# Wie erkenne ich Phishing-E-Mails und Phishing-Webseiten?


**Phishing-E-Mails und Phishing-Webseiten verfolgen vor allem das Ziel, Usern sensible Daten zu entlocken. Die Angreifer:innen werden dabei immer professioneller. Wir verraten Ihnen, wie Sie gefälschte Webseiten und E-Mails trotzdem erkennen.**

Text: Andreas Pillen





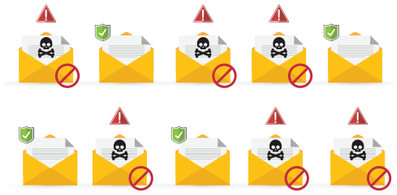
## Was bedeutet Phishing?

**Unter dem Begriff Phishing (Neologismus von fishing, engl. für "Angeln") versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdige:r Kommunikationspartner/in in einer elektronischen Kommunikation auszugeben. Ziel des Betrugs ist es, z. B. an persönliche Daten eines Internet-Benutzers zu gelangen, oder ihn zur Ausführung einer schädlichen Aktion zu bewegen.**

## Spam-Mails im Namen von Unternehmen

**Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) betrug im Februar 2022 die Spam-Ratio 4,5. Das bedeutet, dass auf 100 legitime Mails eines Unternehmens zusätzlich 450 Spam-Mails durch Externe im Namen des Unternehmens entworfen wurden.**

**Das war im Betrachtungszeitraum Juni 2021 bis Mai 2022 ein Spitzenwert. Der Durchschnitt in diesem Zeitraum lag bei Faktor 2 und ist damit auch noch erschreckend hoch: demnach kamen auf 100 legitime Mails im Durchschnitt 200 Spam-Mails.**



*Der Anteil von Phishing-Mails am Gesamtaufkommen der Spam-Mails betrug rund 30%.*

*100 legitime Mails, 200 Spam-Mails -*

***das ergibt 60 Phishing-Mails pro 100 legitime Mails.***

**Es ist also keine Frage, ob Sie bzw. Ihr Unternehmen ein Opfer einer Phishing-Mail oder einer Phishing-Webseite sein werden oder nicht.**

***Es ist lediglich die Frage, wann und mit welchen Folgen!***

**Über den Autor Andreas Pillen:**
Andreas Pillen ist Berater für Informationssicherheit und Datenschutz bei der DATATREE AG. Als Product-Owner für Phishing-Kampagnen sensibilisiert er Kund:innen durch Schulungen und speziell auf das Unternehmen ausgerichtete Kampagnen für den Schutz vor Phishing-Attacken.

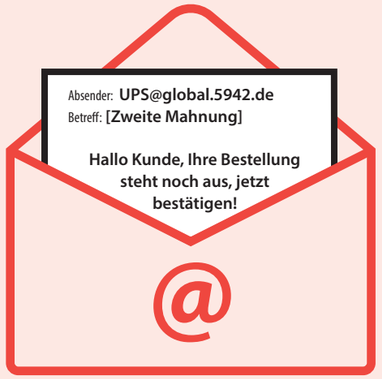
Literatur
*BSI-Lagebericht 2022, Seite 26ff*

## Wie erkenne ich eine Phishing-Mail?

**Nehmen wir als Beispiel eine Mail, die ich vor ein paar Tagen selbst erhalten habe. Hier war der vermeintliche Absender die Firma UPS.**

Zu Beginn sollte unser **gesunder Menschenverstand** walten und wir dürfen uns fragen, warum wir diese E-Mail erhalten haben. – Wenn wir kein Paket über UPS versendet haben und auch keines erwarten, sollten wir bereits jetzt skeptisch hinsichtlich des Erhalts dieser Mail sein.

**Der Absender** der Adresse lautet: UPS@global.5942.de – Für E-Mails verwendet das Unternehmen aber die Domain ups.com, wie schnell im Internet nachvollziehbar ist. Warum sollte UPS über eine Domaine @global.5492.de schreiben? – Wer Zweifel hinsichtlich der Echtheit einer E-Mail hat, kann sich auch mit dem vermeintlichen Absender, hier also UPS, über einen anderen Weg, z. B. per Telefon in Verbindung setzen und nachfragen, ob eine solche Absenderadresse vom Unternehmen überhaupt benutzt wird.




