



Agenda für den PC Stammtisch Eichenau

1. Begrüßung – Vorstellung der Referenten
2. Rückblick (Entwicklung des Online-Banking)
3. Gründe für Online-Banking / Nutzen
4. Sicherungsmittel im Online-Banking
5. Internetanwendungen
6. Softwarelösungen/ Apps
7. Kontowecker
8. Phishing und unser Beitrag für Ihre Sicherheit
9. Sicherheitsfragen im Internet
10. Bezahlformen im Internet (giropay, Paydirekt)
11. Zusammenfassung/ Zeit für Ihre Fragen

1. Begrüßung/ Vorstellung der Referenten

Christian Windele

- Ausbildung zum Bankkaufmann
- Fachseminar Electronic Banking an der Sparkassen-Akademie in Bonn erfolgreich abgeschlossen
- Seit über 25 Jahren im Bereich Electronic Banking tätig
- Hauptberuflich bei der Sparkasse Fürstenfeldbruck (Fachberater Payment)

2. Rückblick (Entwicklung des Online-Bankings)

- **Bei Firmen:** Übermittlung von Daten zur Bank per Magnetband, Diskette und Leitung (Datex-P)
- **Privat:** 1984 Einführung von BTX durch die damalige Deutsche Bundespost als Weiterentwicklung von Videotext.
- Bedienung über Fernseher und BTX-Decoder (Hardware). Navigation über *Auswahlzahl#.
- Übertragungsraten mit Modem 1200 bit/s - aktuell bei Glasfaser bis zu 1000 Mbit (1 kbit = 0,001 Mbit)
- Bereits Absicherung über PIN/Transaktionsnummern

