erstellt von Klaus Förderer

Sicherheit bei Email's

Was ist eine SPAM Mail?

Als **Spam** [spæm] oder **Junk** (englisch für ‚Abfall' oder ‚Plunder') werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden und häufig **werbenden Inhalt** enthalten.
Es wird zwischen normalen **Spam Mails** und **Phishing Mails** unterschieden. Spam Mails werden an sehr viele Empfänger verschickt. Sie beinhalten in der Regel Werbemaßnahmen und versuchen außer viel Arbeit diese zu lesen keinerlei Risiko.

Was ist eine Phishing Mail?

Unter **Phishing** werden Versuche verstanden, über gefälschte **Internet-Adressen**, E-Mail oder Kurznachrichten an **Daten** eines **Internet-Benutzers** zu gelangen und damit Identitätsdiebstahl zu begehen, um mit den erhaltenen Daten beispielsweise **Kontoplünderung** zu begehen und den entsprechenden Personen zu schaden.
Der Begriff ist ein englisches Kunstwort, das sich an **fishing** („Angeln", „Fischen") anlehnt.

Es handelt sich meist um **kriminelle** Handlungen. **Phisher** geben sich als vertrauenswürdige Personen aus und versuchen, durch gefälschte elektronische Nachrichten an sensible Daten wie **Benutzernamen** und **Passwörter** für **Online-Banking** oder **Kreditkarteninformationen** zu gelangen.
Phishing-Nachrichten werden meist per **E-Mail** versandt und fordern den Empfänger auf, auf einer präparierten Webseite geheime Zugangsdaten preiszugeben. Versuche, der wachsenden Anzahl an Phishing-Versuchen Herr zu werden, setzen unter anderem auf geänderte Rechtsprechung, Anwendertraining und technische Hilfsmittel.

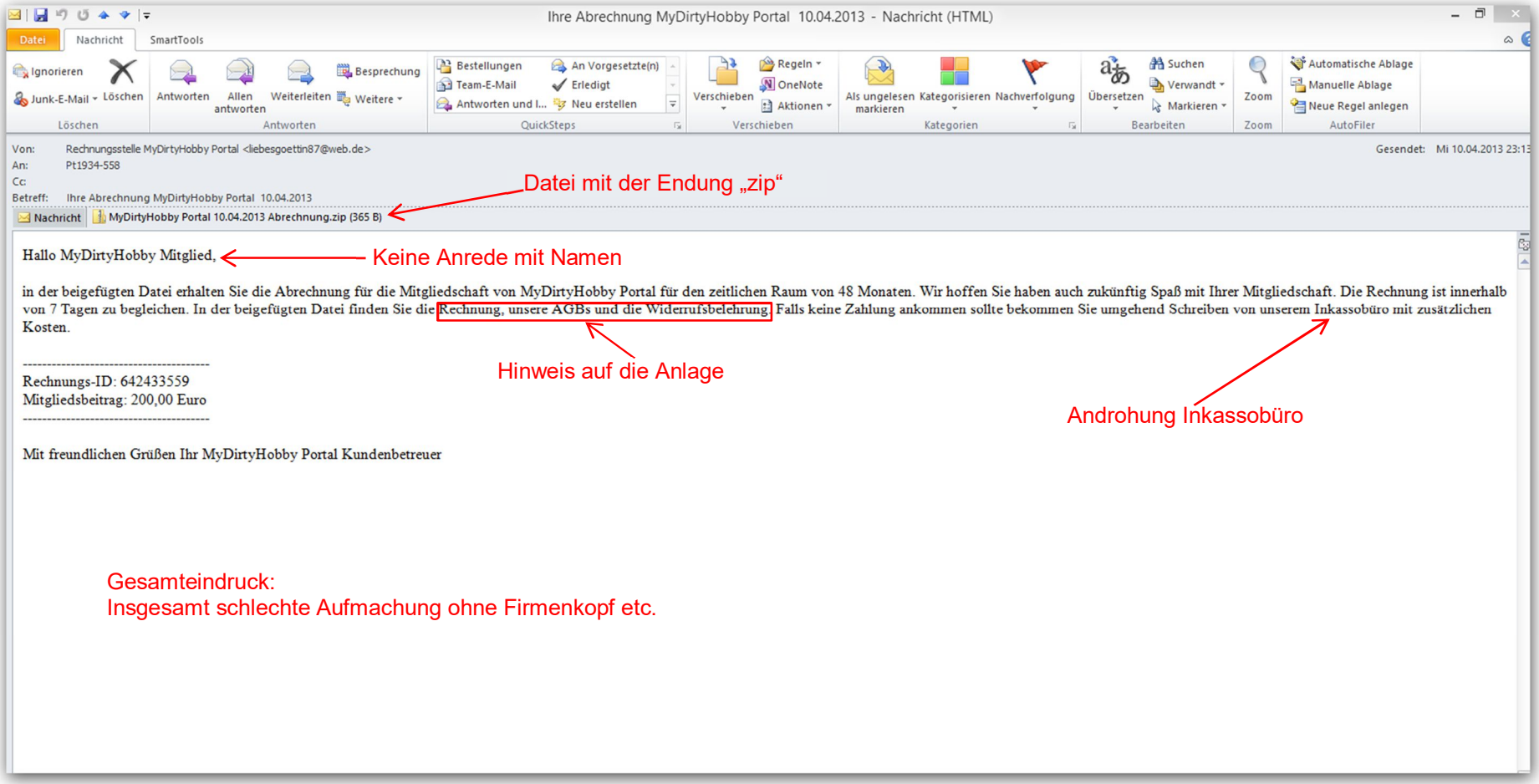
Wie erkenne ich ein Phishing Mail?

