

## **Wichtige Hinweise für die Optimierung der Sicherheit beim Online-Banking:**

- Prüfen Sie beim Öffnen der Sparkassenseite ([www.ksk-syke.de](http://www.ksk-syke.de)), ob Sie auf der richtigen Seite sind (Fingerprint siehe "Merkblatt für Online-Banking"). Sieht die Seite genauso aus wie gewohnt?
- Werden Sie misstrauisch, wenn es zu ungewöhnlichen Fehlermeldungen, Anweisungen oder angeblichen Tests beim Anmelden auf der Sparkassenseite kommt. Beenden Sie den Internetzugang und informieren Sie Ihre Sparkasse unter einer der umseitig genannten Telefonnummern.
- Geben Sie nur dann eine TAN ein, wenn Sie selbst einen Auftrag erteilen wollen. Pro Auftrag wird immer nur eine TAN abgefragt.
- Bevor Sie die TAN eingeben, kontrollieren Sie auf Ihrem mobilen Gerät oder TAN-Generator, ob die richtige Auftragsart, die Kontonummer des Zahlungsempfängers (die letzten 10 Stellen der IBAN) und der richtige Betrag angezeigt werden. Bei smsTAN und pushTAN kontrollieren Sie auch Datum und Uhrzeit.
- Geben Sie Ihren Anmeldenamen und die PIN **niemals** an eine andere Person weiter.
- Schützen Sie Ihren PC vor Viren und Trojanern durch den Einsatz eines aktuellen Betriebssystems (Windows XP ist seit April 2014 nicht mehr aktuell) und eines aktuellen und aktiven Viren-Scanners. Nutzen Sie auf Windows-Rechnern zumindest die vorhandene Firewall. Angreifbare Software wie Internet-Browser, PDF-Reader, Adobe-Flash-Player usw. sollten immer auf dem neuesten Stand sein.
- Nutzen Sie für das Online-Banking keine fremden Netzwerke oder fremdes WLAN (Internetcafe, Hotspots, Flughafen, Hotel usw.)
- Öffnen Sie keine Links in E-Mails, die angeblich von Ihrer Sparkasse kommen. Prüfen Sie solche Mails kritisch und setzen Sie sich bei zweifelhaften Inhalten mit Ihrer Sparkasse in Verbindung. Öffnen Sie auch keine Anhänge aus E-Mails, bei denen der Absender nicht zweifelsfrei ist.
- Beantworten Sie im Internet oder per Mail niemals Fragen nach Ihren Online-Zugangsdaten (Ausnahme: Von Ihnen beauftragte Kontoinformationsdienste oder Zahlungsauslösedienste), Mobilfunkdaten oder sonstigen persönlichen Daten.
- Abmelden nicht vergessen. Melden Sie sich nach Erledigung Ihrer Aufgaben mit der "Abmelden"-Schaltfläche aus dem Online-Banking ab.

## **Unsere Empfehlung für Ihr Online Banking:**

**Reduzieren Sie Ihr Tageslimit** für Online-Banking Aufträge auf einen möglichst geringen Betrag.

**Nutzung einer Online-Banking-Software** (z.B. StarMoney oder SFirm). Bis jetzt sind hier keine Probleme mit Viren oder Trojanern aufgetreten. Bei StarMoney und SFirm wird beim Starten überprüft, ob Programmdateien manipuliert wurden. Außerdem prüft die Software automatisch, dass nur Daten mit der Sparkasse getauscht werden.

**Einsatz einer HBCI-Chipkarte.** Eine Chipkarte kann nur im Zusammenhang mit einer Banking-Software eingesetzt werden. Die PIN-Eingabe erfolgt sicher über ein spezielles Lesegerät.

**Überprüfen Sie bitte regelmäßig den Sicherheitsbereich auf unserer Homepage [www.ksk-syke.de/sicherheit](http://www.ksk-syke.de/sicherheit).** Dort werden aktuelle Informationen veröffentlicht.

