Phishing erkennen ,

leicht gemacht

Phishing erkennen leicht gemacht

Vielen Dank für den Download von meinem Buch Phishing erkennen , leicht gemacht !

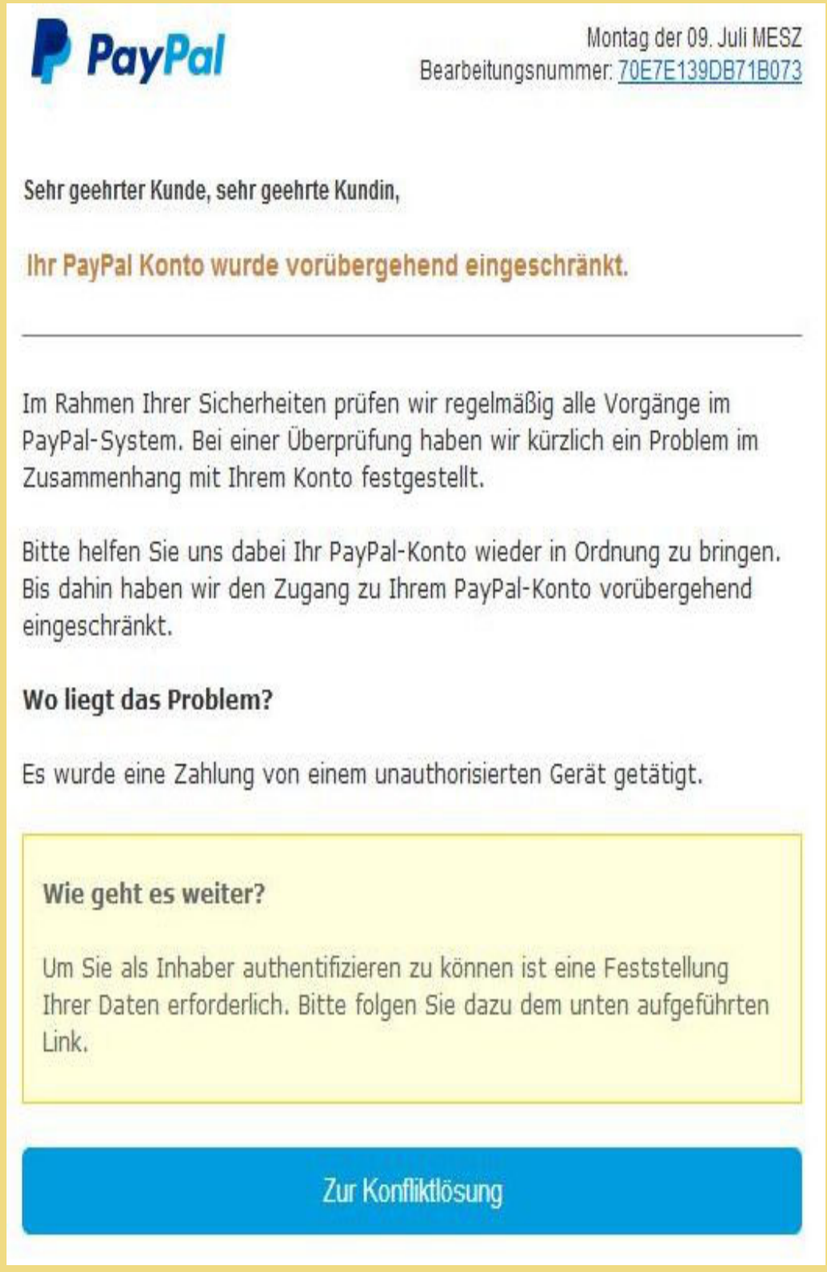
Die Tipps in diesem Buch können Dir helfen, garnicht erst auf betrugsähnliche Mails herein zufallen .

Den Erhalt von Phishing, Spam Nachrichten kann man zwar nicht verhindern - aber mindern !

