Erste Hilfe bei Phishing, Hacking und Online-Betrug

Haben Sie ungewöhnliche Transaktionen auf Ihrem Konto festgestellt? Erhalten Sie Benachrichtigungen von Ihrer BKS Security App, obwohl Sie keine Transaktion in Auftrag gegeben haben? Haben Sie Ihre Zugangsdaten auf einer unseriösen Website eingegeben? ***In diesen Fällen ist schnelles Handeln gefragt!***

1. Karten und Online-Banking sperren

Sollten im Zuge eines Betrugsfalls Ihre Karteninformationen betroffen sein, müssen die involvierten Karten gesperrt werden. Die Sperre kann selbstständig im MyNet, BizzNet oder der BKS Bank App von Ihnen vorgenommen werden. Alternativ kann eine Kartensperre auch über das BKS Kundenservice Center beauftragt werden. Kontaktieren Sie dieses unter **+43 463 5858 (Mo.-Fr.: 07:00-19:00 Uhr)** und schildern Sie die Situation.

Sollten Sie den Verdacht haben, dass auch Ihre Zugangsdaten zum Portal gestohlen wurden, können unsere Mitarbeiter Ihren Online-Banking-Zugang vorübergehend sperren, sodass keine weiteren Transaktionen vorgenommen werden können. Bei zeitnahen Einmeldungen von Betrugsfällen gibt es gegebenenfalls die Möglichkeit, Überweisungen rückgängig zu machen.

Achtung: Außerhalb der Geschäftszeiten können Sie Ihren Zugang selbst sperren, indem Sie die Anmeldeseite ihres Onlinebankings aufrufen und dreimal hintereinander eine falsche PIN eingeben. Kontaktieren Sie das Kundenservice Center anschließend innerhalb der Geschäftszeiten, um alle weiteren Schritte einzuleiten.

2. Informationen sichern

Sammeln Sie alle Informationen, die zur Klärung des Sachverhalts beitragen können. Dazu zählen zum Beispiel Bildschirmaufnahmen, E-Mails oder Links zu dubiosen Websites.

3. Geräte auf Schadsoftware untersuchen

Besteht der Verdacht, dass Ihr Gerät mit Schadsoftware infiziert wurde, scannen Sie Ihre Geräte gründlich mit einer Schutzsoftware oder lassen Sie Ihr Gerät von einem IT-Fachmann untersuchen und bei Bedarf zurücksetzen. Führen Sie keine Online-Transaktionen oder Passwortänderungen durch, solange Ihre Geräte nicht überprüft und bereinigt wurden.

4. Zurücksetzen der Anmeldeinformationen

Im nächsten Schritt werden Ihre Anmeldeinformationen zum Online-Banking zurückgesetzt. Halten Sie sich bei der Vergabe einer neuen PIN an unsere Tipps für starke Passwörter unter www.bks.at. Wir empfehlen Ihnen, für jede Anwendung ein eigenes Passwort zu verwenden. Sollte Schadsoftware auf Ihrem Gerät entdeckt werden, sollten auch alle weiteren Passwörter, die Sie verwenden, geändert werden.

5. Anzeige bei der Polizei

Sollte Ihnen ein monetärer Schaden entstanden sein, erstatten Sie immer eine Anzeige bei der Polizei.

Schutzmaßnahmen für Ihr Onlinebanking

Die Sicherheit beim Onlinebanking ist von entscheidender Bedeutung, um den Schutz Ihrer Daten und die Vermeidung von betrügerischen Aktivitäten zu gewährleisten. Im Folgenden erhalten Sie die wichtigsten Tipps für sicheres Onlinebanking.

- „Geben Sie Ihr Passwort ein." Bitte folgen Sie diesem Befehl nur nach genauer Kontrolle. Überprüfen Sie vor jeder Anmeldung, ob Sie sich auf der richtigen Seite **https://www.bksbank-online.at** befinden.
- Geben Sie die Zugangsdaten zu Ihrem MyNet oder BizzNet auf keinen Fall an Dritte weiter – hierzu gehören auch Familienmitglieder.
- Die Mitarbeiter der BKS Bank und anderer seriöser Unternehmen werden niemals Passwörter, Zugangsdaten oder Kreditkartennummern per E-Mail oder Telefon abfragen.
- Mit der Freigabe in der BKS Security-App wird im Regelfall eine Abbuchung von Ihrem Konto bestätigt. Überprüfen Sie vor jeder Freigabe die angezeigten Informationen in der BKS Security-App. Freizugebende Aktionen in der Security App, die nicht von Ihnen initiiert wurden, dürfen auf keinen Fall freigegeben werden. Es könnte sich dabei um einen Betrugsversuch handeln. Gehen Sie mit Ihrem Online-PIN mit der gleichen Sorgfalt um wie mit Ihrem Bankomat-PIN.
- Wenn Ihnen etwas seltsam vorkommt, brechen Sie die Aktion im Zweifel besser ab und kontaktieren Sie Ihren Kundenbetreuer oder unser Kundenservice-Center unter **+43 463 5858**.
- Wichtige Informationen zu Veränderungen rund um Ihr Bankgeschäft und die verwendeten Sicherheitsverfahren erhalten Sie von uns ausschließlich postalisch, als Nachricht über Ihr Kommunikationszentrum im Onlinebanking oder als Information auf www.bks.at.

Was Sie selbst zu Ihrer Sicherheit beitragen können

Wenn Sie die folgenden Ratschläge beachten, können Sie sich vor Online-Bedrohungen aller Art schützen:

- Für Sie als Internetnutzer heißt es: Aufpassen! Schauen Sie bei den angeklickten Internetadressen besser zweimal hin und überlegen Sie genau, wem Sie welche Daten anvertrauen möchten.
- Bleiben Sie bei Geldforderungen via Telefon, Whats App, SMS oder E-Mail generell immer misstrauisch.
- Achtung: Internet-, E-Mail-Adressen und Telefonnummern können gefälscht werden und sind nicht immer vertrauenswürdig.
- Öffnen Sie keine Dateianhänge von E-Mails unbekannter Absender.
- Erledigen Sie Bankgeschäfte oder Online-Einkäufe nie über eine ungesicherte WLAN-Verbindung oder über öffentlich zugängliche Geräte.
- Speichern Sie weder PINs noch BKS Bank-Online Verfügernummern auf Ihrem Computer, Tablet oder Smartphone.
- Ein Virenschutz, der regelmäßig aktualisiert wird, kann den Rechner vor Angriffen durch Hacker schützen. Regelmäßige Updates gewährleisten, dass auch die Sicherheitsvorkehrungen von Internetbrowsern und Betriebssystemen immer auf dem neuesten Stand sind.
- Informieren Sie sich laufend über aktuelle Betrugsmaschen, um den Betrügern immer einen Schritt voraus zu sein. Wenn etwas zu schön klingt, um wahr zu sein, ist dies auch meist der Fall. Achten Sie daher immer auf Ihr Bauchgefühl.