

Phishing-E-Mails

E-Mails

Immer häufiger hört man davon, dass jmd kuriose E-Mails von dubiosen Absendern erhalten hat. Das Problem dabei ist nur leider, dass die Betrüger immer geschickter werden und deren E-Mails immer originaler aussehen. Oft müssen Experten auch schon ganz genau hinschauen um solche E-Mails zu identifizieren.

Hier mal ein paar Beispiele:

Mögliche Schritte zur Überprüfung von E-Mails

1. Wer ist der Absender?
2. Prüft ob ihr überhaupt Kunde bei der Firma seid, die euch eine Rechnung schickt.
3. Sind Links in der E-Mail enthalten, die auf merkwürdige Seite verlinken?
4. Sind Anhänge in komprimierter Form von ZIP, RAR, 7z o.a. enthalten?

Bestätigung einer Zahlung

[Zahlung_Phishing.png](#)
Image not found. Sorry, type is unknown

1. Wer ist der Absender? 1.1 Absender E-Mailadresse überprüfen, kennt man die? Sieht sie kryptisch aus? Z.B. „rechnung123456@qjadjk.curzdh.ru“ sieht alles andere aus als seriös. In dem Beispiel sieht man den Absender „403341355@“.

Ich denke nicht, dass die Volksbank Rechnungen verschickt von einer Domain namens „tuchachalm.de“.

2. Prüft ob ihr überhaupt Kunde bei der Firma seid, die euch eine Rechnung schickt. Oft höre ich aus Familien- und Freundeskreisen, dass Rechnungen per E-Mail eintrudeln von Firmen wo die Leute gar nicht Kunde sind.

Wenn nicht, löscht einfach die E-Mail.

3. Sind Links in der E-Mail enthalten? Oft ist die Betrugsmasche so, dass ein Link geschickt wird. (siehe Bild oben)

Bei solchen Versuchen kann man oft klar erkennen, dass es sich um einen Betrug handelt. Oft endet der Link auf „.zip“ oder noch besser „.zip.exe“.

In den meisten Fällen enthalten ZIP Dateien Viren, die den Rechner befallen sollen.
Wenn man mit dem Mauszeiger mal über den Link „fliegt“ und dann unten links im Outlook oder im Internetbrowser schaut, sieht man die Seite wo man hingeleitet werden soll.
In unserem Beispiel wollten die Betrüger mich auf folgende Seite weiterleiten:

[„http://cizimmasasi.com.tr/wp-content/themes/twentythirteen/data_protection_officer_volksbank“](http://cizimmasasi.com.tr/wp-content/themes/twentythirteen/data_protection_officer_volksbank)

Wenn man schon auf solche seltsamen Webseiten mit der Endung „.com.tr“ weitergeleitet wird, ist der Betrug schon deutlich zu erkennen. Mal abgesehen von dem Namen der Website „cizimmasasi“.

Entweder werden Rechnungen als PDF im Anhang mitgeschickt oder ihr werdet gebeten euch bei dem Onlineshop einzuloggen und über euer Kundenkonto die aktuelle Rechnung anzuschauen.
Und wenn ihr euch immer noch unsicher seid habt ihr 2 Optionen:

1. Löscht die E-Mail. Wenn jmd eine offene Forderung euch gegenüber hat, wird sich derjenige schon per Post melden.
2. Fragt Stephan oder mich einfach und wir prüfen dann betreffenden E-Mails.

