Sparkasse
Fürstenfeldbruck

Christian Windele / Fachberater Payment

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)

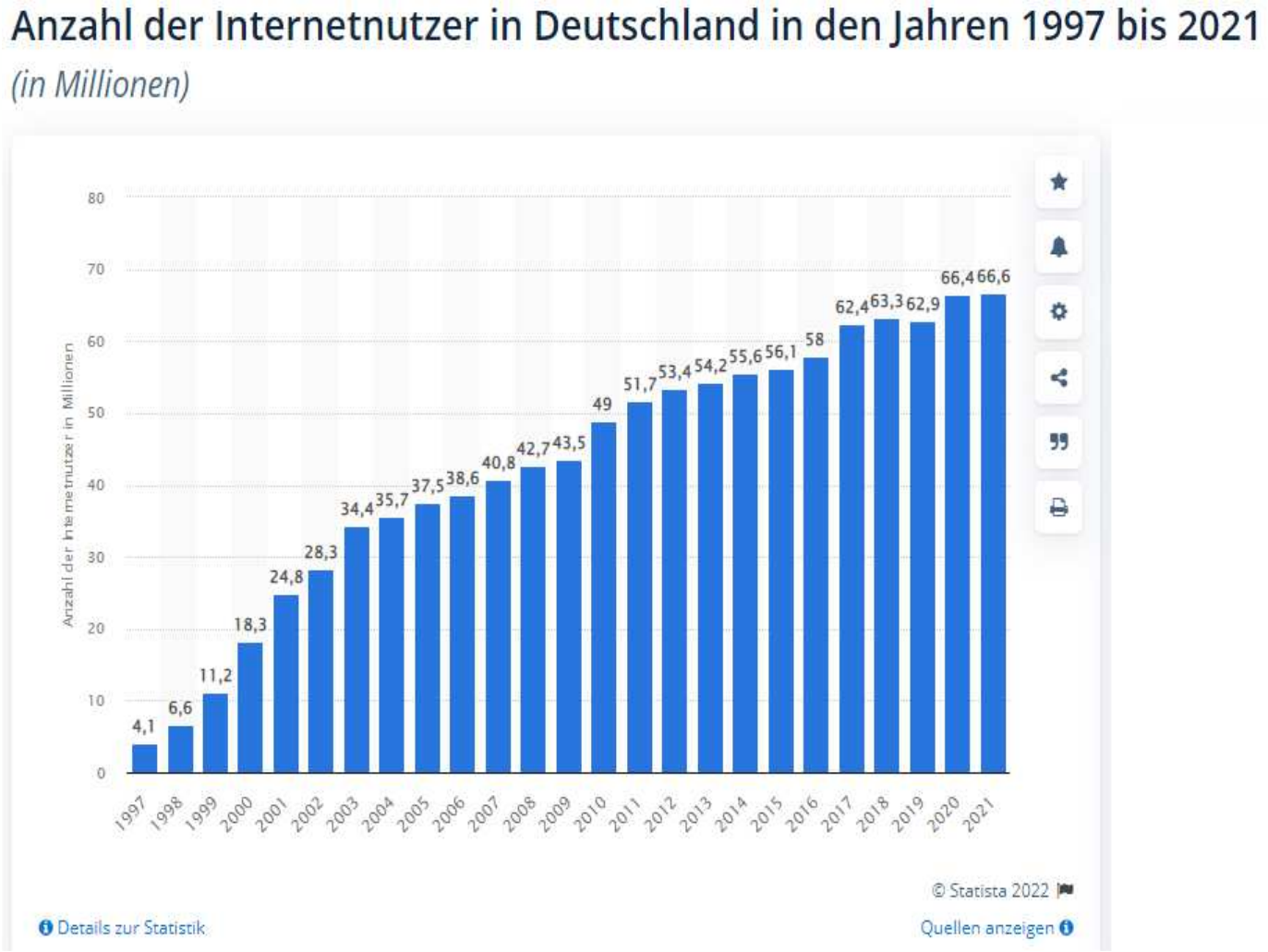
2. Rückblick (Entwicklung des Online-Bankings)

