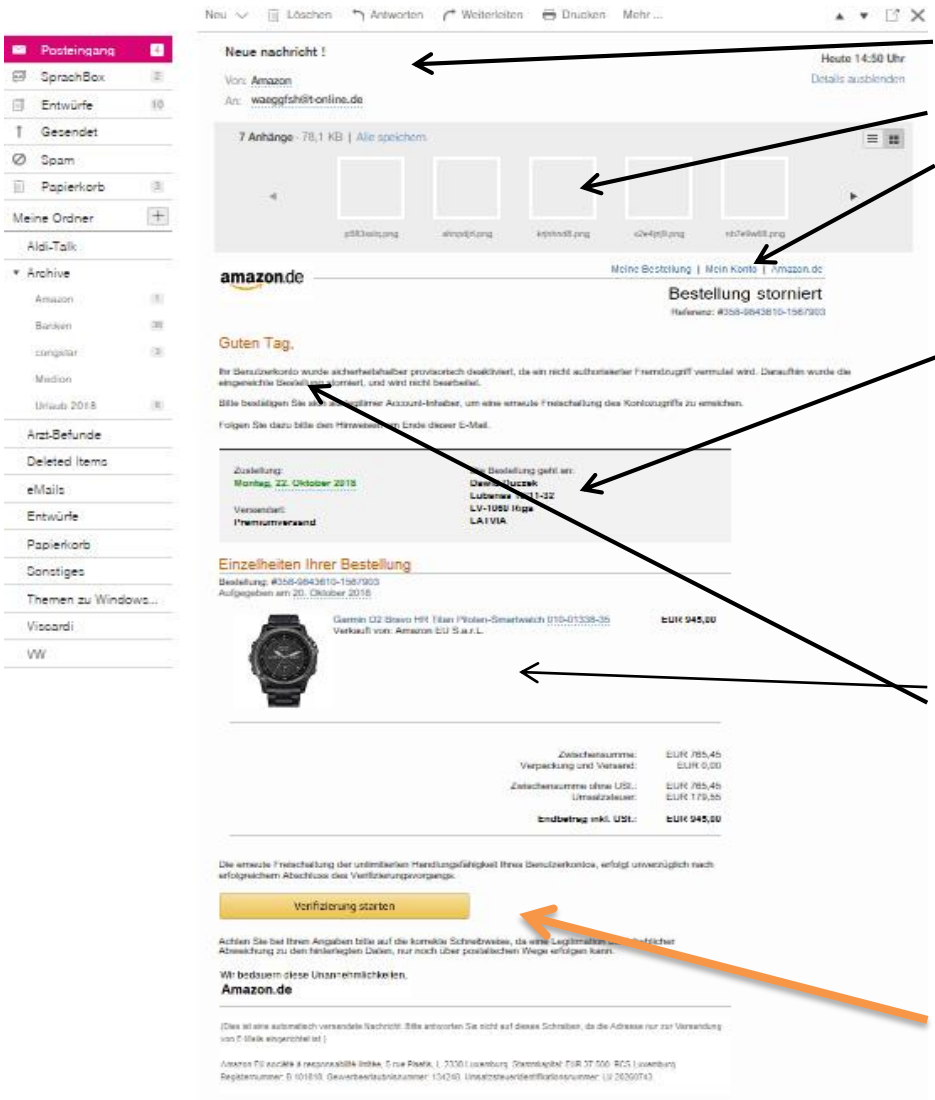
Um weitere Kosten auszuschließen, bitten wir Sie den fälligen Betrag auf unser Konto zu überweisen. Aufgrund des andauernden Zahlungsverzug sind Sie gezwungen zuzüglich, die entstandene Kosten von 15,44 Euro zu tragen.

Berücksichtigt wurden alle Buchungseingänge bis zum 12.10.2018.
Bei Rückfragen erwarten wir eine Kontaktaufnahme innerhalb von drei Tagen.

Mit freundlichen Grüßen

Paycom GmbH
30890 Barsinghausen
USt-Id Nr.: DE 898838545

Falsche Rechnung von „Amazon“



1) Adresse gekidnappt

2) 5+3 Pings **aktiv**

3) Meine Bestellung, mein Konto **inaktiv**

4) Besteller (nicht ich):

Dawid Duczek
Lubanas 10/11-32
LV-1060 Riga
LATVIA (Lettland)

„Ihr Benutzerkonto wurde sicherheitshalber provisorisch deaktiviert, da ein nicht autho-risierter Fremdzugriff vermutet wird. Darauf-hin wurde die eingereichte Bestellung stor-niert, und wird nicht bearbeitet. Bitte bestä-tigen Sie sich als legitimer Account-Inhaber, um eine erneute Freischaltung des Konto-zugriffs zu erreichen.“ **Vorsicht!! Text von „Amazon“ soll Sie in Sicherheit wiegen**

Hier ist die Falle: Niemals Ihre echten Daten eintragen

MELDUNG AN AMAZON

Sie haben eine eigentümliche Rechnung erhalten. Wenn Sie sich nicht im Klaren sind, so leiten Sie diese einfach weiter an Amazon. In wenigen Minuten erhalten Sie u.U. folgende Nachricht:

Guten Tag Herr [redacted],

vielen Dank für das freundliche Telefonat.

Wie besprochen stammt die E-Mail, die Sie erhalten haben, tatsächlich nicht von Amazon.de. Wir sind aber bereits dabei, der Angelegenheit genauer nachzugehen. Wenn möglich schicken Sie uns diese E-Mail als Anhang an: stop-spoofing@amazon.com . So bleiben alle Informationen der Kopfzeile erhalten, mit deren Hilfe wir die Herkunft der E-Mail besser nachverfolgen können. Löschen Sie danach die E-Mail. Wenn Sie die E-Mail nicht als Anhang verschicken können, leiten Sie sie bitte an stop-spoofing@amazon.com weiter. Geben Sie dazu die Information in der Kopfzeile an, wenn dies möglich ist.

Bitte beachten Sie, dass die E-Mail-Adresse stop-spoofing@amazon.com von unserer amerikanischen Website Amazon.com betreut wird und Sie daher eine Empfangsbestätigung auf Englisch erhalten werden. Wenn Sie die Mail weder als Anhang senden noch diese weiterleiten können, kann es sein, dass Ihr E-Mail-Provider das Weiterleiten einer bereits erkannten Phishing-Mail blockiert. In diesem Fall möchten wir Sie bitten, keine Links oder Anhänge zu öffnen und die E-Mail einfach zu löschen.

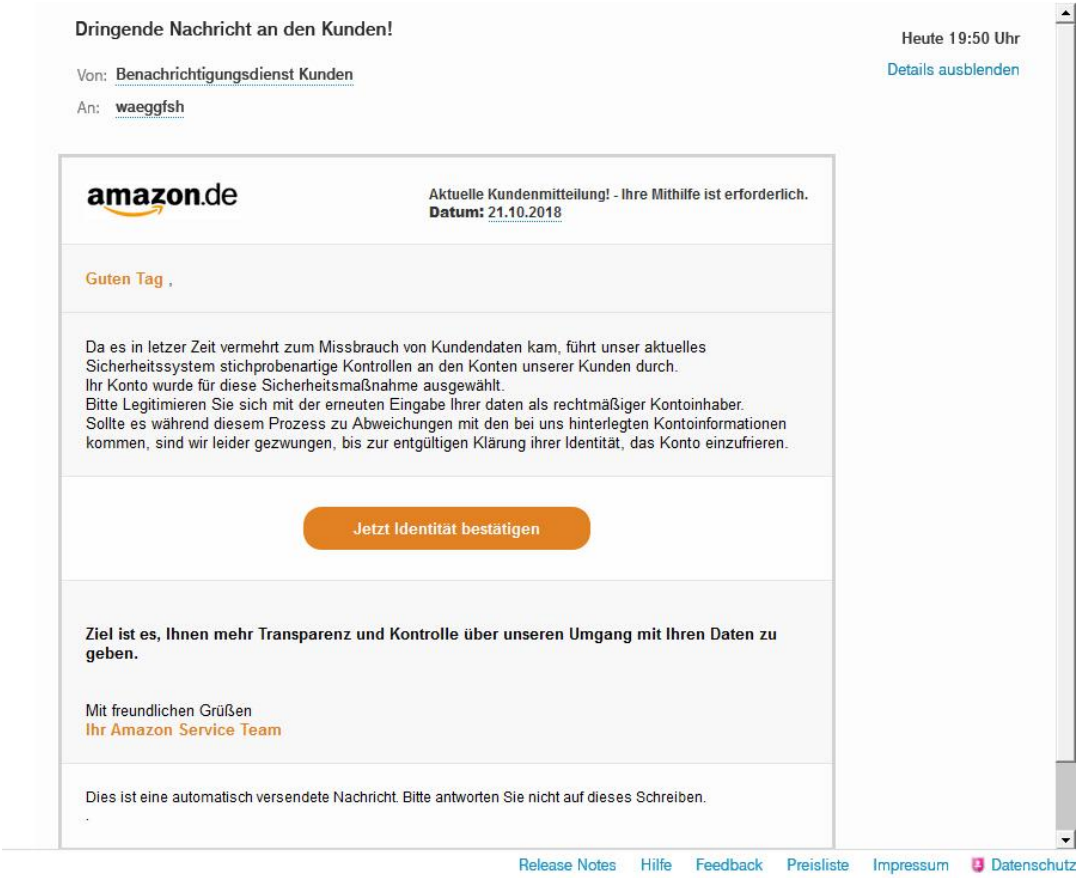
Sie erhalten wichtige Informationen des Kundenservice wie Aktualisierungen der Kontorichtlinien oder Produktrückrufe auch über das Message Center. Sie können das Message Center auch direkt über folgenden Link aufrufen:

https://www.amazon.de/gp/message

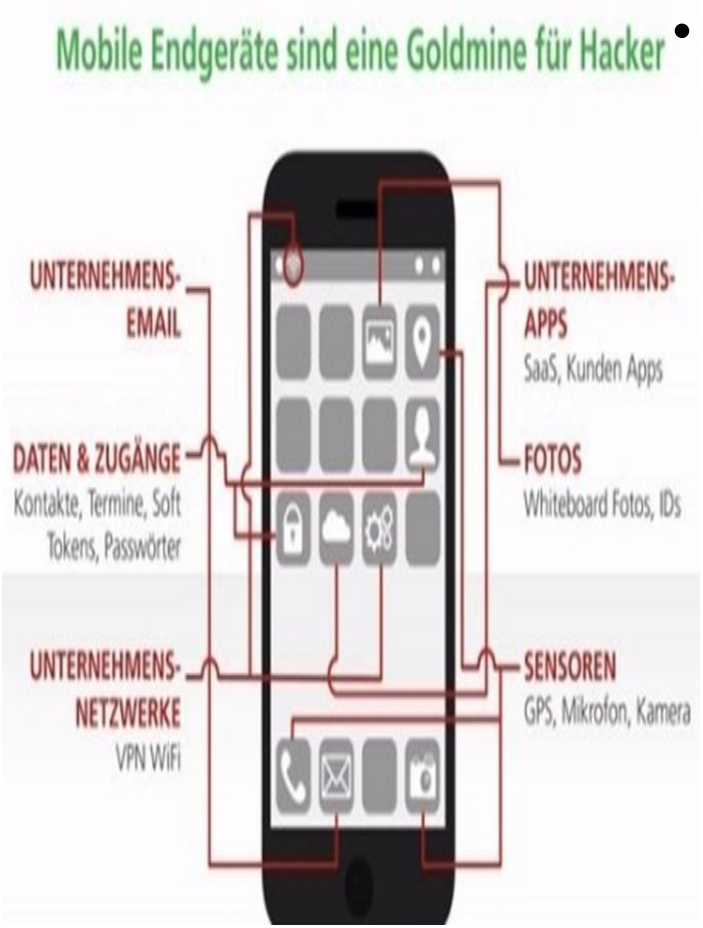
Benachrichtigungsdienst von „Amazon“

Unmittelbar am Folgetag fordert ein „Benachrichtigungsdienst“ dann dazu auf, seine Identität nochmals zu bestätigen. Das kann Zufall sein. Es kann aber auch darauf zielen, dass man bei der vorangegangenen eMail misstrauisch geworden ist und sich mit Amazon wegen einer Überprüfung in Verbindung gesetzt hat.

In diesem Zusammenhang würde die erneute Aufforderung die Identität nochmals zu bestätigen, einen Sinn ergeben. Ansonsten – nicht darauf reagieren, nur löschen und weiterhin **misstrauisch sein**



Und noch eins: Mobile Endgeräte



- Hacker werden immer raffinierter und finden neue Wege, die Unternehmenssicherheit zu umgehen und auf wichtige Daten zuzugreifen. Werden die nächsten großen Datenlecks von mobilen Endgeräten ausgehen? Mobile Geräte bieten viele „attraktive" Angriffspunkte, die einfacher auszunutzen sind als die von PCs. Das liegt schon ihrer Natur: Sie sind immer online und besitzen eine ganze Reihe von Funktionen, die sie zu idealen Überwachungsgeräten machen, einschließlich Mikrofon, hochauflösender Kameras, vorinstalliertem GPS und mehrerer Netzwerktypen wie WLAN, Mobilfunk und Bluetooth.

