Phishing-(Mails)

Die Gefahr von Phishing-Mails

Vielleicht ist Dir das auch schon mal passiert: Plötzlich landet eine unerwartete E-Mail von Amazon, DPD oder auch der Hausbank in deinem Posteingang. Eigentlich nichts Ungewöhnliches, hier kann es aber durchaus gefährlich werden. Denn möglicherweise stammt diese E-Mail nicht von dem Absender, für den er sich ausgibt.

In dem Fall spricht man von Phishing-Mails.

Was ist Phishing und worin besteht die Gefahr?

Der Begriff Phishing (Abwandlung des engl. Wortes „fishing“, zu deutsch „Angeln“) beschreibt den Versuch, sich über gefälschte E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner auszugeben und dadurch persönliche Daten des Internet-Benutzers abzufragen. Dies hat zur Folge, dass möglicherweise Kontoplünderung oder Identitätsdiebstahl begangen wird oder eine Schadsoftware installiert wird. Durch diesen Betrug findet eine soziale Manipulation statt, bei der die Gutgläubigkeit des Opfers ausgenutzt wird.

Heißt also vereinfacht: Jemand möchte an deine Daten oder die des Unternehmens heran. Dies geschieht, indem er sich als jemand anderes ausgibt, meist als eine Person oder ein Unternehmen,

dem Du vertraust – beispielsweise deiner Bank.

Der Trojaner Emotet versendet beispielsweise Mails von bekannten Kollegen oder Geschäftskontakten, mit denen Du zuletzt Kontakt hattest. Auch hier solltest Du also bei ungewöhnlichen Anhängen oder Links vorsichtig sein.

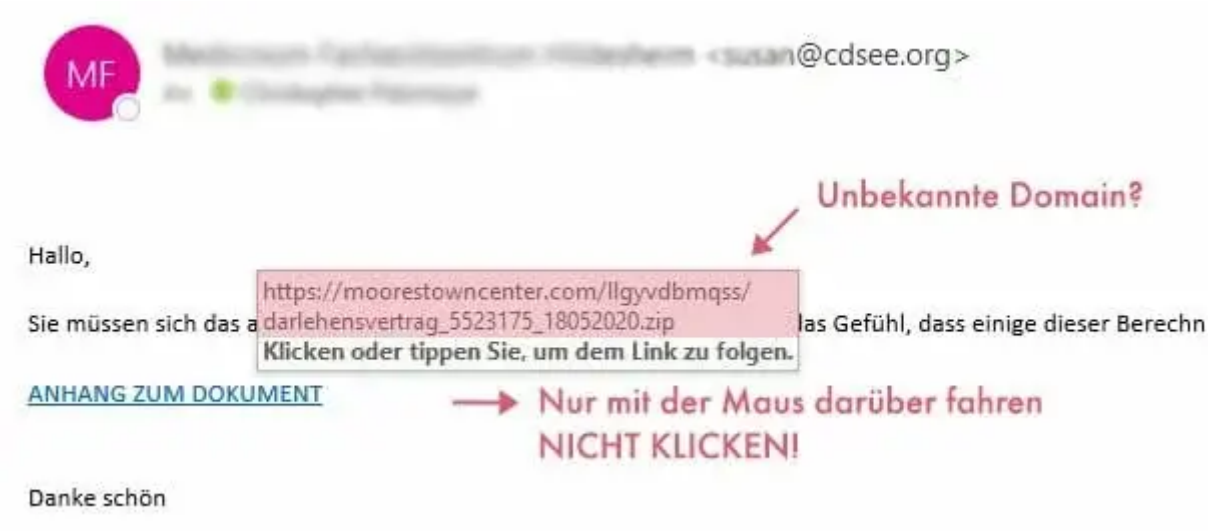
Wie sehen Phishing-Mails aus?