2. Rückblick/ Entwicklung des Online-Bankings

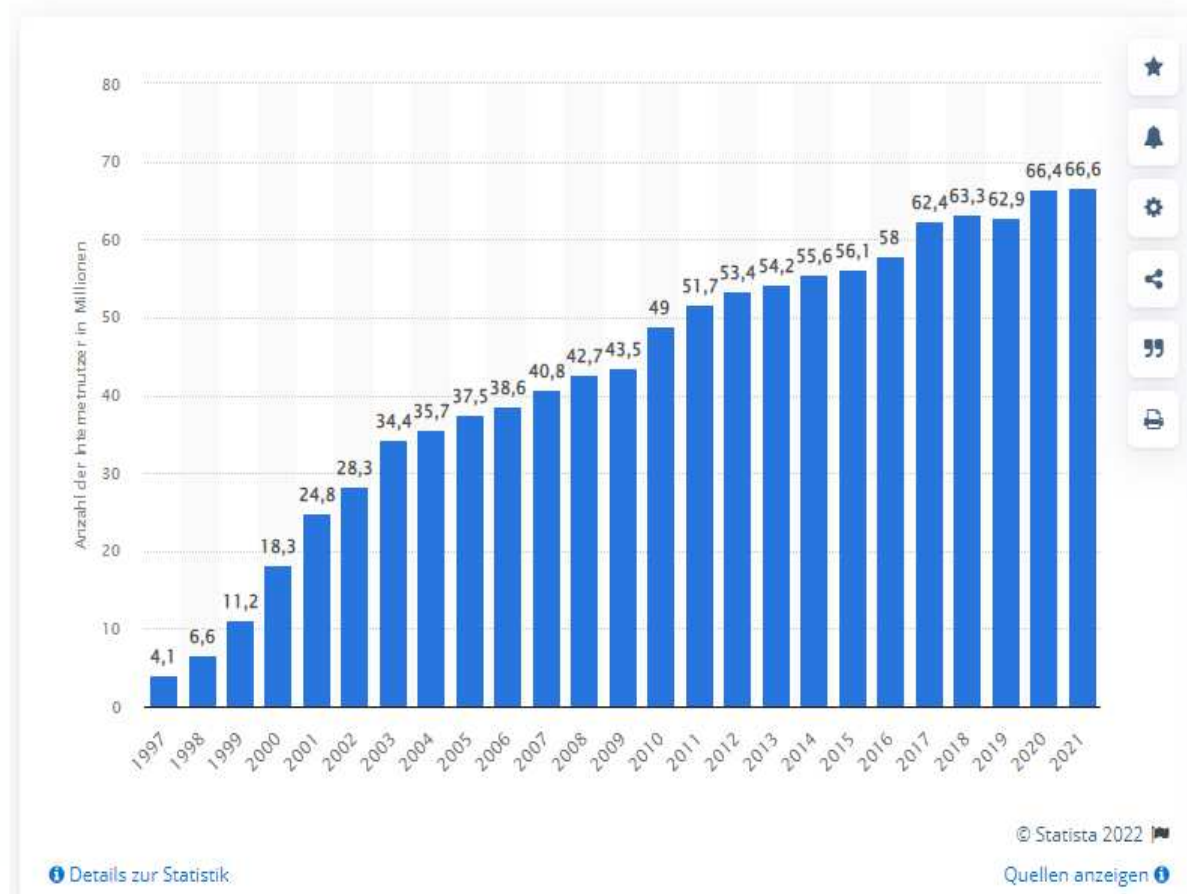
Banking-Anwendung im CEPT-Standard

The screenshot shows a terminal-style banking application window with a menu structure. At the top, there is a menu bar with 'Datei', 'Verbindung', 'Einstellungen', and 'Info'. Below this is a red header bar with a white 'S' logo and the text 'Kontoservice für Kunden'. The main area contains input fields for 'Kontonummer' and 'PIN'. Below these are two sections: 'Konten-Information' with options 10 (Kontenübersicht), 11 (Kontostand), and 12 (Umsatz-Anzeige); and 'Zahlungsverkehr' with options 21 (Einzelüberweisung), 22 (Sammelüberweisung), 23 (Sparübertrag), 24 (Dauerauftrag), 80 (Dienste), and 90 (Verwaltung). At the bottom, there is an 'Auswahl:' field and a red bar with the instruction 'Bitte Kontonummer eingeben, weiter mit #' followed by the account number '50030010823003a'.

```
Datei Verbindung Einstellungen Info
S  Kontoservice für Kunden
Kontonummer: [ ] PIN: [ ]
Konten-Information
10 Kontenübersicht
11 Kontostand
12 Umsatz-Anzeige
Zahlungsverkehr
21 Einzelüberweisung      80 Dienste
22 Sammelüberweisung     90 Verwaltung
23 Sparübertrag
24 Dauerauftrag
Auswahl: [ ]
Bitte Kontonummer eingeben, weiter mit #
50030010823003a
```

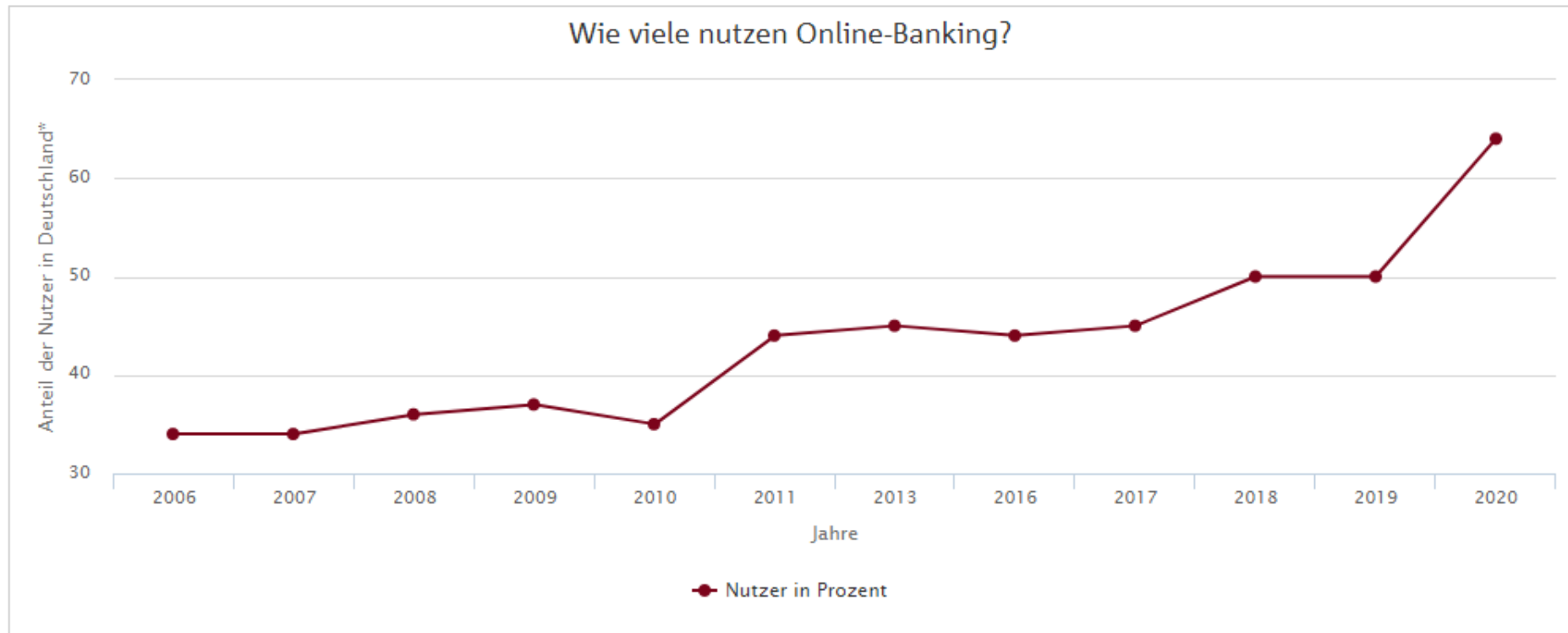
2. Rückblick / Entwicklung der Internet-Nutzung

Anzahl der Internetnutzer in Deutschland in den Jahren 1997 bis 2021
(in Millionen)



2. Rückblick / Entwicklung der Online-Banking-Nutzung

Die Entwicklung der Nutzung von Online-Banking von 2006 bis 2020



Zur Auswahl einzelner Datenreihen bitte in der Legende klicken.

Quelle: Bankenverband / KANTAR, 2020

3. Gründe für Online-Banking/ Nutzen

- Kontozugang weltweit rund um die Uhr mit PC, Smartphone u. Tablet
- Kein Aufwand, zur Sparkasse zu kommen (Parkplatzsuche, Strafzettel, Kraftstoffkosten, Zeitaufwand, körperliche Einschränkungen)
- Kontaktreduzierung / Pandemie
- Überweisungen zu bestimmten Terminen; unberechtigte Lastschriften selber korrigieren; Daueraufträge einrichten, ändern oder löschen; Gelder auf Unterkonten transferieren; Kontostand abfragen.
- Übersichtliche Kontoführung / gute Auswertungsmöglichkeiten
- hohe Sicherheitsstandards beim Online-Banking
- Basis für ePostfach (keine Zwangsauszüge mehr, gesicherte Kommunikation, Archivierung)

4. Sicherungsmittel im Online-Banking

PIN/TAN-Verfahren

chipTAN

Der Kunde erhält einen chipTAN-Generator mit Ziffernfeld und Karteneinschub für die SPK-Card oder eine kontoungebundene HBCI-Karte (liegt in jeder GS bereit)

Nach Eingabe der Zahlung am PC erhält der Kunde eine flackernde Schwarz-Weiß-Fläche oder einen QR-Code, an die er den Generator hält. Auf dem Display kontrolliert der Kunde die Details zum Auftrag und erhält die erforderliche TAN-Nummer für die Freigabe seines Auftrags.