Neue gefährliche Viren 2018 im Überblick

Im dem Jahr davor waren es vor allem Erpresserviren, vor denen man sich bei PC und Smartphone in Acht nehmen musste. In diesem Jahr drohten nun ganz neue Schädlinge.

Dateilose Viren: Schwer erkennbar

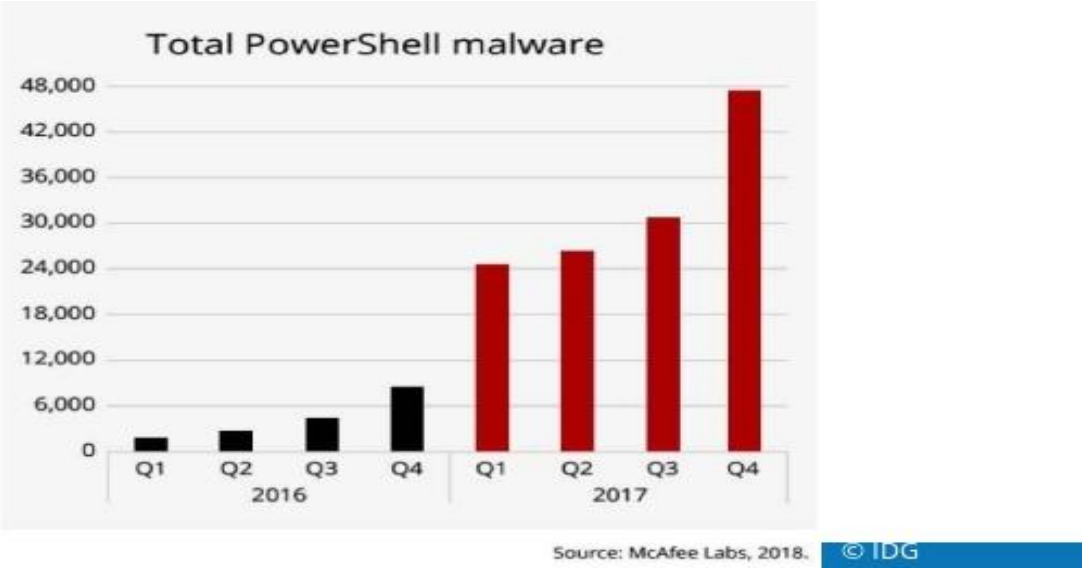
Dateilose Malware sind eine **neue Virenart**, die ohne eine Schadcode-Datei auskommen. Sie bestehen lediglich aus ein paar Zeilen Scriptcode in einer Website oder einer Mail. Diese Art der Malware nutzt auf dem PC des Opfers oft die **Windows Power Shell**, um Befehle in Windows zu starten. Die Power Shell ist ein sehr mächtiges Bordmittel von Windows, das jedoch den meisten Endanwendern unbekannt ist. Dateilose Malware ist für Antivirenprogramme schwer zu erkennen, da die Sicherheitstools darauf spezialisiert sind, **verseuchte Dateien zu analysieren**. Zwar können die meisten Antivirentools auch Scriptcode in Websites erkennen und filtern, doch gelingt das deutlich schwerer.

Ein aktuelles Beispiel für einen dateilosen Schädling waren **Angriffe auf beteiligte Organisationen der Olympischen Spiele in Pyeong-chang**. Unbekannte versandten verseuchte Mails mit wenigen Zeilen Visual Basic Code. Dieser Code aktivierte einige Power-Shell-Befehle und konnte den befallenen PC so komplett unter die eigene Kontrolle bringen.

Der Bitcoin legte dieses Jahr eine beispiellose Rallye hin, zwischenzeitlich lag sein Wert bei 20.000 € und ist jetzt wieder von 1000 auf 7000 € gestiegen.

Alles begann 2008, als ein bis heute unbekannter Verschlüsselungsexperte unter dem Pseudonym Satoshi Nakamoto eine Idee veröffentlichte, wie sich digitales Geld schaffen ließe, das sich nicht kopieren oder fälschen lässt. Kernstück dieser Idee war die Blockchain, eine Art **riesige, verteilte Buchhaltung,** von der es zahllose Kopien gibt und in die **alle** jederzeit hineinsehen können. Wird jede einzelne Überweisung in dieser Datenbank gespeichert, steht immer fest, wem wieviel Geld gehört. **Versuche, die Blockchain zu manipulieren sind zwecklos, da ein Betrüger mehr als die Hälfte der weltweit existierenden Kopien der Blockchain verändern müsste.** Eigentlich ein Ding der Unmöglichkeit. Und obwohl jederzeit Einblick in die Blockchain genommen werden kann, ist Bitcoin völlig anonym. Wem wieviel gehört wird unter einer Bitcoin-Adresse gespeichert, ähnlich einem Schweizer Nummernkonto. Wer Adresse und zugehöriges Passwort kennt, kommt an das Geld.

Krypto-Mining

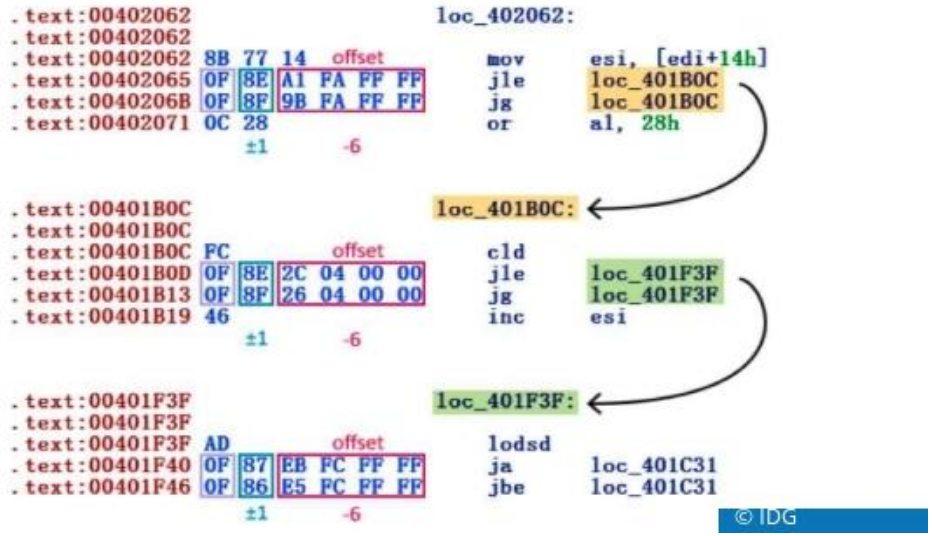


Viele digitalen Währungen lassen sich mit einem PC erzeugen. Man spricht von „Mining“(entliehen aus dem Bergarbeiterbereich). Der schnelle Wertzuwachs bei Bitcoin & Co. hat aber auch sofort Kriminelle auf den Plan gerufen. Angriffe per Viren und Scriptcode mit dem Ziel, Ihren PC zu einer **Mining-Maschine** für eine digitale Währung zu machen, steigen rasant an.

Vorgehensweise für‘s Mining

Kaspersky beschreibt eine Angriffsmethode fürs Mining: Die Opfer werden zum Download von Tools verleitet, die einen versteckten Installer für Mining-Software in sich tragen. Der Installer legt eine legitime Windows-Utility-Software ab, deren Hauptzweck darin besteht, den eigentlichen Miner jetzt von einem entfernten Server herunterzuladen. Nach der Ausführung startet ein legitimer Systemprozess, dessen Code mit schädlichem Code überschrieben wird. Im Ergebnis operiert der Miner anschließend in der Maske eines legitimen Tasks. Damit kann der Nutzer den Schädling **nicht als Mining-**Infektion identifizieren. Bemerkenswert ist außerdem, wie es dieser neue Prozess schafft, nicht gelöscht zu werden. Versucht der Anwender ihn zu stoppen, kommt es zu einem Neustart des Systems. So gelingt es den Cyber-Kriminellen, ihre Verweildauer im System der Opfer zu verlängern und dort lange produktiv zu operieren.

Auch Smartphones sind in Gefahr



Auch Smartphone-Nutzer können Opfer von Krypto-Mining werden. Darauf weisen die Sicherheitsspezialisten von Malwarebytes hin. Die Antivirenexperten von Eset haben den Spionagevirus **Fin Fisher** analysiert. Dieser wehrt sich gegen eine Analyse, indem er nach jedem Befehl drei Sprungmarken einbaut, von denen zwei zu unsinnigem Code führen.

Diebstahl von Cyber-Geld per Trickbetrug

Es musst nicht immer ein Virus sein, um einem Anwender massiven Schaden zuzufügen. Oft genügt schon eine feindliche Website. So lief Anfang 2018 ein Betrug über einen Schadcode ab.

- **Darum geht's:** Ein Münchner hat 53 000 Euro in die digitale Währung Iota investiert und dann das gesamte Geld durch einen Diebstahl verloren. Das berichtete die Münchner Polizei Anfang 2018. Der 44-jährige Münchner kaufte im Zeitraum von Juli bis September 2017 Coins der virtuellen Währung Iota. Diese Coins teilte er im Dezember 2017 auf insgesamt acht elektronische Geldbörsen, sogenannte **Wallets**, auf. Für diese Wallets wollte der 44-Jährige dann Passwörter (sogenannte **Seeds**) generieren. Hierzu suchte er im Internet nach einer Webseite, die er auch fand. Sie erstellte ihm Seeds.
- Was dem Mann nicht klar war: Die Passwörter (Seeds) wurden bei der Generierung zusammen mit den jeweiligen Wallet-Adressen **auf der Website gespeichert**. Mit diesen Daten hatten die Betreiber der Seite dann vollen Zugriff auf die genutzten Wallets und konnten dadurch auch Transaktionen tätigen

Fin Fisher: Spionage-Trojaner

Der Spionage-Trojaner **Fin Fisher** (auch Fin Spy genannt) zählt zu den gefährlichsten Schädlingen überhaupt. Er wird nicht von Cyber-Kriminellen ent-wickelt, sondern von der britisch-deutschen Firma

Fin Fisher GmbH mit Sitz in München.

Fin Fisher wird an Behörden und Unternehmen weltweit ver-kauft und beschert der Firma Fin Fisher einen Millionenumsatz. Entsprechend motiviert ist die Firma, den Trojaner möglichst unentdeckbar für Antiviren-software zu machen. Dem Antivirenspezialisten Eset ist es nun gelungen, zwei Tricks von Fin Fischer zu analysieren, was eine künftige Erkennung erleichtert.

Angriffe über den Router

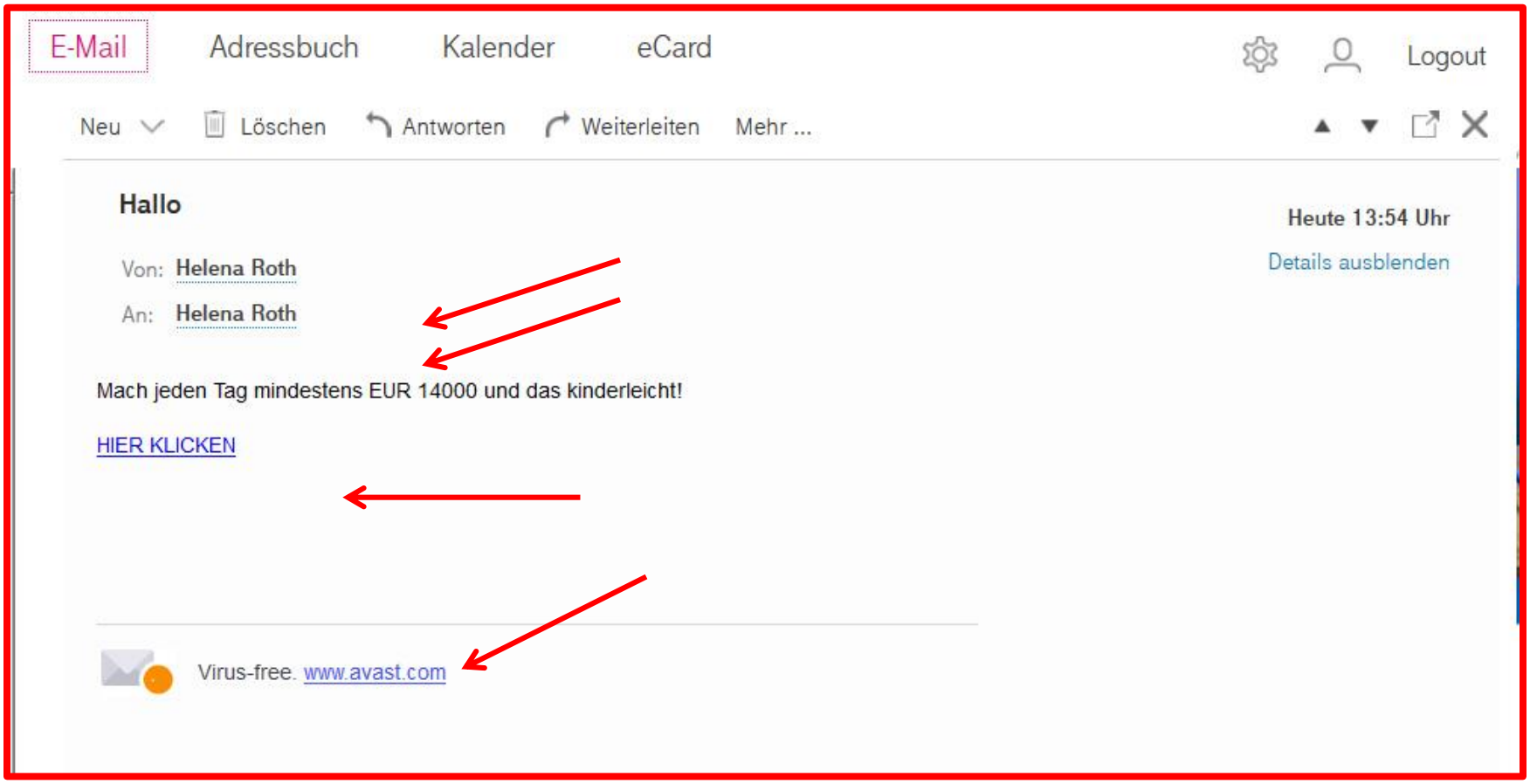
Die Malware **Slingshot** kann von einem Router aus den angeschlossenen PC komplett in Besitz nehmen. Das berichtet der Security-Spezialist Kaspersky. Slingshot soll bereits seit 2012 sein Unwesen treiben, wurde aber erst 2018 entdeckt. Slingshot ist in der Lage, unter Windows im Kernel-Modus zu laufen, und erhält somit vollständige Kontrolle über infizierte Geräte. Laut Kaspersky nutzt der Schädling einige einzigartige Techniken. Erbeutete Daten versendet er zum Beispiel unter Windows in - markierten Datenpaketen versteckt - und kann diese später ohne Spuren wieder aus dem Datenstrom auslesen.