- **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

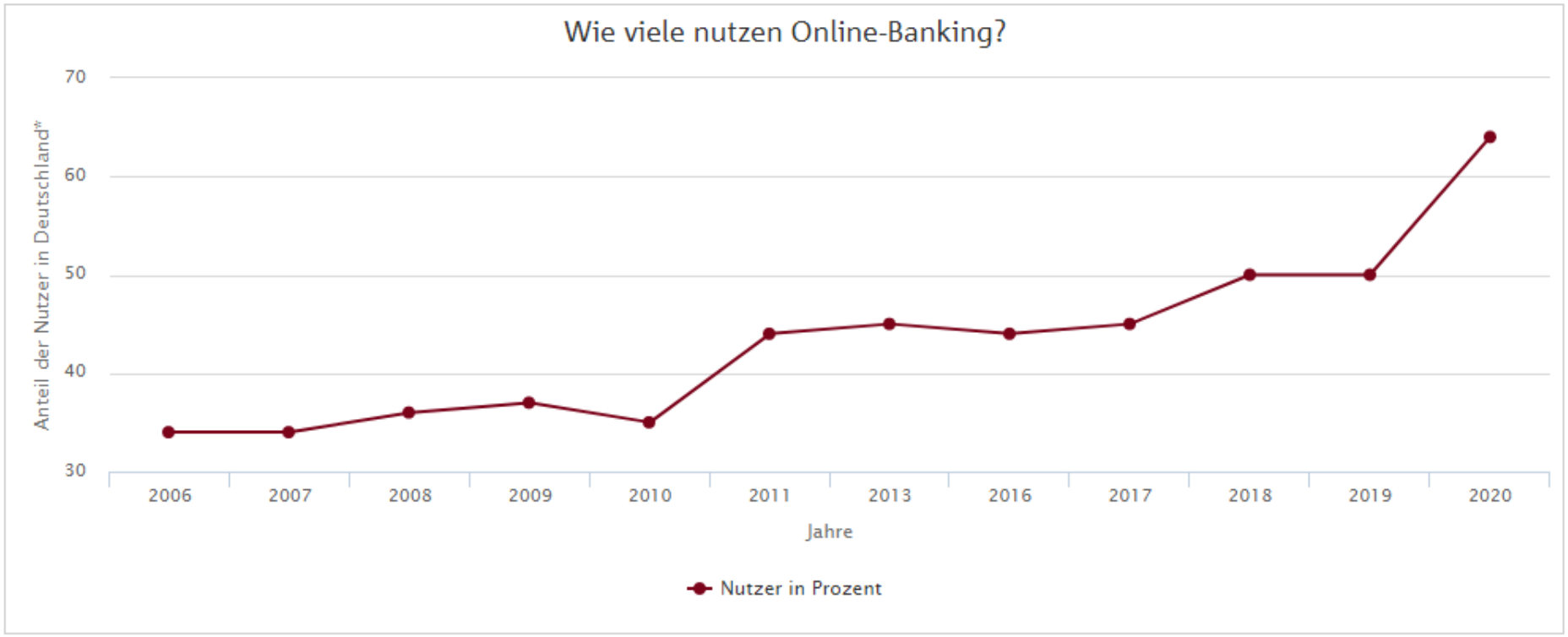
Banking-Anwendung im CEPT-Standard

2. Rückblick / Entwicklung der Internet-Nutzung



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.

