idgard®

by uniscon - A member of TÜV SÜD

Checkliste: Das können Sie tun, wenn Sie in die Phishing-Falle getappt sind

Wie Sie sich und Ihre Mitarbeiter gegen perfide Phishing-Angriffe schützen, haben wir Ihnen bereits in einem privacyblog-Beitrag gezeigt. Doch was tun, wenn Sie doch einmal auf eine gut gefälschte E-Mail hereinfallen und Ihre Konto- oder Account-Zugangsdaten in die falschen Hände geraten?

Keine Sorge, auch für diesen Fall haben wir einige Tipps für Sie parat! Halten Sie sich einfach an unsere Checkliste.

- **Keine Panik!** Bleiben Sie ruhig und beachten Sie die nächsten Schritte.
- **Löschen Sie die verdächtige E-Mail nicht** – sie kann als Beweismittel dienen und bei der Aufklärung des Falls helfen.
- Geht es um Ihr **Bankkonto**, lassen Sie bei Ihrer Bank **alle Konten und Karten sperren**.
- Im Falle von **Account-Phishing** bei Online-Shops, sozialen Netzwerken, Cloud-Diensten etc. loggen Sie sich in Ihren Account ein und **ändern Sie die Zugangsdaten**. Überprüfen und stornieren Sie ggf. von Dritten getätigte Bestellungen. Wenn Sie sich nicht mehr einloggen können, weil Betrüger bereits die Zugangsdaten geändert haben, **kontaktieren Sie den Betreiber** des Dienstes und **veranlassen Sie eine Sperrung Ihres Accounts.**
- **Sollte Ihr idgard®-Account betroffen sein**, wenden Sie sich bitte an die Person, die Sie eingeladen hat. Der- oder diejenige kann die gekaperte **Lizenz einfach erneut vergeben** und den Angreifern somit den Zugang zu sensiblen Daten verwehren. **Denken Sie daran, ein neues Passwort zu vergeben**, wenn Sie sich anschließend erneut registrieren!

  Unsere Mitarbeiter werden Sie niemals nach Ihren idgard®-Zugangsdaten fragen. Geben Sie diese auf keinen Fall an Dritte weiter!

- **Kontaktieren Sie in jedem Fall das Unternehmen** (Bank, Online-Shop, Dienst-Anbieter), in dessen Namen der Phishing-Angriff erfolgt ist. Informieren Sie über den Vorfall und lassen Sie sich beraten.
- **Kontaktieren Sie einen Fachanwalt.** Wenn Betrüger Geld von Ihrem Bankkonto abgebucht haben, können Sie in der Regel zivilrechtliche Ansprüche an die Bank geltend machen.
- Da es sich bei **Phishing um versuchten Betrug** und somit um eine Straftat handelt, empfiehlt es sich außerdem, **Strafanzeige zu erstatten**.
- Sicherheitshalber sollten Sie Ihre **Antivirensoftware aktualisieren** und Ihren **Computer auf Trojaner** überprüfen.
- **Melden Sie – auch erfolglose – Phishing-Angriffe bei der Verbraucherzentrale.** Das **Phishing-Radar** klärt über aktuelle Phishing-Fälle auf und hilft anderen Verbrauchern dabei, sich ebenfalls gegen Angriffe zu schützen. Verdächtige Mails können Sie an die Verbraucherzentrale NRW schicken. Benutzen Sie dazu die E-Mail-Adresse **phishing@verbraucherzentrale.nrw**.

Diese Checkliste ist Teil unserer Secure-Mail-Reihe. Dort zeigen wir Ihnen unter anderem, wie Sie Ihren Mail-Verkehr verschlüsseln und sensible Dokumente und Anhänge versenden. Außerdem erfahren Sie, wie Sie sich und Ihre Mitarbeiter gegen Phishing-Angriffe schützen.

uniscon – ein Unternehmen der TÜV SÜD Gruppe

Die uniscon GmbH ist ein Münchner Anbieter von DSGVO-konformen Cloud- und Datenraum-Lösungen für Unternehmen und einer der führenden Secure-Cloud-Provider in Europa. Die Produkte von uniscon greifen Hand in Hand: uniscons Sealed Platform® bietet eine sichere Ausführungsumgebung für Webanwendungen mit hohem Sicherheitsbedarf bzw. hohen Datenschutzanforderungen.

uniscons Business-Cloud idgard® sichert die digitale Kommunikation und den Datenaustausch mit Partnern, Kunden und Kollegen auf höchstem Niveau ab und vereinfacht sie darüber hinaus. Mehr als 1.200 Unternehmen vertrauen bereits auf den webbasierten Datenraum- und Filesharing-Dienst, darunter IT- und Kommunikationsanbieter (z.B. T-Systems), Unternehmensberatungen (u.a. PwC, Baker Tilly) sowie diverse Anbieter von Finanzdienstleistungen (z.B. Sparkassen und Volksbanken).

Was uniscons Lösung gemeinsam haben? Sie basieren alle auf der international patentierten Sealed Cloud Technologie, welche mit rein technischen Maßnahmen unbefugte Datenzugriffe ausschließt. Die Lösungen werden alle nach dem Grundsatz „Privacy by Design“ entwickelt.

Uniscon wurde 2009 gegründet und ist seit 2018 Teil der Digitalisierungsstrategie von TÜV SÜD. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund kann uniscon die Entwicklung seiner Technologie weiter vorantreiben und ist in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zum Unternehmen und den Lösungen: www.idgard.de und www.uniscon.com

Kontakt:

uniscon GmbH – Sealed Cloud Technologies
E-Mail: contact@uniscon.com
Internet: www.uniscon.com
Telefon: +49 (89) 4161 5988 100

Herausgeber:

uniscon GmbH
Geschäftsführung: Karl Altmann
Ridlerstraße 57 · 80339 München · Telefon 089 / 4161 5988 100
Amtsgericht München HRB 181797