PC-Spionage über die Luft

Forscher der Ben-Gurion-Universität können Daten zwischen zwei PCs alleine durch **Temperaturänderungen** übertragen. Damit lassen sich Systeme ausspionieren, die komplett vom Netz getrennt sind (Bild: **Ben-Gurion-Universität**). Schadcodes können so zwar nicht per Netzwerk auf den PC gelangen um von dort Daten zu stehlen. Dies ist über „ **Air Gap** “ auch nicht nötig: Es gibt außer der Luft keine Verbindung zum System. Tatsächlich lässt sich aber auch der Air Gap für einen ausreichend motivierten Angreifer überwinden. Zumindest funktioniert das Senden von Daten von einem bereits befallenen System nach draußen.

Neuerdings tauchen Totgeglaubte wieder auf

Vorsicht vor eMails mit unbekanntem Absender.



DSGVO: So schützen Sie Ihre Daten vor Betrugs-Mails

Die Schonfrist für die Datenschutz-Grundverordnung endete am 25. Mai. Unternehmen waren deshalb gehalten, ihre Kunden auf diese Änderungen nach DSGVO meist über E-Mail hinzuweisen.

Doch Betrüger missbrauchen das Gesetz, um an vertrauliche Daten von Verbrauchern zu kommen.

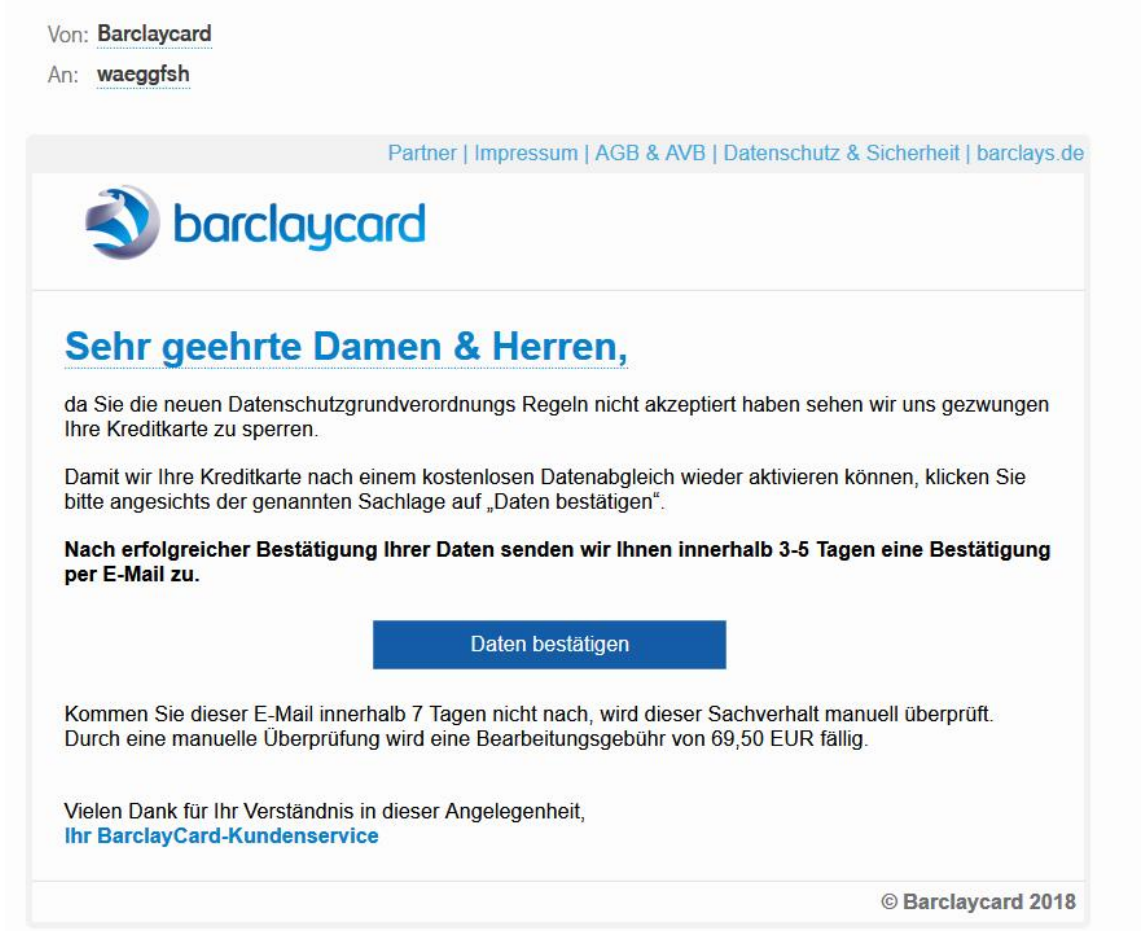
Achten Sie vor allem in den kommenden Wochen auf betrügerische E-Mails. Beispielsweise von angeblichen Banken. Das empfiehlt der Bundesverband deutscher Banken in Berlin.

Betrüger nutzen gefälschte Webseiten

Wer nicht betrogen werden will, braucht gesundes Misstrauen. Grundsätzlich gilt: **Vorsicht ist besser als Nachsicht**. Seien Sie deshalb bei unbekannten Mails skeptisch. Nachrichten, die vertrauliche Daten verlangen, sollten Sie löschen.

S. auch nachfolgende E-Mails.

DSGVO soll für diesen Betrug herhalten



Von: **Barclaycard**

An: **waeggfsh**

Partner | Impressum | AGB & AVB | Datenschutz & Sicherheit | barclays.de

barclaycard

Sehr geehrte Damen & Herren,

da Sie die neuen Datenschutzgrundverordnungs Regeln nicht akzeptiert haben sehen wir uns gezwungen Ihre Kreditkarte zu sperren.

Damit wir Ihre Kreditkarte nach einem kostenlosen Datenabgleich wieder aktivieren können, klicken Sie bitte angesichts der genannten Sachlage auf „Daten bestätigen".

Nach erfolgreicher Bestätigung Ihrer Daten senden wir Ihnen innerhalb 3-5 Tagen eine Bestätigung per E-Mail zu.

Daten bestätigen

Kommen Sie dieser E-Mail innerhalb 7 Tagen nicht nach, wird dieser Sachverhalt manuell überprüft. Durch eine manuelle Überprüfung wird eine Bearbeitungsgebühr von 69,50 EUR fällig.

Vielen Dank für Ihr Verständnis in dieser Angelegenheit,
Ihr BarclayCard-Kundenservice

Eine nicht ganz neue Masche

Ganoven gaukeln hier Probleme mit Kundendaten vor und wollen entsprechende Maßnahmen ergreifen, um die “Sicherheit“ dieser Daten zu aktualisieren.

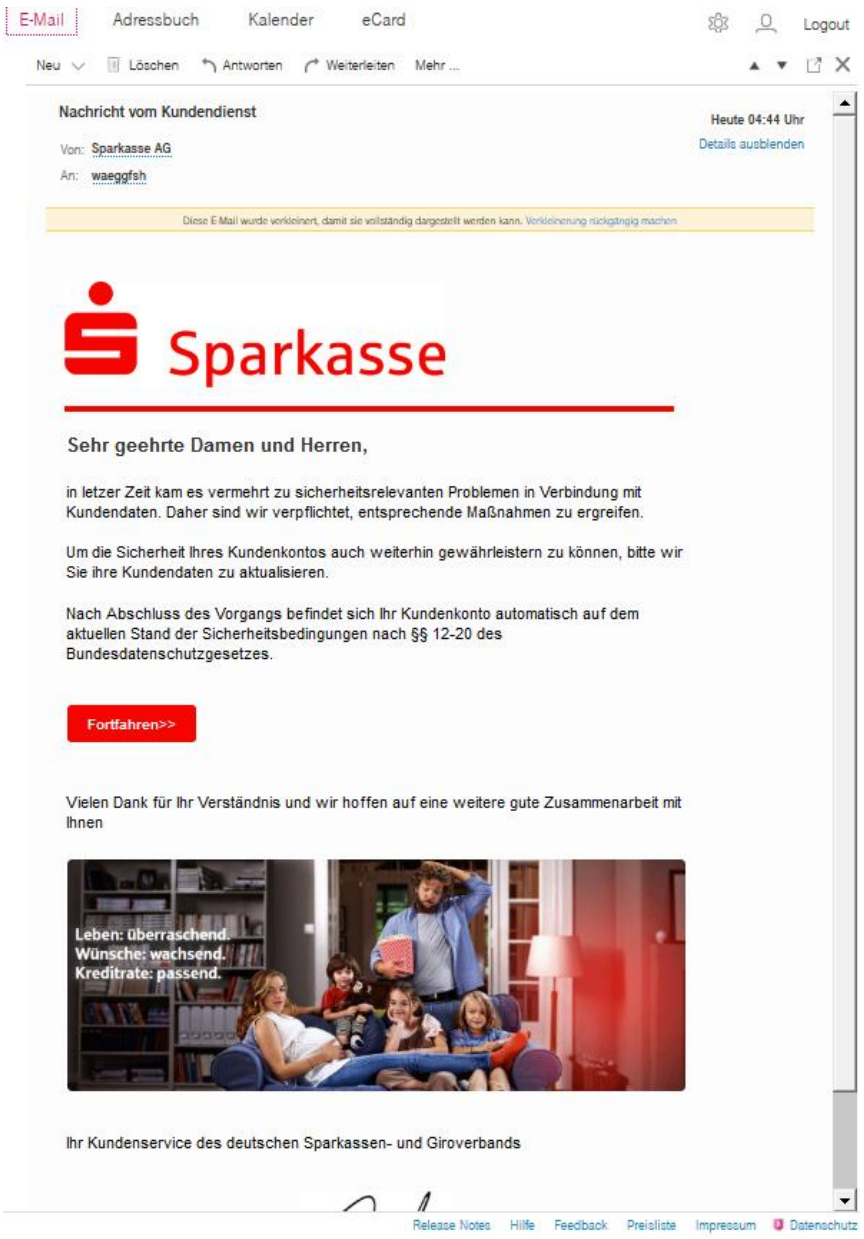
Sie wurden bis jetzt bei derartigen dubiosen Vorgängen vorsichtig, sobald Sie aufgefordert wurden einen Anhang zu öffnen.

Dieser war an einer **BLAUEN** Schrift erkennbar. Nunmehr fordert man Sie auf (in **roter** Schrift) FORTZUFAHREN.

Das Impressum am unteren rechten Bildrand öffnet nur eine leere Seite.

Dies sind alles eindeutige Hinweise, dass hier Unheil droht, wenn Sie unbedarft weitermachen. Also nur **LÖSCHEN**

Professionell gemacht, aber trotzdem „SHEETWARE“



Sparkassen

Sparkasse

Sehr geehrte Damen und Herren,

in letzter Zeit kam es vermehrt zu sicherheitsrelevanten Problemen in Verbindung mit Kundendaten. Daher sind wir verpflichtet, entsprechende Maßnahmen zu ergreifen.

Nach Abschluss des Vorgangs befindet sich Ihr Kundenkonto automatisch auf dem aktuellen Stand der **Sicherheitsbedingungen** nach *§§ 12-20* des **Bundesdatenschutzgesetzes**.

Fortfahren >>

Vielen Dank für Ihr Verständnis und wir hoffen auf eine weitere gute Zusammenarbeit mit Ihnen.

Ihr Kundenservice des **deutschen Sparkassen- und Giroverbands**

[redacted]

Auch Kunden der Sparkassen erhalten Wichtige Benachrichtigungen. In der Phishing-Nachricht **fehlt eine persönliche Anrede**. Und das geht gar nicht.

