Warnung vor Phishing-Mails im Allianz Design

Mit dieser Information möchten wir dazu sensibilisieren, dass derzeit Cyberkriminelle im Internet aktiv sind, die in Phising-Mails unerlaubt Name und Logo der Allianz nutzen. Sie versuchen unter diesem Deckmantel Accounts und Computersysteme sowohl von Kunden als auch Nichtkunden der Allianz zu kompromittieren. Dies geschieht mit Hilfe äußerst realistisch gestalteter Phishing-Mails. Die Allianz selbst ist nicht Ziel dieses Angriffs.

Bitte sind Sie deshalb äußerst vorsichtig in Bezug auf diese potentiell schädlichen E-Mails, die eine Bedrohung für Ihre Computersysteme darstellen .

Überprüfen Sie daher eingehende E-Mails mit Absender Allianz sorgfältig! Klicken Sie insbesondere nicht auf verdächtige Links, welche nicht auf eindeutige Allianz-Seiten verweisen und sind Sie auch beim Öffnen von Anhänge vorsichtig.

Woran erkennen Sie die Phishing-Mails?

Die E-Mails zeigen unterschiedliche Erscheinungsbilder auf, weisen jedoch in der Regel darauf hin, dass neue Dokumente, neue Verträge oder Versicherungsunterlagen zum Herunterladen bereitstehen.

- Die eingebetteten Links in der E-Mail selbst oder den Anhängen verweisen nicht direkt auf die Allianz-Webadresse, sondern werden durch sogenannte "URL-Shortener" wie beispielsweise die Adresse “Bit.ly” verschleiert. Durch das Bewegen des Mauszeigers über den Link, ohne darauf zu klicken, können Sie feststellen, ob tatsächlich eine Webadresse der Allianz hinterlegt ist.
- Obwohl die Absenderadresse der E-Mail zunächst wie eine Allianz-Adresse wirkt, zeigt sich bei genauerer Prüfung der Absenderdetails eine Adresse, die nicht der Allianz zuzuordnen ist. Allianz-Adressen enden immer auf "@allianz" und üblicherweise auf .de oder .com.
- Seien Sie vorsichtig bei E-Mails, die Dringlichkeit suggerieren: Phishing-Versuche enthalten oft Warnungen, dass Ihr Konto gesperrt wird oder ähnliche dringende Handlungsaufforderungen, um Sie zu einer voreiligen Reaktion zu verleiten.

Hier sind einige Beispiele:

[EXT] Ihre Unterlagen AS-893057715

AV [redacted]

Antworten | Allen antworten | Weiterleiten | ...

Mi 13.03.2024 16:44

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

Allianz

Hier sind Ihre Dokumente

nur ein Klick auf **Ihre Dokumente** - und Sie haben viele Unterlagen zu Ihrer Kfz-Versicherung bereits vorliegen. Folgende Dokumente können Sie jetzt abrufen:

