

## Phishing E-Mails erkennen

### Achtung:

Phishing Angriff auf Viseca

Aktuell sind gefälschte E-Mails mit Viseca Absender im Umlauf. Diese E-Mails stammen nicht von Viseca.

### Infolinks zum Thema Phishing:

Aktueller Phishing Angriff Visa

[de.wikipedia.org/wiki/Phishing](https://de.wikipedia.org/wiki/Phishing)

[www.antiphishing.org](http://www.antiphishing.org)

[www.skppsc.ch/10/de/2betrug/7intern/110\\_gratis\\_download\\_pdf\\_ebook\\_der\\_kampagne.php](http://www.skppsc.ch/10/de/2betrug/7intern/110_gratis_download_pdf_ebook_der_kampagne.php)

[www.internetfallen.de](http://www.internetfallen.de)

### Immer wieder tauchen Phishing E-Mails auf mit denen Betrüger versuchen, Kreditkartendaten auszuspionieren, um diese für illegale Transaktionen zu nutzen.

In den letzten Wochen sind wieder vermehrt sogenannte Phishing E-Mails im Umlauf, welche Sie dazu auffordern, Ihre Kartenummer, das Verfalldatum der Karte, die Kartenprüfnummer (CVC), Ihr "Verified by Visa"-Passwort oder Ihren "MasterCard SecureCode" anzugeben. Diese E-Mails stammen nicht von der Viseca, sondern werden von Betrügern versendet. Wir bitten Sie darum, diese E-Mails unverändert und umgehend an uns weiterzuleiten ([internetsecurity@viseca.ch](mailto:internetsecurity@viseca.ch)) und danach zu löschen. Beantworten Sie diese E-Mails auf keinen Fall und geben Sie keine Daten ein. Sollten Sie Ihre Daten versehentlich angegeben haben, setzen Sie sich bitte so schnell wie möglich mit der Viseca Sperrzentrale (+41 58 958 83 83) in Verbindung, um ihre Karte sperren zu lassen und kostenlos eine neue Ersatzkarte zu erhalten.

Unter Phishing versteht man das Ausspionieren von Daten und Zugangsdaten für Kreditkarten, Online-Banking und Zahlungsdiensten wie z.B. PayPal, sowie Handelsplattformen (Ebay, Ricardo, iTunes etc.). Die Absicht der Phisher besteht darin, diese Daten für das Ausrauben der Konten oder für das Durchführen von illegalen Transaktionen zu benutzen.

### Ablauf des Betruges

- Sie bekommen eine E-Mail, die optisch so aussieht, als würde Sie von einer Institution stammen (Bank, Kreditkartenfirma, Zahlungsdienst o.ä.), bei der Sie ein Konto besitzen.
- Sie werden aufgefordert, Ihre Kontoinformationen einzugeben, zu bestätigen oder zu verändern.
- Mitunter werden komplizierte Geschichten von Fehlern erzählt und es wird Ihnen eine Kontosperrung angedroht, falls Sie die Daten nicht preisgeben.
- Sie werden dazu aufgefordert, die Webseite der Institution mittels eines in der E-Mail vorhandenen Links zu besuchen, um die nötigen Eingaben vorzunehmen.
- Der Klick auf den in der E-Mail enthaltenen Link führt Sie dann zu einer gefälschten Webseite, die der echten Webseite täuschend ähnlich sieht.
- Dann werden Sie erneut darum gebeten, die entsprechenden Angaben einzugeben. So werden Ihre Eingaben dann von den Betrügern gespeichert.

- Sie werden ganz normal in das Konto eingeloggt oder es erscheint eine Fehlermeldung. Anschließend werden Sie auf die Originalwebseite geleitet, wo Sie sich dann erneut einloggen müssen.
- Innerhalb kürzester Zeit werden so wichtige Informationen gewonnen, mit denen Sie geschädigt werden können.

### Erkennungsmöglichkeiten

- Die Visa Card Services SA, sowie alle anderen Banken und Kreditinstitute, fordern grundsätzlich keine vertraulichen Daten per E-Mail von Ihnen an.
- Verwenden Sie zum Aufruf einer Webseite immer Ihre Bookmarks / Favoriten oder geben Sie die URL mittels Eingabe in den Browser über Ihre Tastatur ein. Klicken Sie nicht auf Links in E-Mails zur Eingabe von Benutzerdaten oder Passwörtern.
- Geben Sie niemals Ihre PIN oder Passwörter an!
- Installieren Sie eine Phishing-Erkennungssoftware, bleiben Sie aber trotzdem wachsam und befolgen Sie die obigen Regeln.
- Warnen Sie Internetneulinge in Ihrem Freundeskreis vor dieser Betrugsart und erklären Sie diesen, wie Sie sich schützen können.
- Neben Spamfilter, Antivirensoftware und Firewall sollten Sie auch immer den gesunden Menschenverstand einsetzen.