Schutz vor Phishing-Attacken auf Facebook

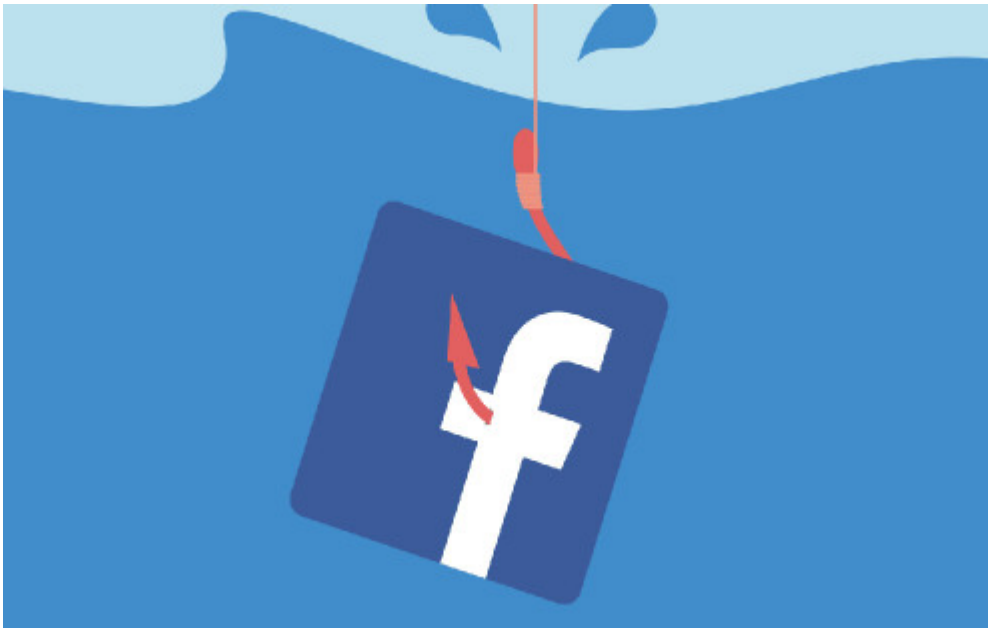


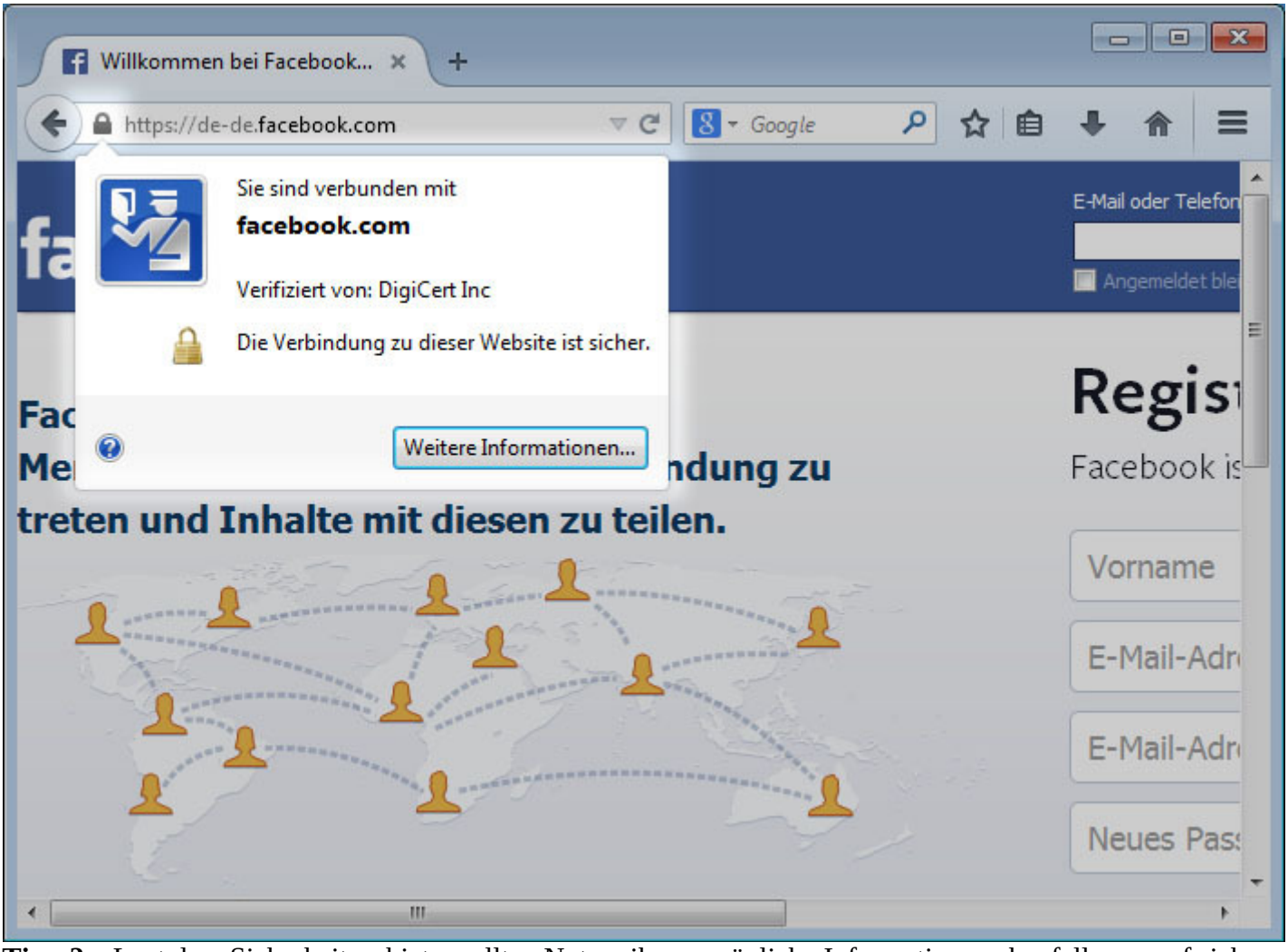
Foto: Kaspersky

Phishing gibt es überall, auch in sozialen Netzwerken. Sieben Sicherheit-Tipps zeigen Facebook-Nutzern, wie sie sich vor dem Diebstahl persönlicher Daten schützen.
Internet-Nutzer haben die meiste Angst vor Phishing. Und da Facebook heutzutage auf fast jeder Webseite mit seinen Schaltflächen zum Liken und Teilen integriert ist, wird das soziale Netzwerk erst recht gerne von Angreifern – den sogenannten Phishern – missbraucht, um private Daten abzugreifen. Der Sicherheitsanbieter Kapersky gibt sieben Tipps zum Schutz vor Phishing-Angriffen auf Facebook-Konten.

Da Phishing nur funktioniert, wenn Anwender allzu vertrauensselig sind, sollten Facebook-Nutzer ominöse Benachrichtigungen des vermeindlichen sozialen Netzwerks genauestens untersuchen. Als Beispiel seien hier Passwort-Reset-Anfragen oder die Aufforderung Login-Daten über einen bestimmten Link einzugeben oder an Dritte zu senden genannt. Dabei handelt es sich mit hoher Wahrscheinlichkeit um Phishing-Meldungen, die nicht von Facebook kommen, sondern von Angreifern, die das soziale Netzwerk nachahmen, um Daten abzugreifen.
Facebook gibt zum Thema Sicherheit noch einen weiteren Hinweis: Keine Freundschaftsanfragen von Personen akzeptieren, die man nicht kennt. Des Weiteren sollten grundsätzlich auch die Regeln für sichere Passwörter beachtet werden. Außerdem hilft ein aktueller Browser, Phishing-Weiterleitungen abzuwehren.