Den Erhalt von Phishing- als auch Spam - Nachrichten kann man zwar nicht verhindern - aber mindern !

Merke ! Online Gauner sind oft sehr kreativ und setzen bei ihrer Strategie auf Deine eigene Gier oder auf die problemelose Panik .

Wer sich zum lesen seiner Post keine Zeit gönnt, übersieht sehr schnell **die nicht persönliche Anrede** und wird ebenso mit hoher Wahrscheinlichkeit auch den Online Gauner **blind folgen** in dem er auf den Button zur Konfliktlösung klickt.



PayPal

Montag der 09. Juli MESZ
Bearbeitungsnummer: 70E7E139DB71B073

Sehr geehrter Kunde, sehr geehrte Kundin,

Ihr PayPal Konto wurde vorübergehend eingeschränkt.

Im Rahmen Ihrer Sicherheiten prüfen wir regelmäßig alle Vorgänge im PayPal-System. Bei einer Überprüfung haben wir kürzlich ein Problem im Zusammenhang mit Ihrem Konto festgestellt.

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?

Es wurde eine Zahlung von einem unauthorisierten Gerät getätigt.

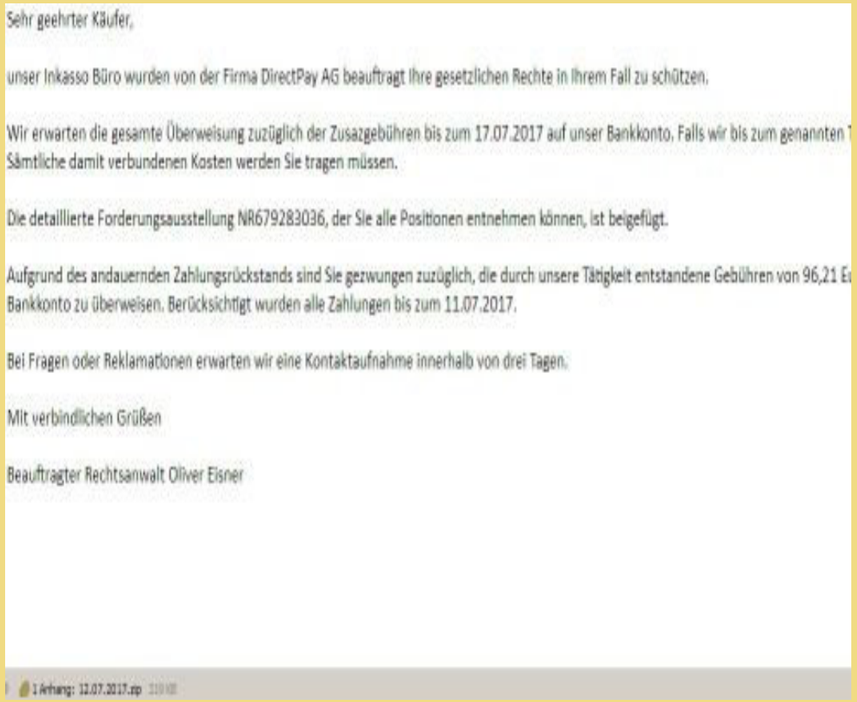
Wie geht es weiter?

Um Sie als Inhaber authentifizieren zu können ist eine Feststellung Ihrer Daten erforderlich. Bitte folgen Sie dazu dem unten aufgeführten Link.

Zur Konfliktlösung

Was versteht man unter den Begriff Phishing?

Der Begriff Phishing (nach Daten fischen) steht für das manipulieren von Telefonnetzen, dem Ausspionieren von Daten und bzw. Zugangsdaten für Kreditkarten, Online Banking und Handelsplattformen (eBay, Amazon, usw.) sowie sonstige Zahlungsdienste wie zum Beispiel MoneyBookers, Paypal und so weiter



Sehr geehrter Käufer,

unser Inkasso Büro wurden von der Firma DirectPay AG beauftragt Ihre gesetzlichen Rechte in Ihrem Fall zu schützen.

