Sicherheit

Informationen, Tipps und Hinweise zum Schutz Ihrer Finanzen

Hier erhalten Sie verschiedene Informationen zum Thema Sicherheit

Sollten Sie einen Betrug vermuten, sperren Sie sofort Ihren Online-Banking-Zugang und/oder Ihre Karten und informieren Sie Ihre Bank

Phishing und Trojaner

Beim Phishing versuchen Betrüger Sie dazu zu bringen eine Überweisung zu tätigen, das TAN-Verfahren zu wechseln oder Ihre Zugangsdaten für das Online-Banking und Ihre Kreditkartendaten preiszugeben. Phishing-Angriffe nutzen verschiedenste Kommunikationskanäle: E-Mail, SMS, Telefon, gefälschte Internetseiten oder soziale Netzwerke. Es gibt sehr unterschiedliche Arten von Phishing, aber alle nutzen Vorwände, gefälschte Absenderdaten, Webseiten und Eingabemasken, die zum Beispiel der Banking-Anwendung oder einer gängigen Händlerseite ähneln.

Ein Trojaner ist eine Schadsoftware, mit der Betrüger häufig arbeiten. Diese Schadprogramme können unter anderem die Webseite des Online-Bankings mit eigenen Inhalten überblenden, die dem tatsächlichen Design der Bank entsprechen. Dort wird zur Eingabe einer TAN oder zur Übermittlung der Mobilfunknummer aufgefordert, zum Beispiel in Verbindung mit der Installation einer Software auf dem Mobiltelefon. In der Annahme, auf der korrekten Online-Banking-Plattform ihrer Bank zu sein, geben Empfänger dann ihre Daten ein.

Beispiele für Phishing sind:

- Aufruf, Software oder Bankdaten zu aktualisieren
- Aufforderung, persönliche Daten preiszugeben
- Warnung vor Phishing-Mails
- Gefälschte Mahnung, zum Beispiel mit Bezug auf Ihre Telefonrechnung
- E-Mail mit einem angehängten Dokument, das Sie prüfen oder mit einem Formular, das Sie ausfüllen sollen. Das Dokument oder Formular weist in der Regel ein ungewöhnliches Dateiformat auf (.EXE, .SCR, .CMS …)
- Hinweis, dass Ihre Kreditkarte oder Girocard (Debitkarte) abgelaufen sei
- Hinweis, dass Ihr Konto gesperrt wurde
- Aufforderung, Ihr Passwort zu erneuern
- Aufruf, Daten für Umfragen oder Gewinnspiele zu bestätigen
- Enkel- oder Neffentrick

Phishing Mails verwenden oft eine unpersönliche Anrede, enthalten die Aufforderung persönliche Daten einzugeben oder Anhänge zu öffnen, täuschen dringenden Handlungsbedarf oder die Androhung von Konsequenzen bei Nichthandeln vor. Oft enthalten diese Mails auch sprachliche Ungenauigkeiten oder sind in einer fremden Sprache verfasst. Prüfen Sie grundsätzlich jeden Link, den Sie erhalten. Am besten geben Sie die URL für die Bankenseite direkt in die Adressleiste Ihres Browsers ein. Sollte eine TAN abgefragt werden, ohne dass eine Transaktion erfolgt, sollten Sie misstrauisch werden.

So können Sie sich und Ihr Gerät schützen:

- Klicken Sie keine Links in E-Mails an

- Öffnen Sie keine E-Mails von unbekannten Absendern
- Banken fordern Sie niemals auf, Ihre Authentifikationsdaten preiszugeben
- Kontrollieren Sie regelmäßig Ihre Kontoumsätze
- Halten Sie Antiviren-Programme, Software, Browser und Betriebssystem aktuell
- Beziehen Sie Apps nur aus vertrauenswürdigen Quellen
- Nutzen Sie den Sperrcode Ihres Geräts sowie die automatische Bildschirmsperre

Eine der wichtigsten Regeln beim Online-Banking und beim Online-Einkauf lautet: Gehen Sie mit Sorgfalt vor. Wenn Sie Ihre Angaben auf den Überweisungsformularen und die Inhalte von Bestätigungsnachrichten genau überprüfen, bevor Sie sie bestätigen, erschweren Sie Betrügern den Erfolg erheblich.

Überprüfen Sie vor Eingabe einer TAN immer die angezeigten Werte auf dem Display Ihres TAN-Generators oder in der empfangenen SMS bzw. in der TAN-App. Weichen die Werte von denen der Originalrechnung ab, brechen Sie den Vorgang ab. Es wird immer die Transaktion ausgeführt, deren Werte im TAN-Generator bzw. im Mobiltelefon erscheinen.

Sollten Sie vermuten, Opfer eines Betrugs zu sein, handeln Sie umgehend:

- Sperren Sie ihre Karten und/oder das OnlineBanking: Sie erreichen den einheitlichen Sperrnotruf für Girocard (Debitkarte), Mastercard® und Visa Karte (Debitkarte oder Kreditkarte), digitale Karten und OnlineBanking unter der Nummer **+ 49 116 116** (alternativ, sofern Sie die 116 116 aus dem Ausland nicht erreichen: + 49 30 40 50 40 50)
- Nehmen Sie Kontakt zu Ihrer Bank auf
- Erstatten Sie Anzeige bei der Polizei
- Sichern Sie Beweise