Wichtige Hinweise zu gefälschten E-Mails, Phishing und Spyware

Was ist Phishing?

Immer mehr Menschen nutzen das Internet für bequeme Services wie Online Banking oder Online Shopping. Leider verwenden auch Kriminelle das Internet, um an Ihre persönlichen Daten zu gelangen: Sie versenden E-Mails, die als Absender einen bekannten Serviceanbieter vortäuschen. Diese E-Mails sehen erstaunlich echt aus und werden als Phishing E-Mails bezeichnet.

Wie erkennt man eine Phishing E-Mail?

Sie erhalten eine unerwartete E-Mail – scheinbar von Ihrer Bank oder einem anderen Serviceanbieter. Doch in Wirklichkeit gibt sich dabei jemand als Ihre Bank oder Ihr Serviceanbieter aus. In solchen E-Mails werden Sie in der Regel aufgefordert, Angaben zu Ihrem Bankkonto und manchmal auch Ihre PIN (Geheimzahl) einzugeben - entweder per E-Mail oder über eine Website, die man über eine eingebettete Verknüpfung (Hyperlink) in der E-Mail erreicht.
Kriminelle versuchen, Sie zu täuschen, indem sie Begriffe wie „Sicherheit und Datenpflege" oder „Untersuchung von Unregelmäßigkeiten" verwenden. Oft finden sich auch Mitteilungen wie „Ihr Konto wurde gesperrt", „Ihre Kontoangaben müssen erneut bestätigt werden", oder sogar „Sie haben einen hohen Geldbetrag auf Ihrem Konto, bitte überprüfen Sie die Transaktionen". Damit soll die Wahrscheinlichkeit erhöht werden, dass Sie den Hyperlink anklicken, um sich einzuloggen oder eine Reihe von Fragen zu beantworten.

Spyware

Kriminelle setzen auch so genannte Spyware ein. Diese Software kann unbemerkt auf Ihrem Computer installiert werden und ist in der Lage, im Hintergrund nach sensiblen Daten wie Kontoinformationen oder Passwörtern zu suchen oder Ihre Tastatureingaben aufzuzeichnen. Die Daten werden dann ebenfalls unbemerkt an eine fremde E-Mail-Adresse oder einen fremden Server verschickt. Kriminelle bauen Spyware in Internetseiten, E-Mails oder E-Mail-Anhänge ein. Sobald ein infiziertes Objekt geöffnet wird, installiert sich die Spyware auf Ihrem Computer – ohne, dass Sie es merken.
Sogenannte Viren, Würmer und Trojanische Pferde greifen in Betriebssystemabläufe ein und sind somit in der Lage, Tastatureingaben und Bildschirmanzeigen abzufragen und an unbefugte Dritte weiterzugeben. Werden solche Programme bewusst oder unbewusst (z.B. aus Unwissenheit über die Herkunft) durch Sie gestartet, dann können diese Aktivitäten völlig unbemerkt stattfinden.
Deshalb - löschen Sie bitte verdächtige E-Mails ohne sie zu öffnen. Öffnen Sie bitte keine verdächtigen Anhänge, auch wenn sie von einer Ihnen bekannten E-Mail-Adresse zu kommen scheinen. Deaktivieren Sie die Autovorschau-Funktion, um ein automatisches Öffnen der E-Mails zu verhindern.

Was Sie wissen sollten...

Die ATEbank wird Sie niemals nach Ihren Kontoangaben oder Ihrer PIN (Geheimzahl) per E-Mail fragen. Bitte beantworten Sie solche E-Mails nicht und folgen Sie auch nicht den dort angegebenen Instruktionen – selbst wenn man Ihnen mitteilt, dass Ihr Konto gesperrt oder gelöscht wird oder Ihnen mit einer Geldstrafe gedroht wird.

Im Verdachtsfall informieren Sie uns bitte über unsere Filiale in Frankfurt a.M. oder rufen Sie unsere kostenlose Service Hotline unter der Rufnummer +49 69 240011 414 an.