Paypal Beispiel

Diese Woche erreichte mich eine sog. Phishing E-Mail eines Kumpels, die richtig gut war!
Auf dem Bild steht schon mal info@paypal.de , da könnte man annehmen, dass die E-Mail von Paypal selber kommt.
Weiter schreiben die Betrüger, dass in seinem Account die Adresse geändert wurde auf irgendeine Adresse in Hamburg.
Dort wohnt er aber nicht und er hat auch so nichts mit der genannten Adresse zu tun.
Dann wird wie gewohnt ein Link platziert wo man drauf klicken soll um in einem Formular seine Daten einzugeben um das Konto zu verifizieren.
Dieser Link verweist wieder mal auf eine Betrüger Website.
Für den Laien sieht alles echt aus, aber Achtung!
Eine Internetadresse verweist ja immer auf eine Domain, z.B. die Domain google.de oder amazon.de.
Als Besitzer einer Domain kann man aber sog. Subdomains (Unterdomains) anlegen und benutzen um seine Prozesse zu strukturieren.
Man könnte z.B. im Shoppingbereich für den Vertrieb die Subdomain Vertrieb erstellen, das würde dann so aussehen: "vertrieb.shop.de"
Hier versuchen die Betrüger dem Laien vorzugaukeln man würde auf die originale Paypal.com Seite weiterleiten. Denn der Link beinhaltet „paypal.com.secure-team.net“. Die eigentliche Domain ist aber „secure-team.net“. „paypal.com.“ sind nur Subdomains.
Was mir auch aufgefallen ist, sind die angeblichen Links zu dem „Hilfe-Center“ und dem „Sicherheits-Center“ in dem unteren Bereich.
Das sind nämlich keine Verlinkungen, sondern lediglich formatierter Text.

Mittlerweile ist die Website wo man seine Daten eingeben soll schon gar nicht mehr online.

[Paypal_Phishing.png](#)

Image not found or type unknown

Amazon Beispiel

Hier mal noch ein einfaches Beispiel, dass nicht gut gemacht wurde von den Betrügern. Hier sieht man bei allen rot markierten Sachen Fehler oder nicht seriöse Infos.

1. Am oberen Rand sieht man ganz deutlich eine Internetadresse (Domain) namens **bunpork9.com**, die definitiv nicht zu Amazon gehört.
2. Die Anrede ist fehlerhaft. Erstens ist mein Name mit Vor- und Nachnamen angegeben und dann auch noch klein geschrieben. Der Vorname hat hier normalerweise nix zu suchen.
3. Der ominöse, orange hinterlegte Link enthält eine Verlinkung auf einen Internetanbieter, der sehr lange Internetadressen verkürzt. Prinzipiell ist das nichts schlechtes aber so etwas ist mir noch nie in einer Amazon, ebay oder Paypal E-Mail untergekommen.

[Amazon_Phishing.png](#)

Image not found or type unknown

Wie ihr seht lässt sich dieses Beispiel schnell analysieren und als Phishing - Betrug identifizieren.

Sparkasse Beispiel

Heute erreichte mich auf der Firmen E-Mail Adresse eine Phishing E-Mail, die so gebaut wurde, dass sie aussieht als wäre sie von der Sparkasse geschickt wurden.

An dem Beispiel kann man genauso gut wieder die typischsten Merkmale einer Phishing E-Mail zeigen.

1. Absender E-Mail: Die Domäne "support.com" hat überhaupt nichts mit der Sparkasse zu tun. Die Sparkasse nutzt ihre eigene Domäne "sparkasse.de" oder speziell für ein Bundesland "spk-burgenlandkreis.de".
2. Anrede: Die Anrede ist wieder absolut beispielhaft! Sie ist total neutral gehalten. Auch bei automatisch generierten E-Mails wird man in der Regel mit Namen angesprochen. Sicherlich gibt es Ausnahmen aber das hier sollte euch immer erstmal stutzig machen.
3. merkwürdige Verlinkungen: Hier haben wir mal ein Beispiel, das ich persönlich nicht so oft bekomme. Der gesamte Inhalt der E-Mail ist als Bild verankert und als Verlinkung auf eine Internetseite eingebaut. Somit wollen die Betrüger erzwingen, dass man immer auf die Seite weitergeführt wird - egal wohin man klickt.

[Phishing-Sparkasse.png](#)

Image not found or type unknown

Revision #5

Created 16 September 2018 20:43:50 by Mario

Updated 17 July 2020 08:57:54 by David