Kosten: chipTAN-Generator einmalig ab 20,-- € / keine weiteren Kosten für TAN-Erzeugung

smsTAN

Der Kunde erhält die TAN-Nummer für die Freigabe seines Auftrags, sowie die Auftragsdetails per SMS auf sein Mobiltelefon. Die Kanaltrennung ist zu beachten (Auftragserteilung und SMS-Empfang nicht am gleichen Gerät). Aus Sicherheitsgründen nur mit deutschen Mobilfunk-Nummern möglich.

Kosten: keine Einmal-/Fix-Kosten, monatlich 2 TAN-Nummern frei – jede weitere 0,08 €

pushTAN

Der Kunde erhält die TAN-Nummer in einer separaten App (pushTAN-App) – somit kann er den Auftrag auf dem gleichen Mobiltelefon erfassen und auch freigeben.

Die für den Versand benötigte TAN-Nummer wird ihm in der gesicherten pushTAN-App angezeigt.

Kosten: keine Kosten



Sparkasse
Fürstentfeldbruck

4. Sicherungsmittel im Online-Banking

HBCI-Chipkarte

Der Kunde benötigt für diese Sicherungsvariante einen Chipkartenleser, der per USB-Anschluss an den PC angeschlossen wird, sowie eine HBCI-Chipkarte.

Die Legitimierung des Auftrags erfolgt über die Karte und die vom Kunden eingegebene PIN am Chipkartenleser.

Die Nutzung einer Onlinebanking Software wird für dieses Verfahren empfohlen!

Kosten: HBCI-Karte 8,-- € einmalig, HBCI-Kartenleser ab 58,93 € im Spk.-Shop + ggf. Software

seit 31.12.2021 abgeschalten!

5. Internetanwendungen

Internetbanking

www.sparkasse-ffb.de

Zielgruppe:
Privatkunden

Browserbanking –
Nutzung des
Onlinebankings von
einem beliebigen -
PC/Smartphone/Tablet

Umsatzdarstellung
zeitlich begrenzt

Import von XML-Datei
möglich

Einbindung weiterer
Banken über
„Multibanking-
Funktion“ möglich

Demokonto verfügbar



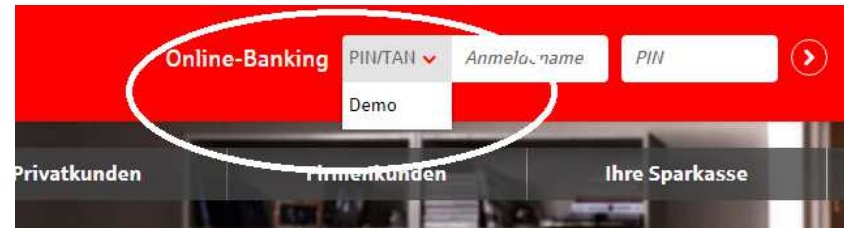
The screenshot shows the Sparkasse Fürstenfeldbruck online banking interface. At the top, the user is identified as 'Max Mustermann' with options to 'Abmelden' (Log out) and '5 Minuten' (5 minutes). The navigation bar includes 'Online-Banking', 'Privatkunden', 'Firmenkunden', 'Ihre Sparkasse', and 'Service-Center'. A greeting 'Guten Abend Herr Mustermann,' is followed by a security notice. A 'Hinweise' section mentions pending transactions. The 'Finanzstatus' section displays a table of accounts:

Giro- und Tagesgeldkonten**	
Privatgirokonto - Lebensmittel DE25 7005 3070 0000 1234 56 Mustermann, Max	1.000,00 EUR
Firmenkonto DE12 7005 3070 0000 1299 95 Test, Tina	-125,50 EUR
Tagesgeld - Rücklage DE28 7005 3070 0000 2009 05 Mustermann, Max	18.235,00 EUR
Girokonto (USD) DE69 7005 3070 0000 6543 21 Mustermann, Max	1.000,00 USD (734,65 EUR)
Summe	19.844,15 EUR

On the right, the 'Postfach' (Mailbox) shows 2 new messages, and 'Favoriten' (Favorites) includes 'Einzelanfrage' and 'Umsätze'.

Christian Windele / Fachberater Payment

5. Internetanwendungen / Demokonto



A screenshot of the Sparkasse website. The top navigation bar is red with the Sparkasse logo and 'Fürstenfeldbruck' on the left, and a search bar with 'Was su' on the right. Below the navigation bar, there are four tabs: 'Privatkunden', 'Firmenkunden', 'Ihre Sparkasse', and 'Service-Center'. The main content area is titled 'Demo Online-Banking pushTAN'. Below the title, there is a text box with the following text: 'Testen Sie selbst. Verwenden Sie dazu bitte folgende Zugangsdaten:'. Below this text, there are three lines of text: 'Anmeldename: pushDEMO', 'PIN: 12345', and 'TAN: beliebige 6-stellige Zahl'. Below these lines, there are two input fields: 'Anmeldename:' and 'PIN:'. At the bottom right, there is a red button with the text 'Sicher anmelden' and a red arrow. Above the button, there is a red lock icon and the text 'Sicherheitshinweise'.

