Ausgezeichneter Schadenservice
4,7 / 5
Kundenzufriedenheit (Kundenbefragung 2023)

HISCOX

PHISHING: CHECKLISTE FÜR DEN ERNSTFALL

Was versteht man unter Phishing?

Cyberkriminelle nutzen gefälschte E-Mails, Nachrichten in Messengern oder Posts in sozialen Medien, um Menschen zu betrügen. Diese Nachrichten zielen darauf ab, Benutzer dazu zu verleiten, sensible Informationen wie Passwörter, Kontodaten oder Kreditkarteninformationen offenzulegen. Empfänger werden aufgefordert, einem Link zu folgen.

Das Risiko dabei ist, dass diese Links zu nachgeahmten Webseiten führen, auf denen dann die persönlichen Daten der Nutzer unbemerkt gestohlen werden. Die Betrugsversuche sind hochprofessionell gestaltet, sodass die Nachrichten und die Absender auf den ersten Blick sehr vertrauenswürdig erscheinen. Deswegen erkennen viele Personen die Betrugsversuche nicht und übermitteln unwissentlich ihre sensiblen Informationen direkt an die Betrüger.

DIESE SCHRITTE SIND EMPFOHLENSWERT, FALLS ...

... Sie Ihre Zahlungsinformationen preisgegeben haben:

- ☐ Blockieren Sie den Zugang zu Ihrem Bankkonto.
- ☐ Überwachen Sie die Bewegungen auf Ihrem Konto sorgfältig und treten Sie umgehend in Kontakt mit Ihrem Kreditinstitut.
- ☐ Nachdem der Zugang wieder freigegeben wurde, verwenden Sie bitte ausschließlich neue Passwörter und PINs für Ihr Bankkonto.

... Sie Zugangsdaten zu anderen Konten, z. B. wie zum Beispiel für Online-Shopping-Plattformen, weitergeleitet haben:

- ☐ Setzen Sie ein neues Passwort fest.
- ☐ Treten Sie in Verbindung mit dem jeweiligen Dienstleister.
- ☐ Kontrollieren Sie weiterhin, ob Ihre Zahlungsinformationen kompromittiert wurden und setzen Sie sich gegebenenfalls auch mit Ihrem Kreditinstitut in Verbindung.

... Sie Ihre Zugangsdaten für Ihr E-Mail-Konto preisgegeben haben:

- ☐ Vergeben Sie ein neues Passwort.
- ☐ Da der Zugriff auf Ihr E-Mail-Postfach möglicherweise dazu geführt hat, dass auch Zugangsdaten zu anderen Online-Services gefährdet sind – diese könnten etwa verändert oder unrechtmäßig übernommen worden sein –, ist es notwendig, dass Sie auch bei diesen Diensten die Passwörter erneuern. Dies betrifft alle Online-Profile, die Sie nutzen, um sich bei verschiedenen Diensten, wie beispielsweise einem Online-Shop, anzumelden.

HISCOX

Ausgezeichneter Schadenservice
4,7 / 5
Kundenzufriedenheit (Kundenbefragung 2023)

DAS SOLLTEN SIE TUN, WENN ...

... Sie auf einen Link geklickt haben und daraufhin Geldforderungen erhalten:

- ☐ Überweisen Sie unter keinen Umständen Geld an Betrüger.
- ☐ Bei Geldforderungen von Unbekannten ist es ratsam, sich an die Polizei, die Verbraucherzentrale zu wenden oder juristischen Rat einzuholen.

... den Verdacht haben, dass jemand Ihre Daten unrechtmäßig erlangt hat:

- ☐ Erstatten Sie unabhängig von der Stärke Ihres Verdachts eine Anzeige bei der Polizeidienststelle in Ihrer Nähe. Als Betroffene/r von Cyberkriminalität stehen Ihnen dieselben Rechte zu wie Personen, die Opfer anderer Arten von Straftaten geworden sind.

SO SCHÜTZEN SIE SICH IN ZUKUNFT VOR PHISHING

- ☐ Aktualisieren Sie Software und Betriebssysteme auf all Ihren Geräten stets umgehend und installieren Sie Sicherheitssoftware.
- ☐ Behandeln Sie E-Mails von unbekannten Absendern mit Vorsicht.
- ☐ Beachten Sie, dass Organisationen wie Banken, Serviceanbieter oder staatliche Einrichtungen Sie niemals auffordern würden, über einen Link in einer E-Mail persönliche Informationen wie Passwörter zu aktualisieren. Sollten Sie Unsicherheiten bezüglich der Authentizität einer E-Mail haben, ist es ratsam, die Echtheit direkt beim Absender telefonisch zu verifizieren.
- ☐ Vermeiden Sie es dabei, Telefonnummern zu verwenden, die in der fraglichen E-Mail angegeben sind; recherchieren Sie stattdessen die Kontaktdaten selbst.
- ☐ Seien Sie besonders vorsichtig mit E-Mail-Anhängen, die in Formaten wie .exe oder .scr vorliegen, da diese potenziell Schadsoftware enthalten können, die ohne Ihr Wissen auf Ihr Gerät heruntergeladen wird. Achten Sie zudem auf irreführende Doppelendungen bei Dateinamen, beispielsweise „Dokument.pdf.exe“, die darauf abzielen, Sie zu täuschen.
- ☐ Nutzen Sie für zusätzlichen Schutz Ihrer verschiedenen Online-Konten einer Zwei-Faktor-Authentifizierung. Diese zusätzliche Sicherheitsebene stellt sicher, dass Kriminelle selbst mit Kenntnis Ihres Passworts keinen Zugang zu Ihren Daten erhalten können.

Hiscox
Arnulfstraße 31, 80636 München
T +49 89 54 58 01 700 **F** +49 89 54 58 01 199
E business-academy@hiscox.de **W** **hiscox.de**