- Eine Aufforderung, etwas anzuklicken, etwas zu ergänzen wie z.B. persönliche Kundendaten oder sogar Zahlungsaufforderungen
- Teilweise schlechte oder unverständliche Grammatik und Rechtschreibung. Dies ist aber nicht immer der Fall, oftmals sehen die E-Mails auch sehr echt aus
- Eine unpersönliche Anrede wie „Sehr geehrte Kundinnen und Kunden“ ist verdächtig. Allerdings gibt es mittlerweile auch viele Beispiele, in denen die Kunden mit ihrem richtigen Namen angesprochen werden. Deshalb solltest Du auch bei korrekter persönlicher Anrede jede E-Mail kritisch prüfen
- Sind Links vorhanden? Dann überprüfe diese, indem Du mit der Maus nur über den Link hoverst ohne ihn anzuklicken, denn oftmals führen diese Links zu gefälschten Internetseiten, was sich meist aus der Internetadresse schon herauslesen lässt.

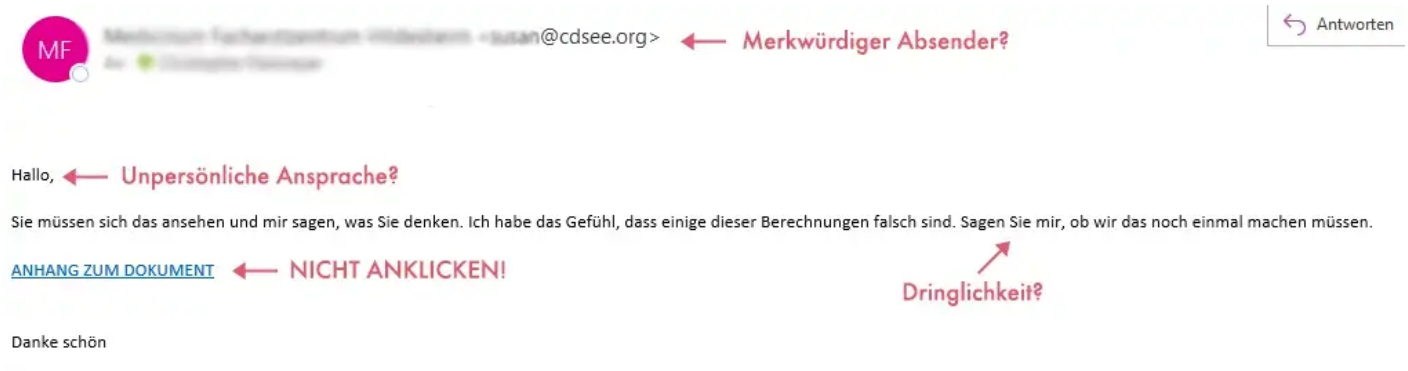
Wichtig: Lies die Internetadresse genau! Manchmal verändern die Betrüger nur Kleinigkeiten, sodass statt www.meinehauskasse.de zum Beispiel www.meinehauskassse.de mit drei „s“ erscheint. Am besten klickst Du niemals einen Link in einer E-Mail an, sondern öffnest die bekannte echte Seite des jeweiligen Unternehmens im Browser und schau dort nach.

Falls Du dir nicht sicher bist, rufst Du das jeweilige Unternehmen am besten an und fragst dort persönlich nach. Viele Unternehmen, wie z.B. Banken, informieren auch öfter über Phishing-Versuche.

So kann eine Phishing-Mail aussehen:



Beim genauem Anschauen des Links:



Fällt Dir etwas auf?

In diesem Fall zeigt das Vorschaufenster des Links an, dass es sich um eine seltsame Domain handelt („mooretowncenter.com“) und eine .zip-Datei heruntergeladen werden soll.

Hierbei müssten jetzt bei Dir alle „Alarmglocken klingeln“. Solche E-Mails gehören sofort gelöscht. Informiere ggf. auch Kollegen und die zwei von der Tankstelle bzw. IT-Abteilung, denn häufig werden Phishing-Versuche auch gleich an mehrere Empfänger eines Unternehmensnetzwerks adressiert.

So, wieder etwas schlauer. Jetzt Augen auf beim Mailverkehr.

Revision #2
Created 27 January 2025 12:02:10 by Thomas Fried
Updated 27 January 2025 12:33:52 by Thomas Fried