Wir erwarten die gesamte Überweisung zuzüglich der Zusazgebühren bis zum 17.07.2017 auf unser Bankkonto. Falls wir bis zum genannten T
Sämtliche damit verbundenen Kosten werden Sie tragen müssen.

Die detaillierte Forderungsausstellung NR679283036, der Sie alle Positionen entnehmen können, ist beigefügt.

Aufgrund des andauernden Zahlungsrückstands sind Sie gezwungen zuzüglich, die durch unsere Tätigkeit entstandene Gebühren von 96,21 E
Bankkonto zu überweisen. Berücksichtigt wurden alle Zahlungen bis zum 11.07.2017.

Bei Fragen oder Reklamationen erwarten wir eine Kontaktaufnahme innerhalb von drei Tagen.

Mit verbindlichen Grüßen

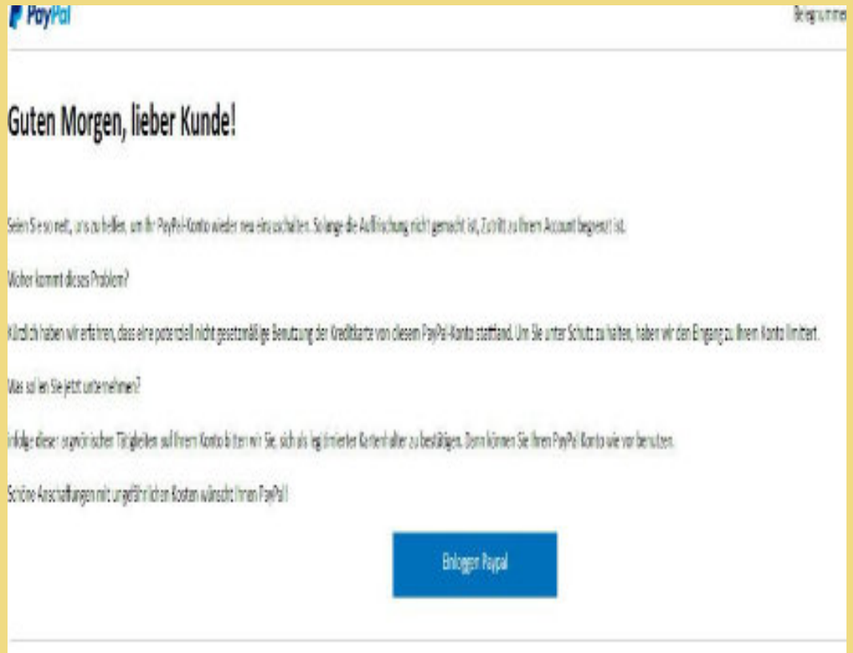
Beauftragter Rechtsanwalt Oliver Eisner

1 Anhang: 12.07.2017.zip

In diesem Fall gilt, absolute Ruhe zubewahren, sicherlich keine leichte Aufgabe. Persönlich kenne ich keine Gestz wonach man verpflichtet wäre, den virtuellen Postkasten täglich zu entleeren und dem entsprechend die Post zu lesen .

Das Ziel vom Phishing

Das Ziel von Phishing besteht darin, vom ahnungslosen Opfer vertrauliche persönliche Daten von Konto – und Kreditkarte usw. oder andere höchstpersönliche Daten per Telefon oder E-Mail möglichst kurz und schmerzlos zu entlocken. Wer spätestens hier den Schlaf der Gerechten träumt, überläßt dem Gauner die Spielführung.



PayPal

Guten Morgen, lieber Kunde!

Seien Sie so nett, uns zu helfen, um Ihr PayPal-Konto wieder neu einzuschalten. Solange die Auffrischung nicht gemacht ist, Zutritt zu Ihrem Account begrenzt ist.

Woher kommt dieses Problem?

