Umgang mit Phishing Mails

Inhaltsverzeichnis

Was ist eine Phishing Mail?

Phishing - eine Kombination aus den englischen Wörtern "Password" und "Fishing", also "Passwort-Angeln", ist eine Methode um Nutzer dazu zu bringen, ihre persönlichen Daten (Login-Informationen, Bankdaten, Kreditkarteninformationen...) bei einem vermeintlichen, wichtigen Grund preiszugeben. Phishing nutzt also die Gutgläubigkeit/Naivität der Nutzer aus, um an sensible Informationen zu gelangen.

Dieser Artikel beschäftigt sich mit Phishing-Mails, also E-Mails, welche dem Nutzer durch gezieltes Täuschen dazu bringen sollen, sensible Informationen herauszugeben, Links in der Mail anzuklicken oder den Anhang zu entpacken(und damit wahrscheinlich Malware zu installieren).

Damit Sie nicht Opfer einer solchen Phishing-Mail werden, wird dieser Artikel alles Wichtige aufklären, damit Sie bei verdächtigen E-Mails wissen, wie Sie handeln können.

Merkmale einer Phishing Mail

Anhand dieser Merkmale lassen sich die meisten Phishing-Mails entlarven. Sollten Sie eine Mail erhalten, welche Ihnen verdächtig vorkommt, können Sie auf diese Merkmale achten. Weiterhin sehen Sie am Ende dieses Artikels ein paar Phishing-Mail Beispiele. Sie wären überrascht, wie täuschend echt diese teilweise wirken können. Beispiele von Phishing-Mails

Generell gilt aber die Faustregel: Wenn Sie sich trotz aller Merkmale noch unsicher sind, können Sie die Mail jederzeit an den NCC mit bitte um Hilfe weiterleiten. Siehe Ansprechpartner

Unbekannter Absender

Hier steckt der Teufel im Detail. Sieht die Absender-Adresse merkwürdig aus, ist Vorsicht geboten. Häufig kann es sein, das bekannt und viel genutzte Social-Media seiten wie Facebook oder Twitter, aber auch Online-Händler wie Amazon als Pseudo-Absender gewählt werden. Damit ist gemeint, das die Mailadresse aussieht, als ob diese von einer eben seriösen Seite stammen könnte, obwohl dies nicht so ist. Oft sieht sie dem Original zum täuschen ähnlich, wie zum Beispiel:

- noreply@**amzon**.com anstelle von noreply@**amazon**.com

Bei genauem hinschauen lässt sich soetwas erkennen. Häufig werden auch ähnliche Zeichen miteinander vertauscht. Bei Schrifarten wie Arial sehen sich die "1" und "l" sehr ähnlich.

Allerdings ist dies als alleinstehendes Merkmal nicht sonderlich verlässlich, da auch bekannte Kontakte gehackt sein können. Seien Sie daher Misstrauisch bei E-Mails, welche Sie auffordern, Seiten zu öffnen ("Schau mal, wo ich dich verlinkt habe ..." oder "Ich habe hier ein Bild von dir geteilt").

Fehlende persönliche Anrede

Ihre Bank oder andere Geschäftspartner sprechen Sie in E-Mails grundsätzlich mit ihrem persönlichem Namen an und nicht mit "Sehr geehrter Kunde" oder "Sehr geehrter Nutzer". Hier sollte beachtet werden, das besonders geschickte Phishing-Angreifer ihren Namen bereits herausgefunden haben könnten.

Ausübung von Zeitdruck oder dringender Handlungsbedarf

Es ist eine beliebte Taktik, das Opfer durch eine kurze Frist zur vorschnellen Handlung zu bewegen. Androhung zur Kontosperrung, Inkassounternehmen o.Ä. sind nur ein paar Beispiele. Seien Sie bei solchen Dingen misstrauisch, es wird darauf gesetzt, dass das Opfer unter Zeitdruck unüberlegt handelt.

Dateneingabe

Kommen Sie aufforderungen, sensible persönliche Daten wie Benutzername/Passwort, PINs oder TANs einzugeben nicht nach! Banken sowie Online-Zahlungsdienste werden Sie niemals per Mail bitten diese einzugeben. Dies gilt natürlich auch für vermeintliche Hochschul-Mails. Mitarbeiter der Hochschule und des NCC werden Sie nie nach ihrem Passwort fragen!

