Vorsicht Erpressermails: Phishing, E-Mail-Spoofing und Phishing

Wie schütze ich mich vor Erpressermails? – Ein Leitfaden zum Durchatmen

Erpressermails können echt nerven, oder? Aber keine Sorge, Panik ist der falsche Weg! Erfahrt hier, warum diese Mails meist nur heiße Luft sind und wie ihr euch effektiv schützt. Von Passwort-Tricks bis zu proaktiven Maßnahmen – ich rüste euch mit dem nötigen Know-how aus.

Warum sind Erpressermails größtenteils nur leere Drohungen?

Ah, Erpressermails! Sie sind wie der nervige Nachbar, der immer droht, das Ordnungsamt zu rufen, es aber nie wirklich tut. Aber warum sind diese Mails größtenteils nur heiße Luft? Lasst uns das mal genauer unter die Lupe nehmen.

SEO-Küche Internet Marketing GmbH & Co. KG
Fraunhoferstr. 6, 83059 Kolbermoor
Telefon 08031 / 2575-100
Telefax 08031 / 2575-101
E-Mail: info@seo-kueche.de

SEO-Küche Internet Marketing GmbH & Co. KG,
HRA 11167 AG Traunstein
pers. Haftende Gesellschafterin:
SEO-Küche Verwaltungs GmbH, Kolbermoor, HRB 22414 AG Traunstein
Geschäftsführer: Christian Brunnenmayer, Patrick Keller, Oliver Lindner
Ust-IdNr.: DE 286 985 708, Steuer Nr. 156/174/08500

HypoVereinsbank
IBAN DE45 700202700015260147
BIC HYVEDEMMXXX

SEO-Küche Internet Marketing GmbH & Co. KG
Fraunhoferstr. 6, 83059 Kolbermoor
Telefon 08031 / 2575-100
Telefax 08031 / 2575-101
E-Mail: info@seo-kueche.de

SEO-Küche Internet Marketing GmbH & Co. KG,
HRA 11167 AG Traunstein
pers. Haftende Gesellschafterin:
SEO-Küche Verwaltungs GmbH, Kolbermoor, HRB 22414 AG Traunstein
Geschäftsführer: Christian Brunnenmayer, Patrick Keller, Oliver Lindner
Ust-IdNr.: DE 286 985 708, Steuer Nr. 156/174/08500

HypoVereinsbank
IBAN DE45 700202700015260147
BIC HYVEDEMMXXX

Erpressermails können richtig gefährlich werden. Zumindest, wenn man falsch reagiert.

Gängige Tricks vs. Realität

Trick in der Mail	Realität dahinter
Passwort-Trick	Passwörter sind oft aus anderen Datenlecks und frei im Netz verfügbar.
Mail-Spoofing	Technischer Trick, der keinen wirklichen Zugriff auf das Mail-Konto bedeutet.

Psychologische Spielchen

Die Betrüger setzen auf eure Angst und Unsicherheit. Durch das Nennen eines echten, aber unsicheren Passworts oder das Vortäuschen eines eigenen Absenders wollen sie Glaubwürdigkeit schaffen. Doch in Wahrheit haben sie überwiegend keinen Zugriff auf persönliche Daten oder Konten.

Was sie wirklich wollen

- Geld, meist in Form von Kryptowährungen
- Schnelle Reaktionen, die zu unüberlegten Handlungen führen
- Unsicherheit als Hebel für ihre Maschen nutzen

Was steckt hinter dem Passwort-Trick?

Stellt euch vor, ihr öffnet eine Mail und seht ein Passwort, das ihr tatsächlich mal verwendet habt. Schockierend, oder? Aber keine Panik!

Die Wahrheit hinter dem Trick

Die Wahrheit ist, dass diese Passwörter oft aus anderen Datenlecks stammen und frei im Netz verfügbar sind. Die Betrüger sind also meist Trittbrettfahrer, die auf eure Angst setzen.

Was ihr tun solltet

- Ändert sofort das kompromittierte Passwort

SEO-Küche Internet Marketing GmbH & Co. KG
Fraunhoferstr. 6, 83059 Kolbermoor
Telefon 08031 / 2575-100
Telefax 08031 / 2575-101
E-Mail: info@seo-kueche.de

SEO-Küche Internet Marketing GmbH & Co. KG,
HRA 11167 AG Traunstein
pers. Haftende Gesellschafterin:
SEO-Küche Verwaltungs GmbH, Kolbermoor, HRB 22414 AG Traunstein
Geschäftsführer: Christian Brunnenmayer, Patrick Keller, Oliver Lindner
Ust-IdNr.: DE 286 985 708, Steuer Nr. 156/174/08500

HypoVereinsbank
IBAN DE45 700202700015260147
BIC HYVEDEMMXXX

- Überprüft andere Konten auf die Verwendung des gleichen Passworts
- Bleibt ruhig und lasst euch nicht unter Druck setzen

Was ist Mail-Spoofing, und wie funktioniert es?