Kunden sollen laut der Mail ihre Daten aufgrund "sicherheitsrelevanter Probleme“ in Verbindung mit Kundendaten" aktualisieren. Löschen Sie die Nachricht.

Einstellungen

Routersicherheit: Passwörter und Firmware

Alle Einstellungen am Router werden über eine Weboberfläche vorgenommen. Die Adresse, die Sie dafür in den Browser eingeben müssen, stehen samt Standard-Benutzernamen und Standard-Passwort meist auf der Rückseite des Routers. Genau diese Standard-Log-in-Daten sollten Sie ändern.

Routersicherheit: So sichern Sie das WLAN

Doch nicht nur das Passwort, sondern auch die Art, mit der die übertragenen Informationen verschlüsselt werden, ist wichtig. So sollten Sie die Verschlüsselungsmethode auf WPA2 PSK setzen, die momentan die höchste Sicherheit biet

Routersicherheit: Fernzugriff, Gastnetzwerk, Zeitschaltung

Einige Router wie die Fritzbox unterstützen den Fernzugriff auf ihre Weboberfläche. Dies eröffnet die Möglichkeit, von unterwegs auf angeschlossene USB-Sticks oder die Anruferliste zuzugreifen. Wer diese Funktion nicht benötigt, sollte sie sicherheitshalber **abschalten**

WLAN-Router vor Angriffen schützen

Onlinefestplatte, Drucker und Webkameras – immer mehr Geräte sind in das Heimnetzwerk eingebunden. Die Vielzahl vernetzter Komponenten erhöht allerdings das Sicherheitsrisiko und vergrößert die Angriffsfläche für Hacker. Denn einen Virenschutz bieten sie im Gegensatz zu einem PC nicht.

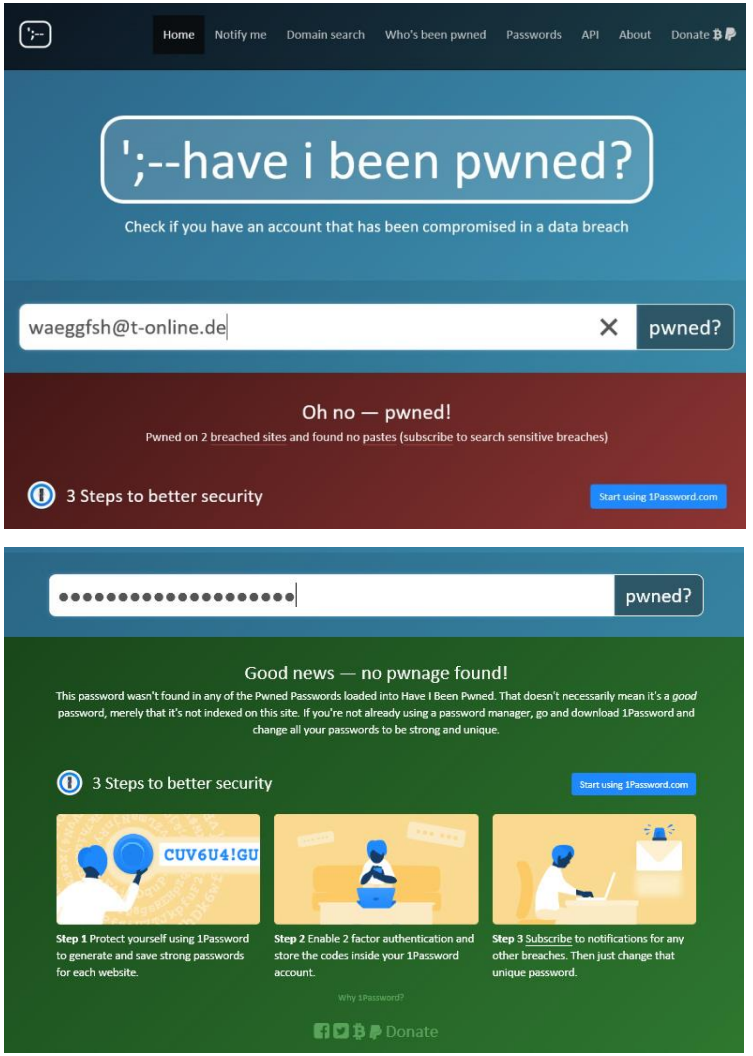
Im Internet ist ein gewaltiger Datensatz mit gestohlenen Log-in Informationen aufgetaucht

Millionen Passwörter veröffentlicht

18.01.19

Im Internet ist ein gewaltiger Datensatz mit gestohlenen LOG-IN-Informationen aufgetaucht. Darin enthalten sind ca. 773 Millionen verschiedener eMail-Adressen und über 21 Millionen im Klartext lesbare Passwörter. Die IT-Firma Troy Hunt weist darauf hin, dass mehr als 1 Milliarde Kombinationen aus der Sammlung „Collection #1“ für beide Informationen zulässt. Wer überprüfen will, ob seine eMail-Adresse auftaucht, kann dazu den Hunts-Dienst nutzen.

https://havebeenpwned.com



Kostenfalle Ping-Calls

Bundesnetzagentur warnt

Die Bundesnetzagentur hat am Montag eine Rechnungslegung und Inkassierung von Verbindungen zu mehreren weißrussischen Rufnummern untersagt. Damit müssen Verbraucher, die **Ping-Anrufe** von diesen Rufnummern aus Weißrussland erhalten und darauf reagiert haben, nicht mehr für die damit verbundenen Kosten aufkommen. Die Betrüger hatten eine Ähnlichkeit zur Ortsvorwahl **0375** in Sachsen ausgenutzt – die Vorwahl für Weißrussland lautet **00375**. Etwa 300 Menschen hatten sich bei der Bundesnetzagentur über derartige Anrufe beschwert.

Immer wieder gibt es Wellen von "Ping-Anrufen" oder ähnlichen Lockanrufen. Das Prinzip: Betrüger versuchen, über solche Ping-Anrufe **Rückrufe** der Verbraucher zu **provozieren**, die oft mit hohen Kosten verbunden sind. Mehrere Euro pro Minute können dabei berechnet werden.

Pfändungsbeschluss per Telefon

Am 17.4.2018 13:16

(Rufnummer 0211 32664655) erhielt ich einen Anruf von einem angeblichen Forderungsmanagement, dass hier ein **Pfändungsbeschluss** über einen Betrag von **611,- €** vorläge. Ich habe dem widersprochen und habe dem „feinen“ Herren bedeutet er solle sein dummes Geschwätz sein lassen. Anschließend kam noch ein Gefasel über einen Gerichtsvollzieher. Ich habe den Hörer einfach aufgelegt. Und schon war Ruhe – und „eigenartigerweise“ kein Gerichtsvollzieher

Neueste Raffinesse von „Microsoft“

Sie erhalten eine „System-Warnung“, dass Ihr Windows - System beschädigt ist und Sie dieses sofort aktualisieren müssen bevor Ihre Daten gelöscht werden.

1.) Dies ist sicherlich nur ein Fake, da sich das Fenster **Meldung von Webseite** nicht schließen lässt. Man will Sie also zwingen den Button **Aktualisieren** (Achtung!) zu drücken.

2.) Grammatikalischer Fehler mahnt zur Vorsicht: **Microsoft haben festgestellt…**

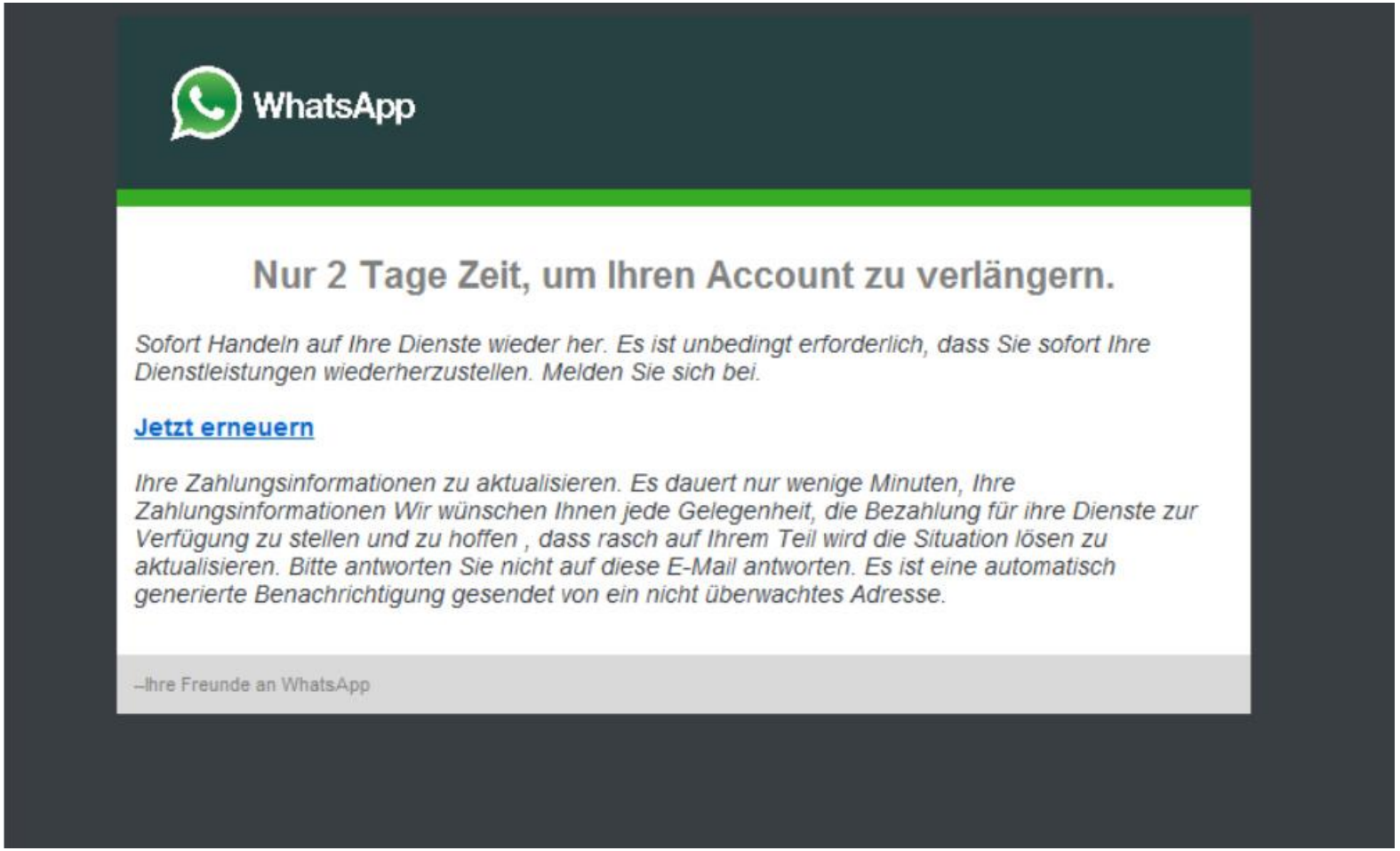
3.) Das Symbol vor der **System Warnung** stammt von Windows 7, nicht von Windows 10

Also Ruhe bewahren : Über Taskmanager diese Seite schließen. Wenn Sie beunruhigt sein sollten, lassen Sie Ihren Virenscanner noch einmal arbeiten

Vorsicht bei Maestro-Card Debit

Die neuen MasterCard werden mit der Möglichkeit über WLAN-Verbindungen Daten mit anderen Datenträgern auszutauschen, ausgeliefert. Diese Möglichkeit wird entweder durch ein **WLAN-Symbol** auf der Vorderseite der MasterCard oder durch einen Eintrag **debit** angezeigt. So „sinnvoll“ diese Einrichtung für „Faule“ sein mag, so birgt sie doch auch große Gefahren. So kann ich berührungslos an Geschäftskassen nur durch Vorbeigehen an einem Lesegerät bezahlen (swu) – oder mit geeigneter Schadsoftware die Kartendaten auslesen und mir z.B. über das DARKNET Blankokarten besorgen, mit diesen Daten bestücken, und anschließend ohne weiteres – nur gegen Unterschrift – bezahlen. Immer vorausgesetzt - die Dame an der Kasse handelt oberflächlich und lässt sich den Personalausweis wegen Unterschriftenvergleich nicht vorlegen.