- Banken werden niemals Benutzernamen, PIN, Kontonummern, Kennwörter etc. abfragen
- Phishing Mails weisen oftmals grammatikalische Mängel auf
- Im Text der Mail wird auf die Details, die sich im Anhang der Mail befinden, hingewiesen
- Die Anlage ist meist eine Datei mit der Dateiendung „zip“
- Da diese Mail’s an beliebige Personen verschickt werden ist die Anrede meist unpersönlich. Sie werden mit „lieber Kunde“, „liebes Mitglied“ etc. angesprochen. Banken hingegen werden Sie immer direkt mit ihrem Namen anschreiben
- In der Mail wird ihnen mitgeteilt, dass sie bei nicht Einhaltung der Fristen erheblich Folgekosten tragen müssen

Tipps

- Verdächtige Mails können direkt an die Banken weitergeleitet werden. Diese haben in der Regel eine Stelle für Phishing Mails
- **MASTERCARD** wird niemals wegen Probleme mit ihren Kreditkarte mit ihnen in Kontakt treten da **MASTERCARD** **nicht** die Ausgabestelle dieser Kreditkarten ist. **MASTERCARD** genehmigt den Banken die Ausgabe von Kreditkarten mit dem Aufdruck **MASTERCARD**. Die Banken sind somit die eigentlichen Ausgabestellen dieser Kreditkarten.
- Wenn ich mir sicher bin, keinen solchen Einkauf getätigt zu haben, dann einfach alles ignorieren

Phishing Mail 1 (Zahlungsaufforderung)