6. Softwarelösungen/ Apps

StarMoney

Zielgruppe:
Privatkunden,
kleine Firmen

Verwaltung vieler
Auftragsvorlagen und
Archivierung der
Umsätze,
Haushaltsbuch

Multibankfähig – alle
Konten aller Banken
komfortabel verwalten.
Ebay-, Amazonkonten

Weitere Infos unter
www.starmoney.de

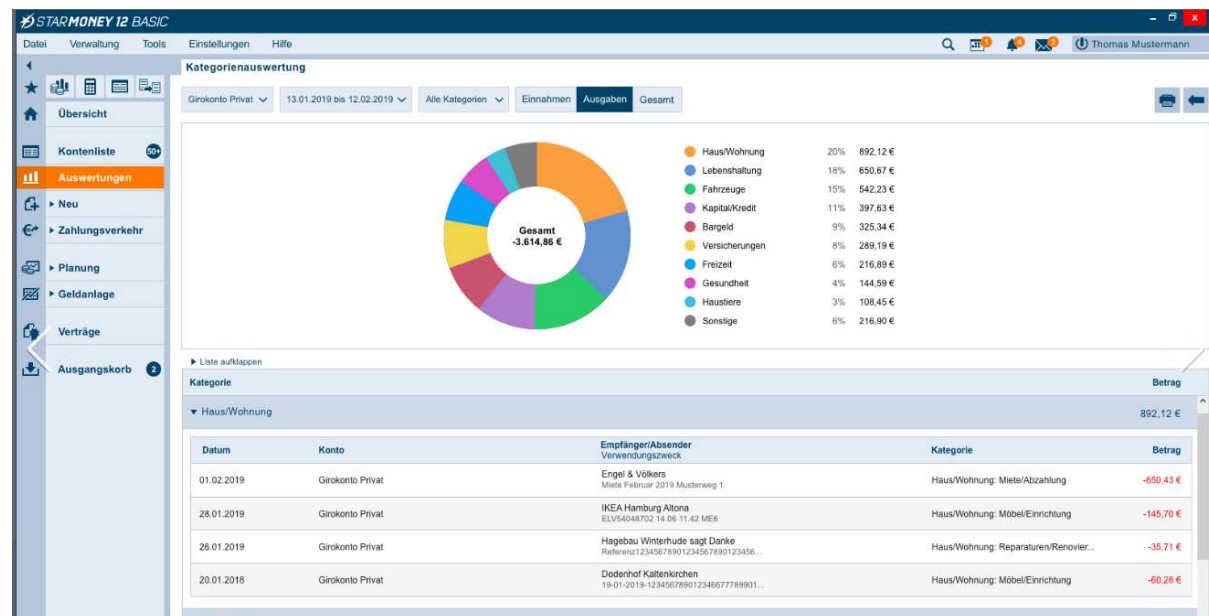
Ab 38,90 € im Spk. Shop
regelmäßig kostenpfl.
Updates! – oder Abo.



STAR MONEY 12 BASIC

Kontenliste

Kontoart	Kontenname	Kontonummer	IBAN	Kontowährung	Saldo vom	Buchungssaldo
Darlehenskonto	Standardkonto 5	12345678	DE88123456780012345678	EUR	13.02.2019	-745,31 EUR
Darlehenskonto	Standardkonto 4	12345677	DE04123456780012345677	EUR	13.02.2019	4.674,57 EUR
Girokonto	Standardkonto 1	12345676	DE31123456780012345676	EUR	13.02.2019	6.275,13 EUR
Girokonto	Standardkonto 2	12345675	DE66123456780012345675	EUR	13.02.2019	146,24 EUR
Girokonto	Standardkonto 3	12345674	DE89123456780012345674	EUR	13.02.2019	-3.667,95 EUR
Kreditkartenkonto	Standardkonto 6	12345673		EUR	13.02.2019	-4.839,40 EUR
Sparkonto	Standardkonto 8	12345672	DE06123456780012345672	EUR	13.02.2019	103,97 EUR
Sparkonto	Standardkonto 7	12345671	DE92123456780012345671	EUR	13.02.2019	17.300,51 EUR



6. Softwarelösungen/ Apps

Sfirm

Zielgruppe:

Firmen, Kommunen,
Vereine (zum Beitrags-
Einzug)

Import- /Export Funktionen

Große Flexibilität durch
modularen Aufbau

49,90 € einmalig – für Vereine

Ab 69,90 einmalig für Firmen -
zzgl. 5,-- € mtl. Lizenz- und
Servicevertrag

SEPA-Überweisungen - SFirm 3.0 (Datenbank 1)

schließen X

Datei Start Ausgabe Auswertung Cash Depooling Extra Wartungszentrum

Neu 3 Arbeiten Kopieren Löschen Gesperrt Ausgeben nach... Zahlung

IBAN/BIC- Fremddatei importieren Extra

Versandauftrag Wechseln zu

Empfänger/Kunden Zurücksetzen Alle Vorschau

Kontoinformationen Aktualisieren Keine Drucken

Pauschaländerung Spalten Ansicht Auswahl Druck

Umkehren PDF

Ordner-/Kontonamen suchen

SEPA-Überweisungen

Zahlungsverkehr > Zahlungsverkehr > SEPA-Überweisungen

Daten suchen

Ziehen Sie eine Spaltenüberschrift in diesen Bereich, um nach dieser zu gruppieren