Ihr denkt, die Mail kommt von eurem eigenen Account? Falsch gedacht!

Der technische Trick

Mail-Spoofing ist ein technischer Trick, bei dem der Absender der Mail so gefälscht wird, dass es so aussieht, als käme sie von eurem eigenen Account. Ziel ist es, die Empfänger zu verwirren und den Inhalt glaubhafter wirken zu lassen.

Was ihr tun solltet

- Ignoriert die Mail und öffnet keine Anhänge oder Links
- Überprüft eure Mail-Konten auf verdächtige Aktivitäten
- Meldet die Mail als Spam oder Phishing-Versuch

Jetzt wisst ihr Bescheid! Lasst euch nicht von diesen windigen Typen in die Enge treiben. Ihr habt jetzt das Rüstzeug, um solchen Erpressermails die kalte Schulter zu zeigen. ?

Wie reagiere ich richtig auf eine Erpressermail?

Ihr habt also eine Erpressermail bekommen und fragt euch jetzt, was ihr tun sollt? Keine Sorge, ihr seid nicht allein, und es gibt klare Schritte, die ihr befolgen könnt.

Erste Schritte nach Erhalt einer Erpressermail

Was ihr tun solltet	Was ihr vermeiden solltet
Ruhe bewahren	In Panik geraten
Nicht antworten	Auf die Mail antworten
Beweise sichern	Beweise löschen

SEO-Küche Internet Marketing GmbH & Co. KG
Fraunhoferstr. 6, 83059 Kolbermoor
Telefon 08031 / 2575-100
Telefax 08031 / 2575-101
E-Mail: info@seo-kueche.de

SEO-Küche Internet Marketing GmbH & Co. KG,
HRA 11167 AG Traunstein
pers. Haftende Gesellschafterin:
SEO-Küche Verwaltungs GmbH, Kolbermoor, HRB 22414 AG Traunstein
Geschäftsführer: Christian Brunnenmayer, Patrick Keller, Oliver Lindner
Ust-IdNr.: DE 286 985 708, Steuer Nr. 156/174/08500

HypoVereinsbank
IBAN DE45 700202700015260147
BIC HYVEDEMMXXX

Bei ominösen E-Mails gilt: Ruhe bewahren.

Der erste Schock

Der erste Schock ist natürlich groß, aber es ist wichtig, einen kühlen Kopf zu bewahren. Die Erpresser setzen genau auf eure schnelle, emotionale Reaktion.

Was die Erpresser erreichen wollen

- Euch so schnell wie möglich zu einer Zahlung bewegen
- Euch dazu bringen, weitere persönliche Informationen preiszugeben
- Euch in einen Zustand der Unsicherheit und Angst versetzen

Sollte ich das Lösegeld zahlen?

Jetzt mal Butter bei die Fische: Sollte man das Lösegeld zahlen? Die klare Antwort ist: Nein!

Warum nicht zahlen?

Zahlen ist keine Garantie dafür, dass die Erpresser ihre Drohungen nicht wahr machen oder euch in Ruhe lassen. Im Gegenteil, es könnte sie sogar ermutigen, weiterzumachen.

Was ihr stattdessen tun solltet

- Keinesfalls auf Geldforderungen eingehen
- Die Erpressung bei einer Polizeidienststelle vor Ort oder bei der Onlinewache der zuständigen Landespolizei anzeigen

Wie und wo melde ich eine Erpressermail?

Gut, ihr habt also entschieden, nicht zu zahlen. Aber wie und wo meldet ihr jetzt diese unschöne Mail?

Anlaufstellen für die Meldung

Die beste Anlaufstelle ist die nächste Polizeidienststelle. Ihr könnt die Erpressung aber auch online bei

der Onlinewache der zuständigen Landespolizei melden.

Was ihr für die Meldung benötigt

- Screenshots oder Ausdrucke der Erpressermail als Beweis
- Eventuell weitere Informationen, die zur Identifizierung der Täter beitragen könnten

Wie schütze ich mich proaktiv vor Erpressermails?

Ihr wollt nicht erst reagieren, sondern gleich von vornherein sicher unterwegs sein? Klasse, Prävention ist immer der beste Schutz!

