Phishing

Authentisch oder nicht authentisch?

1. Ist diese E-Mail authentisch?
   - **Die Absenderadresse** *hat mit dem angeblich werbenden Unternehmen nichts zu tun.*
   - Die **Anrede** („Liebe…“) *erfolgt nicht namentlich.*
   - *Viele* **Grammatikfehler.**

   ➔ Diese E-Mail ist ***nicht echt***.

E-Mail01

➢ Die E-Mail wurde unverlangt zugestellt und enthält werbenden Inhalt. Das nennt man **Spam**.
Der Begriff SPAM stammt von einer Marke für Dosenfleisch.
Er setzt sich aus **Sp**iced h**am** (gewürztes Schinkenfleisch in Dosen) zusammen.

➢ Eine Suche mit der Formulierung „ergreifen sie diese airberlin gutschein spam“ (E-Mail02) führt zu der Meldung (Stand: September 2016):

2. Beschreibe das Ziel dieses Spammers.

   Er versucht, Inhaber von Bonuspunkten über den Link „Wählen Sie Ihr Traumziel jetzt“ zu einem gefälschten Internetauftritt zu lotsen. Dort werden Zugangsdaten abgefischt, mit denen der Betrüger dann Geld erbeuten kann.

➢ **Phishing** (von engl. „fishing“ für „Angeln“) bedeutet, einem Internetnutzer mit Hilfe einer gefälschten Webseite vertrauliche Daten zu entlocken. Als „Köder“ dienen häufig E-Mails oder Kurznachrichten. Mit den Daten kann ein Betrüger auf Kosten des Opfers Geld erbeuten.

- Du meinst, auf so etwas kann doch kein Mensch hereinfallen?

  Laut einer Berechnung des Deutschen Instituts für Wirtschaftsforschung aus dem Jahr 2015 entsteht in Deutschland ein jährlicher Schaden von **etwa 800 Millionen Euro** alleine für Privatpersonen und nur durch **Phishing** (Quelle: Deutsches Institut für Wirtschaftsforschung e.V. – DIW Berlin, https://www.diw.de/documents/publikationen/73/diw_01.c.498298.de/15-12-6.pdf, S. 301).

3. Überprüfe die E-Mail auf Authentizität.

   *Die **Absenderadresse** ist plausibel,*

   ***keine Grammatikfehler**.*

   *Es gibt zwar keine **namentliche Anrede**,*

   das ist bei so einfachen Werbemails aber

   auch nicht üblich.

   Eine missglückte persönliche Anrede

   sollte eher Verdacht erregen.

   ➔ *Die Authentizität **ist möglich**.*

E-Mail02

- Spammer versenden ihren Unfug natürlich nicht von einem persönlichen E-Mail-Account aus, sondern von *gekaperten E-Mail-Accounts* oder Fake-Accounts aus.
  Deshalb haben die **Absenderadressen** oft nichts mit dem Inhalt der E-Mail zu tun.

Verlassen kann man sich darauf aber nicht. Die Absenderangabe kann gefälscht werden!
Es gibt weiteren Methoden, die Authentizität einer E-Mail festzustellen.
Die Vorgehensweise wird hier beschrieben. Du führst die Schritte später für ein anderes Beispiel aus.