Der **Betreff** der E-Mail lautet: „[Zweite Mahnung] Hallo Kunde, Ihre Bestellung steht noch aus, jetzt bestätigen!“ Hier wird ein dringender Handlungsbedarf suggeriert, gerade auch, wenn eine „Erste Mahnung“ wissentlich nicht besteht.

Bei einem Blick auf den **Text selbst** fällt sofort die unpersönliche Anrede „Hallo Kunde“ ins Auge, wie sie bereits im Betreff benutzt wurde. Weiterhin ist der Text inhaltlich verwirrend formuliert: Der gesamte Textfluss passt nicht zu einem weltweit agierenden Global Player, der für die Erstellung seiner Texte Marketing-Expert: innen engagiert.

**Die Erklärung in diesem Fall:**
Oftmals werden Phishing-Mails oder -Webseiten im Ausland erstellt und durch Übersetzungsprogramme in die jeweilige Landessprache übersetzt. Das Ergebnis sind folglich Formulierungen, die professionell agierenden Muttersprachlern nicht zugerechnet werden können.

Bei Betrachtung mittels „Mouseover“ des **Links** hinter dem Button „Vereinbaren Sie eine Zustellung“, kommt folgende **Ziel-URL** zum Vorschein: https://jlfhjlfhljfhlfhjmiptuip.page.link/Eit5jfgdghldgjldgjl

**Auch dieser Link hat nichts mit einem Link der Firma UPS zu tun. Er ist ein eindeutiger Hinweis auf eine Phishing-Mail.**

**Klicken Sie auf gar keinen Fall auf diesen Link!**

**Haben Sie es doch getan, sind folgende Dinge zu erwarten:**

- Start des Downloads von Schadsoftware (z. B. Ransomware) auf den eigenen Rechner sowie deren Ausführung;
- Weiterleitung auf eine gefälschte Webseite von „UPS“, auf der Informationen, wie Zugangsdaten oder Daten einer Bankverbindung, abgefragt werden;
- Aufforderung zum Download von weiterer Schadsoftware, die z. B. als vermeintliche

### 5 TIPPS, wie Sie eine Phishing-E-Mail erkennen

- Gefälschte Absender-Adresse
- Abfrage vertraulicher Daten
- Vorgetäuschter „dringender“ Handlungsbedarf
- Links zu gefälschten Webseiten

## Wir nehmen Phishing-Webseiten für Sie unter die Lupe.

**So gehen wir in unserem Webseiten-Test vor:**

**Im Rahmen einer besonders gesicherten Systemumgebung machen wir uns auf den Weg, um zu erfahren, was hinter dem Link steckt.**

Auf der folgenden Seite werden sogar die Daten einer Kreditkarte (Name des Karteninhabers, Kartennummer, Gültigkeit und CVV) abgefragt, um die in der E-Mail genannte ausstehende Summe von 1,95 € an UPS zu zahlen. Der Betrag ist dabei bewusst sehr niedrig gewählt, damit wir nicht lange nachdenken, sondern schnell bezahlen.

Hätten wir alle Daten gehorsam eingegeben, hätten die Initiatoren der Phishing-Mail alle Informationen, um z. B. einen Account bei einem Online-Händler einzurichten und dann auf die von uns angegebene Kreditkarte zu bestellen. Wenn Sie also noch nie gesehen haben, wie eine Kreditkarte „raucht“, geben Sie die Informationen auf einer solchen Webseite ein. Wollen Sie aber von einem größeren finanziellen Schaden verschont bleiben, lassen Sie es lieber bleiben.

**Es gibt einige Anzeichen, an denen wir erkennen, ob wir einer Phishing-Webseite ausgesetzt sind:**
Zunächst durch die **URL.** Auch wenn die Webseite suggeriert, dass wir die Online-Präsenz eines bekannten Unternehmens besuchen, sagt die URL etwas anderes. Entweder unterscheidet sie sich grundlegend von der für das Unternehmen erwarteten URL, oder sie unterscheidet sich nur in Nuancen, z. B. durch Hinzufügen oder Weglassen einzelner Buchstaben.