Kürzlich haben wir erfahren, dass eine potenziell nicht gesetzmäßige Benutzung der Kreditkarte von diesem PayPal-Konto stattfand. Um Sie unter Schutz zu halten, haben wir den Eingang zu Ihrem Konto limitiert.

Was soll ein Sie jetzt unternehmen?

Infolge dieser ungerechtfertigten Tätigkeiten auf Ihrem Konto bitten wir Sie, sich als legitimierter Kartenhalter zu bestätigen. Dann können Sie Ihren PayPal Konto wie vor benutzen.

Schöne Anschaffungen mit ungefährlichen Kosten wünscht Ihnen PayPal!

Einlogen Paypal

So eine Mail klingt natürlich bedrohlich und einschüchternd. Wer seinen Computer mit seiner verbauten Hardware genau kennt, fällt natürlich auf so einen Schwachsinn erst garnicht rein.

Mit der erschlichenen Identität hat der Gauner für eine Gewisse Zeit freie Hand und kann im Namen des Opfers (Deine Identität) Banküberweisungen tätigen, deine gesamten Ersparnisse plündern, natürlich auch auf Deine KOSTEN großzügig einkaufen und wiederum andere über den Tisch ziehen.

Du hingegen, befindest Dich zu nächst einmal in der glücklichen Lage das Du Deine Unschuld beweisen musst und dies möglichst sehr schnell.

Phishing durchleuchtet

Phishing Mails sehen auf den ersten Blick sehr professionell aus, sind oft in einem perfektem deutsch und können daher den uninformierten Leser leicht täuschen.

In der Nachricht wird dir vorgegaukelt, dass dein Benutzerkonto bei xx gesperrt wurde, der Zugriff auf dein Konto eingeschränkt wurde, oder Du morgen Kohle abdrücken musst wenn Du nicht sofort auf den Button in der Mail klickst

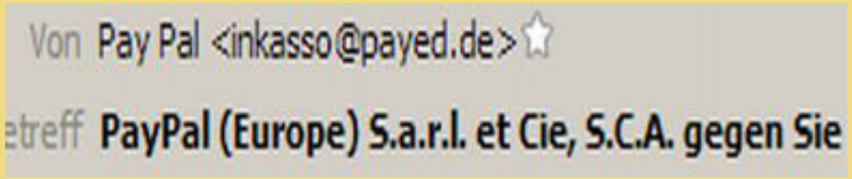
Wer sich wirklich etwas Zeit zum Lesen nimmt - läuft nicht Gefahr voreilig oder unbedacht zu handeln.

Gelgendlich kommt es auch bei mir mal vor, das die eine oder andere Mail von irgend einem Hans Wurst im Glück am süssen Honig sich vorbei navigiert.

Wer sich also zum lesen seiner Post etwas Zeit nimmt, wird die die einen oder anderen Ungereimtheiten finden und im Zweifel nicht der Aufforderung durch den Gauner folgen.

Der erste Blick

Um Dein Auge etwas schulen zu können, solltest du das Bild genauer betrachten.



Vielen vom Stress geplagten fällt der kleine Schreibfehler, in der Adressezeile vom Absender nicht , auf dem ersten Blick auf !

Dies liegt entweder daran, das sie sich mit Informationen vollgepumpt fühlen oder halt nicht wissen wie man eine vorgetäuschte Nachricht durch einen Gauner vom Original unterscheiden können.

Der Blick auf die Adresszeile sollte dir sagen, dass der Absender nicht von Paypal sondern von einer täuschend ähnlich klingenden Domain „ Payed.de „ stammt. Es kann sich somit also nur um eine Fälschung bzw. Dich hinder das Licht führen zu wollen handeln.

Gelegendlich strandet auch mal eine wirklich gute Phishing Mail in deinem Postfach, welche man auf dem ersten Blick nicht von einer seriösen Mail unterscheiden kann. Hier hilft dann nur der Blick in den Quelltext um wieder Klarheit über die Quelle vom Absender zu bekommen.