Beste Deutsch wo gibt, anschauen, lächeln und löschen

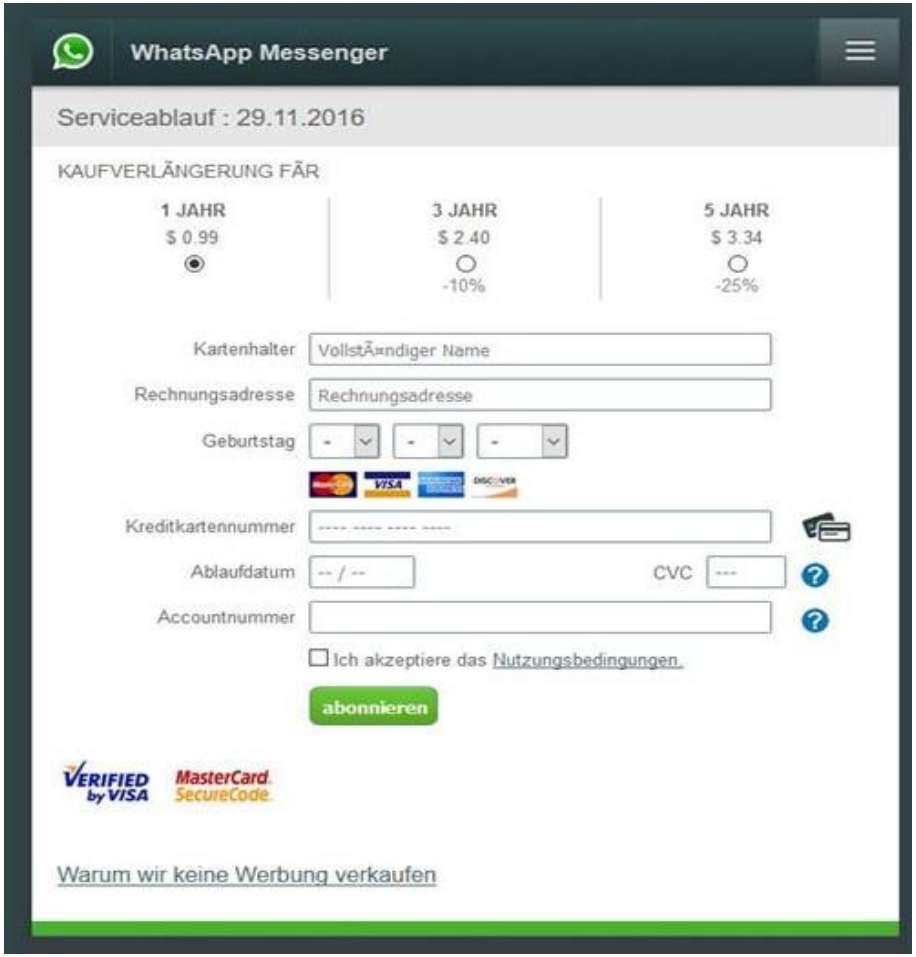


Wer reinfällt, den straft das Leben

Mit der „Fortsetzung“ eines WhatsApp-Abos gegen Zahlung einer Abo-Gebühr von 0,99 € wird ihr Abo verlängert. Wenn sie innerhalb von 24 Std. nicht zahlen, wird der Dienst angeblich deaktiviert.

Hoffentlich wissen sie, dass der Dienst grundsätzlich **kostenfrei** ist. Die Drohung mit der Deaktivierung ist absoluter Nonsens

Verlängerung Ihres Abos



Wenn Sie also Ihre Zahlungsdetails „aktiviert“ haben, so können Sie auch ihre „Vertragsverlängerung“ in die Wege leiten.

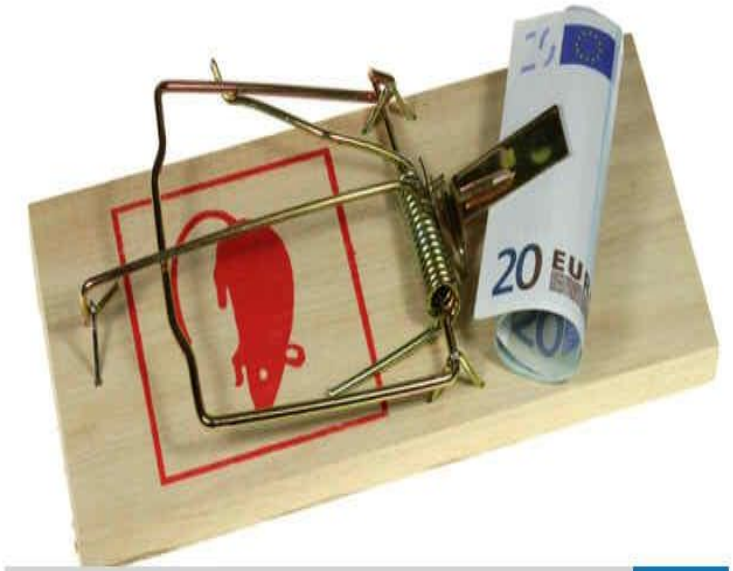
In der Mail ist ein Link platziert, der keinesfalls angeklickt werden sollte. Der Link führt ebenfalls zu einer Fake-Seite, die Originalgetreu wie WhatsApp aussieht, um eben keinen Verdacht zu schöpfen. Im nächsten Schritt sollen Sie ihre Kreditkarten Daten in das Formular eingeben, damit ihnen der Betrag vom WhatsApp Abo regelmäßig abgebucht werden kann. Klicken Sie nun auf Fortsetzen, hat die Falle auch schon zugeschlagen und ihre Daten werden zu den Betrügern weitergeleitet.

„Sicherheitsupddate“ für WhatsApp

Betrüger verteilen über WhatsApp eine Nachricht, dass der WhatsApp-Dienst gehackt wurde und man schnell diesen Sicherheitsupdate installieren soll. Hierzu müsse man nur auf den beigefügten Link klicken. Wer das tut, hat verloren, denn das Update hat es in sich: Der Klick öffnet kein Sicherheitsupdate sondern installiert stattdessen jetzt einen Online-Banking-Trojaner. Er setzt sich im Smartphone-Betriebssystem Android fest und versucht, Kontodaten abzugreifen. Der Schädling soll so perfide sein, dass er nur über die Einstellung **Werkszustand** entfernt werden kann.

Polizei warnt vor Mails mit gefälschten Rechnungen und Malware

Betrüger versuchen mit Mails, die sich als Rechnungen tarnen, Malware auf Windows-PCs einzuschmuggeln. Eine aktuelle Liste der angeblichen Absender.



Polizei: Mails mit gefälschten Rechnungen und Malware

Vergrößern

© istockphoto.com/foto-ruhrgebiet

Die Polizei von Niedersachsen warnt davor, dass Internet-Betrüger immer noch im großen Stil Fake-Rechnungen per Mail an potenzielle Opfer versenden. Die Ganoven verwenden unterschiedliche Firmennamen als Absender für ihre angeblichen Rechnungen. Die Firmennamen sind teilweise frei erfunden, teilweise handelt es sich aber auch um tatsächlich existierende Unternehmen. Die Betreffzeile der Betrügermails nimmt Bezug auf eine angeblich nicht durchführbare Kontoabbuchung. Die Mails sind in nahezu einwandfreiem Deutsch geschrieben und wirken vergleichsweise authentisch. In den Mails wird den Adressaten mit unterschiedlichen Maßnahmen gedroht, beispielsweise mit Einleitung von Gerichtsverfahren oder der Hinzuziehung eines Inkassobüros. In der Mail stehen, wie die Polizei betont, „fast ausschließlich reelle komplette Personendatensätze (Vorname, Nachname, Anschrift und Rufnummer) der Angeschriebenen“. Die Betrüger wollen mit den gefakten Rechnungsmails Schadsoftware auf die PCs der Adressaten schmuggeln. Die Malware verbirgt sich entweder in einem **Mailanhang** oder soll per **Link** heruntergeladen werden.

Mithilfe von Phishing-Mails versuchen Kriminelle, an Daten ihrer Opfer zu kommen. Auf diese aktuellen Betrugs-Versuche sollten Sie achten.

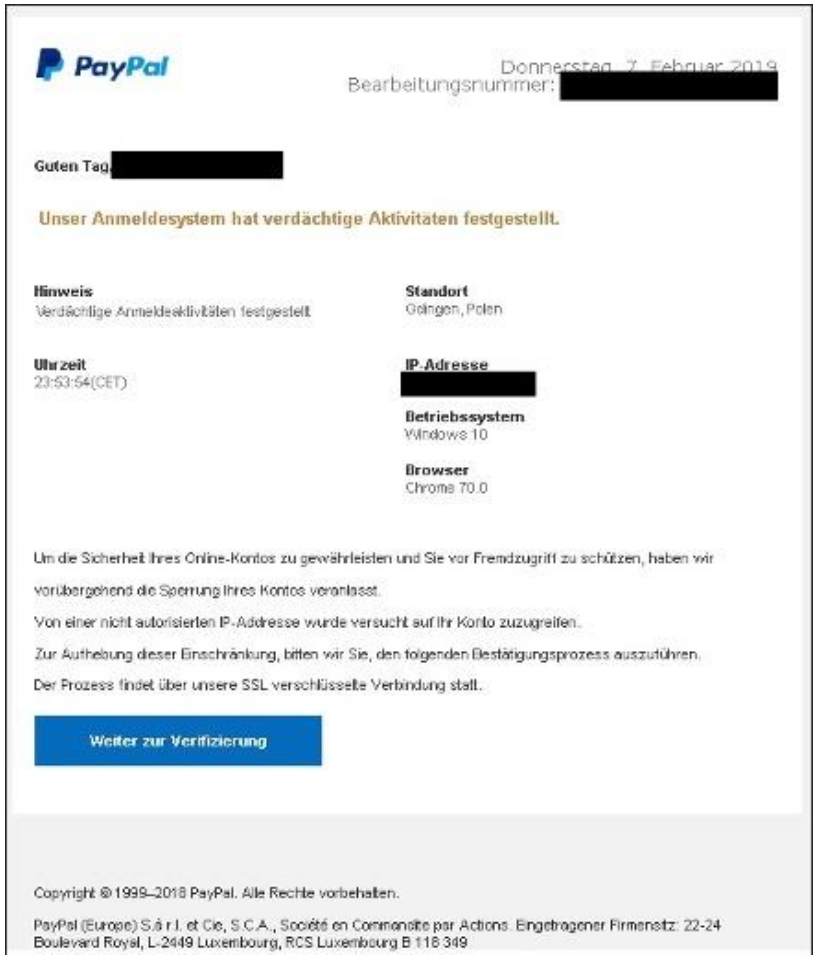
- **Die Verbraucherzentrale Nordrhein-Westfalen warnt im "Phishing-Radar "regelmäßig vor Phishing-Mails. Mit Hilfe solcher Nachrichten versuchen Kriminelle an vertrauliche Daten von Nutzern zu kommen.**
- **Hierzu nachfolgend weitere Beispiele aus der jüngsten Zeit**

Wie erkennt man Phising Mails

Wer Phishing-Mails erkennen will, muss auf verschiedene Details in der Nachricht achten. Beispielsweise **schwächelt** bei solchen Nachrichten **die Rechtschreibung**. Auch verlangen Banken oder Online-Händler generell **keine Kontaktdaten** per Mail zu aktualisieren oder persönliche Daten einzugeben. Zudem **fehlt meist eine persönliche Anrede**. Banken und Online-Händler schreiben ihre Kunden generell mit richtigem Namen an. Wenn Sie also persönlich angesprochen werden, prüfen Sie ob Ihre eMail-Adresse evtl. Ihren Vor- und Zunamen enthält. Aus diesen Daten lässt sich nämlich leicht die persönliche Anrede generieren. Ein weiterer Tipp bei Phishing-Mails und was Sie tun sollten, wenn Sie Opfer eines Betrugs geworden sind: **Phishing-Mails löschen** doch **vorher** die falsche Nachricht an die Verbraucherzentrale weiterleiten. Auf ihrer Webseite listen die Verbraucherschützer nämlich die falschen Nachrichten und informieren so andere Nutzer. Die Mail-Adresse lautet: phishing@vz-nrw.de.

Schicken Sie die Phishing-Mail am besten auch an den echten Anbieter, beispielsweise die betroffene Bank oder dem Online-Händler.

Paypal ist diesmal besonders im Visier



PayPal

Donnerstag, 7. Februar 2019
Bearbeitungsnummer: [redacted]

Guten Tag [redacted]

Unser Anmeldesystem hat verdächtige Aktivitäten festgestellt.

Hinweis
Verdächtige Anmeldeaktivitäten festgestellt

Standort
Gdingen, Polen

Uhrzeit
23:53:54(CET)

IP-Adresse
[redacted]

Betriebssystem
Windows 10

Browser
Chrome 70.0

Um die Sicherheit Ihres Online-Kontos zu gewährleisten und Sie vor Fremdzugriff zu schützen, haben wir vorübergehend die Sperrung Ihres Kontos veranlasst.
Von einer nicht autorisierten IP-Adresse wurde versucht auf Ihr Konto zuzugreifen.
Zur Aufhebung dieser Einschränkung, bitten wir Sie, den folgenden Bestätigungsprozess auszuführen.
Der Prozess findet über unsere SSL verschlüsselte Verbindung statt.

Weiter zur Verifizierung

Copyright © 1999–2018 PayPal. Alle Rechte vorbehalten.