**Eine nur sehr schwer zu durchschauende Methode ist dabei der Austausch von Buchstaben durch solche, die den originalen ähnlich sind. Beispielsweise kann ein „i“ durch ein „ì“ (i mit accent grave) ausgetauscht werden. Hätten Sie den Unterschied bemerkt?**

Die meisten Webseiten sind mittlerweile durch ein **SSL-Zertifikat** („https“) geschützt. Hacker versuchen jedoch, diese Zertifikate zu fälschen, um ihre Opfer in vermeintlicher Sicherheit zu wähnen. Andererseits kann es auch vorkommen, dass die gefälschten Webseiten auf SSL-Zertifikate verzichten, die beim Original vorhanden sind.
Ein weiteres Indiz dafür, dass Sie auf einer gefälschten Webseite gelandet sind, ist das **falsche Logo** oder ein Logo in einer sehr schlechten Auflösung.


**Vieles an der gefälschten Webseite macht insgesamt optisch nicht den Eindruck, sich auf der Original-Webseite aufzuhalten.**

Auf gefälschten Webseiten werden Sie oft aufgefordert, **sensible Informationen** einzugeben. Dieser Punkt ist nicht immer eindeutig. Wer als Erstkunde einen Original-Webshop besucht, wird bei der Erstellung des Nutzeraccounts aufgefordert, die Adresse anzugeben und ein Zahlungsverfahren auszuwählen. Beides wird bei wiederholten Transaktionen nicht immer neu abgefragt. Ebenso vermeiden es Banken und Kreditinstitute, im Rahmen eines Mailings bzw. im Rahmen der Reaktion darauf, die Passwörter ihrer Kund:innen in ganzer Länge abzufragen; sie beschränken sich dabei oft auf drei oder vier Ziffern („Bitte nennen Sie die ersten drei Stellen Ihrer Online-PIN.“)

Wie bereits bei Phishing-Mails, so gilt auch bei Phishing-Webseiten, dass diese **Fehler in der Grammatik und in der Rechtschreibung** aufweisen, wenn aus dem Ausland Texte mittels Übersetzungsprogramme ins Deutsche überführt werden. Aber auch solche Programme werden immer besser.

Es ist daher wichtig, immer aufmerksam zu sein und sicherzustellen, dass Sie eine gültige Webseite besuchen, bevor Sie persönliche Informationen eingeben. Recherchieren Sie im Vorfeld in einer Suchmaschine den Namen der Firma, die Sie besuchen wollen/sollen und schauen Sie sich deren URL an, bevor Sie etwas in einer Webseite eingeben, die Sie aus einer nicht gesicherten Quelle erhalten haben.

### 5 TIPPS, wie Sie eine Phishing-Website erkennen

- Unbekannte URL
- Falsche Zertifizierung
- Gefälschtes Firmenlogo
- Verlangen nach sensiblen Informationen
- Schlechte Grammatik und Rechtschreibung

## Sie haben auf eine Phishing-Mail reagiert – Was nun?

**Haben Sie nun einmal eine Phishing-Mail erhalten und einen Link wider besseren Wissens angeklickt, dann heißt es: Ruhe bewahren und einen kühlen Kopf behalten.**

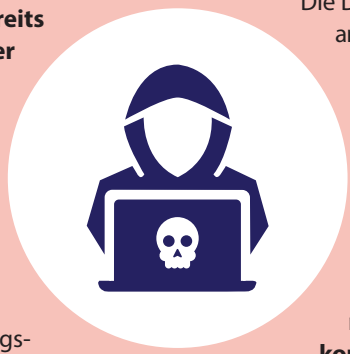
Machen Sie sich erst einmal klar, was passiert ist. Sie haben z. B. eine E-Mail erhalten. Löschen Sie diese nicht! Aus ihr kann die IT-Abteilung ableiten, was passiert ist.