Dateianhänge

Seien Sie wachsam bei Dateianhängen. Häufig versteckt sich in der angehängten Datei ein Virus oder Trojaner. Die Anhänge haben oft keinen richtigen Namen und tarnen sich als Bild, PDF oder gar Word/Excel - Datei. Auch in einer verpackten Archivdatei .zip oder .rar kann sich Malware befinden. Wenn Sie eine E-Mail mit einem verdächtigen Anhang erhalten haben und sich unsicher sind, leiten Sie diese einfach an den NCC weiter. Vor allem

wenn es für den Absender eher untypisch ist, Ihnen solche Mails zu schicken. Sollte der Absender ein Bekannter sein, fragen Sie am besten persönlich nach!

Ungewöhnliche Formatierung

Oft werden Phishing-Mails in Englisch oder einer anderen Fremdsprache verfasst und automatisiert auf Deutsch übersetzt. Dies führt dazu, das die Formatierung, der Satzbau oder die Grammatik ungewöhnlich schlecht sind oder die Mail in "Denglisch", also eine Mischung aus Deutsch und Englisch, geschrieben ist.

Hilfsfragen zur Selbstkontrolle

- Kenne ich den Absender / Stimmt die Absender-Adresse?
- Stimmt die Anrede und die Formatierung?
- Werde ich aufgefordert, sensible Daten preiszugeben?
- Wird dringender Handlungsbedarf vorgetäuscht?
- Enthält die E-Mail Verlinkungen, die auf andere Webseiten verweisen? Welche Ziel-URL wird bei einem Mouseover angezeigt?

Überprüfung des Mail-Headers

Der sog. "Header" sozusagen die "Kopfzeile" einer E-Mail enthält Informationen und genaue Details über die dazugehörige E-Mail. Den Mail-Header zu überprüfen ist eine gute Methode um gefälschte Absenderadressen aufzudecken.

Als erstes müssen Sie sich den Mail-Header anzeigen lassen. Öffnen Sie die E-Mail in einem eigenem Fenster. In dem Mailprogramm Thunderbird können Sie nun bei den Aktions-Buttons rechts vom Absender auf "Mehr" und anschließend "Quelltext anzeigen". Damit wird Ihnen der Mail-Header in einem neuem Fenster angezeigt.

Bei Microsoft Outlook öffnen Sie ebenfalls die E-Mail als eigenes Fenster und klicken auf "Datei" und anschließend auf "Eigenschaften". Dort finden Sie die Option "Internetkopfzeile anzeigen".

Im Mail-Header stehen viele nützliche Informationen. Auf folgende Einträge sollten Sie einen Blick werfen:

- **Return-Path**: Hier finden Sie den Absender. Steht hier eine kryptische E-Mail, kann dies bereits ein Hinweis auf eine Phishing-Mail sein. Allerdings ist dieser Eintrag manipulierbar, also könnte auch eine seriöse E-Mail abgebildet sein.

- **Recieved from**: Die IP-Adresse des Absenders ist hier hinterlegt. Der Absender-Server ist eindeutig kenntlich gemacht und die IP-Adresse in eckigen Klammern dahinter aufgelistet. Der Name des Servers muss allerdings nicht stimmen - aber mit der IP-Adresse lässt sich überprüfen, ob der Name des Servers und die IP-Adresse übereinstimmen. Damit kann herausgefunden werden, woher die E-Mail wirklich kommt.

Dabei gehen Sie wie folgt vor:

Öffnen Sie eine Kommandozeile ihrer Wahl. Unter Windows beispielsweise klicken Sie in der Taskleiste unten links auf "Start" und tippen "cmd" ein. Damit öffnet sich die Windows-Kommandozeile. Unter Linux reicht das normale Terminal. Anschließend geben Sie folgenden Befehl ein:

```
nslookup <IP-Adresse>
```

nslookup steht für "Name Server lookup" und dient dazu, bei DNS-Servern anzufragen welcher Server hinter einer IP-Adresse steckt und umgekehrt. Sie erhalten eine Ausgabe in der zuerst ihr Server und IP-Adresse angegeben wird, von dem Sie die Anfrage gestartet haben, und anschließend die angefragte IP-Adresse und den zugehörigen Server. Das sieht zum Beispiel so aus:

```
nslookup 8.8.8.8

Name:    google-public-dns-a.google.com
Address:  8.8.8.8
```

Somit lässt sich in diesem Beispiel feststellen, das die IP-Adresse 8.8.8.8 zu Google.com gehört.