Zur Quelle der Wahrheit

Ein Blick in den Quelltext (besteht aus dem Programmiercode) sollte die nötige Klarheit schaffen.
Und im Quelltext sieht der Text der Absenderadresse dann so aus.

```
Return-Path: <inkasso@payed.de>
Received: from mail.3skill.com ([37.156.28.41])
```

Return – Path bedeutet soviel wie der Weg zurück zu payed.de

Received steht für empfangen von in diesem Fall von 3skill.com

Du findest beides im Kopfbereich (oder auch Header genannt)

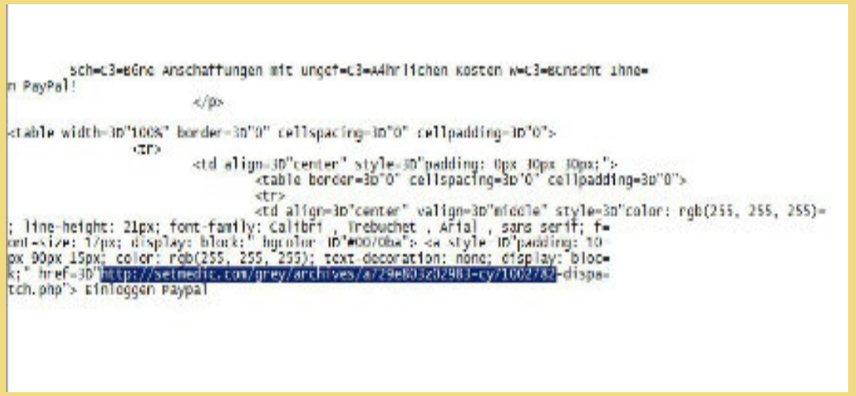
Der zweite Blick !

Etwas schwieriger wird der Blick wohin Dich der Button „ zum einloggen, der angeblichen Sicherheitsüberprfüfung, der Identitätsfeststellung und weiterer Schwachsinn„ führt. !

Im Quelltext besteht der bunte Button leider nur aus einem Programmiercode.

Damit Du diesen Code aber realtiv schnell, je nach dem wie oft Du Dein Auge bereits geschult hast, auch relativ einfach finden kannst, ein kleiner Tipp.

Setze den Fokus bei der suche, nicht auf den Button sondern nur auf den Text oder eventuell der Überschrift " Was müssen Sie tun ? " direkt über den Button.



Spätestens an dieser Stelle sollten alle Zweifel ausgeräumt wurden sein, das diese Mail nur von einem Online Betrüger stammen kann.

Nutze zum Aufrufen deiner Online Bank oder Handelsplattform immer deine eigenen Bookmarks oder tippe die URL direkt in den Browser ein und nutze NIEMALS aus Bequemlichkeit den Link in der übersandten E-Mail .

Banken, Kreditinstitute und seriöse Unternehmen fordern grundsätzlich keine vertraulichen Daten per E-Mail, per Telefon oder per Post von Dir an, daher kann so eine Anforderung auch nur von einem Gaunern stammen.

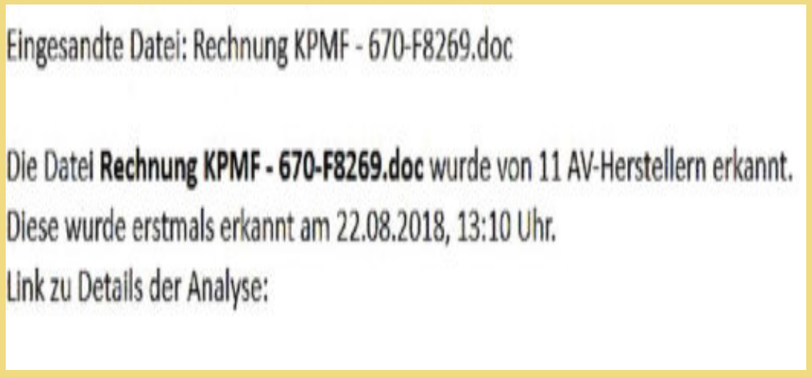
Verdächtige Mail ,

Erhalten , was nun ?