PayPal (Europe) S.à r.l. et Cie, S.C.A., Société en Commandite par Actions. Eingetragener Firmensitz: 22-24 Boulevard Royal, L-2449 Luxembourg, RCS Luxembourg B 118 349

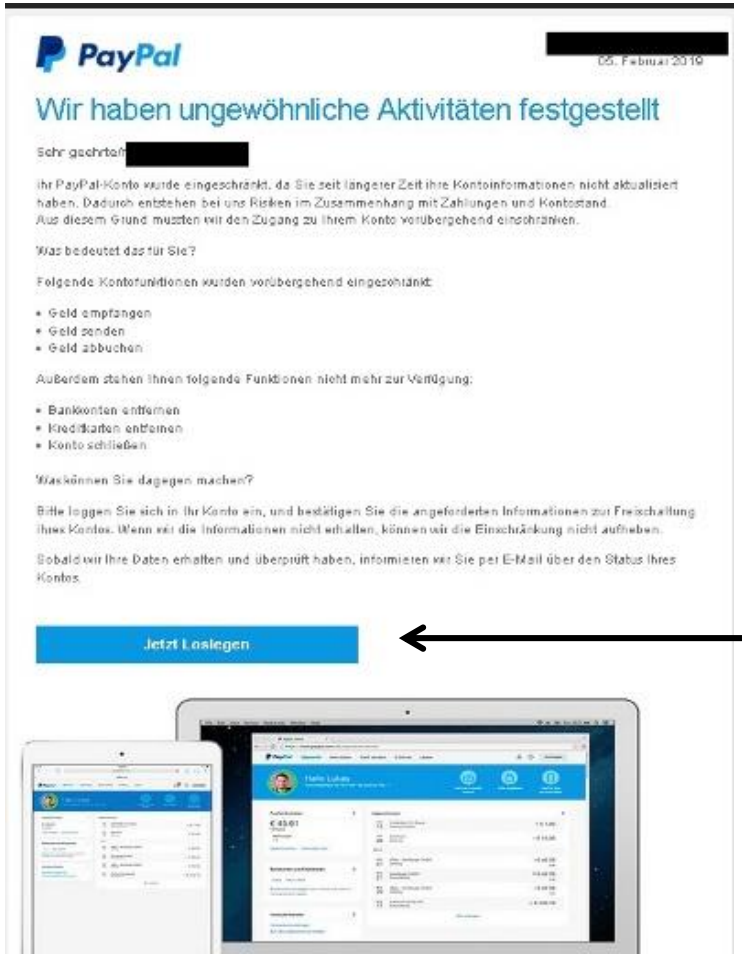
Bei einem Firmenschreiben ist grundsätzlich eine Fußzeile vorhanden. Unter anderem ist hier ein **Impressum** angegeben. Dieses enthält den Firmennamen, PLZ, Ort, Adresse und die Rufnummer. Wenn Sie also ihre Maus hierauf führen, muss diese sich im Aussehen ändern (Zeigefinger). Wenn das unzutreffend ist, ist schon etwas faul an dem Schreiben. Wenn diese Fußzeile gänzlich fehlt ist das sogar oberfaul. Am besten gleich vernichten – ab in den Papierkorb

„Unregelmäßigkeiten“ bei Paypal

PayPal

In falschen PayPal-Mails schreiben Unbekannte, dass das Konto missbraucht wurde oder Unregelmäßigkeiten entdeckt wurden. Aus diesem Grund wurde das Konto gesperrt. Um es zu entsperren, sollen Nutzer mit einem Klick auf einen Button zur PayPal-Seite und dort ihre Daten eingeben. Die Nachrichten unterscheiden sich dabei in der Aufmachung und beim Text in der Betreffzeile. In der Fotoshow (oben) zeige ich beispielhaft auf, wie die Phishing-Mails aussehen können.

Andere „Aktivitäten“ bei Paypal



PayPal

[redacted]
05. Februar 2019

Wir haben ungewöhnliche Aktivitäten festgestellt

Sehr geehrte/r [redacted]

Ihr PayPal-Konto wurde eingeschränkt, da Sie seit längerer Zeit Ihre Kontoinformationen nicht aktualisiert haben. Dadurch entstehen bei uns Risiken im Zusammenhang mit Zahlungen und Kontostand.
Aus diesem Grund mussten wir den Zugang zu Ihrem Konto vorübergehend einschränken.

Was bedeutet das für Sie?

Folgende Kontofunktionen wurden vorübergehend eingeschränkt:

- Geld empfangen
- Geld senden
- Geld abbuchen

Außerdem stehen Ihnen folgende Funktionen nicht mehr zur Verfügung:

- Bankkonten entfernen
- Kreditkarten entfernen
- Konto schließen

Was können Sie dagegen machen?

Bitte loggen Sie sich in Ihr Konto ein, und bestätigen Sie die angeforderten Informationen zur Freischaltung Ihres Kontos. Wenn wir die Informationen nicht erhalten, können wir die Einschränkung nicht aufheben.

Sobald wir Ihre Daten erhalten und überprüft haben, informieren wir Sie per E-Mail über den Status Ihres Kontos.

Jetzt Loslegen

Datum 05.02.2019

Sofern Ihre eMail Adresse Vor- und Zunamen enthält, generieren Unbekannte Ihre Anrede hieraus. Damit steht fest, dass ihre eMail-Adresse gehackt wurde. Weiter wird eine Ansicht aus **Skype** oder **WhatsApp** mit eingeblendet, um ihnen aufzuzeigen,dass das Konto „eingeschränkt“ wurde, um die Glaubwürdigkeit dieser eMail zu manifestieren. Um es zu entsperren, sollen Nutzer mit einem Klick auf einen Button zur PayPal-Seite und dort ihre Daten eingeben.

Also **NICHT** Jetzt Loslegen

Banken sind sehr beliebt

.comdirect

Guten Tag [redacted]

damit Sie weiterhin in vollem Umfang am mTAN-Verfahren der comdirect bank AG teilnehmen können, müssen wir Sie auffordern die Mobilfunknummer Ihres Smartphones abzugleichen. Der Abgleich garantiert Ihnen als Kunde eine erhöhte Sicherheit und eine reibungslose Nutzung unserer Dienstleistungen.

Ein Abgleich Ihrer Mobilfunknummer ist zwingend notwendig, um weiterhin den Sicherheitsstandards gerecht zu werden und Ihre Sicherheit im Mobilfunknetz zu gewährleisten. Grund dafür sind steigende Angriffe auf Sicherheitslücken einiger Mobilfunkbetreiber.

> Zum Formular

Wir bitten um Ihr Verständnis. Für Fragen nehmen Sie bitte Kontakt mit dem Kundenservice auf.

Mit freundlichen Grüßen

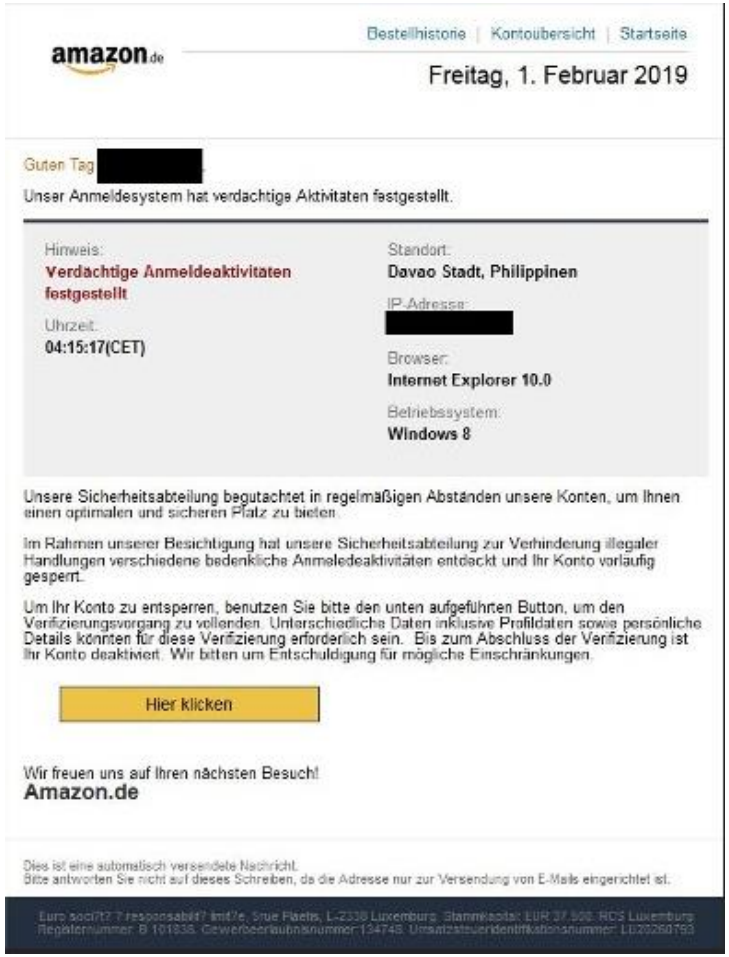
Ihr comdirect Kundenservice

Kunden der .comdirect-Bank sollen angeblich ihre Handy-Nummer abgleichen, um das mTAN-Verfahren weiter nutzen zu können. Dazu sollen Kunden ein Formular auf einer Webseite ausfüllen, die der .comdirect-Seite "täuschend ähnlich sieht", schreibt die Verbraucherzentrale. Zudem nutzen die Kriminellen in der Mail wie gehabt eine persönliche Anrede – generiert aus ihrer eMail-Adresse.

Auch Volksbanken müssen daran glauben

Kunden der Volksbanken Raiffeisenbanken werden in der Phishing-Nachricht dazu aufgefordert, "wegen geänderter Nutzungsbedingungen" ihre Daten zu bestätigen. Die Betreffzeile lautet **Wichtige Mitteilung**. Auch hier nutzen Kriminelle eine persönliche Anrede, um die Phishing-Mail echter aussehen zu lassen.

Auch Amazon ist ein Versuch wert



amazon.de

Bestellhistorie | Kontoübersicht | Startseite

Freitag, 1. Februar 2019

Guten Tag [redacted]

Unser Anmeldesystem hat verdachtige Aktivitaten festgestellt.

Hinweis:
Verdächtige Anmeldeaktivitäten festgestellt

Uhrzeit:
04:15:17(CET)

Standort:
Davao Stadt, Philippinen

IP-Adresse:
[redacted]

Browser:
Internet Explorer 10.0

Betriebssystem:
Windows 8

Unsere Sicherheitsabteilung begutachtet in regelmäßigen Abständen unsere Konten, um Ihnen einen optimalen und sicheren Platz zu bieten.

Im Rahmen unserer Besichtigung hat unsere Sicherheitsabteilung zur Verhinderung illegaler Handlungen verschiedene bedenkliche Anmeldeaktivitäten entdeckt und Ihr Konto vorläufig gesperrt.

Um Ihr Konto zu entsperren, benutzen Sie bitte den unten aufgeführten Button, um den Verifizierungsvorgang zu vollenden. Unterschiedliche Daten inklusive Profildaten sowie persönliche Details könnten für diese Verifizierung erforderlich sein. Bis zum Abschluss der Verifizierung ist Ihr Konto deaktiviert. Wir bitten um Entschuldigung für mögliche Einschränkungen.

Hier klicken

Wir freuen uns auf Ihren nächsten Besuch!
Amazon.de

Dies ist eine automatisch versendete Nachricht.
Bitte antworten Sie nicht auf dieses Schreiben, da die Adresse nur zur Versendung von E-Mails eingerichtet ist.

Euro sociTZ ? responsabil? limit?e, srue Fleets, L-2338 Luxemburg. Stammkapital: EUR 37.500. RCS Luxemburg Registernummer: B 101838. Gewerbeerlaubnisnummer 134748. Umsatzsteueridentifikationsnummer: LU20260793

Amazon

Der Name des Online-Händlers Amazon wird gerne von Kriminellen für Phishing-Mails missbraucht. Aktuell warnt die Verbraucherzentrale vor Nachrichten, die auf "verdächtige Anmeldeaktivitäten" hinweisen. Um das angebliche Problem zu lösen, sollen Nutzer einem Link folgen und ihre Daten eingeben

Was ist eigentlich "Money Muling"?

- Die Sicherheitsmaßnahmen einer Bank sollen angeblich durch Interessenten **gegen Honora**r geprüft werden. Dazu ist hier ein Konto zu eröffnen. Zunächst läuft alles glatt. Doch dann ändert der Auftraggeber die Zugangsdaten, kapert Ihr Konto und eröffnet unter Ihrem Namen einen Fake-Shop. Kunden bezahlen darauf Waren im Voraus und erhalten **NICHTS**. Sie werden so als „**Geldesel**“ missbraucht. Deshalb heißt diese Masche auch „Money Muling“. Sie leisten so ahnungslos Beihilfe zu Geldwäsche oder Betrug.
- **Geld- und Haftstrafen drohen**
- Wichtig bei der Sache ist: Unwissenheit schützt vor Strafe nicht. Wer auf die Masche reinfällt und sie anzeigt, muss laut Kripo dennoch mit einem Bußgeld rechnen. Wer erst über ein Ermittlungsverfahren ausfindig gemacht wird, dem könnte sogar eine Haftstrafe drohen. 2018 waren es mit 232 schon mehr als doppelt so viele Fälle wie in 2017

E-Mails vom „Beitragsservice“

Schulden beim Rundfunkbeitrag? Zwangsvollstreckung? Betrüger verschicken solche Mails momentan. Sie wollen Empfänger zum Öffnen gefährlicher Dateien drängen.
So erkennen Sie falschen Mahnmails.