Nicht mehr 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

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

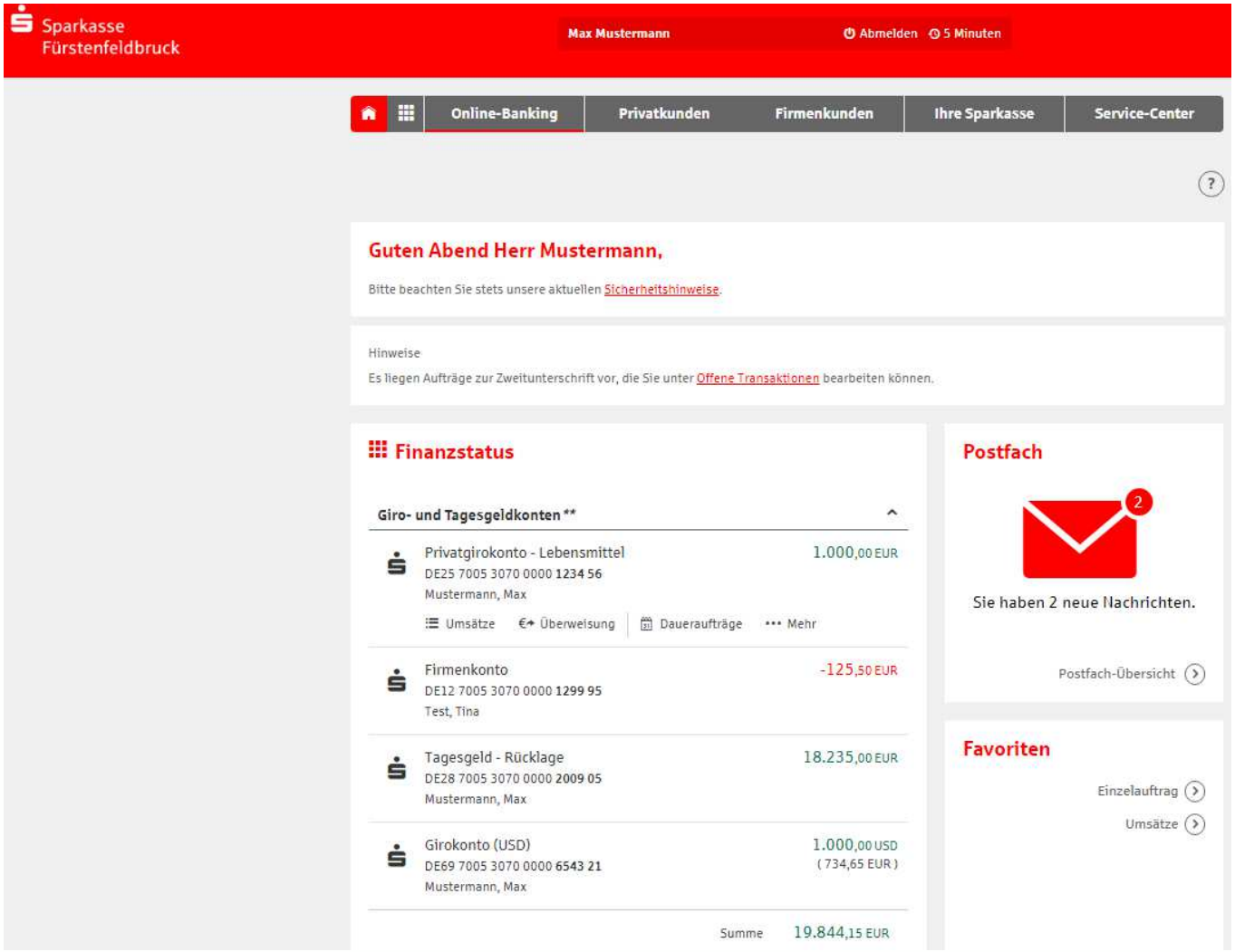
Browserbanking – Nutzung des Onlinebankings von einem beliebigen - PC/Smartphone/Tablet