- die **Versicherungsinformationen**

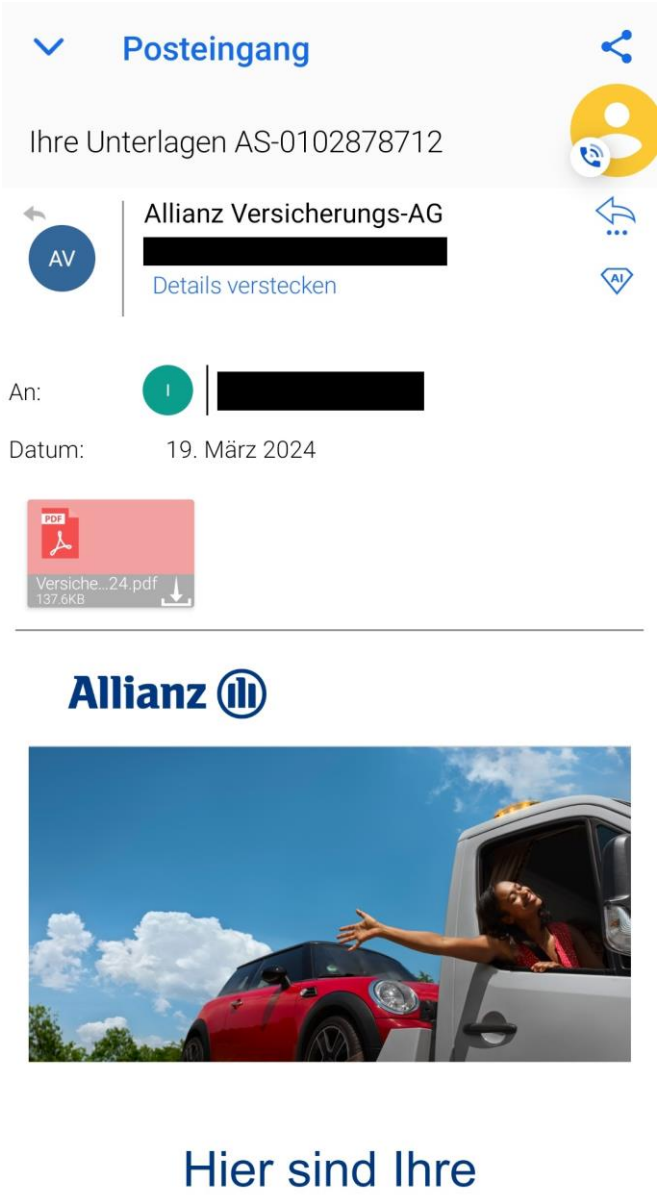
Bis bald
Ihre Allianz

Haben Sie noch Fragen?

Wir helfen Ihnen gerne.
Rufen Sie uns an unter 08 00.4 10 01 01,
oder kontaktieren Sie uns unter sachversicherung@allianz.de

Ilse Allianz

Impressum:
Allianz Versicherungs-Aktiengesellschaft
Vorsitzender des Aufsichtsrats: Dr. Klaus-Peter Röhler.
Vorstand: Frank Sommerfeld, Vorsitzender;
Dr. Lucie Bakker, Laura Gersch, Dr. Jan Malmendier,
Dr. Dirk Steingröver, Ulrich Stephan, Dr. Rolf Wiswesser, Ulrike Zeiler.
Für Umsatzsteuerzwecke: USt-IdNr.: DE 811 150 709;
Für Versicherungsteuerzwecke: VersSt-Nr.: 802/V90802004778.
Finanz- und Versicherungsleistungen i.S.d. UStG / MwStSystRL sind von der Umsatzsteuer befreit.
Sitz der Gesellschaft: München; Registergericht: Amtsgericht München HRB 75727



Link in einer Phishing-Mail geklickt – was nun?

Aktuell beobachten wir, dass der Angriff nur auf Windows Geräte abzielt. Sollten Sie also den Link auf einem Handy oder Mac, oder Linux PC geöffnet haben, so kann man davon ausgehen, dass ihr Rechner nicht infiziert ist.

Haben Sie auf einen Link in einer verdächtigen E-Mail geklickt, wurde ein kleines Programm auf ihren Rechner heruntergeladen. Haben Sie dieses ausgeführt, beispielsweise mit einem Doppelklick geöffnet, so kann es sein, dass Sie ihren Computer mit einem Schadprogramm infiziert haben. Gleiches gilt, wenn Sie die Anhänge einer Betrugsmail öffnen. Bei der aktuellen Phishing Kampagne, die wir beobachten, wird auf Ihrem Rechner ein Programm installiert, mit dem der Hacker beliebige Befehle auf Ihrem Rechner ausführen kann.

- Unser Tipp ist, setzen Sie den Rechner zurück oder installieren Sie das Betriebssystem komplett neu. Dies ist zwar mit einigem Aufwand verbunden, jedoch können Sie so sicher sein, dass Sie die Infektion beseitigt haben. (Vergessen Sie nicht wichtige Daten vorher zu sichern)
- Ändern Sie ebenfalls Ihre, auf dem Rechner gespeicherten, Passwörter
- Ebenfalls empfehlen wir ein Anti-Virenprogramm auf Ihrem Rechner zu installieren und stets auf dem neuesten Stand zu halten.

Woher kennen die Kriminellen meine E-Mail-Adresse?

Um an E-Mail-Adressen für Phishing-Angriffe zu gelangen, nutzen Cyberkriminelle häufig folgende Quellen:

- **Datenlecks**: E-Mail-Adressen die durch Sicherheitsverletzungen bei Unternehmen und Diensten öffentlich geworden sind.
- **Social Engineering**: Durch geschickte Manipulation und Täuschung können Angreifer Personen dazu bringen, E-Mail-Adressen preiszugeben.
- **Öffentliche Verzeichnisse und Websites**: Viele Organisationen veröffentlichen Kontaktinformationen im Internet. Angreifer können diese Informationen sammeln, indem sie Websites durchsuchen oder spezielle Tools verwenden, um E-Mail-Adressen zu extrahieren.
- **Kauf von E-Mail-Listen**: Es gibt illegale Märkte, auf denen Listen mit E-Mail-Adressen verkauft werden. Diese Listen können aus früheren Datenlecks stammen oder durch andere betrügerische Methoden zusammengestellt worden sein.
- **Automatisierte Sammelwerkzeuge**: Angreifer verwenden manchmal sogenannte Bots und andere automatisierte Tools, um das Internet nach E-Mail-Adressen zu durchsuchen. Diese Tools können Foren, Kommentarbereiche und andere Online-Plattformen scannen.