Status	Rhythmus	Ausgabe am	Begünstigter	Betrag	Währung	Verwendungszweck
Fällig	2-monatlich	06.01.2010	NORDEA INVESTMENT	9.876,50	EUR	01234567890/987654 Z-No. 20382038
Fällig	einmalig	06.01.2010	Patteri Industrie S.p.A.	108.866,44	EUR	C-No. 092349288 Invoice No. 5675665 SFirm Hannover ./ . 3.367,00 EUR DISCOUNT
Fällig	einmalig	06.01.2010	Schwarz, Renate	45.678,90	EUR	Lieferung Bueromaterial Rechnungsnr. 2834734 Kundenr. 92372739283
Erfasst	einmalig	07.03.2014	Schwarz, Renate	23.654,00	EUR	Das neue SEPA-Datenformat basiert auf dem ISO Standard 20022. Es wurde für den Interbanken-Zahlungsverkehr
Fällig	einmalig	07.03.2012	MAX MUSTERMANN	456,00	EUR	LOREM IPSUM DOLOR SIT AMET, CONSETETUR SADIPSCING ELITR SED DIAM NONLUMY EIRMOD TEMPOR INVIDUNT UT LABOR
Erfasst	einmalig	07.03.2014	SCHWARZ, RENATE	654,00	EUR	DAS NEUE SEPA-DATENFORMAT BASIERT AUF DEM ISO STANDARD 20022. ES WURDE FÜR DEN INTERBANKEN-ZAHLUNGSVERKEHR.
Ausgegeben	einmalig	07.03.2012	TEST TESTER	987.654,00	EUR	VWZ-ZEILE 1 VWZ-ZEILE 2 VWZ-ZEILE 3 VWZ-ZEILE 4
Fällig	einmalig	07.03.2012	MAX MUSTERMANN	1.234,00	EUR	
Fällig	einmalig	14.10.2011	Max Mustermann	11,00	EUR	test
Erfasst	einmalig	07.03.2014	Schwarz, Renate	23.654,00	EUR	Das neue SEPA-Datenformat basiert auf dem ISO Standard

Favoriten

Kontoinformationen

Zahlungsverkehr 1

Melddaten

Elektronische Rechnungen

Übertragungen

Stammdaten

6. Softwarelösungen/ Apps

Übersicht Sparkassen-Apps



App „Sparkasse“

Mit der kostenfreien App behalten Sie alle Ihre Konten stets im Blick:

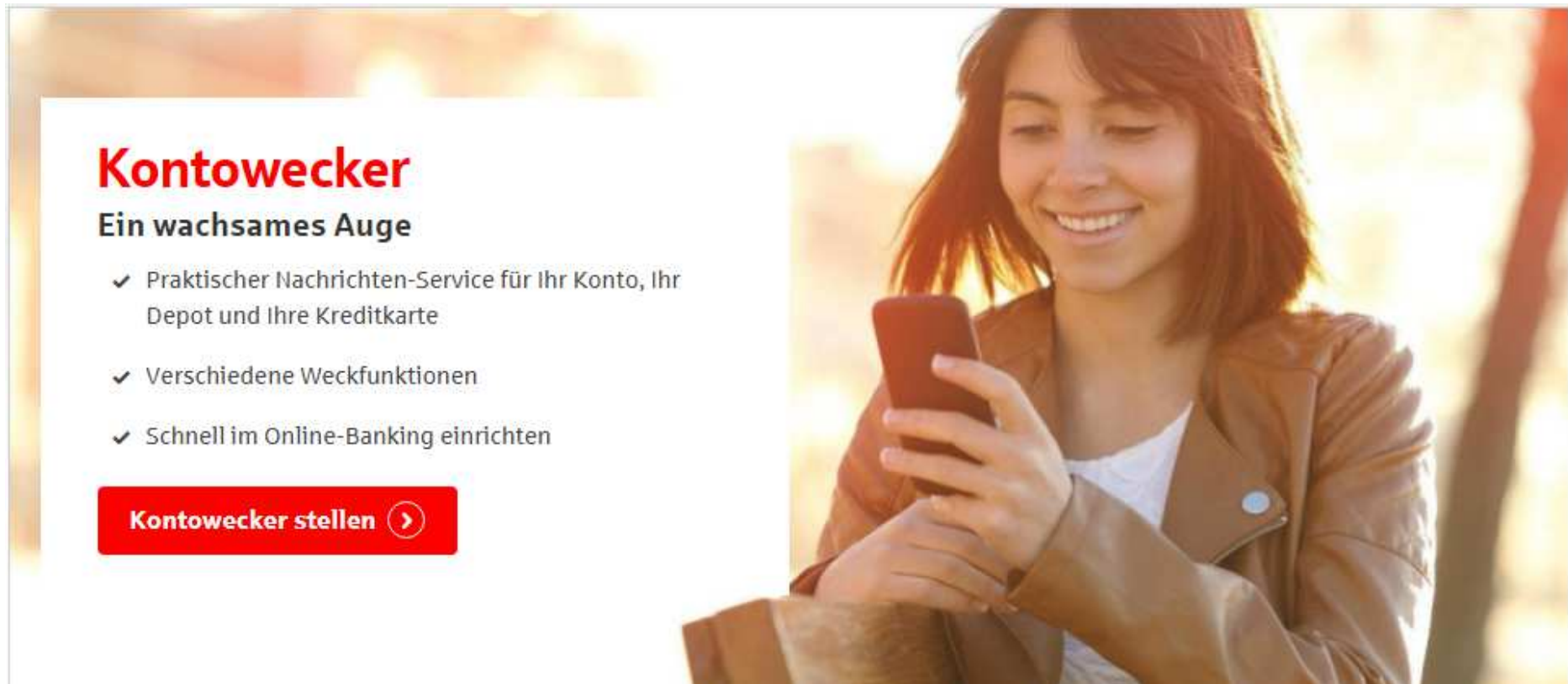


S-pushTAN-App

Für Ihr mobiles Banking mit der Sparkassen-App: TANs erzeugen in der passwortgeschützten S-pushTAN-App.