Umsatzdarstellung zeitlich begrenzt

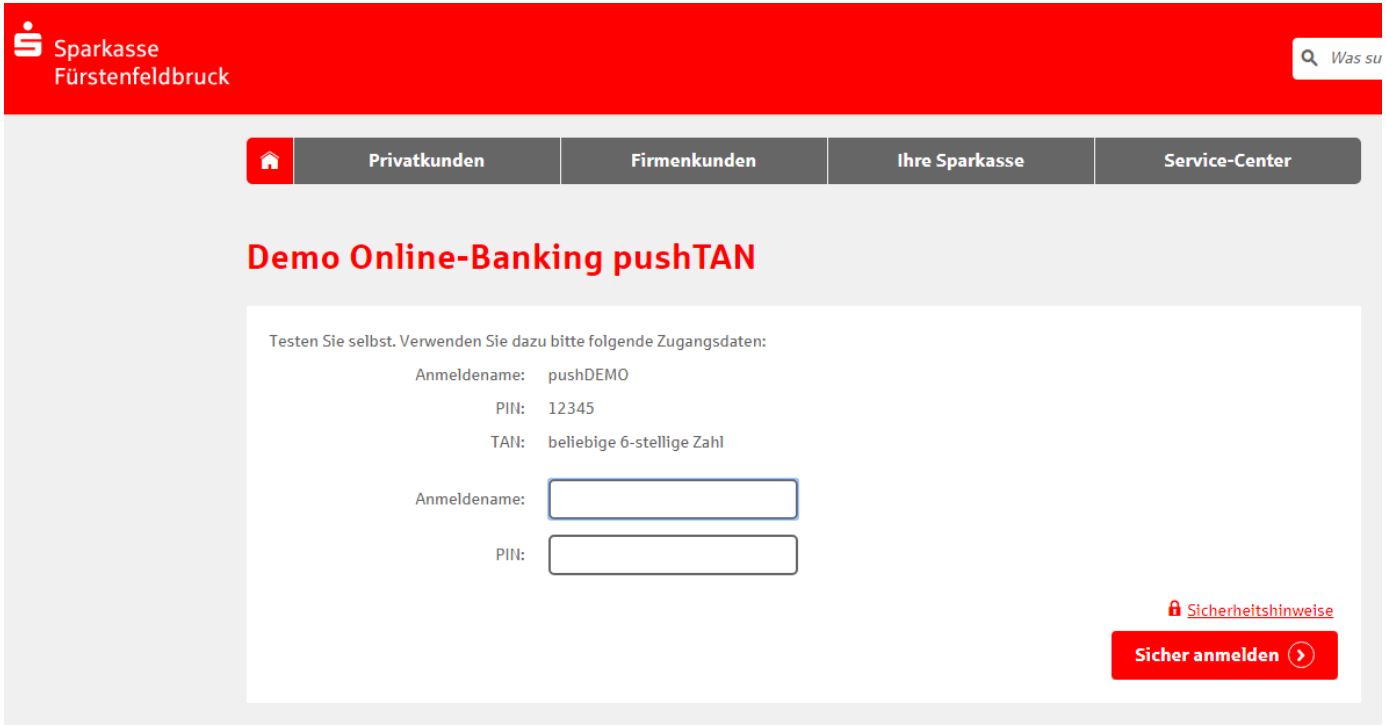
Import von XML-Datei möglich

Einbindung weiterer Banken über „Multibanking-Funktion“ möglich

Demokonto verfügbar



5. Internetanwendungen / Demokonto



6. Softwarelösungen/ Apps

StarMoney

