(Foto: psdesign1 - Fotolia)

25.04.2024

# Achtung: So funktionieren die Phishing-Maschen

Im Postfach landet eine seriös aussehende Mail von einer angeblichen, aber falschen DIHK- oder IHK-Adresse mit der Bitte um Datenaktualisierung. Sie nutzt ein gefälschtes DIHK-/IHK-Logo, klingt dringend und warnt vor negativen Folgen bei Nichtbefolgung. Dabei können die Absender-Adressen variieren. Die Domains heißen beispielsweise firmenaktualisieren.net, datenaktualisieren.com, firmenaktualisieren.org oder informations-aktualisierung.com.

Aber es gibt zahllose Varianten. Denn sobald uns eine Adresse als Phishing-Domain aufgefallen ist, melden wir sie beim jeweiligen Registrar. Der sperrt die Domain, um weiteren Schaden zu vermeiden. Doch die Täter registrieren sofort neue Domains, da diese nicht nur für neue Mail-Adressen, sondern auch für die Phishing-Website selbst genutzt werden. Daher ist es wichtig auf Mail-Texte und Eingabe-Masken zu achten. Diese sieht immer gleich aus – und stammt niemals von der DIHK. Denn wir fragen Ihre Daten nicht über derartige Mails ab. Wenn Sie unsicher sind, kontaktieren Sie die vermeintlich abfragende Stelle, aber dann über einen Kontakt über deren offizielle Website.

Ansonsten gilt: Bitte geben Sie Ihre Daten also nicht in solche Masken ein, löschen Sie diese Mails, reagieren Sie nicht darauf. Wenn Sie die Daten einmal eingeben haben, sind sie in den falschen Händen.

Wir stehen in Kontakt mit den Behörden, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem CERT-Bund, dem Computer Emergency Response Team für Bundesbehörden.

In diesem Artikel aktualisieren wir für Sie die Phishing-Maschen. (Link: https://www.dihk.de/de/aktuelles-und-presse/aktuelle-informationen/warnung-neue-maschen-zum-datenklau-86302) Die ausführliche Version dieses Artikels mit Beispielen und weiteren Informationen finden Sie hier. (Link: https://www.dihk.de/de/achtung-so-funktionieren-die-phishing-maschen-116624)