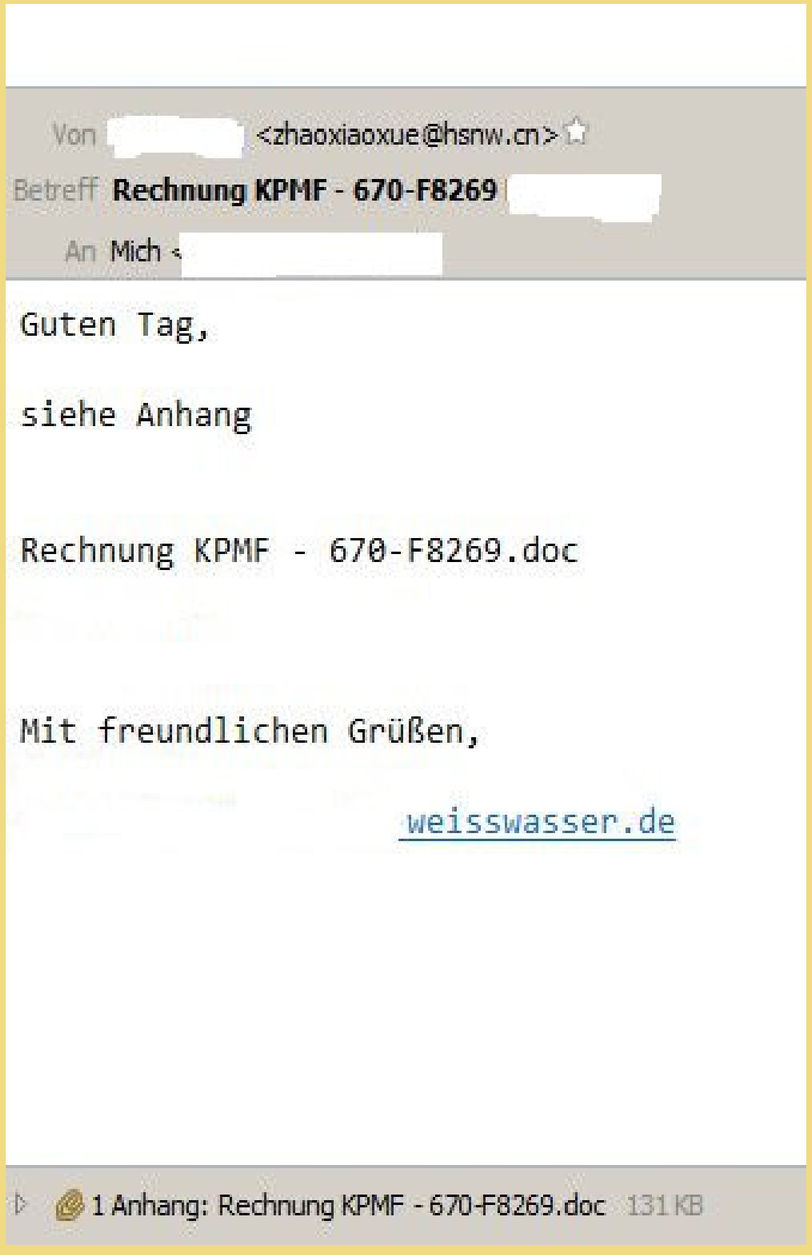
Experten , raten immer dazu, Phishing als auch Spam – Mails einfach zu löschen.
Persönlich teile ich diese Meinung nicht.

Wer bei so einer Mail nicht aufpasst, läuft Gefahr, nicht nur seine Daten auf dem Computer zu verlieren, die Du dank von einem Backup mit etwas Zeitaufwand wieder herstellen könntest sondern auch noch ausspioniert oder gar Deiner Identität beraubt zu werden.