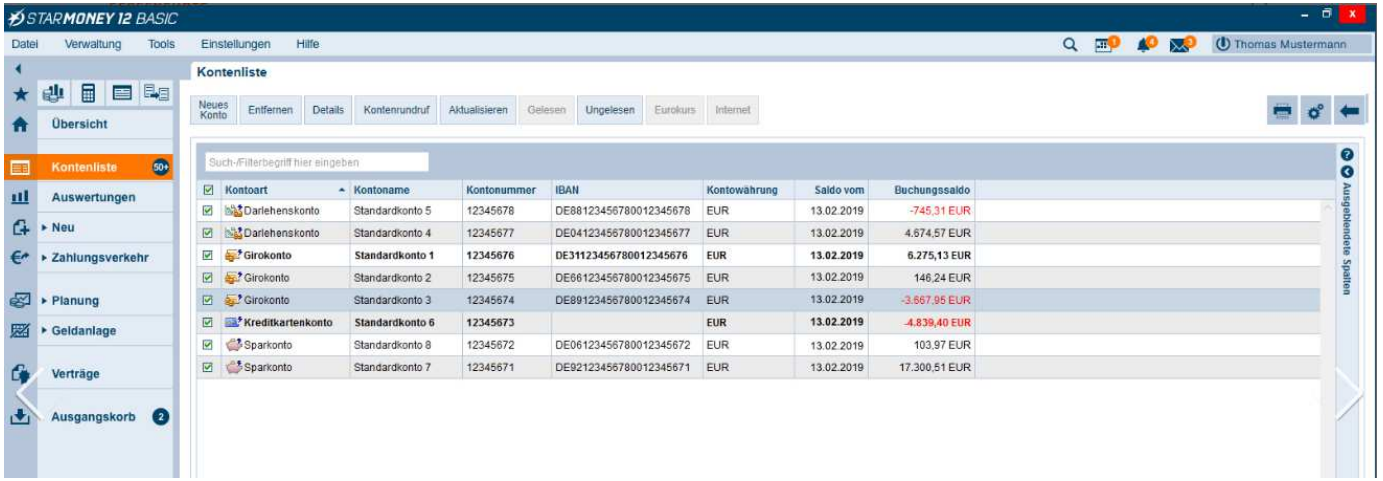
Zielgruppe:
Privatkunden,
kleine Firmen

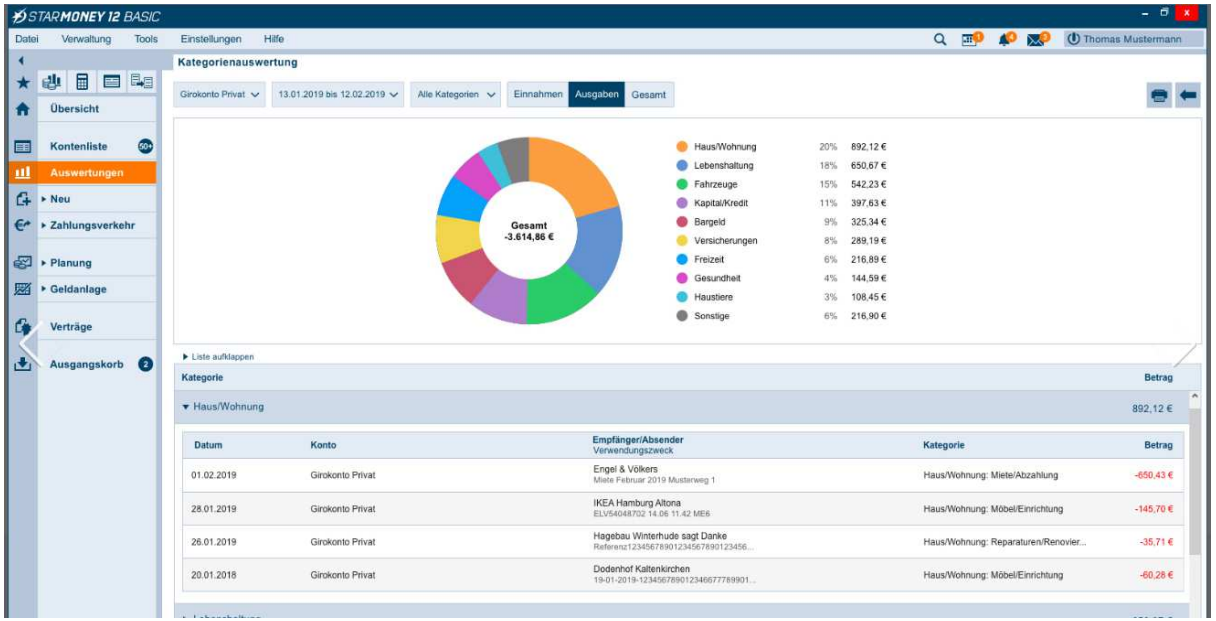
Verwaltung vieler Auftragsvorlagen und Archivierung der Umsätze, Haushaltsbuch

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.





