03.08.2020

Neue Phishing-Welle

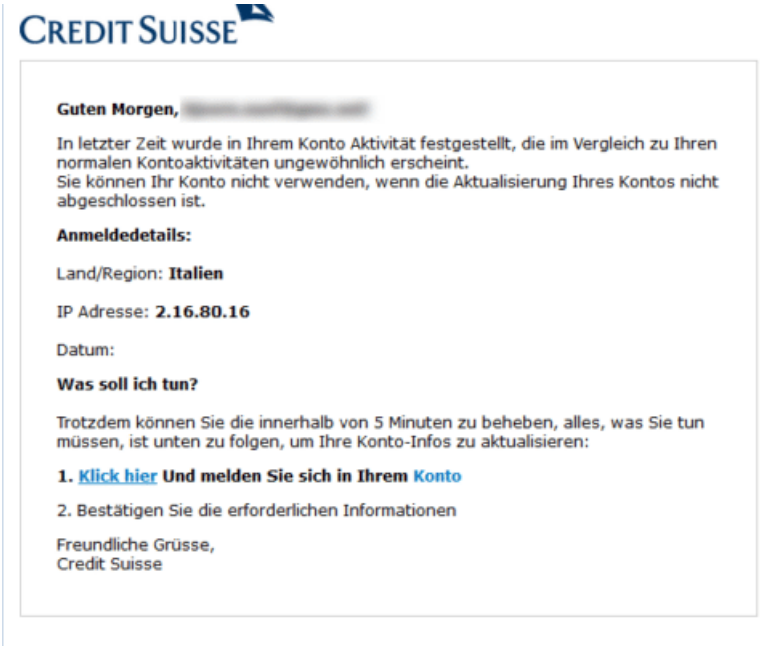
Aktuell sind gefälschte E-Mails von Finanzinstituten im Umlauf, die E-Banking Kunden auf ebenfalls gefälschte Bankenwebsites locken. Lassen Sie sich nicht täuschen!

Betrüger versuchen zurzeit wieder verstärkt, mit vermeintlichen E-Mails von Finanzinstituten wie der Credit Suisse Bankkunden auf nachgebaute E-Banking-Seiten zu locken. Ziel der aktuellen Phishing-Welle ist das Stehlen von Zugangsdaten und Kreditkarteninformationen.

Die Betrüger üben dabei Druck auf die Bankkunden aus: Unter einem Vorwand – z.B. der Kunde müsse seine persönlichen Daten aktualisieren – werden Bankkunden dazu verleitet, auf einen Link zu klicken, der zu einer gefälschten E-Banking-Seite führt.

Im Gegensatz zu früheren Angriffswellen kommen die E-Mails und die gefälschten Webseiten visuell und inhaltlich täuschend echt daher, in fast perfektem Deutsch und mit original Bank-Logos. Zudem verfügen die Seiten über ein gültiges Sicherheitszertifikat (SSL-Zertifikat) und zeigen dem potenziellen Opfer damit eine gesicherte Verbindung inklusive https:// und Schloss-Symbol in der Adresszeile des Browsers.

Zu erkennen sind die Fälschungen jedoch an der Adresse, welche nicht mit der des jeweiligen Finanzinstituts übereinstimmt, z.B. «https://entry.credit-suisse.services» oder «https://entry.swisscard.services».



CREDIT SUISSE

Guten Morgen, [redacted]

In letzter Zeit wurde in Ihrem Konto Aktivität festgestellt, die im Vergleich zu Ihren normalen Kontoaktivitäten ungewöhnlich erscheint.
Sie können Ihr Konto nicht verwenden, wenn die Aktualisierung Ihres Kontos nicht abgeschlossen ist.

Anmeldedetails:

Land/Region: **Italien**

IP Adresse: **2.16.80.16**

Datum:

Was soll ich tun?

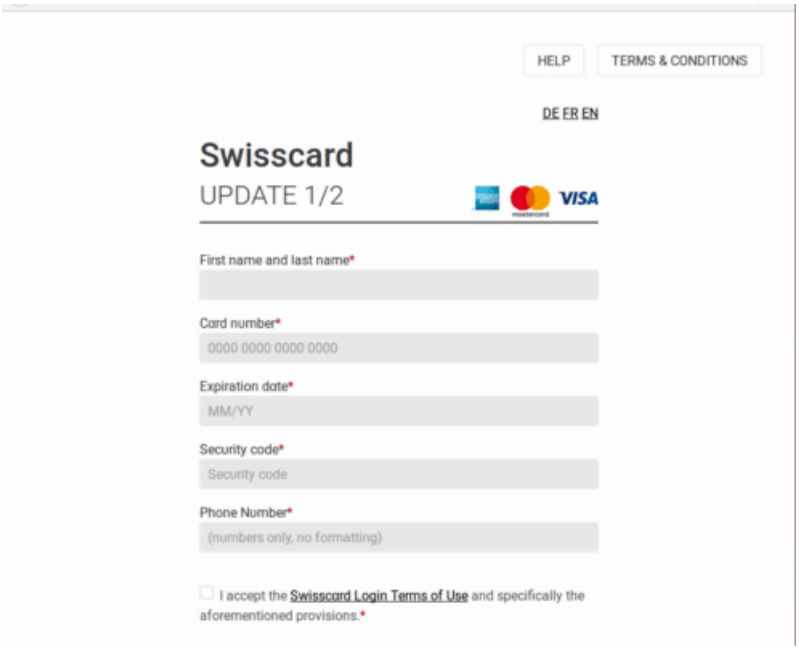
Trotzdem können Sie die innerhalb von 5 Minuten zu beheben, alles, was Sie tun müssen, ist unten zu folgen, um Ihre Konto-Infos zu aktualisieren:

1. Klick hier Und melden Sie sich in Ihrem Konto

2. Bestätigen Sie die erforderlichen Informationen

Freundliche Grüsse,
Credit Suisse

(https://www.ebas.ch/wp-content/uploads/2020/08/mail.png)



(https://www.ebas.ch/wp-content/uploads/2020/08/schritt2.png)

Schutz gegen Phishing bieten die folgenden Verhaltensregeln:

- Seien Sie vorsichtig im Umgang mit E-Mails. Auch bei vermeintlich bekannten Absendern Anhänge nicht gleich öffnen und auf Links nicht sofort klicken. Im Zweifel beim angeblichen Absender auf anderem Kanal (z.B. offizielle Telefonnummer der Bank) nachfragen. **Finanzinstitute fordern Sie nie per E-Mail zum Login oder zur Eingabe Ihrer Zugangsdaten auf!**
- Lassen Sie sich nicht unter Druck setzen («Ihr Konto wird gesperrt» etc.).
- Geben Sie die Adresse zur Anmeldeseite des Finanzinstituts immer manuell in die Adresszeile Ihres Browsers ein.
- Prüfen Sie die SSL-Verbindung (Grünes Schloss, Domain-Name, Zertifikat).
- Kontaktieren Sie bei Unsicherheit oder Fehlern umgehend Ihr Finanzinstitut.
- Erstellen Sie den Grundschutz mit unseren «5 Schritte für Ihre digitale Sicherheit» (https://www.ebas.ch/5steps) : Regelmässige Sicherungskopien erstellen, Virenschutz und Firewall verwenden, Betriebssystem und Programme aktuell halten, aufpassen und wachsam sein.

Weitere Hinweise zum Thema Phishing finden Sie hier (https://www.ebas.ch/phishing) .