Proaktive Maßnahmen

Was ihr tun könnt	Warum es hilft
Passwort-Manager verwenden	Starke, einzigartige Passwörter für jedes Konto
Datenlecks überprüfen	Frühzeitiges Erkennen von kompromittierten Daten

Der beste Schutz ist Vorsorge

Vorbeugen ist besser als heilen, sagt man ja so schön. Und im digitalen Zeitalter gilt das mehr denn je. Ein guter Passwort-Manager und regelmäßige Checks können Dir viel Ärger ersparen.

Was ihr immer im Hinterkopf behalten solltet

- Keine gleichen Passwörter für verschiedene Konten verwenden
- Regelmäßig Software und Sicherheitsmaßnahmen aktualisieren
- Vorsichtig bei unbekannten Mails und Links sein

Welche Passwort-Manager sind empfehlenswert?

Ihr fragt euch, welcher Passwort-Manager der richtige für euch ist? Da gibt’s ein paar richtig gute Kandidaten!

Warum ein Passwort-Manager?

Ein Passwort-Manager hilft dabei, für jedes Konto ein starkes, einzigartiges Passwort zu erstellen und sicher zu speichern. So müsst ihr euch nicht zig verschiedene Passwörter merken.

Empfehlenswerte Passwort-Manager

- LastPass: Einfach zu bedienen und mit vielen Features
- Dashlane: Bietet zusätzlich einen VPN-Schutz
- 1Password: Besonders sicher durch 2-Faktor-Authentifizierung

Wie überprüfe ich, ob meine Daten im Netz kompromittiert wurden?

Ihr wollt wissen, ob eure Daten schon mal in einem Datenleck gelandet sind? Kein Problem, das lässt sich leicht herausfinden.

Tools zur Überprüfung

Es gibt spezielle Dienste wie den Identity Leak Checker des Hasso-Plattner-Instituts oder Haveibeenpwned.com, die solche Datensätze sammeln und Dir ermöglichen, eine E-Mail-Adresse daraufhin zu überprüfen.

Schritte zur Überprüfung

- Geht auf eine der genannten Websites
- Gebt eure E-Mail-Adresse ein
- Führt den Check durch und befolgt gegebenenfalls die angegebenen Schritte zur Absicherung

Was ist Phising?

Phishing ist eine Art von Cyberangriff, bei dem Betrüger versuchen, sensible Informationen wie Benutzernamen, Passwörter und Kreditkarteninformationen von Opfern zu erlangen, indem sie sich als vertrauenswürdige Einrichtung ausgeben. Dies geschieht meist über betrügerische E-Mails, Websites oder Nachrichten.

Ein typisches Beispiel: Ein Nutzer erhält eine E-Mail, die scheinbar von seiner Bank stammt, mit der Aufforderung, auf einen Link zu klicken und sich anzumelden. Der Link führt jedoch zu einer gefälschten Website, die der echten Bankenwebsite ähnlich sieht. Wenn der Nutzer seine Anmeldedaten eingibt,

werden diese vom Betrüger erfasst.

Es gibt auch fortgeschrittenere Phishing-Techniken, wie Spear-Phishing (gezielte Angriffe auf bestimmte Personen oder Organisationen) und Whaling (gezielte Phishing-Angriffe auf hochrangige Individuen).

SEO-Küche Internet Marketing GmbH & Co. KG
Fraunhoferstr. 6, 83059 Kolbermoor
Telefon 08031 / 2575-100
Telefax 08031 / 2575-101
E-Mail: info@seo-kueche.de

SEO-Küche Internet Marketing GmbH & Co. KG,
HRA 11167 AG Traunstein
pers. Haftende Gesellschafterin:
SEO-Küche Verwaltungs GmbH, Kolbermoor, HRB 22414 AG Traunstein
Geschäftsführer: Christian Brunnenmayer, Patrick Keller, Oliver Lindner
Ust-IdNr.: DE 286 985 708, Steuer Nr. 156/174/08500

HypoVereinsbank
IBAN DE45 700202700015260147
BIC HYVEDEMMXXX

SEO-Küche Internet Marketing GmbH & Co. KG
Fraunhoferstr. 6, 83059 Kolbermoor
Telefon 08031 / 2575-100
Telefax 08031 / 2575-101
E-Mail: info@seo-kueche.de

SEO-Küche Internet Marketing GmbH & Co. KG,
HRA 11167 AG Traunstein
pers. Haftende Gesellschafterin:
SEO-Küche Verwaltungs GmbH, Kolbermoor, HRB 22414 AG Traunstein
Geschäftsführer: Christian Brunnenmayer, Patrick Keller, Oliver Lindner
Ust-IdNr.: DE 286 985 708, Steuer Nr. 156/174/08500

HypoVereinsbank
IBAN DE45 700202700015260147
BIC HYVEDEMMXXX

Besonders Passwörter sollten gut geschützt werden.