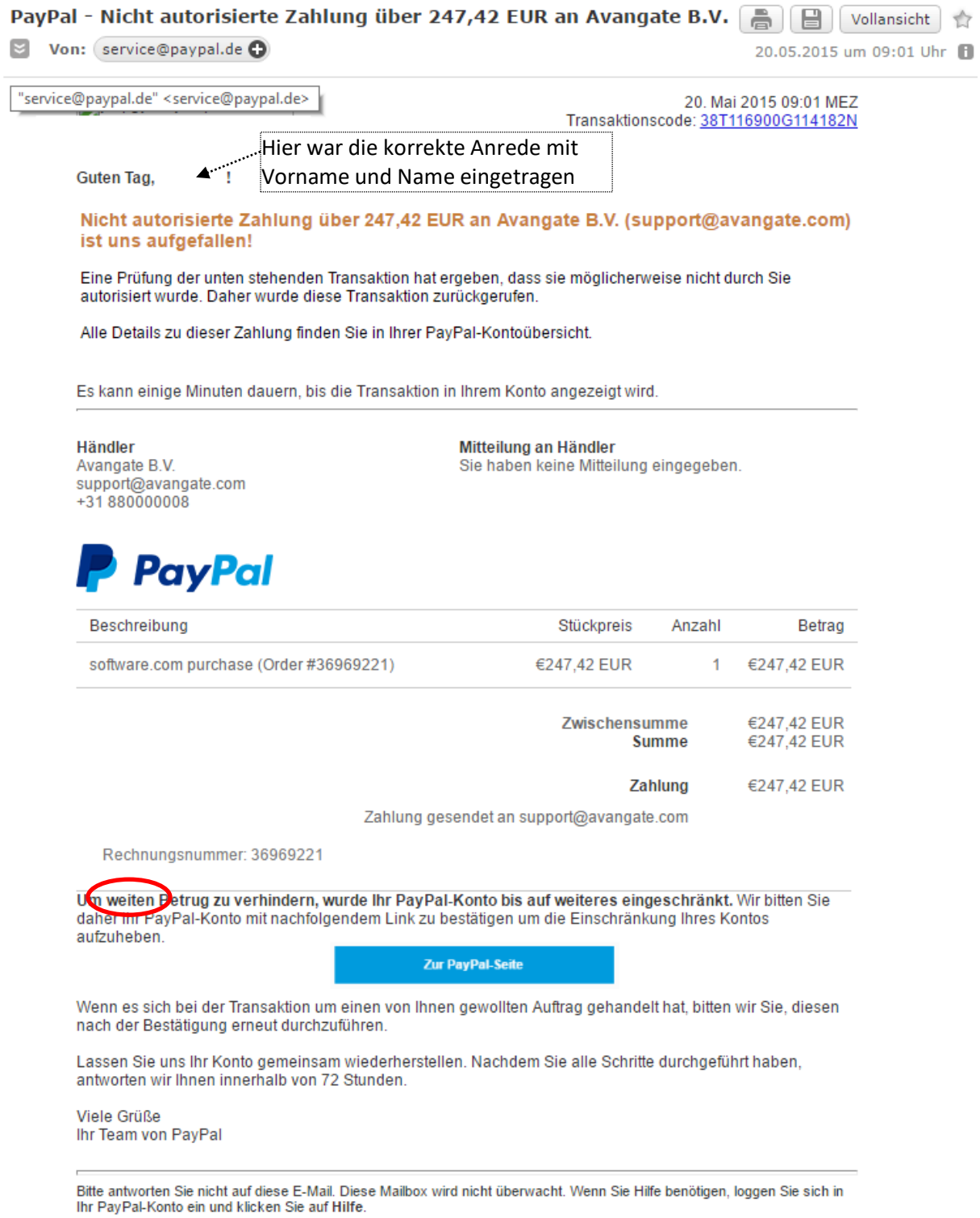
- Suche mit Hilfe einer Suchmaschine nach einer prägnanten Formulierung in der E-Mail02, ergänzt um den Suchbegriff „spam“. Begriffe in der Grafik sind nutzlos.
  (Beispiel: „airbaltic only 3 days left spam“)
  Ergebnis: Die Suche führt zu keinem Hinweis auf unerwünschte Inhalte (Stand: September 2016)
- Verwende **nicht** den Link in der E-Mail, sondern suche den Internetauftritt des angeblichen Anbieters in einem neuen Tab oder Browserfenster: Gibt es dort Hinweise auf Spam?
  Ergebnis: https://www.airbaltic.com/de-DE/index -> Suche -> „spam“
  Auch diese Suche führt zu keinem aktuellen Hinweis (Stand: September 2016)

➔ **Wenn du dir nicht sicher bist und der Inhalt der E-Mail nicht so wichtig ist, lösche die E-Mail.**

Für die beiden vorangegangenen Werbemails ist der Aufwand, die Authentizität in aller Ausführlichkeit zu prüfen, übertrieben. Wenn dir ein Sonderangebot für einen Flug entgeht, hält sich der Schaden in Grenzen.

Etwas anderes ist das bei E-Mails, bei denen der Empfänger befürchten muss, Probleme zu bekommen oder einen finanziellen Schaden zu erleiden, wenn er auf die E-Mail nicht reagiert.
Das könnten z. B. Zahlungsaufforderungen sein oder Warnungen vor verdächtigen Zahlungen.
Oft werden dann Inhalte auch dramatisch dargestellt, um die Empfänger zu verunsichern.

4. Handelt es sich bei der folgenden E-Mail um eine Warnung oder um einen Köder? Führe die oben beschriebene Vorgehensweise zur Prüfung der Authentizität aus und notiere die Ergebnisse.



PayPal - Nicht autorisierte Zahlung über 247,42 EUR an Avangate B.V.

