

Hinweise zur Erkennung von Fake- oder Spam-Mails

Da uns in letzter Zeit immer mehr Spam Mails erreichen, welche potentiell gefährliche Links beinhalten, möchten wir euch ein paar Tipps geben, um diese Mails in Zukunft besser zu erkennen.

Zunächst als Erklärung:

Ein potentiell gefährlicher Link ist nicht direkt einhergehend mit dem Download einer Schadsoftware durch einen solchen Link. Vielmehr steckt im Regelfall eine Aufforderung dahinter selbst Daten und Passwörter einzugeben, welche später ggf. für eine Attacke verwendet werden könnten.

Zu 99% ist nicht der Link gefährlich, sondern die Person, die den Link anklickt und anschließend diverse Eingaben tätigt, oder einen Download aktiv anstößt.

Grundsätzlich sollte sich jeder beim Aufrufen eines Links innerhalb einer Mail selbst hinterfragen, ob es überhaupt einen Sinn ergibt, dass diese Daten von einem abgefragt werden bzw. überhaupt etwas im Internet aufgerufen werden soll.

Generell würde kein seriöser Kunde, Anbieter oder auch wir selbst, verlangen ohne weiteres auf einer Internetseite Daten jeglicher Art einzugeben.

Zur Erkennung von fake- bzw. Spam-Mails:

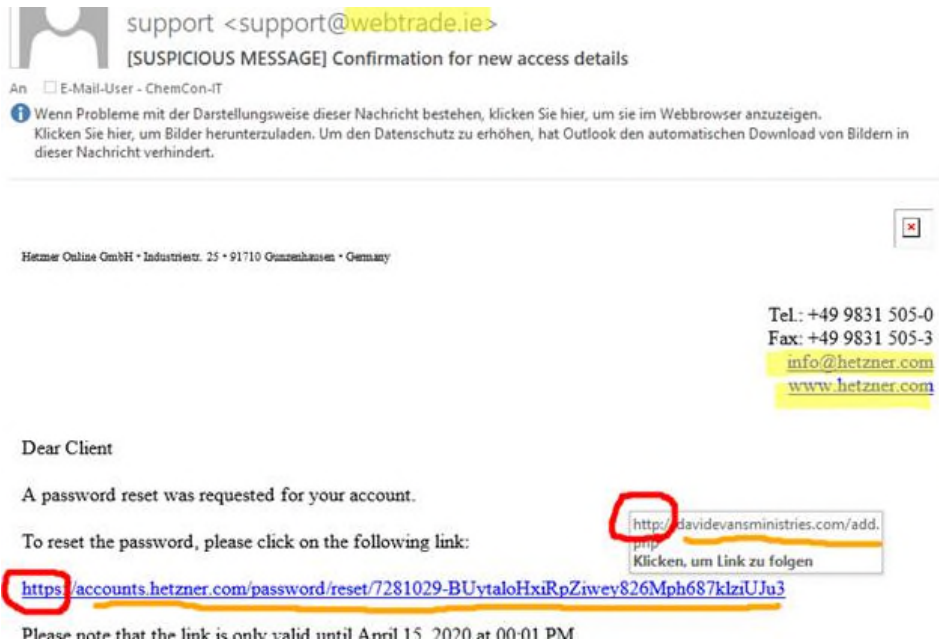
1. Bitte werft einen ersten Blick auf die direkte Absenderadresse. Achtet hierbei zunächst nicht auf den angezeigten Namen vor der Adresse, sondern auf die Adresse selbst.
 - Macht diese Adresse überhaupt Sinn?
 - Ist sie mir bekannt?
 - Hat Sie eine verdächtige Domain Endung? (@*****.net.ae ; @*****.hinet.net)
 - Steht die angezeigte Adresse in einem vernünftigen Zusammenhang mit dem davor angezeigten Absender? (Bekannter Name zu vollkommen anderer Adresse dahinter)
2. Wie ist der Eindruck der Mail insgesamt? Oftmals machen Spam Mails direkt einen unseriösen Eindruck. Das gesamte Design wirkt unprofessionell, ungewöhnliche Schriftarten werden verwendet, der Textaufbau wirkt schlecht, oder ungewöhnlich strukturiert.
3. Wie steht es um die Rechtschreibung im geschriebenen Text? Sicherlich unterlaufen jedem Fehler. Jedoch keine 10 in 3 Sätzen.
4. Bei bestehenden Kunden, Lieferanten, Dienstleister etc. kann man auch davon ausgehen, dass eine Anrede einen Ansprechpartner enthält. Nicht nur einfach „Guten Tag“ oder ähnliches da steht.
5. Spam Mails enthalten im Regelfall mindestens einen Link.
 - Überprüft Links in den Mails bitte indem ihr mit dem Mauszeiger über den Link fahrt. Nach einem kurzen Moment wird euch die tatsächliche Linkadresse angezeigt.
 - Spätestens hier sind nahezu alle fake Links leicht zu erkennen.
 - Achtet darauf, ob der tatsächliche angezeigte Link mit dem Geschriebenen im Text übereinstimmt. Oftmals sind diese komplett unterschiedlich, oder unterscheiden sich in besonders gemeinen Fällen durch so etwas wie den Austausch eines Buchstaben O mit der Zahl 0.
 - Des Weiteren beginnt der angezeigte Link sehr häufig mit http:// statt https://
 - Das fehlende „s“ ist hier extrem wichtig. Das „s“ signalisiert eine Verschlüsselung.
 - Linkadressen die mit http:// ohne das „s“ beginnen sollten generell gemieden werden!
 - Es gibt hier Ausnahmen, diese sind jedoch extrem selten, daher an dieser Stelle ein generelles NEIN.
6. Hinterfragt euch grundsätzlich selbst! Der beste Schutz ist eine generelle Skepsis.