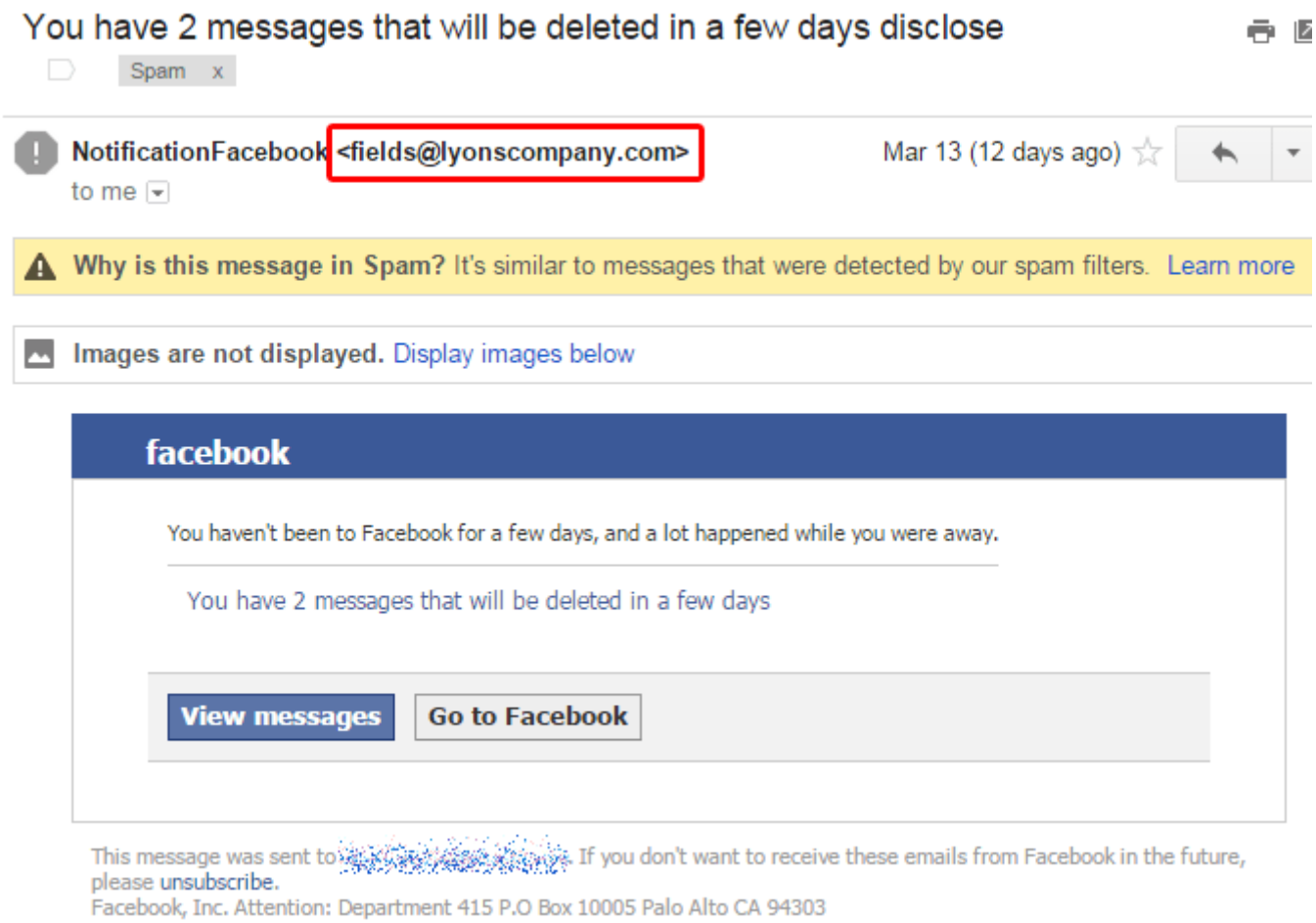
7 Tipps für den Schutz vor Facebook-Phishing

Tipp 1 – Ganz oben auf Kasperskys Liste steht die Preisgabe von persönlichen Daten wie Nutzernamen, Passwörter und PINs aufgrund einer E-Mail-Abfrage. Nachrichten wie "Wir hatten eine Server-Panne, bitte senden Sie uns ihr Passwort nochmals zu." oder Ähnliches sollten getrost ignoriert werden. In dem Zusammenhang siehe auch Tipp 4