Betrüger geben sich derzeit als Beitragsservice für den Rundfunkbeitrag aus und versenden Mahnungen per E-Mail. Darin wird Empfängern mit einer Zwangsvollstreckung gedroht. Die gute Nachricht für Betroffene: Nein, der echte Beitragsservice verschickt keine derartigen E-Mails. Bei den Schreiben handelt es sich um eine Fälschung von Kriminellen. Wer solche Mails erhält, sollte sie gleich löschen und auf keinen Fall enthaltene Anhänge öffnen

So erkennen Sie die falschen Mahnmails

Die E-Mails tragen den Betreff "**Ankündigung der Zwangsvollstreckung**" und ähneln in ihrer Aufmachung der Website des Beitragsservices Rundfunkbeitrag.de.

Mögliche Absender der Mails sind Adressen wie:

mahnung@beitragsservice-de.com

mahnung@beitragsservice-deutschland.com

Im Schreiben wird behauptet, Empfänger hätten ihren Rundfunkbeitrag nicht gezahlt. 161 Euro seien angeblich offen und würden bald zwangsvollstreckt. Dazu wird auf Informationen im angehängten Schreiben hingewiesen. Dieser Anhang – eine Word-Datei **"Mahnbescheid.doc"** – enthält allerdings **Schadsoftware.**

Kontaktlos bezahlen

Die kontaktlose Zahlung erfolgt online mittels Kreditkarte zu einem Kartenleser über Wifi. Die neuen EC-Karten sind dazu mit NFC (Near Field Communication) bestückt. Sie benötigen dazu keinen Akku. Ihre EC-Karte wirkt dabei vielmehr wie ein Spiegel, der von einem Kartenterminal auf kurze Entfernung “ausgelesen” werden kann. Diese Funktion kann bei Ihrer Bank aber auch deaktiviert werden. Momentan sind Rechnungen bis 25 € kontaktlos abbuchbar. Doch auch hier haben Hacker schon durch Simulation ohne/trotz Eingabe Ihres Pincodes, das Kassenterminal betrogen. Dabei wird an der Kasse der Zahlbetrag richtig angezeigt. Die **manipulierte Kreditkarte** setzt den Rechnungsbetrag auf 25 € und “erspart“ dem Hacker trotz der Eingabe des 4-stelligen PIN-Codes – erforderlich bei Beträgen > 25 € - den Differenzbetrag zum Nachteil des Verkäufers.

So leicht lässt sich Geld beim kontaktlosen Bezahlen abfischen

Kontaktloses Bezahlen macht den Bezahlvorgang an der Kasse bequem und einfach. Es ist aber genauso leicht, mit der Technik das Geld anderer Leute abzufischen. Dies wird mit Hilfe eines elektronischen Zahlungsterminals bewerkstelligt, einem Gerät mit dem Händler ihren Kunden die kontaktlose Bezahlung per Karte, Handy oder Smartwatch ermöglichen. Dieses Geräte lässt sich nämlich ziemlich leicht auch dazu missbrauchen, das Geld fremder Leute zu ergaunern. Einzige Abhilfe ist in der Deaktivierung oder der Beschaffung von speziell entwickelten Abschirmschutzhüllen zu finden.

Wie einfach ist Datendiebstahl

Durch NFC-Chips in Kredit- und EC-Karten können Sie kontaktlos bezahlen. PIN und Unterschrift sind dann nicht mehr nötig. **In der Regel** klappt das nur für Kleinbeträge unter 25 Euro.

Die NFC-Chips sollen maximal 4 cm weit funken. So wird verhindert, dass niemand aus Versehen zu nah mit seiner Karten an den Terminal der Kasse gelangt. Einige Karten lassen sich mit handlichen Lesegeräten auch über eine Entfernung von bis zu 20 cm auslesen. Genau dort beginnt das Problem:

Kriminelle können unter Menschenmassen spielend leicht das Lesegerät für wenige Sekunden an das Portemonnaie in Ihrer Hosentasche halten. Die Daten werden ausgelesen und im Anschluss auf eine Blanko-Karte übertragen, mit welcher der Dieb dann einkaufen gehen kann.

EC-Karten mit NFC vor Datenklau schützen

Damit niemand Ihre EC- oder Kreditkarte unbemerkt auslesen und duplizieren kann, sollten Sie Karten mit NFC abschirmen. Das gelingt mit speziellen Hüllen.

In den Hüllen sind meist sehr dünne Drähte eingenäht, welche die Funkwellen der NFC-Chips stören. Ein Zugriff von außen ist somit nicht mehr möglich.

Die NFC-Hüllen kosten meist weniger als einen Euro pro Stück. Mittlerweile gibt es auch NFC-Portemonnaies, sodass Sie keine zusätzliche Hülle benötigen

Hack: Visa-Zahlungen ohne PIN-Abfrage möglich

Wer mit seiner Visa-Karte an kontaktlosen Bezahl-Terminals bezahlt, muss erst ab einer Summe von 25 Euro eine PIN eingeben. Mitarbeiter des US-Cybersecurity-Unternehmens **Positive Technologies** haben eine Methode gefunden, um diese Limitierung zu umgehen und die nötige PIN-Abfrage auszuhebeln. Maximal waren Zahlungen bis 101 Pfund möglich. Die Methode funktioniert nur bei **Visa-Karten.**

Die Methode umfasst das Umgehen der PIN-Abfrage durch eine „Man-in-the-Middle“-Attacke, bei der die Kommunikation zwischen Visa-Karte und Bezahlterminal manipuliert wird. Auf diese Weise geht die Karte davon aus, dass es sich nur um einen Kleinstbetrag handelt, das Bezahlterminal hingegen denkt, dass die Verifikation schon erfolgt ist. Im Gegensatz zu anderen Kreditkartenanbietern verzichtet Visa auf eine verpflichtende Verifikation über dem Grenzwert.

Wichtiger Sicherheitshinweis Ihrer Bank!

Aktuell rufen verstärkt vermeintliche "**Microsoft-Mitarbeiter**" an, um Daten abzufragen und Zahungen zu erzwingen. Zusätzlich befindet sich ein Rückzahlungs-Trojaner im Umlauf.

Bitte beachten Sie unbedingt die aktuellen Sicherheitshinweise.

Phishing-Angriff vor dem Login ins Online-Banking

Eine sehr authentisch wirkende Phishing-Masche kursiert derzeit in einer nachgebauten Login-Seite des Online-Banking. Der User wird hierbei vor geklonten SIM-Karten gewarnt. Er wird gebeten, zum Schutz seines Smartphones eine Synchronisation durchzuführen. Hierzu muss der User sein Handymodell angeben. Im weiteren Verlauf wird er gebeten, das bevorzugte TAN-Verfahren anzugeben.

Solche Anforderungen kommen nicht von Ihrer Sparda-Bank!

Aktuelle Sicherheitshinweise Ihrer Sparda-Bank München

03.09.2019

Phishing-Mail "Kreditkarte freischalten"

Trojanerwarnung: Rückzahlung von Fehlüberweisung

Betrug durch falsche Microsoft-Mitarbeiter

Trojanerwarnung: Betrüger haben es auf mTANs abgesehen

Trojanerwarnung: Umstellung auf SMS-TAN

Phishing-Mail "Sperrung Benutzerkonto"

Phishing-Mail zu neuem Sicherheitssystem

Phishing-Mail "Unerlaubter Zugriff"

Quiz: Kennen Sie sich mit Phising-Mails aus?

Phishing-Betrüger verschicken falsche E-Mails im Namen von Unternehmen – in der Hoffnung, dass Nutzer anbeißen und private Daten verraten. Wie leicht lassen Sie sich austricksen? Machen Sie den Test!

Phishing-Mails zählen zu den häufigsten Formen des Online-Betrugs. Mit gefälschten Mails im Namen großer Unternehmen versuchen Betrüger, an private Daten, Passwörter und Log-in-Informationen zu kommen. Dazu locken die Täter ihre Opfer auf gefälschten Seiten oder verbreiten Schadsoftware im Mail-Anhang. Doch es gibt Warnzeichen, an denen Nutzer den Betrugsversuch erkennen können.

Im vorliegenden Quiz sind 10 Beispiele zusammengetragen worden, die entweder echten Mails oder Phishing-Versuchen nachempfunden sind. Können Sie Original von Fälschung unterscheiden? Raten Sie mit und testen Sie Ihr Phishing-Wissen!

Frage 1 von 10

Ihr Postfach ist voll.

Outlook-Nutzer kennen diesen gelben Balken, der signalisiert, dass das Postfach voll ist. Folgen Sie dem angebotenen Link, um das Problem zu lösen?

26540 Teilnehmer

Ja	Nein

Lösung zu Frage 1

Ihr Postfach ist voll.

Outlook-Nutzer kennen diesen gelben Balken, der signalisiert, dass das Postfach voll ist. Folgen Sie dem angebotenen Link, um das Problem zu lösen?

Richtig!

Bei dieser Mail handelt es sich um einen Phishing-Versuch, was sich unter anderem an der Absenderadresse "outlook-support@yahoo.de" erkennen lässt. Falls Ihr Postfach wirklich voll ist, erhalten Sie außerdem eine Warnung ohne Links.

Frage 2 von 10

Die Sparkasse braucht Ihre Mithilfe.

Ihre Bank muss einen Datenabgleich vornehmen, weil sich die Datenschutzgesetze geändert haben. Stimmt das?

26540 Teilnehmer

Ja	Nein

Lösung zu Frage 2

Die Sparkasse braucht Ihre Mithilfe.

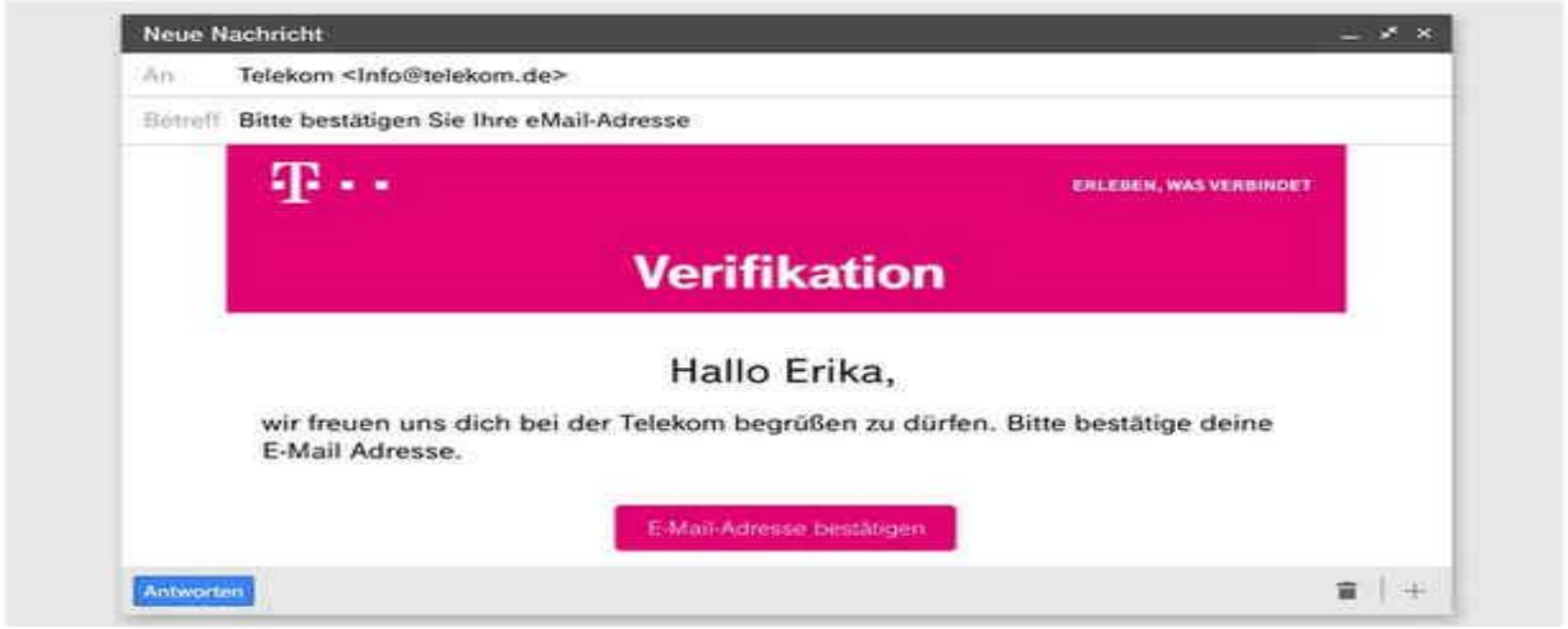
Ihre Bank muss einen Datenabgleich vornehmen, weil sich die Datenschutzgesetze geändert haben. Stimmt das?

26540 Teilnehmer

Nächste Frage

Richtig!

Dieser Phishing-Versuch zielt auf Ihre Bankdaten ab, daher sollten Sie besonders vorsichtig sein. Alles an dieser Mail ist frei erfunden: Weder gibt es einen "§56 Datenschutzgesetz Absatz 1B" noch eine "Sparkasse AG". Auch die diversen Rechtschreibfehler in der Nachricht sollten die Alarmglocken schrillen lassen.



Frage 3 von 10

Die Telekom bittet um Verifizierung.

Neukunde bei der Telekom? Dann bestätigen Sie bitte zuerst Ihre E-Mail-Adresse! Muss das wirklich sein?