Was kann ich als Phishing-Opfer tun?

Falls Sie vermuten, Opfer einer Phishing-Mail gewesen zu sein, lassen Sie ihre Daten **unverzüglich** vom Original-Anbieter prüfen.

Unterbrechen Sie die Verbindung zum Internet. Falls Malware installiert wurde wird diese höchstwahrscheinlich Daten an den Hacker schicken.

Ändern Sie sofort sämtliche Zugangsdaten, wie Nutzername und Passwort. Sollten Sie einen Passwortmanager installiert haben, empfiehlt es sich, **sämtliche** Passwörter zu ändern, die sie im Manager abgespeichert haben.

Wenn Sie **Antivirensoftware** installiert haben, scannen Sie ihren Computer nach **Malware**.

Ansprechpartner

Sollten Sie eine verdächtige Mail erhalten haben, zögern Sie nicht und melden sich beim NCC. Wir helfen Ihnen gerne weiter.

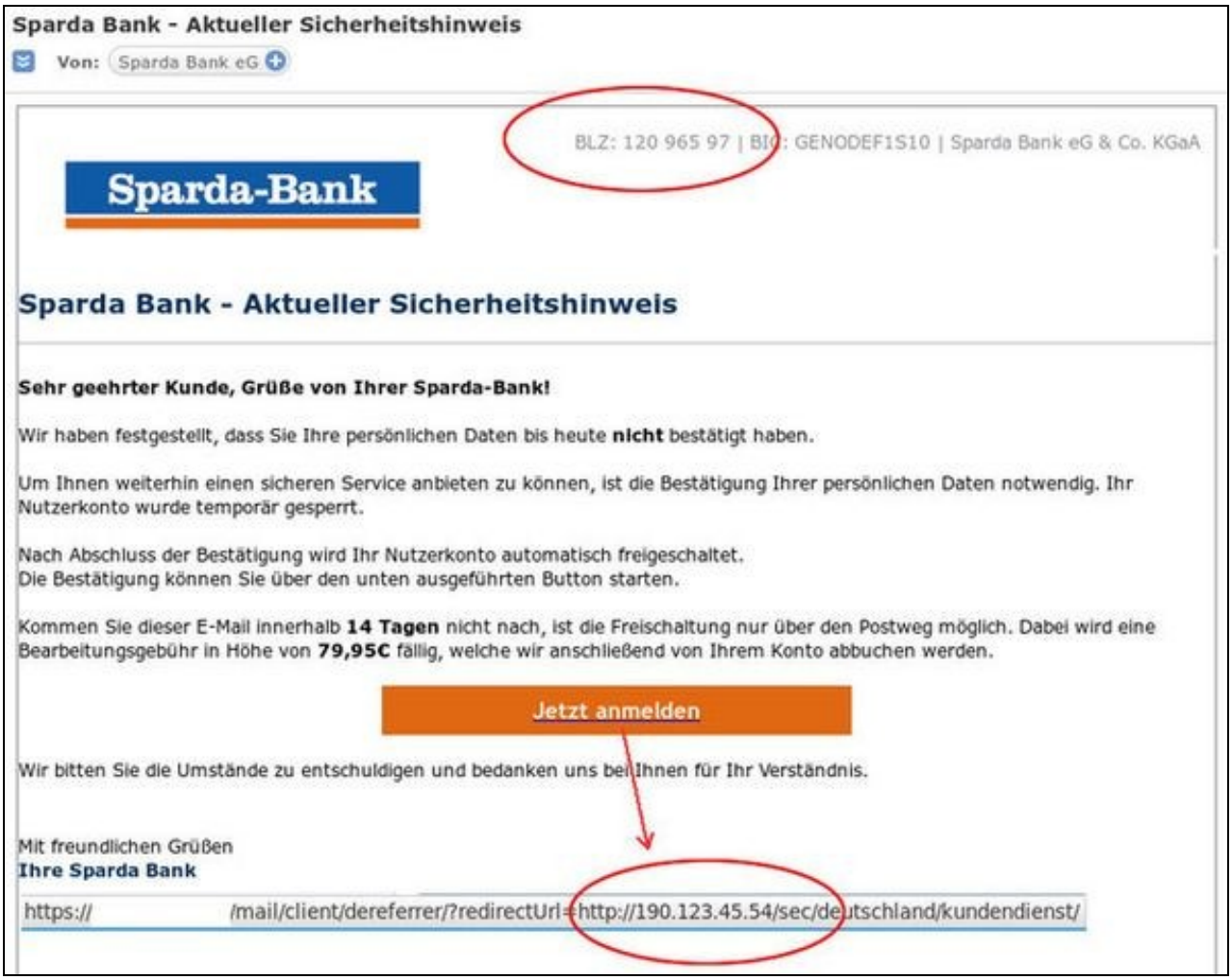
Hier können Sie uns erreichen:

- Mail: service@hs-mittweida.de
- Tel.: +49 3727 58-1410

Alternativ finden Sie hier ein Kontaktformular.

Beispiele von Phishing-Mails

Wir weisen darauf hin, dass auch Kunden anderer als der hier beispielhaft aufgeführten Banken und E-Commerce Unternehmen Opfer von Phishing-Angriffen werden können. Dies sind nur Beispiele.



Merkmale:

- Keine Formale und persönliche Anrede
- Aufforderung zur sofortigen Zahlung, Nutzer wird unter vermeintlichen Zugzwang gesetzt
- Verdächtig hohe Kosten für trivialen Aufwand
- Aufforderung zur Online-Anmeldung(übergabe persönlicher Daten)
- Link führt zu einer völlig anderen Seite
- Angegebene BLZ ist von einer anderen Bankfiliale

Sollten Sie jemals eine solche Mail - welche durchaus auf den ersten Blick seriös wirkt - erhalten, ist es am besten direkt bei der Bank anzurufen, oder beim nächsten Kundencenter persönlich vorbeizuschauen und sich dort zu informieren. Damit helfen Sie nicht nur sich selbst, sondern weisen die Bank auch darauf hin das ein Betrüger unterwegs ist, und die Bank kann nun auch andere Nutzer warnen.

eBay Mitteilung

Phishing-E-Mail

Lieber eBay Benutzer,

Nach Betrugbeanstandungen von den eBay Mitgliedern, hatte eBay Inc. ein ein Sicherheit Programm gegen die fraudulend Versuche der Kontodiebstähle entwickelt. Für das müssen wir securise alle Mitgliedsinformationen, indem wir die eingetragenen Informationen aktualisieren und überprüfen. Bestätigen Sie bitte Ihre Informationen, indem Sie die Form von der Verbindung unten ausfüllen, also können wir Ihre Kontogültigkeit und Ihre Identität überprüfen :

http://signin.ebay.de/aw-cgi/eBayISAPI.dll?SignIn&ssPageName=h:h:sin:eBayproblems

Bitte LOGON zu eBay zwecks Ihre Informationen aktualisieren.

Dieser process Prozeß dauert 5 Tage , Periode, als Sie nicht in der LageSIND, Ihr eBay Konto zugänglich zu machen. Nachdem diese Periode Sie Anweisungen hereinzukommen und securise Ihr eBay Konto empfangen.

Wie in unserer Benutzer-Vereinbarung skizziert schicken, eBay Wille Ihnen Informationen über Aufstellungsortänderungen und verbesserungen regelmäßig.
Besuchen Sie unsere privacy policy und Benutzer-Vereinbarung wenn Sie irgendwelche Fragen haben.

[mailto:support_num_[redacted]@sparkasse.de]
Gesendet: Freitag, 9. September 2005 00:05
An: [redacted]
Betreff: SPARKASSE ONLINE-BANKING [Thu, 08 Sep 2005 15:10:39 -0700]

Sparkasse

Sehr geehrte Kundin, sehr geehrter Kunde,

Der technische Dienst der Bank fuhrt die planmassige Aktualisierung der Software durch Fur die Aktualisierung der Kundendatenbank ist es notig, Ihre Bankdaten erneut zu bestatigen. Dafuer mussen Sie unseren Link (unten) besuchen, wo Ihnen eine spezielle Form zum Ausfullen angeboten wird.

https://www.sparkasse.de/firmenkunden/B_electronic-banking/online_banking_cud.html

Diese Anweisung wird an allen Bankkunden gesandt und ist zum Erfullen erforderlich.

Wir bitten um Verstandnis und bedanken uns fur die Zusammenarbeit