Vergewissere dich nach Möglichkeit, mit wem du es zu tun hast. Ein geübter Blick in den Quellcode sorgt für die notwendige Aufklärung !


Eingesandte Datei: Rechnung KPMF - 670-F8269.doc

Die Datei **Rechnung KPMF - 670-F8269.doc** wurde von 11 AV-Herstellern erkannt.
Diese wurde erstmals erkannt am 22.08.2018, 13:10 Uhr.
Link zu Details der Analyse:


Von [redacted] <zhaoxiaoxue@hsnw.cn>
Betreff **Rechnung KPMF - 670-F8269** [redacted]
An Mich <[redacted]

Guten Tag,

siehe Anhang

Rechnung KPMF - 670-F8269.doc

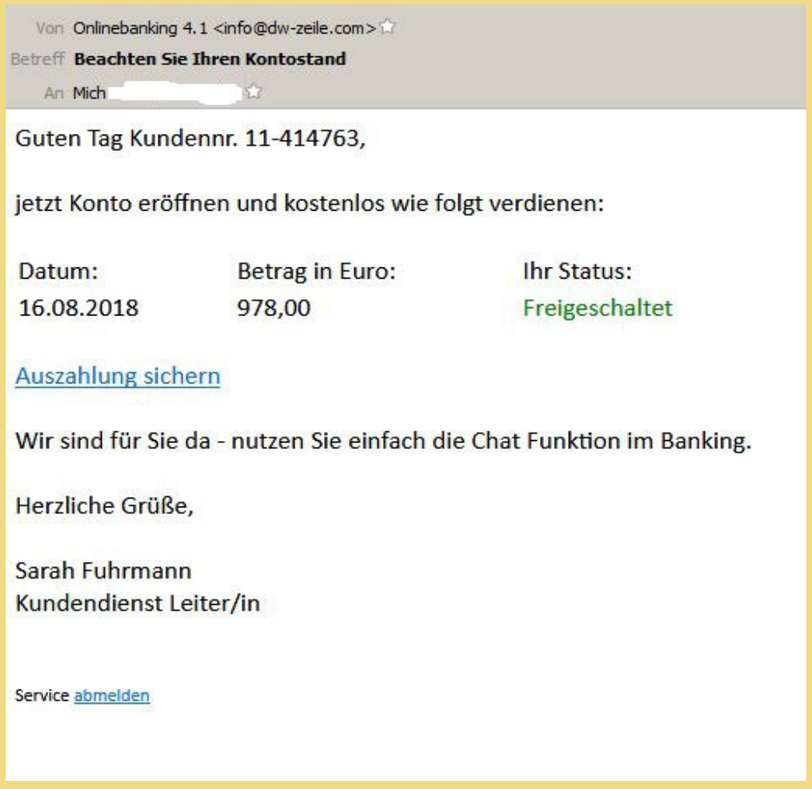
Mit freundlichen Grüßen,

weisswasser.de

1 Anhang: Rechnung KPMF - 670-F8269.doc 131 KB

Allgemeine Tipps

Öffne nur Mails von Adressaten die du kennst. Mails von Unbekannten können Schadprogramme beinhalten.



Von Onlinebanking 4.1 <info@dw-zeile.com>
Betreff **Beachten Sie Ihren Kontostand**
An Mich

Guten Tag Kundennr. 11-414763,

jetzt Konto eröffnen und kostenlos wie folgt verdienen:

Datum:	Betrag in Euro:	Ihr Status:
16.08.2018	978,00	Freigeschaltet

Auszahlung sichern

Wir sind für Sie da - nutzen Sie einfach die Chat Funktion im Banking.