Der tägliche Fake: Erpressermails im Umlauf

Beispiele für Erpressermails

Erpressermails können auf verschiedene Arten und Weisen auftreten. Hier sind einige gängige Beispiele, mit denen Internetnutzer konfrontiert werden könnten:

1. "**Ich habe dich beim Besuch einer erwachsenen Website erwischt und habe jetzt Zugriff auf deine persönlichen Daten. Wenn du nicht innerhalb von 24 Stunden eine Zahlung in Bitcoin leistest, werde ich kompromittierendes Material über dich veröffentlichen.**"

2. "**Dein Computer wurde gehackt und ich habe alle deine Passwörter abgefangen. Zahle mir eine hohe Summe in Kryptowährung oder ich werde sensible Informationen über dich an deine Kontakte weitergeben.**"

3. "**Ich kenne dein schmutziges Geheimnis und fordere Geld von dir, um es geheim zu halten. Wenn du nicht zahlst, werde ich deiner Familie davon erzählen.**"

4. "**Leider gibt es schlechte Nachrichten für Sie.**
Vor etwa einigen Monaten habe ich Zugriff auf Ihre Geräte erhalten, mit denen Sie im Internet gesurft haben.
Anschließend habe ich Ihre Internetaktivitäten verfolgt."

Diese sind nur einige Beispiele für die verschiedenen Variationen von Erpressermails da draußen. Es ist wichtig zu erkennen, dass sie oft keine Substanz haben und einfach versuchen, Angst auszulösen.

Die Taktiken der Erpresser reichen von Drohungen mit Veröffentlichungen peinlicher Informationen bis hin zur Behauptung eines gehackten Computersystems. Es gibt jedoch keinen Grund zur Panik! In den nächsten Abschnitten werden wir besprechen, wie man diese betrügerischen E-Mails identifizieren kann und was man tun sollte, falls man ihnen zum Opfer fällt.

Fazit: Erpressermails – Ein Phänomen, das man ernst, aber nicht zu

ernst nehmen sollte

So, wir sind am Ende unseres Beitrags angelangt. Was haben wir gelernt? Erpressermails sind wie ein schlechter Zaubertrick: Sie sehen gefährlich aus, sind aber meist nur Rauch und Spiegel.

Wichtige Take-aways

Was ihr wissen solltet	Was ihr tun könnt
Erpresser setzen auf Angst	Ruhe bewahren und nicht zahlen
Passwörter sind oft alt	Passwort-Manager verwenden
Meldung ist wichtig	Bei der Polizei anzeigen

Die richtige Balance finden

Es ist wichtig, eine gesunde Balance zwischen Vorsicht und Gelassenheit zu finden. Ja, ihr solltet wachsam sein und wissen, wie ihr euch schützen könnt. Aber nein, Ihr solltet euch nicht verrückt machen lassen. Die Wahrscheinlichkeit, dass die Erpresser wirklich etwas gegen euch in der Hand haben, ist gering.

Abschließende Gedanken

- Erpressermails sind unangenehm, aber meist harmlos
- Vorsorge ist der beste Schutz
- Wissen ist Macht – je mehr ihr wisst, desto sicherer seid ihr

Und damit verabschiede ich mich für heute. Ich hoffe, ihr fühlt euch jetzt ein wenig sicherer und gewappneter gegen die dunklen Seiten des Internets. Also, Kopf hoch und immer schön auf der Hut bleiben! Bis zum nächsten Mal! ?

SEO-Küche Internet Marketing GmbH & Co. KG
Fraunhoferstr. 6, 83059 Kolbermoor
Telefon 08031 / 2575-100
Telefax 08031 / 2575-101
E-Mail: info@seo-kueche.de

SEO-Küche Internet Marketing GmbH & Co. KG,
HRA 11167 AG Traunstein
pers. Haftende Gesellschafterin:
SEO-Küche Verwaltungs GmbH, Kolbermoor, HRB 22414 AG Traunstein
Geschäftsführer: Christian Brunnenmayer, Patrick Keller, Oliver Lindner
Ust-IdNr.: DE 286 985 708, Steuer Nr. 156/174/08500

HypoVereinsbank
IBAN DE45 700202700015260147
BIC HYVEDEMMXXX