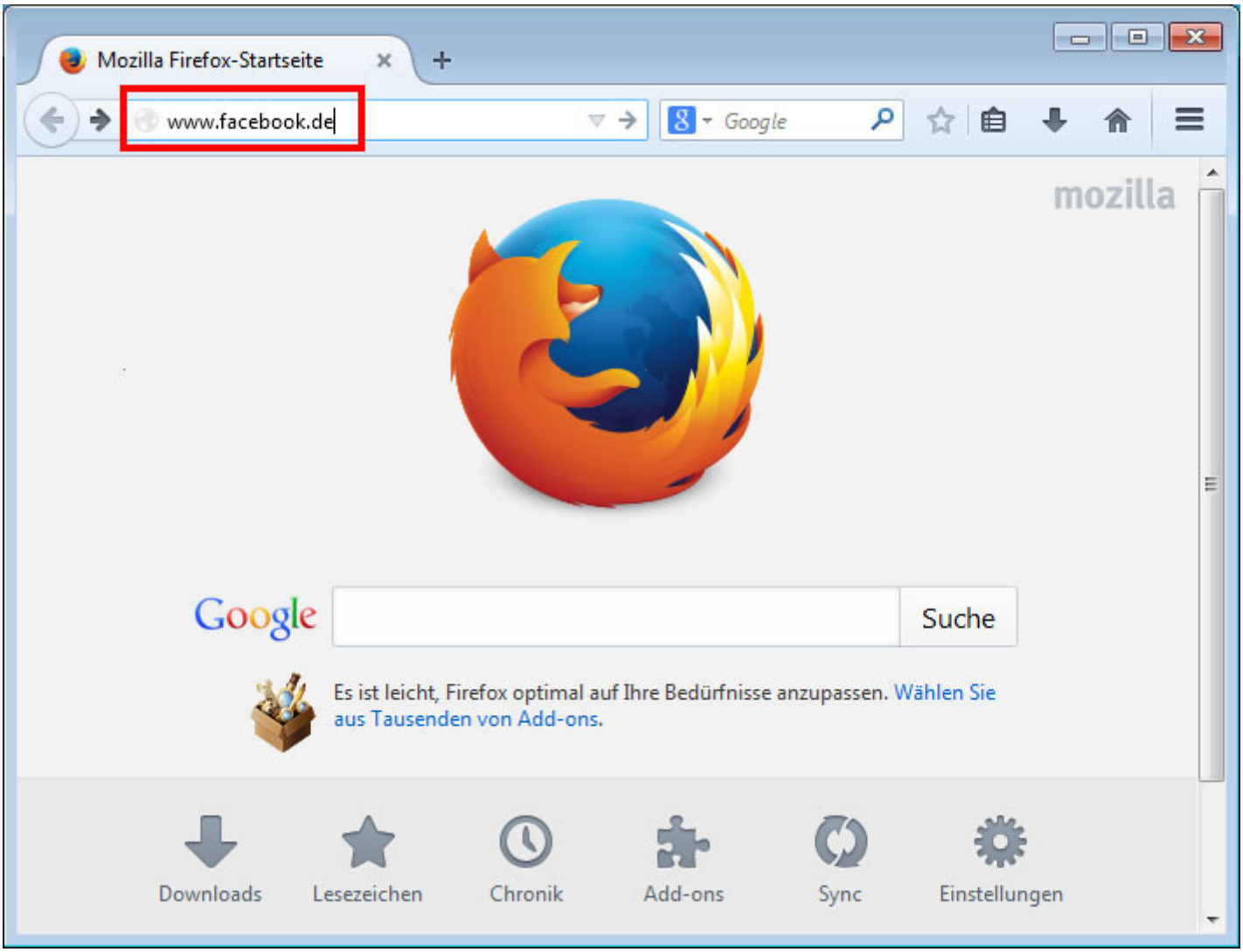


Tipp 2 – Laut dem Sicherheitsanbieter sollten Nutzer ihre persönliche Informationen ebenfalls nur auf sicheren Webseiten eingegeben, die in der Adressleiste mit "https://" beginnen und ein Sicherheitszertifikat aufweisen.

Dies wird etwa im Browser Firefox durch ein Vorhängeschloss in der Adressleiste gekennzeichnet. Ein Klick darauf zeigt weitere Details zur Webseite an