Vollansicht

Von: service@paypal.de 20.05.2015 um 09:01 Uhr

"service@paypal.de" <service@paypal.de>

20. Mai 2015 09:01 MEZ
Transaktionscode: 38T116900G114182N

Hier war die korrekte Anrede mit Vorname und Name eingetragen

Guten Tag, !

Nicht autorisierte Zahlung über 247,42 EUR an Avangate B.V. (support@avangate.com) ist uns aufgefallen!

Eine Prüfung der unten stehenden Transaktion hat ergeben, dass sie möglicherweise nicht durch Sie autorisiert wurde. Daher wurde diese Transaktion zurückgerufen.

Alle Details zu dieser Zahlung finden Sie in Ihrer PayPal-Kontoübersicht.

Es kann einige Minuten dauern, bis die Transaktion in Ihrem Konto angezeigt wird.

Händler
Avangate B.V.
support@avangate.com
+31 880000008

Mitteilung an Händler
Sie haben keine Mitteilung eingegeben.

PayPal

Beschreibung	Stückpreis	Anzahl	Betrag
software.com purchase (Order #36969221)	€247,42 EUR	1	€247,42 EUR

Zwischensumme €247,42 EUR
Summe €247,42 EUR

Zahlung €247,42 EUR

Zahlung gesendet an support@avangate.com

Rechnungsnummer: 36969221

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.

Zur PayPal-Seite

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

Lassen Sie uns Ihr Konto gemeinsam wiederherstellen. Nachdem Sie alle Schritte durchgeführt haben, antworten wir Ihnen innerhalb von 72 Stunden.

Viele Grüße
Ihr Team von PayPal

Bitte antworten Sie nicht auf diese E-Mail. Diese Mailbox wird nicht überwacht. Wenn Sie Hilfe benötigen, loggen Sie sich in Ihr PayPal-Konto ein und klicken Sie auf **Hilfe**.

- Abgleich der Absenderadresse mit dem E-Mail-Text.

  Die Absenderadresse service@paypal.de ist plausibel.

- Überprüfen der Grammatik und Rechtschreibung.

  Grammatik und Rechtschreibung sind beinahe in Ordnung (siehe Markierung im Text der E-Mail auf der vorigen Seite).

- Klären der Notwendigkeit einer persönlichen Anrede.

  Die persönliche Anrede ist korrekt.
  Hinweis: Betrüger können Datensätze erwerben, bei denen E-Mail-Adressen und weitere persönliche Daten vorhanden sind. Diese stammen dann aus Datendiebstählen bei anderen Websites.

- Internetrecherche mit Hilfe einer Suchmaschine nach einer prägnanten Formulierung, evtl. ergänzt um den Suchbegriff „spam". Begriffe in Grafiken sind nutzlos.

  Eine Suche nach „paypal nicht autorisierte zahlung an avangate email" liefert Ergebnisse, z. B.:

  „Verbraucherschutz.de bittet die Verbraucher diese Mail sofort zu löschen,

  keinem Link zu folgen, keine Anhänge zu öffnen, und nicht auf diese Mail zu antworten!"

  (https://verbraucherschutz.de/spam-mail-angeblich-von-paypal-zahlung-avangate-b-v/)

  ➔ ***Die E-Mail sollte sofort gelöscht werden.*** *Zur Sicherheit können in einem neuen Browserfenster direkt bei PayPal die Transaktionen kontrolliert werden.*

- Internetrecherche mit Hilfe des Internetauftritts des angeblichen Anbieters. Verwende **nicht** den Link in der E-Mail, sondern öffne einen neuen Tab oder ein neues Fenster.

  Die Suche auf https://www.paypal.com/de/ gestaltet sich etwas umständlich:

  Paypal bietet keine Suche innerhalb der Website an (Stand: September 2016).

  Ganz unten auf der Startseite findet sich aber ein Link „Sicherheit".

  Dort wiederum ganz unten auf der Seite gibt es den Link „Gefälschte E-Mails (Phishing)".

  Hier finden sich allgemeine Informationen zu „Betrügerischen E-Mails:

  - *„Wir senden Ihnen nie Anhänge.*
  - *Öffnen Sie keine Anhänge in verdächtigen E-Mails, diese können Viren oder Trojaner enthalten.*
  - *Wir fordern Sie nie auf, persönliche Daten direkt auf einer Website einzugeben. Wenn wir Ihre Hilfe benötigen, fragen wir Sie immer über eine Nachricht in Ihrem PayPal-Konto."*

  (Quelle: https://www.paypal.com/de/webapps/mpp/phishing, September 2016)