**Genau das sollte Ihr nächster Schritt sein:**

- Geben Sie Ihrer IT-Abteilung Bescheid - warten Sie auf keinen Fall ab!
- Im Rahmen der Mail wurden Sie aufgefordert, auf einen Link/Button zu drücken. Der Mitarbeitende der IT-Abteilung wird dann unter anderem prüfen, ob etwas in Ihrem Download-Verzeichnis heruntergeladen wurde. Wenn ja, werden diese Dateien isoliert und später analysiert. In einem nächsten Schritt wird ein VirenScan Ihr komplettes System durchlaufen.
- Denken Sie anschließend darüber nach, wohin Sie durch die Betätigung des Buttons/Links geleitet wurden und welche Informationen Sie auf den folgenden Seiten eingegeben haben. Wurden Sie aufgefordert, Ihren Namen, private oder geschäftliche Zugangsdaten einzugeben oder wurden Sie nach Bankdaten oder sonstigen vertraulichen (Zahlungs-) Informationen gefragt?
- Wurden Sie aufgefordert, ein privates Passwort zu übertragen, ändern Sie das Passwort für den entsprechenden Account. Haben Sie dasselbe Passwort bei anderen Accounts eingesetzt, ändern Sie auch dort unverzüglich Ihre Passwörter. Hacker haben in der Regel den Verdacht, dass Sie sich auch bei anderen Accounts mit der von Ihnen eingegebenen Kombination aus User-ID und Passwort angemeldet haben.
- Haben Sie Kontodaten im Rahmen der Phishing-Webseite eingegeben, informieren Sie Ihre Bank oder Ihr Finanzinstitut und beobachten Sie regelmäßig ihre Kontenbewegungen auf ungewöhnliche Transaktionen.
- Nach der Aufbereitung und ggf. Abstimmung mit Ihrer IT-Abteilung löschen Sie die Phishing-E-Mail aus Ihrem Posteingang und alle Kopien, die Sie vielleicht davon gemacht haben.

## Sicher vor Hackern: Handlungssicherheit mit der Phishing-Kampagne

**Wir Menschen selbst sind die größte Sicherheitslücke in unseren IT-Systemen. Bereits ein Klick auf den falschen Link oder der Download einer verseuchten Datei aus einer Phishing-Mail kann Ihre komplette IT lahmlegen.**



Um das zu vermeiden, haben wir eine Phishing-Kampagne entwickelt: Wir proben mit Ihren Mitarbeitenden den Ernstfall!

Das Gute daran: Von dieser Sensibilisierungsmaßnahme profitieren Ihre Mitarbeitenden auch privat. Damit wird der Nutzen für den Einzelnen schnell begreifbar – ein Wissensgewinn, der sich wiederum positiv auf Ihr Unternehmen auswirkt!

Die Phishing-Kampagne wird individuell auf die Bedürfnisse Ihres Unternehmens erstellt. Damit alle relevanten Zielgruppen in Ihrem Haus angesprochen werden, berücksichtigen wir die Auswahl eines passenden Themas und eine optimale Terminierung der Kampagne. Wir erstellen zwei professionelle Webseiten für Sie, mit denen wir den Ernstfall mit Ihren Mitarbeitenden erproben. Im Anschluss erfolgt das Tracking des Nutzerverhaltens je Teilnehmergruppe. Die Datenverarbeitung erfolgt selbstverständlich anonym. Aus den Ergebnissen erstellen unsere Experten für Cyber-Security einen umfangreichen Abschlussbericht für Sie und Ihr Management.

**Wie geht es weiter? Gemeinsam mit Ihnen besprechen wir die Gefahren und Potenziale für Ihre Mitarbeitenden. Hieraus leiten wir einen Maßnahmenplan für Sie ab und geben Ihnen konkrete Hilfestellungen, wie Sie und Ihr Team Gefahren zukünftig vermeiden. Sprechen Sie uns an – wir helfen Ihnen, gegen Phishing-Attacken sicher zu sein!**

*Vereinbaren Sie einen unverbindlichen Beratungstermin mit unseren Phishing-Experten unter:*
**sales@datatree.ag**