# Merkblatt für Online-Banking

Sehr geehrte Kundin, sehr geehrter Kunde,

unser Online-Banking erreichen Sie über die Internetadresse [www.ksk-syke.de](http://www.ksk-syke.de). Geben Sie diese Adresse aus Sicherheitsgründen immer von Hand in die Adresszeile Ihres Internetprogrammes ein. Speichern Sie die Adresse bitte nicht als Lesezeichen und rufen Sie unsere Internetseite bitte nicht über eine Suchmaschine wie z.B. Google auf.

Um Ihnen die Möglichkeit zur Echtheitsprüfung unserer Internet-Bankingseiten zu geben, haben wir diese mit einem Echtheitszertifikat versehen. Dieses Zertifikat wird aus Sicherheitsgründen regelmäßig erneuert, womit sich auch die im Zertifikat enthaltenen Fingerabdrücke (Fingerprints) ändern. Die unten stehenden Fingerprints gelten ab dem

**29. August 2018**

Bitte achten Sie beim Internet-Banking darauf, die Fingerprints im Zertifikat der Anmeldeseite zu prüfen. Die Darstellung des Fingerprints hängt vom verwendeten Web-Browser (Internet Explorer, Firefox, Opera usw.) ab.

Die aktuellen Fingerprints für die Internetseite [www.ksk-syke.de](http://www.ksk-syke.de) lauten:

SHA1 Fingerprint: 43:03:2F:6B:AF:B2:E3:DC:F5:E5:B8:0A:CE:B9:58:37:74:71:80:2D

Bei der Anmeldung über Giropay ([giropay.ksk-syke.de](http://giropay.ksk-syke.de)):

SHA1 Fingerprint: F0:66:83:E5:0C:48:5B:56:0B:A4:B9:F6:33:2B:D2:53:8F:44:F2:06

## Die erste Anmeldung:

Bei der ersten Anmeldung ändern Sie die Start-PIN in Ihre geheime PIN. Ihre neue PIN **muss 5-stellig** sein.

## Erlaubte Zeichen zur Vergabe der PIN sind:

- Kleinbuchstaben von a - z
- Großbuchstaben von A - Z
- Ziffern von 0 - 9 (Jedoch keine Einfachkombinationen wie z. B. 12345 oder 11111)
- Sonderzeichen ä, ö, ü bzw. Ä, Ö, Ü und ß sowie ! \$ % & / ( ) = ? + # , . - :

**Achten Sie bitte auf die Hinweise auf der Seite "PIN ändern"**

**Erst nachdem Sie die Start-PIN geändert haben, können Sie auf Ihre Konten zugreifen!**

## Banking-Software

Wenn Sie eine Banking-Software benutzen, benötigen Sie für die Einrichtung Ihrer Konten bei uns einige Zugangsdaten:

**PIN/TAN:** Ihre Legitimations-ID oder Ihren Anmeldenamen  
Kommunikationsadresse = **banking-ni1.s-fints-pt-ni.de/fints30**  
HBCI-Version = 3.0  
Port 443

**HBCI-Chipkarte:** Benutzerkennung = erhalten Sie mit Ihrer neuen HBCI-Karte  
Kommunikationsadresse = **banking-ni1.s-fints-pt-ni.de**  
IP-Adresse = 62.181.154.128  
HBCI-Version = 3.0  
Port 3000

**Falls Sie den Verdacht haben, dass mit der Banking-Anwendung irgendetwas nicht stimmt: Sperren Sie Ihren Zugang. Wenden Sie sich dazu entweder direkt an Ihre Sparkasse oder wählen Sie rund um die Uhr den Sperr-Notruf 116 116 – deutschlandweit kostenfrei. Auch aus dem Ausland ist der Sperr-Notruf erreichbar.**

**Unsere Online-Banking Spezialisten stehen Ihnen unter der Telefonnummer 04242 161 660 für Firmenkunden und 04242 161 670 für Privatkunden zur Verfügung.**