Beispiel 1:

Absende-E-Mail-Adresse passt nicht zum angeblichen Auftraggeber „Hetzner“. Hetzner hat eine eigene Domain. Wird diese also auch in den E-Mail-Adressen verwenden (siehe Gelbmarkierung)

Offensichtlicher Link beginnt mit https:// ... aber fährt man ohne anzuklicken mit dem Mauszeiger drauf, wird eine http:// - Adresse angezeigt (siehe Rotmarkierung)

Und die tatsächlich hinterlegte Adresse weicht komplett von der vorgeschlagenen https://-Adresse ab (siehe Orangemarkierung)



Beispiel 2:

Sämtliche E-Mails von Chemcon-Systemen haben als Absender „...@chemcon.com“ und sind in 99,9999 % der Fälle nicht in Englisch verfasst.

Im nachfolgenden Beispiel sieht man, dass diese 2 Faktoren nicht zu treffen.

Zwar steht im Anzeigenamen unter „Von:“ chemcon.com support, aber in der eigentlichen E-Mail-Adresse dahinter, eine Adresse, die nichts mit Chemcon zu tun hat.

Von: chemcon.com support [mailto:support@erscateringequipment.com.au]
Gesendet: Montag, 6. Juli 2020 07:38
An: [REDACTED]
Betreff: Your firewall prevented some email delivery

Dear [REDACTED]

E-mail Quarantine

Your security system has prevented the delivery of (3) new emails to your inbox. You can review these messages and choose what happens to them within your email quarantine portal.

[Click here to review messages](#)

Emails will be deleted automatically within 24hrs.

Subject	Date (UTC) Time	
Payment confirmation	07/05/2020 11:38:05 pm	
DHL Express (missed delivery)	07/05/2020 11:38:05 pm	

Zudem hat ein Spam-Appliance-System keinen Quarantäne-Pool auf den der einzelne User selbst zugreifen kann. Warum sollte die Spam erst geblockt werden, wenn der User sie dann doch selbst holen kann.

Auf nachfolgender Seite noch ein Beispiel für Phishing-Mails.

Hierzu noch der Hinweis, dass Raphael interne Mails nicht auf englisch schreibt.

Von: Raphael Vogler <preshyberryluxuryapartments@gmail.com>
Gesendet: Freitag, 5. April 2024 12:47
An: [REDACTED] <[REDACTED]@chemcon.com>
Betreff: CONFIDENTIAL: For Your Reference Only

***** Warnung: Externe Nachricht - Links und Anhänge vor dem Öffnen prüfen *****

Dear Employee,

After our initial meeting with the management Board, we decided to change all employees code of conduct.

Due to:

- *Employees Behaviors
- *Employees Work Rate
- *Clients Analysis
- *Upcoming quarterly Bonus

This code of conduct was changed for the upcoming quarterly bonus in regard to employees work rate.
Please read the attached PDF carefully, there are some significant changes, and all instructions must be strictly adhered to for you to claim the 1st quarter employee bonus.

Best Regards,

Raphael Vogler
CEO/President

Im Klartext steht zwar Raphael Vogler, aber es ist offensichtlich, dass der wirkliche Absender ein anderer ist (preshyberryluxuryapartments@...)

Antworten Allen antworten Weiterleiten



Do 18.11.2021 03:10

chemcon.com - Scanned Files <xerors@cabillupdate.info>

Helpdesk Scanned : [Xerox Multifunction device-ID]

An Frey, Georg, Dr., ChemCon

Hello Georg.Frey,

Attachment File Type: PDF/HTML

Number of Images: 11

[Please Preview Scanned Documents File Here](#)

Device Name: DocuCentre-SCANFX-2EFF73

Device Location: Frontdesk chemcon.com

Thank you for using Xerox Scanner for secured Documents

Im Klartext steht zwar Chemcon, aber es ist offensichtlich, dass der wirkliche Absender ein anderer ist (... M.msciadri.....).