- ✓ Banking mit Smartphone oder Tablet: Überweisungen ausführen, Daueraufträge einrichten oder Umsätze abfragen
- ✓ Bequem den nächsten Geldautomaten und die nächste Sparkasse finden
- ✓ Praktische Funktionen für komfortables Banking: Mit giropay | Kwitt von Handy zu Handy Geld überweisen – Beträge bis 30 Euro in der Regel ohne Freigabe (TAN)¹
- ✓ Schnell und bequem Rechnungen bezahlen: Durch Fotoüberweisung oder das Einscannen des Rechnungs-QR-Codes (GiroCode)
- ✓ Nutzen Sie die App auch für Ihr Banking bei anderen Banken

7. Kontowecker



Kontowecker
Ein wachsames Auge

- ✓ Praktischer Nachrichten-Service für Ihr Konto, Ihr Depot und Ihre Kreditkarte
- ✓ Verschiedene Weckfunktionen
- ✓ Schnell im Online-Banking einrichten

[Kontowecker stellen >](#)

8. Phishing / Betrugsversuche

Es gibt verschiedene Angriffs-Szenarien:

„Sicherheitsabfrage“:

Von: Sparkasse Online [<mailto:onlineteam@sparkasse.de>]

Gesendet: Freitag, 9. Januar 2015 10:12

Betreff: Sparkasse Online-Konto Aktualisierung

Sehr geehrter Kunde,

wir möchten Sie darauf hinweisen, dass der Zugang zu Ihrem Online-Konto in Kurze abläuft. Um dieses weiterhin nutzen zu können, bitten wir Sie Ihre Daten bei folgendem Link zu bestätigen:

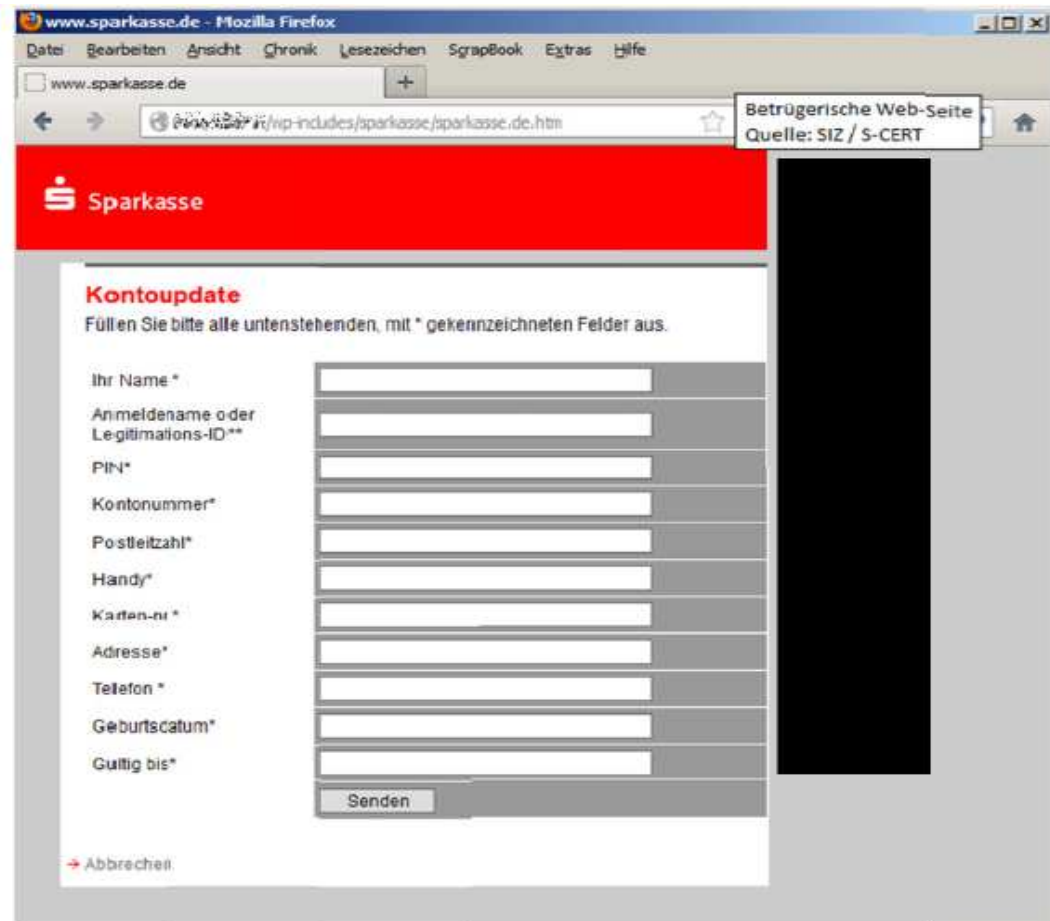
Sparkasse Online-Konto Aktualisierung: [klicken Sie hier](#)

Um diese Dienste weiterhin problemlos nutzen zu können, führen Sie bitte das Update so schnell wie möglich durch.

Mit freundlichen Grüßen,
Ihr Sparkasse Kundenservice

8. Phishing / Betrugsversuche

Die so erbeuteten Daten werden für „Social Engineering-Anrufe“ beim Kunden und bei der Sparkasse (!) benutzt.



8. Phishing / Betrugsversuche

„Panik-Mails“: Sollten Kunden dazu verleiten, einen infizierten Anhang zu öffnen (Zahlungsaufforderungen, Paketbenachrichtigungen, Strafanzeige, Mahnung, Kündigung...)



8. Phishing / Betrugsversuche

Anschließend wird der Banking-Dialog manipuliert, um im Hintergrund unbemerkt größere Beträge zu transferieren (Rücküberweisung fingierter Zahlungseingänge, Gewinnspielteilnahme mit TAN-Abfrage, etc.)

