

Tipps zur Prüfung der Echtheit von E-Mails

Nehmen Sie sich Zeit

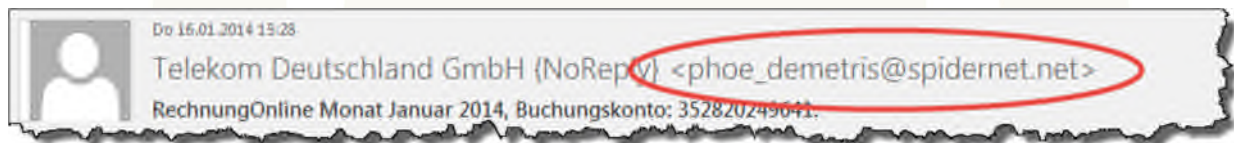
Nehmen Sie sich ausreichend Zeit, um den Inhalt einer E-Mail zu erfassen und die nachfolgenden Punkte zu prüfen, bevor Sie eine Nachricht „bearbeiten“. Dies gilt insbesondere, wenn der Absender in seiner E-Mail Druck aufbaut und auf eine außergewöhnlich hohe Rechnung in der Anlage hinweist oder die baldige Sperrung eines Kundenkontos androht.

Auch, wenn viele E-Mails im Posteingang warten und Sie diese schnell loswerden wollen, sollte dies mit Bedacht geschehen. Überlegen Sie, wie viel Zeit im Gegensatz dazu die Identifikation und Beseitigung einer eingefangenen Schadsoftware in Anspruch nimmt.

Prüfen Sie den Absender

Verifizieren Sie den Absender der E-Mail. Ist Ihnen der Absender bekannt? Stimmt die gesamte Mailadresse (vor und nach dem @-Zeichen) mit der angeblichen Person bzw. der Firma des Absenders überein? Ist eine E-Mail mit dieser Absenderadresse üblich (z. B. von Ihrer Bank)?

Im nachstehenden Beispiel haben der angezeigte Absendername (der vom Absender im Übrigen vollkommen frei gestaltet werden kann) und die tatsächliche E-Mail Adresse des Senders nichts miteinander zu tun.



Prüfen Sie den Inhalt der E-Mail

Erscheint Ihnen der Inhalt der E-Mail nach kritischer Prüfung seriös und stimmig? Ist die Sprache üblich und der in der E-Mail geschilderte Sachverhalt plausibel? Sind andere E-Mails dieses Absenders (z. B. Rechnungen Ihres Telefonanbieters oder Internetproviders) immer genau so oder nur so ähnlich (z. B. Zeitpunkt der Abrechnung, Formulierung des Inhalts, Absenderangaben am Ende der E-Mail)?

Prüfen Sie Anhänge

Seien Sie aufmerksam bei E-Mails mit Anhängen. Erwarten Sie eine Anlage von diesem Absender? Ist die beigefügte Datei in der E-Mail angekündigt und erläutert? Besondere Vorsicht sollten Sie bei ZIP-Dateien walten lassen: Der Sinn von ZIP-Dateien besteht darin, Dateien zu komprimieren sowie mehrere Dateien in einem ZIP-Archiv zu sammeln. Beides ist bei einer vermeintlichen Rechnung, einer Auftragsbestätigung oder einem Fragebogen prinzipiell nicht erforderlich. Aber selbst in einer PDF-Datei kann Schadsoftware verborgen sein und sollte daher erst nach Prüfung geöffnet werden.

Prüfen Sie Links

Aufgepasst bei Internetlinks in E-Mails! Die Anzeige eines eingefügten Links kann mit jedem beliebigen Text versehen werden, der mit dem eigentlichen Ziel des Hyperlinks möglicherweise nicht das Geringste zu tun hat. Wenn Sie mit der Maus auf einen Link zeigen (nicht klicken!), wird bei den meisten E-Mail Programmen der eigentliche Link angezeigt.

Entspricht der in einer E-Mail enthaltene Link der angekündigten bzw. von Ihnen erwarteten Internetadresse? Wichtig ist dabei immer die von Vorne erste Endung (z. B. .de oder .com) eines Links, die danach stehenden Einträge sind sog. Subdomains, die vom Inhaber der Webseite beliebig vergeben werden können.

Dementsprechend zeigt der Link in nachstehendem Beispiel auf eine russische Internetadresse (serverrequiestcont.ru). Das Unterverzeichnis (telekom_deutschland) soll dem vorsichtigen Nutzer ein gutes Gefühl geben.