Von: Chemcon.com - IT <m.msciadri@innovagram.com>
Gesendet: Freitag, 9. Juli 2021 00:36
An: Woydt, Michael Dr., ChemCon <Michael.Woydt@chemcon.com>
Betreff: MANDATE: Account Process Thursday, July 8, 2021
Priorität: Hoch

Outlook Web App

Hello michael.woydt,

We've noticed that michael.woydt@chemcon.com have not confirmed the email address associated with your Outlook Web App account.

You're getting this email to make sure it is you that has the account.

[Confirm Account](#)

Regards,
The Mail Team

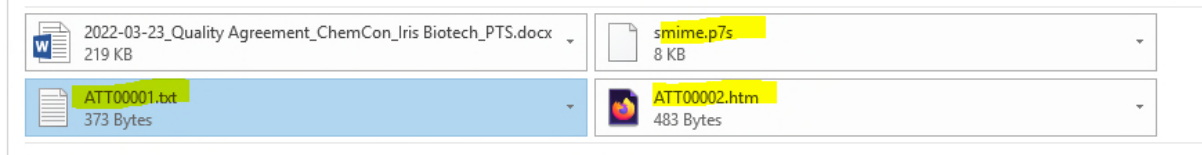
This notification was sent to michael.woydt@chemcon.com of microsoft.com

Bitte beachtet die „Signale“.

Hundertprozentige Sicherheit können wir hier nicht geben. Es liegt an Euch vorsichtig mit e-Mails unbekannter Herkunft oder auch gefakter Herkunft umzugehen.

Bitte bei Eingang von Mails wie oben angezeigt, diese löschen und danach auch im Verzeichnis „gelöschte Elemente / Objekte“ zusätzlich löschen.

Wenn man eine E-Mail mit den drei gelbmarkierten Anhängen erhält, hat dies nachfolgenden Grund:



Mit der Datei kam tatsächlich nur der Anhang, der vom Absender geschickt wurde, an.

Die anderen drei Anhänge wurden von unserer Spam-Appliance generiert.

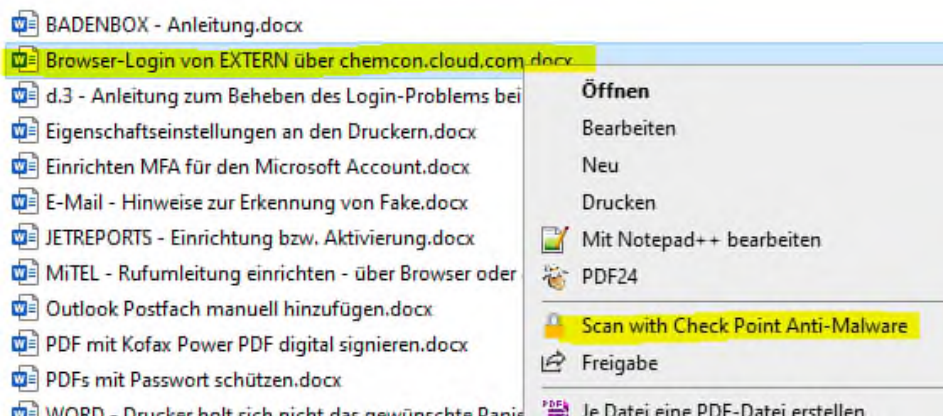
Da die E-Mail verschlüsselt kam (erkennt man am Anhang smime.p7s), konnte unsere Spam-Appliance den Zusatz „* * * Warnung: Externe Nachricht – Links und Anhänge vor dem Öffnen prüfen * * *“ nicht direkt oberhalb des Mailtextes einfügen.

Daher wird der Zusatz als .txt- und .htm-Datei im Anhang beigefügt. Die Datei smime.p7s sagt aus, dass es sich um eine verschlüsselte E-Mail handelt.

Sollte Ihr Dateien herunterladen, achtet bitte auf die Dateiendungen.

Sollte die Datei-Endung der heruntergeladenen Datei „.docm“, „.xlsm“ oder „.pptm“ sein, dann bitte das Makro nicht ausführen, wenn Du beim Öffnen der Datei aufgefordert wirst.

Außerdem kannst Du bei jeder Datei, ob heruntergeladen oder woanders her, über den Rechtsklick auf die Datei im Kontextmenü „Scan with Check Point Anti-Malware“ den Dateiscann durchführen.



Noch mal zu Info:

**Systemmails von den ChemCon-Servern
sind grundsätzlich in DEUTSCH geschrieben.**