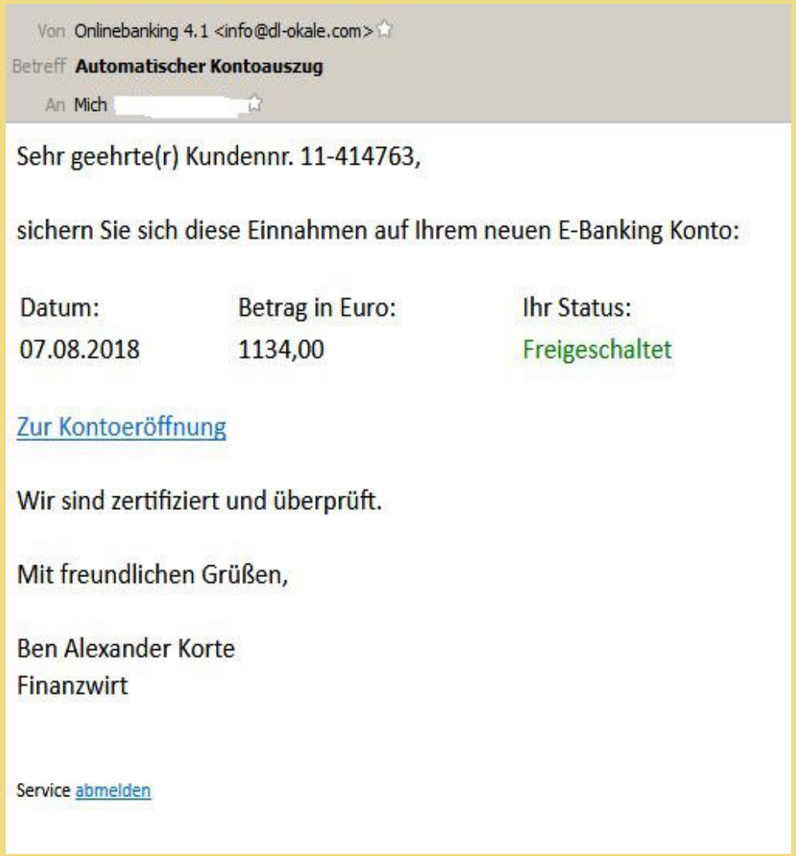
Herzliche Grüße,

Sarah Fuhrmann
Kundendienst Leiter/in

Service abmelden

Wer aus Zweifel oder eben purer Neugier den Anhang in der E-Mail öffnet, wird nicht selten mit einem Trojaner überrascht.

Klicke niemals auf Links von Finanzinstituten bei dem du angeblich ein Konto besitzt.



Von Onlinebanking 4.1 <info@dl-okale.com>
Betreff **Automatischer Kontoauszug**
An Mich

Sehr geehrte(r) Kundennr. 11-414763,

sichern Sie sich diese Einnahmen auf Ihrem neuen E-Banking Konto:

Datum:	Betrag in Euro:	Ihr Status:
07.08.2018	1134,00	Freigeschaltet

Zur Kontoeröffnung

Wir sind zertifiziert und überprüft.

Mit freundlichen Grüßen,

Ben Alexander Korte
Finanzwirt

Service abmelden

Wenn du so eine Mail bekommst, kann sie nur von Gaunern stammen.

Rechtzeitig informiert

Polizeiliche Kriminalprävention der Länder und des Bundes

www.polizei-beratung.de/startseite-und-aktionen/

Ratgeber Internet Kriminalität der Polizei Niedersachsen

www.polizei-praevention.de/home.html

Schweiz

Schweizerische Kriminalprävention

www.skppsc.ch/de/

Republik Österreich

Bundesministerium Inneres

www.bmi.gv.at

Tipps gegen Cybercrime

Die Föderation der Gegenseitigkeit e.V. ist ein

Verein für Kriminalprävention / Umweltschutz

www.fdg-ev.com

Watchlist Internet

Ist unabhängige Informationsplattform zu Internet-Betrug und
betrugsähnlichen Online-Fallen aus Österreich

www.watchlist-internet.at

Autor

Heiko Buresch
Karl – Liebknecht – Straße 10
02943 Weißwasser