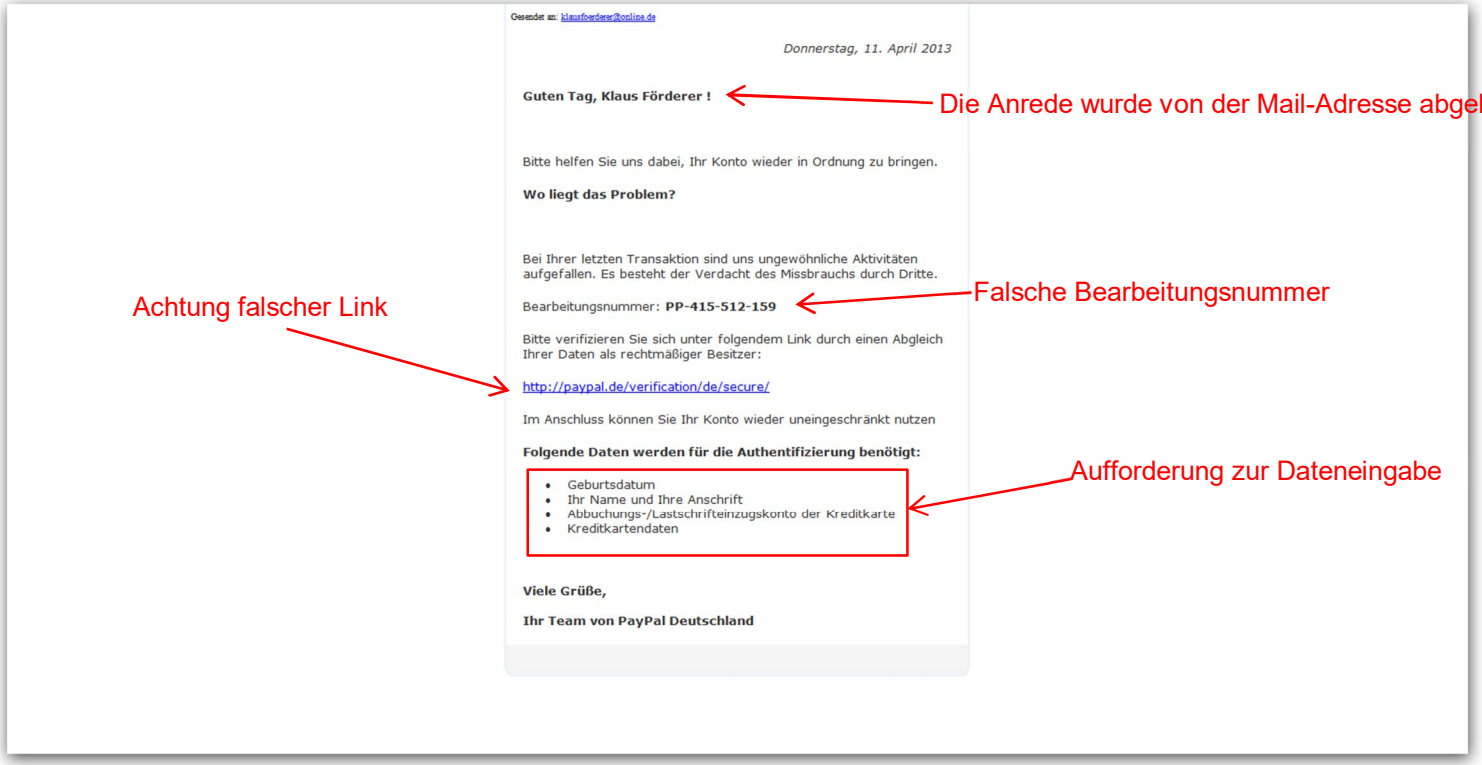


Gesamteindruck:
Insgesamt schlechte Aufmachung ohne Firmenkopf etc.

Maßnahmen:

- Mail einfach ignorieren
- Nur auf einen gerichtlichen Zahlungsbefehl reagieren, diesem muss widersprochen werden

Phishing Mail 2 (Aufforderung zur Eingabe von Daten)



Maßnahmen:

- Direktes einloggen auf der Internetseite von Paypal und prüfen ob es die angegebene Bearbeitungsnummer gibt.
- Link niemals folgen
- Mail direkt an Paypal schicken. Banken etc. haben in der Regel eine Stelle die solche Mail’s bearbeiten