The screenshot shows a banking website interface with a navigation bar at the top containing links: Home, Ihre Sparkasse, Service, Übersicht, Beruf und Karriere, Media-Center. A search bar on the right contains the text 'Suchbegriff'. Below the navigation bar, there is a 'Hinweise' section with a message: 'Sehr geehrter Kunde, am 27.09.2013 wurde auf Ihr Konto 200905 eine Summe in einer Höhe von 4.720,00 EUR gutgeschrieben. Laut unseren Informationen wurde das Geld versehentlich auf Ihr Konto überwiesen, daher ist Ihr Konto vorübergehend gesperrt. Wir empfehlen Ihnen die Summe an den Absender zurück zu überweisen, Ihr Konto wird automatisch wieder freigeschaltet. Bitte drücken Sie auf "erstatten" um das Geld zurück zu überweisen. Bitte entschuldigen Sie die Unannehmlichkeiten.' Below the message is a red button labeled 'erstatten'. The main content area is titled 'Giro-Detail-Übersicht' and contains a table with account details. To the right of the table is a sidebar with an 'Info-Box' warning: 'Zu Ihrer Sicherheit erfolgt die automatische Abmeldung in 12 Min.', a 'Mini-Finanzstatus' table, and a 'Service-Telefon' section.

Kontobezeichnung	Kontonummer	Kontostand**	Verfügbar**	Funktionen
Privatgirokonto	123456	1.000,00 EUR	3.500,00 EUR	[Icons]
Mustermann, Max Lebensmittel		2.500,00 EUR	0,00 EUR	
Firmenkonto	129995	-125,50 EUR	1.674,50 EUR	[Icons]
Test Tina		2.000,00 EUR	0,00 EUR	
Tagesgeld	200905	22.955,00 EUR	22.955,00 EUR	[Icons]
Mustermann, Max Rücklage		0,00 EUR	0,00 EUR	

Konto	Kontost. (EUR)
123456	1.000,00
129995	-125,50

Service-Telefon
0464 696 0

Filiale finden

Notfallnummern

Newsletter-Abo

IBAN-Rechner

8. Phishing / Betrugsversuche

Polizei warnt vor Microsoft-Masche

Eine 63-jährige Feldgedingerin wurde vor wenigen Tagen Opfer einer perfiden Betrugsmasche: Vermeintliche Microsoft-Mitarbeiter verschafften sich Zugang auf den Rechner der Frau, in der Hoffnung, dort Kontodaten stehlen zu können. Die Polizei weiß um das Thema – und warnt eindringlich!

VON STEFANIE ZIPPER

Dachau – Renate Z. (Name geändert; die Red.) hatte vor einigen Wochen einen harten Tag, sie hatte „einiges um die Ohren“, wie sie sich im Gespräch mit der Heimatzeitung erinnert. Just an diesem Tag aber klingelte bei der 63-jährigen das Telefon. Ein Anrufer „mit starkem Akzent“, so Z., stellte sich ihr als Mitarbeiter von Microsoft vor. Z.'s Computer sei gehackt worden; sie müsste, um diese Schadsoftware wieder loszuwerden, unbedingt ein neues – kostenloses – Programm downloaden. Der Download dauere zehn Minuten, erklärte der Anrufer, wobei Z. währenddessen gerne von ihrem Computer weggehen dürfe. Das Programm installiere sich dann von selbst. Zuvor aber müsse die 63-Jährige ihm Zugriff auf ihren Rechner erlauben, er würde sie dann auf die Microsoft-Seite lotsen und ihr beim Start des Downloads helfen.

Heute weiß Renate Z., dass hier längst alle Alarmglocken bei ihr hätten läuten müssen, doch sie folgte dem angeblichen Microsoft-Mitarbeiter weiter. Erst als sie bemerkte, dass an ihrem Computer die Kamera eingeschaltet war und der Anrufer ihr bereits die letzten vier Ziffern ihrer Kontonummer sagen konnte – wobei Z. ihm doch bitte die vollständige Nummer nennen solle – wurde die Feldgedingerin misstrauisch. Sie legte auf und zog den Netzstecker ihres Computers.

In buchstäblich letzter Sekunde. Denn so konnte der Anrufer keine weiteren Daten von ihrem Computer klaben. „Klar, es war ein Fehler, wenn man so hinterher drüber nachdenkt“, sagt Z. Aber wenn man mal bearbeitet werde. „dann machst du Sachen, die du einfach nicht tun solltest“.

Günther Findl, Sprecher bei der Polizei in Dachau, kennt das Phänomen des sogenannten Microsoft-Betrugs seit vielen Jahren. Die Täter sitzen in aller Regel in Call-Centern in Indien, über Online-Telefonbücher würden sie sich willkürlich Opfer aus-

suchen, „dann übernehmen sie die Steuerung des Computers“, so Findl. Die letzte Stufe sei schließlich, dass der Cyber-Eindringling nach Kontodaten, um liebsten beim Online-Bezahldienst Paypal, sucht; „Er schaut, wo er überall rein kann“, so Findl, und nimmt mit, „was er an sensiblen Daten kriegen kann“.

