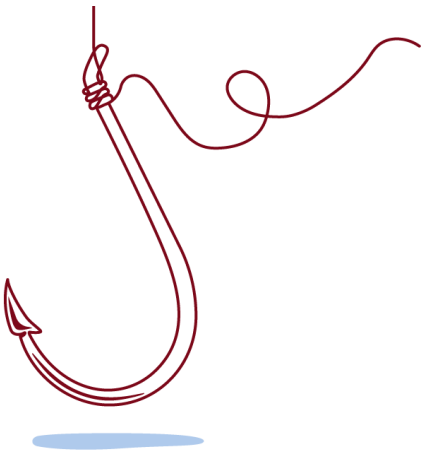
Tipps zum Schutz vor Phishing im Netz

18.10.2019
von

Altmann, Kathleen

Schlagworte

Phishing
Online-Shopping
Verbraucher
Onlinebanking
Dossier ECSM
Cybersicherheit
ECSM
Dossier Tipps zum Schutz



Mehr als die Hälfte der Bankkunden nutzt Onlinebanking zu Hause am Computer oder erledigt ihre Bankgeschäfte unterwegs mit Smartphone oder Tablet. Trotz hoher Sicherheitsstandards besteht dabei immer auch die Gefahr, dass Kriminelle versuchen, persönliche Zugangsdaten auszuspähen oder digitale Identitäten zu missbrauchen. Dieses als „Phishing“ bezeichnete Ausspionieren oder „Abfischen“ von Daten machte laut Bundeskriminalamt (BKA) 2017 immerhin rund zwölf Prozent aller angezeigten Cybercrime-Fälle aus. Durchschnittlich betrug der Schaden dabei 4.000 Euro pro Fall. Um solchen Schäden vorzubeugen und damit Onlinebanking sicher auf dem Computer oder Smartphone betrieben werden kann, gilt es einige grundsätzliche Regeln zu beachten.

Schutz gegen Phishing: Halten Sie Betriebssystem, Virenscanner, Firewall und Banking Apps aktuell

Der heimische Computer kann ein Einfallstor für Kriminelle sein. Wenn er nicht ausreichend geschützt ist, steht die „Haustür“ offen. Wer seine Bankgeschäfte online erledigt, sollte daher unbedingt einen Virenscanner und eine Firewall nutzen. Wer regelmäßige Updates veranlasst, bleibt so auf dem neuesten Stand. Diese sollten auch für die übrige Software einschließlich des Betriebssystems durchgeführt

werden. Verfügbare Updates sollten umgehend installiert werden, um einen ausreichenden Schutz vor Viren und Trojanern zu gewährleisten.

*In unserem Blogbeitrag erfahren Sie alle über **Smishing, Vishing, Phishing: So arbeiten Kriminelle im Netz und das können Sie tun***

Onlinebanking auf unbekannten Rechnern empfiehlt sich daher nicht, weil man nicht sicher sein kann, ob der Computer ausreichend geschützt ist. Auch für Smartphones und andere mobile Geräte gilt: Wer Bankgeschäfte damit erledigt und Banking Apps nutzt, muss das Betriebssystem und die Apps stets auf dem aktuellen Stand halten.

Banking Apps nur aus autorisiertem App Store laden zum Schutz gegen Phishing

Banking Apps sollten ausschließlich aus dem autorisierten App Store des Smartphones oder Tablets installiert werden (Google Play Store/Apple App Store). Für die Installation sollte dabei keinen, möglicherweise gefälschten „Hinweisen" zu einem Download aus werblichen E-Mails oder Webseiten nachgegangen werden. Vorsicht bei Gratis-Versionen! Allerdings sollte man auch bei kostenpflichtigen Apps stets Skepsis walten lassen, denn auch hierbei könnte es sich um Schadsoftware handeln.

*Wir beantworten alle Fragen rund um das Thema in unserem **Lexikon Cyberkriminalität** - und geben weitere Tipps, wie Sie sich schützen können.*

Speichern Sie PINs, TANs und andere Zugangsdaten nicht

Kennwörter, persönliche Geheimzahlen (PINs) und Transaktionsnummern (TANs) sollten niemals unverschlüsselt in Apps, in einer Cloud oder auf der Festplatte gespeichert werden. Auch wenn sie als Telefonnummern im Adressbuch abgespeichert werden, bietet dies keinen ausreichenden Schutz. Zugangsdaten sollten zudem regelmäßig geändert

werden. Dies gilt für die gesamten Nutzerkonten, nicht nur fürs Onlinebanking.

Schutz gegen Phishing: Prüfen Sie die Banking-Webseites

Bei Phishing-Angriffen versuchen Betrüger unter anderem, ahnungslose Nutzer per E-Mail oder SMS auf eine vermeintliche Onlinebanking-Webseite der Bank zu locken, um die Daten abzufangen. Bevor Bankkunden sich einloggen, sollten sie stets überprüfen, ob es sich wirklich um die verschlüsselte Seite der Bank handelt. Das ist unter anderem am „Schloss"-Symbol im Internet-Browser zu erkennen und daran, dass die Webadresse mit „https" beginnt.

Bleiben Sie Aufmerksam gegen Cybercrime

Auf E-Mails oder SMS der vermeintlich eigenen Bank, die zu einer Bestätigung der sensiblen Daten auffordern, etwa über die Abfrage von PINs oder TANs, sollte nicht geantwortet werden. Auf Links zu klicken, die zu einer weiteren Eingabeseite führen, sollte man ebenfalls unbedingt unterlassen. Banken fragen solche Daten niemals ab, weder per E-Mail oder SMS, aber auch nicht telefonisch. Wenn ein vermeintlicher Bankmitarbeiter anruft und dazu drängt, gemeinsam eine Transaktion vom Konto durchzuführen, sollte man das Gespräch umgehend beenden.

*Wir beantworten alle Fragen rund um das Thema in unserem Blogbeitrag „**Cybersicherheit geht uns alle etwas an**".*

Blog abonnieren

Phishing: Was tun, wenn es passiert ist?

Wer den Verdacht hat, Opfer eines Phishings geworden zu sein, sollte sich umgehend an die eigene Bank wenden und Anzeige bei der Polizei erstatten. Die Phishing-Nachricht kann in diesem Fall als Beweis dienen.

Immerhin: Seit 2014 lässt sich laut BKA ein rückläufiger Trend bei Phishing-Fällen im Onlinebanking feststellen. Das liegt neben der gestiegenen Aufmerksamkeit der Bankkunden auch daran, dass Banken ihre Erkennungsmechanismen stetig weiterentwickeln.