Website-Kommunikation zu Kundensicherheit und Betrugserkennung

Unsere Sicherheitsstrategie

Wenn es um Ihre Finanzdaten geht, hat Ihre Sicherheit für uns oberste Priorität, und wenn Sie auf Ihr E-Geld-Konto zugreifen, müssen wir sicher sein können, dass Sie es sind. Das gewährleisten wir unter anderem wie folgt:

Mit Login-Daten

Sie bekommen Online-Login-Daten von uns, die nur für Sie gelten. Zu Ihrem eigenen Schutz empfehlen wir Ihnen, diese vor anderen geheim zu halten.

Mit Sicherheitsfragen

Wenn Sie Kontakt mit unserem Kundenserviceteam aufnehmen, werden Sie gegebenenfalls gebeten, durch Beantworten der Sicherheitsfragen, die Sie bei der Erstellung Ihres Online-E-Geld-Kontos angegeben haben, Ihre Identität zu bestätigen.

Mit einmaligen Sicherheitscodes

In folgenden Fällen senden wir zwecks zusätzlicher Sicherheit diese einmaligen Codes an Ihre E-Mail-Adresse, die vom Administrator Ihres Unternehmens bereitgestellt wird:

- regelmäßig beim Einloggen, nur um sicherzustellen, dass Sie es sind;
- wenn Sie um Änderung Ihrer personenbezogenen Daten bitten.

Übermittlung von Informationen

Wir werden Sie niemals nach Ihrem Online-Passwort oder Ihrer PIN fragen. Wir werden Sie immer auffordern, unsere Milo App oder Self-Service-Website zu verwenden

Meldung von Betrug

Wenn Sie etwas Verdächtiges bemerken und glauben, dass es sich um (versuchten) Betrug handeln könnte, bitten wir Sie, uns so bald wie möglich unter Verwendung der unten stehenden Details zu kontaktieren.

Meldung von Betrug:	servicedesk@xximo.de oder 0180 6 – 555333*
Verlorene oder gestohlene Karten:	0180 6 – 555333*
Verdächtige E-Mails:	servicedesk@xximo.de oder 0180 6 – 555333*

* (35 Cent/Anruf aud dem dt. Festnetz; Mobilfunk max. 60 Cent/Anruf)

Wie Sie sich vor Betrug schützen

Helfen Sie mit, sich vor Betrügern zu schützen, indem Sie die unten aufgeführten Tipps befolgen. Handeln Sie nicht, wenn Sie Zweifel an etwas haben. Ein echtes Unternehmen drängt Sie niemals dazu, etwas zu tun.

Sorgen Sie dafür, dass Ihre bei uns registrierte Mobiltelefonnummer und E-Mail-Adresse immer aktuell sind. Wir werden diese verwenden, um Sie zu kontaktieren, wenn wir ungewöhnliche Aktivitäten auf Ihrem E-Geld-Konto feststellen.

Einige Tipps zur sicheren Nutzung Ihres E-Geld-Kontos und Ihrer Prepaid-Karte

Beim Zugriff auf Ihr Online-E-Geld-Konto

- Verwenden Sie eine Antivirensoftware und eine Firewall.
- Sorgen Sie dafür, dass Ihr Computer und Ihr Browser immer auf dem neuesten Stand sind.
- Verwenden Sie gesicherte Netzwerke.

- Verwenden Sie sichere Passwörter.
- Geben Sie keine Passwörter weiter, auch keine Ihnen zugesandten einmaligen Sicherheitscodes.

Bei der Verwendung einer mobilen Anwendung
- Installieren Sie nur Apps über offizielle App-Stores.
- Prüfen Sie die App-Bewertungen und Rezensionen.
- Seien Sie sich bewusst, welche Zustimmungen Sie erteilen.
- Behandeln Sie Ihr Mobiltelefon wie Ihre Brieftasche.

Beim Einkaufen im Internet oder in einem Geschäft
- Wenn Sie in einem bestimmten Onlineshop zum ersten Mal einkaufen, sollten Sie einige Recherchen anstellen, um sicherzustellen, dass er echt ist.
- Antworten Sie nicht auf unerbetene E-Mails von Unternehmen, die Sie nicht kennen.
- Stellen Sie vor dem Eingeben Ihrer Prepaid-Kartendaten sicher, dass der Link sicher ist. Im Browser-Fenster sollte ein Vorhängeschloss-Symbol zu sehen sein, das beim Anmelden oder Registrieren angezeigt wird. Wenn dieses Symbol auf der Website und nicht im Browser erscheint, kann dies auf eine betrügerische Website hinweisen. Die Webadresse sollte mit https://beginnen. Das „s“ steht für „sicher“.
- Melden Sie sich nach der Nutzung immer von der Website ab. Das einfache Schließen des Browsers reicht nicht aus, um die Sicherheit Ihrer Daten zu gewährleisten.
- Bewahren Sie Ihre PIN sicher auf und geben Sie sie nicht weiter.
- Achten Sie beim Eingeben Ihrer PIN auf Personen in Ihrer Umgebung und verdecken Sie Ihre PIN-Nummer.
- Überprüfen Sie immer Ihre Kontoauszüge.

Wenn Sie ein altes Mobiltelefon, einen Computer, einen Laptop oder ein Tablett spenden, weiterverkaufen oder recyceln, sollten Sie nicht vergessen sicherzustellen, dass Sie vorher alle Daten und Anwendungen vollständig entfernen, da andernfalls der nächste Besitzer Ihres alten Geräts Zugriff darauf erlangen kann.