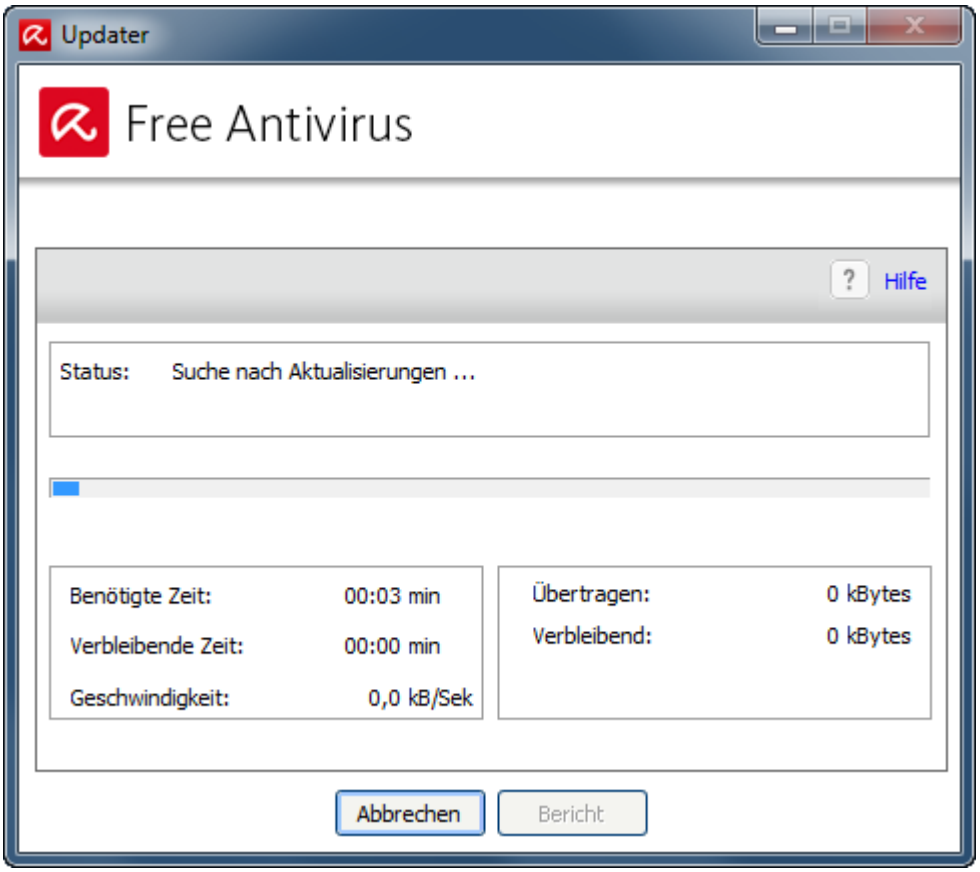


Tipp 3 - Wenn E-Mails nach privaten Daten fragen, sollten diese genauer untersucht werden. Schreibfehler oder eine unpersönliche Anrede sind oft ein klares Warnsignal für eine Phishing-Meldung. Sicher kann man sein, wenn der Link, über den die eigenen Daten eingegeben werden sollen, auf eine andere Webseite verweist als die Angekündigte, oder wenn der Absender eine untypische E-Mail-Adresse nutzt. So wird Facebook beispielsweise nicht die Absender-Adresse "fields@yonscompany.com" nutzen (Bildquelle: Kaspersky).



Tipp 4 - An vierter Position nennt Kaspersky Links, die nach persönlichen Daten fragen. Statt darauf zu klicken, ist es besser direkt die entsprechende Webseite im Browser aufzurufen – also dort etwa www.facebook.de einzutippen.

Tipp 5 - Eine aktuelle Antiviren-Software mit Phishing-Schutz steht bei Kaspersky auf Punkt Nummer fünf. Bekannte Antivirenprogramme sind Avira Antivir, Avast Pro Antivirus und AVG Antivirus. Die besten Virenscanner für Windows finden sich hier.



Tipp 6 - Passend zu Punkt fünf sollten Nutzer darauf achten ihren Virenscanner stets mit neuen Sicherheits-Patches aktuell zu halten, da jeden Tag neue Malware programmiert und verteilt wird. Virenscanner sollten beim Windows-Start automatisch nach Updates suchen und diese installieren. Falls dies nicht der Fall ist, hilft meistens ein Blick in die Einstellungen des Programms.

Tipp 7 - Zu guter Letzt sollten erkannte Phishing-Versuche sowie verdächtige Nachrichten direkt an Facebook geschickt werden. Das Netzwerk kann dann darauf reagieren, gegebenenfalls andere Nutzer warnen und bestenfalls die Phishing-Meldungen stoppen. Wie Nutzer verdächtige Meldungen bei Facebook melden, steht auf der zugehörigen Webseite.