Konsumentenschutz-Info

Beim eBanking ist was anders. Aber was genau?

„Zwei-Faktor-Authentifizierung“ nennt sich der sperrige Begriff, der den zusätzlichen Schutz vor unberechtigtem Kontozugriff beschreiben soll.

STARKE KUNDENAUTHENTIFIZIERUNG BEIM EBANKING IST PFLICHT

eBanking soll sicherer werden, daher wird seit 14. September 2019 ein Mehr an Schutz vorgeschrieben. Das Zahlungsdienstegesetz sieht in der Umsetzung einer EU-Richtlinie vor, dass sich Bankkunden beim eBanking mit mindestens zwei von drei Authentifizierungsmerkmalen ausweisen müssen:

1. Über den Besitz von etwas, das ausschließlich von Konsumenten verwendet wird: Bsp.: Chip-Tan-Gerät, Handy
2. Wissen über Passwort oder PIN
3. Inhärenz: Eigenschaften, die der Person zugeordnet werden, also Fingerabdruck, Netzhaut, Gesichtserkennung (Face ID).

In Österreich erfolgt die Umsetzung dieser Anforderung an die Banken meist durch zusätzliche Apps.

PUSH-TAN-VERFAHREN UND REGISTRIERTE GERÄTE

Nach Eingabe der Überweisungsdaten wird in der zusätzlichen App, diese kann auch in der bisherigen App integriert sein, ein Push-TAN zur Verfügung gestellt. Dieser wird nur an registrierte Smartphones mit Internetzugang gesendet. SMS-TANs werden im Gegensatz dazu an eine Telefonnummer versendet. Der Zugriff auf dieses Gerät ist mit Passwort bzw. PIN oder Fingerscan gesichert. Der Push-TAN gilt nur für die erfassten Überweisungen. Werden diese verändert, so wird der TAN ungültig.

WAS GEHT NOCH OHNE SMARTPHONE? ALTERNATIVEN?

Es gibt Alternativen in Form von Card-TANs, SMS-TANs und Security APPs für den Desktop (PC) bei den Banken. Für die Verwendung von Card-TANs (nicht bei allen Banken möglich) wird allerdings ein eigenes Kartenlesegerät benötigt.

WAS KOSTET DIE SICHERHEIT?

Die Apps und Push-TANS sind kostenlos. Die Kartenlesegeräte werden meist von den Banken noch kostenlos abgegeben.

Information

Gefahrenhinweise des AK-Konsumentenschutzes

Erfahrungsgemäß werden Neuerungen auch als willkommene Gelegenheit für Betrüger wahrgenommen. Informieren Sie sich nur über gesicherte Webseiten Ihrer Bank (http://) bzw. die Kundenhotline bezüglich Merkmale und Installation des neuen Verfahrens. Absolute Vorsicht bei scheinbar vertrauenswürdigen E- Mails. Steigen Sie nicht über darin enthaltene Links in Ihr eBanking ein. Weitere Infos zum Schutz vor Cyber Crime auf der AK-Homepage: **ooe.konsumentenschutz.at**