Microsoft selbst betont in diesem Zusammenhang, „dass es unter keinen Umständen technischen Support von sich aus anbietet“. Jeglicher Kontakt für eine von Microsoft angebotene Supportleistung müsse vom Kunden ausgehen. Polizist Findl ergänzt außerdem, dass Angerufene „im Zweifel immer bei der Polizei nachfra-

„Wenn von 50 Angerufenen einer mitmacht, ist das für die schon ein Erfolg.“

Poliziesprecher Günther Findl

suchen. „Wenn von 50 Angerufenen einer mitmacht, ist das für die schon ein Erfolg“, weiß Findl. Erst Ende des vergangenen Jahres hat die indische Polizei – nach mehr als 7000 Beschwerden von Microsoft-Kunden aus 15 Ländern – 26 dieser betrügerischen Call-Center durchsucht und 63 Personen verhaftet. Allerdings mit wenig Erfolg: Nur wenige Wochen später setzte die von der Polizei als „Microsoft-Welle“ bezeichnete Betrugsmasche wieder ein.

Dabei gehen die Täter Findl zufolge stets sehr ähnlich vor: „Stufe 1“ sei, dass Opfer angerufen und auf angebliche Schadsoftware auf ihren Rechnern hingewiesen würden. Um dies zu belegen, verweisen sie dabei oft auf Fehlerprotokolle, die laut Findl aber auf jedem Rechner zu finden sind und eigentlich keine Bedeutung haben. Stufe 2 sei dann, dass die angeblichen Microsoft-Experten aber erklären, das Problem aus der Welt schaffen zu kön-

gen“ beziehungsweise sich über die Internetseiten www.polizei.bayern.de und www.verbraucherzentrale.de über etwaige Betrugsmaschinen informieren sollten. Günther Findl zufolge würde es die Anrufer auch oftmals beeindrucken, wenn man auf eine Rückrufnummer bestünde. Die auf dem Display erscheinende Telefonnummer sei nämlich in aller Regel ebenso falsch wie die Geschichte der angeblichen Schadsoftware auf dem Computer der Opfer.

Auch wenn Renate Z. – zum Glück – nicht geschädigt wurde, betont Polizei-Sprecher Findl dennoch, dass alle derartigen Fälle gemeldet werden sollten. Die Polizei nehme sie auf alle Fälle zu Protokoll und verwende sie für ihre Öffentlichkeitsarbeit. Die einzige Möglichkeit, derartigen Betrügereien ein Ende zu setzen, sei nämlich, die Leute aufzuklären, damit sie sich nicht in der „Microsoft-Welle“ untergehen...

9. Sicherheit im Internet

www.sparkasse-ffb.de/sicherheit

Neben **Sicherheitstipps** finden Sie auch **nützliche Links, Infos zu Betrugsvarianten und aktuelle Meldungen.**

Sicherheitstipps

Beachten Sie ein paar einfache Regeln bei der Nutzung Ihres Online-Bankings. So schützen Sie Ihr Konto vor unberechtigten Zugriffen.

Gehen Sie vorsichtig mit Ihrer PIN und TAN um

Geben Sie Ihre PIN und TAN nie für „Testüberweisungen“ oder sonstige angebliche „Überprüfungen“ ein. Ihre Sparkasse wird Sie niemals auffordern, eine TAN für Gewinnspiele, Sicherheits-Updates oder vermeintliche Rücküberweisungen einzugeben.

Mehr erfahren 

Sicherer Umgang mit Telefonaten, E-Mails und Anhängen

Ignorieren und melden Sie Anrufe und E-Mails, in denen Sie aufgefordert werden, persönliche Daten wie IBAN, PIN, TAN oder Kreditkartendaten preiszugeben und öffnen Sie keine E-Mail-Anhänge unbekannter Herkunft.

Mehr erfahren 

Aufmerksam bleiben und Tageslimit festlegen

Behalten Sie Ihre Kontoumsätze regelmäßig im Blick und legen Sie die maximale Höhe Ihrer täglichen Verfügungen fest.

Mehr erfahren 


Sperren Sie im Zweifel Ihren Online-Banking-Zugang

Sperren Sie Ihren Zugang über den deutschlandweit kostenfreien Sperr-Notruf 116 116.

Sollten Sie kein Telefon zur Hand haben, geben Sie einfach dreimal eine falsche PIN in die Anmeldemaske zum Online-Banking ein. So ist Ihr Zugang vorläufig gesperrt.

Halten Sie PC und Smartphone stets aktuell

Setzen Sie auf Ihrem PC und Smartphone stets aktuelle Antiviren-Software ein und halten Sie Ihre Programme und Betriebssysteme regelmäßig auf dem neuesten Stand.

Mehr erfahren 

Nutzen Sie einen sicheren Internet-Zugang und Browser

In öffentlichen Bereichen wie Bahnhöfen, Flughäfen und bei Großveranstaltungen ist Vorsicht geboten. Ihre Bankgeschäfte sollten Sie niemals über einen öffentlichen Hotspot erledigen. Verwenden Sie bei der Nutzung des Internets auf Ihrem PC und mobilen Geräten zudem stets einen namhaften Browser.

Mehr erfahren 

10. Bezahlformen im Internet

Pandemiebedingt starke Zunahme von Online-Shopping und den damit verbundenen Bezahlverfahren:

- Giropay / Paydirekt
- Lastschrift
- Kreditkarte
- Überweisung / Vorkasse
- Paypal
- ...
- (z. T. mit Käuferschutz)



Kontaktlos bezahlen mit Karte & Handy



PSD 2 – seit 2019 / Gründe und Auswirkungen



Starke Kundenauthentifizierung:

- Keine Papier-TAN-Listen mehr
- Regelmäßig TAN-Abfrage bei Umsatzabruf / z.T. keine TAN bei Überweisungen
- Auch bei Kreditkartenzahlungen im Internet (3D-Secure/S-ID-Check)

Drittanbieter-Schnittstelle (Zahlungsdiensteanbieter / Kontoinformationsdienste)

11. Zusammenfassung – Zeit für Ihre Fragen

Gibt es noch Fragen?



11. Zusammenfassung

Vielen Dank!