26540 Teilnehmer

Ja	Nein

Lösung zu Frage 3

Die Telekom bittet um Verifizierung.

Neukunde bei der Telekom? Dann bestätigen Sie bitte zuerst Ihre E-Mail-Adresse!
Muss das wirklich sein?

26540 Teilnehmer

Nächste Frage

Richtig!

Diese Mail ist tatsächlich echt. Die Nutzerin hatte sich zuvor beim Streamingdienst MagentaTV angemeldet und dementsprechend eine solche Nachricht erwartet. Falls Sie so eine Mail aus heiterem Himmel erhalten, stimmt wahrscheinlich etwas nicht!

Frage 4 von 10

Netflix will Geld von Ihnen.

Offensichtlich stimmt was nicht mit Ihren Zahlungsinformationen bei Netflix. Kann das sein?

26540 Teilnehmer

Ja	Nein

Lösung zu Frage 4

Netflix will Geld von Ihnen.

Offensichtlich stimmt was nicht mit Ihren Zahlungsinformationen bei Netflix. Kann das sein?

26540 Teilnehmer

Nächste Frage

Richtig!

Diese Phishing-Mail ist ein wenig lieblos zusammengeklöppelt: Es fehlt unter anderem das Logo und ein ordentliches Impressum. Die Absenderadresse "netflix@support.de" ist ebenfalls erfunden.

Frage 5 von 10

Ihr DHL-Paket kommt später.

Die gute Nachricht: Ihr Paket kommt am Mittwoch. Die schlechte: Sie sollen dafür zahlen. Wer hat das denn bestellt? Klicken Sie auf die Sendungsverfolgung, um nachzusehen?

26540 Teilnehmer

Ja	Nein

Lösung zu Frage 5

Ihr DHL-Paket kommt später.

Die gute Nachricht: Ihr Paket kommt am Mittwoch. Die schlechte: Sie sollen dafür zahlen. Wer hat das denn bestellt? Klicken Sie auf die Sendungsverfolgung, um nachzusehen?

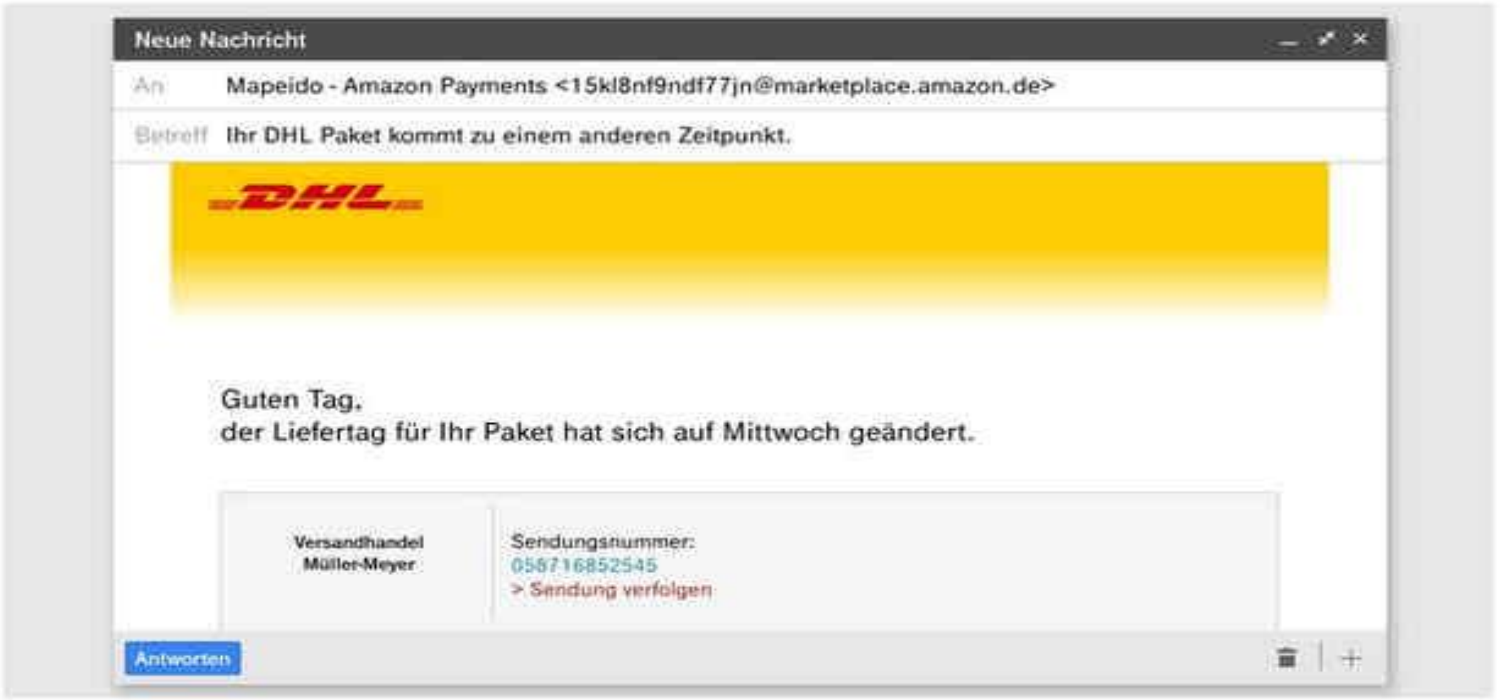
26540 Teilnehmer

Nächste Frage

Richtig!

Diese Mail ist eine Falle! Durch die Behauptung, dass Sie jemandem Geld schulden, wird natürlich Druck erzeugt. Ein Blick auf den Absender lässt den Betrug aber auffliegen.

Wichtig: Viele Mail-Programme zeigen nur den Namen an. Gewöhnen Sie sich an, immer die vollständige Absenderadresse zu überprüfen, bevor Sie auf Links klicken.



Frage 6 von 10

Noch mal Post von DHL.

Wie sieht es mit diesem Paket aus? Ist da wirklich was unterwegs zu Ihnen?

26540 Teilnehmer

Ja	Nein

Lösung zu Frage 6

Noch mal Post von DHL.

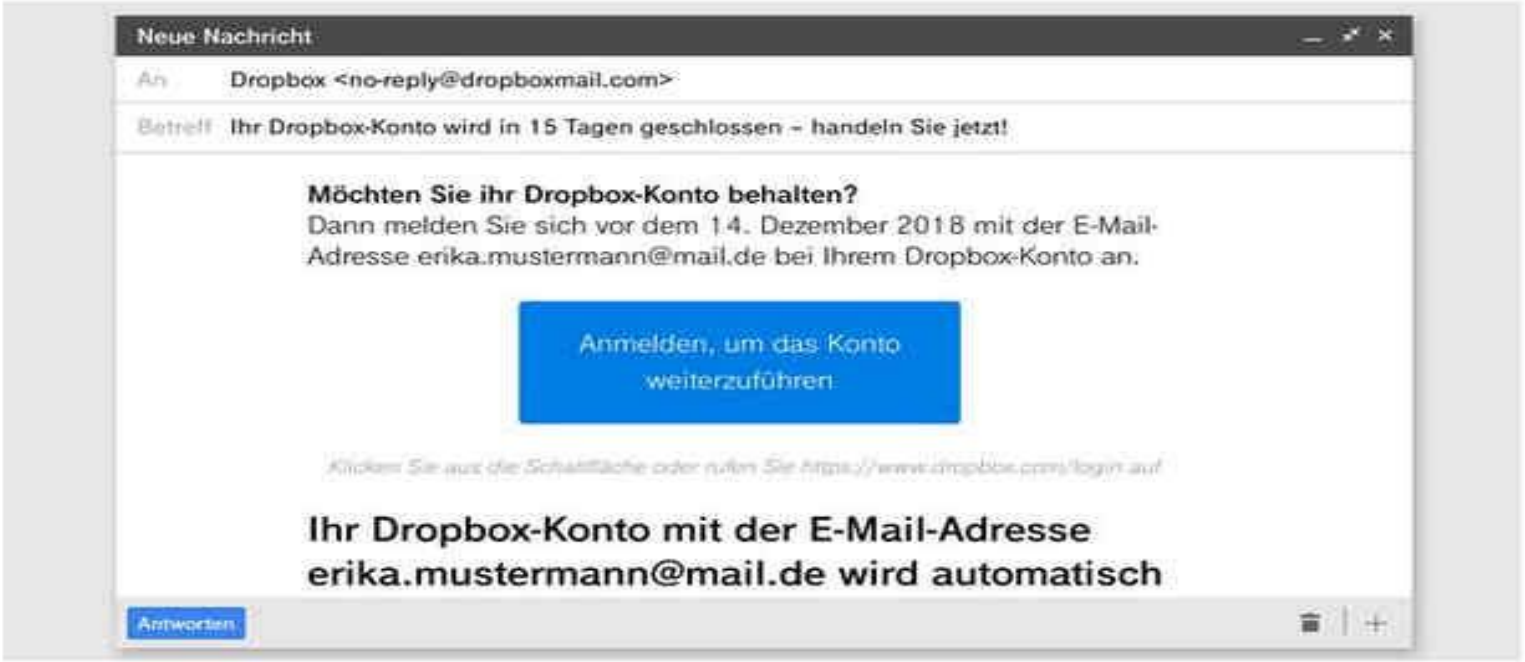
Wie sieht es mit diesem Paket aus? Ist da wirklich was unterwegs zu Ihnen?

26540 Teilnehmer

Nächste Frage

Richtig!

Diese Mail ist einer echten DHL-Mitteilung nachempfunden. Die Absenderadresse sieht seltsam aus, das scheint bei Bestellungen bei Amazon Marketplace-Händlern aber üblich zu sein. Trotzdem gilt natürlich immer: Wenn Sie nichts bestellt haben, sollten Sie vorher alles überprüfen. Wohin führt der Link? Ein Mouseover verrät es!



Frage 7 von 10

Ihr Dropbox-Konto wird geschlossen.

Sieht so aus, als seien Sie schon länger nicht mehr bei Dropbox aktiv gewesen.
Brauchen Sie die Daten noch? Dann klicken Sie hier!

26540 Teilnehmer

Ja	Nein

Lösung zu Frage 7

Ihr Dropbox-Konto wird geschlossen.

Sieht so aus, als seien Sie schon länger nicht mehr bei Dropbox aktiv gewesen.
Brauchen Sie die Daten noch? Dann klicken Sie hier!

26540 Teilnehmer

Nächste Frage

Richtig!

Diese Mail wird tatsächlich von Dropbox verschickt, wenn man sein Konto länger nicht mehr genutzt hat. Vorausgesetzt natürlich, Sie haben ein Dropbox-Konto.

Frage 8 von 10

Ihre Amazon-Bestellung wurde versandt.

Das Buch, das Sie bei Amazon gekauft haben, ist auf dem Weg. Hier können Sie die Lieferung verfolgen. Kann man auf den Link gefahrlos klicken?

26540 Teilnehmer

Ja	Nein

Lösung zu Frage 8

Ihre Amazon-Bestellung wurde versandt.

Das Buch, das Sie bei Amazon gekauft haben, ist auf dem Weg. Hier können Sie die Lieferung verfolgen. Kann man auf den Link gefahrlos klicken?

26540 Teilnehmer

Nächste Frage

Richtig!

So sieht eine echte Versandbestätigung von Amazon aus. Doch Vorsicht: Jeder kann so eine Mail fälschen – so wie wir. Achten Sie auf ein ordentliches Impressum und seien Sie besonders skeptisch, wenn Sie kein Paket erwarten.

Frage 9 von 10

Die Telekom schickt eine Rechnung.

Wer eine solche Mail erhält, erschrickt erst mal. Öffnen Sie den Anhang?

26540 Teilnehmer

Ja	Nein

Lösung zu Frage 9

Die Telekom schickt eine Rechnung.

Wer eine solche Mail erhält, erschrickt erst mal. Öffnen Sie den Anhang?

26540 Teilnehmer

Nächste Frage

Falsch!

Falsche Telekom-Mails wie diese können gefährlich werden. Im Anhang findet sich ein Dokument mit der Endung "doc.x", das eine Schadsoftware enthält. Die Telekom verschickt Rechnungen normalerweise im PDF-Format. Zum Glück erkennen Sie in diesem Fall schon am Absender, dass diese Mail von Betrügern stammt.

Frage 10 von 10

Ihr Online-Banking-Account wurde gesperrt

Die Sparkasse musste Ihren Online-Banking-Account aus Sicherheitsgründen sperren. Hier können Sie den Zugang wieder freischalten. Stimmt das?

26540 Teilnehmer

Ja	Nein

Lösung zu Frage 10

Whatsapp-Betrüger locken mit Milka-Schokolade (2022)

Über Whatsapp gibt es angeblich Osterkörbe voll mit Milka-Schokolade zu gewinnen. Nun warnt Milka vor der Masche.

Zur Osterzeit nehmen Online-Betrüger verstärkt die Nutzer auf Whatsapp & Co. mit gefälschten Gewinnspielen ins Visier. Dabei wird auch der bekannte Markenname "Milka" missbraucht. Über Whatsapp werden Nachrichten weitergeleitet, laut denen Milka kostenlose Oster-Geschenkkörbe verschenkt. Und das ausgerechnet aus Russland

Und das ist der grösste Computer-Hacker