Sparkasse Fürstenfeldbruck

6. Softwarelösungen/ Apps

Sfirm

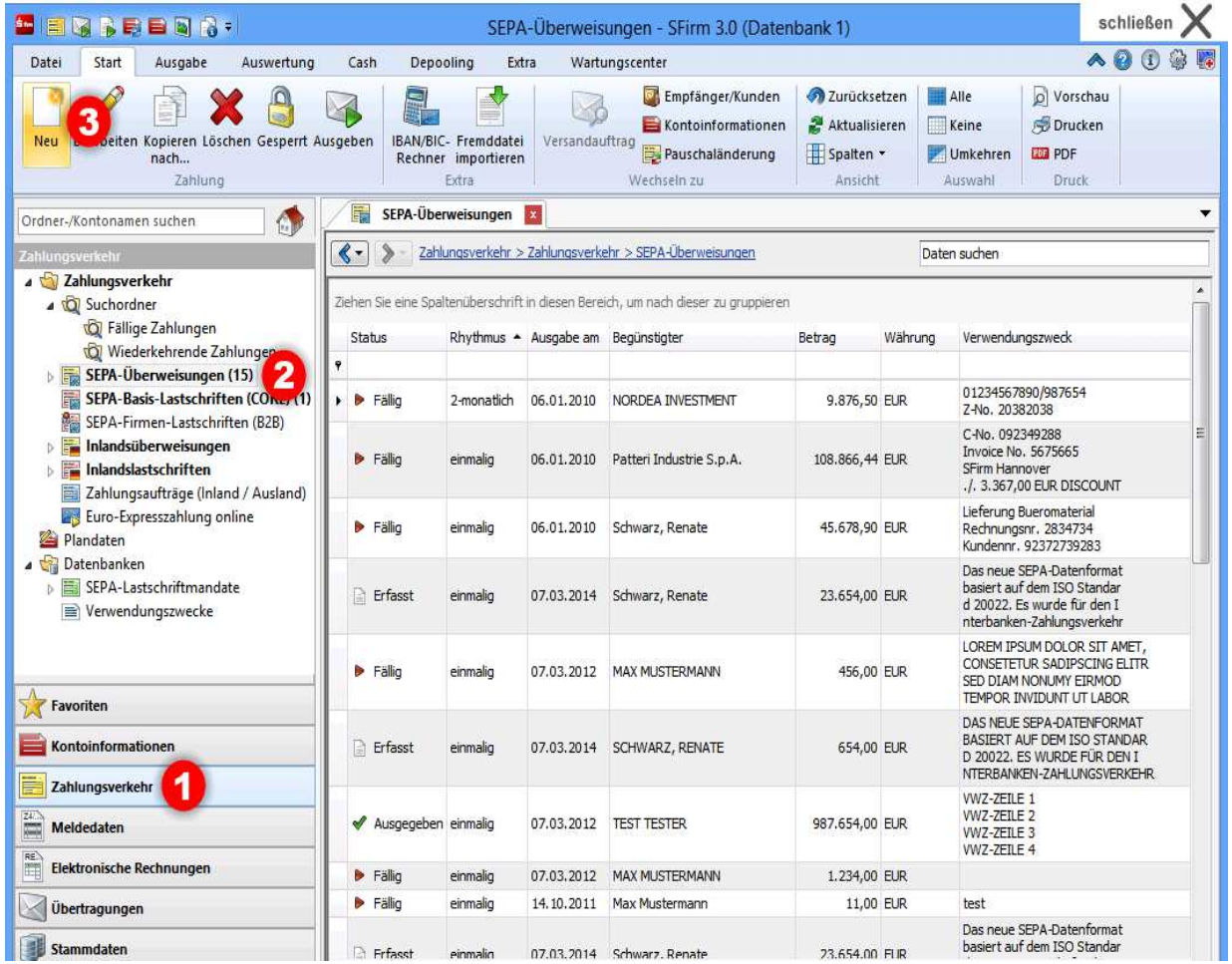
<u>Zielgruppe:</u>
Firmen, Kommunen, Vereine (zum Beitrags-Einzug)

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



6. Softwarelösungen/ Apps

Übersicht Sparkassen-Apps

App „Sparkasse“

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

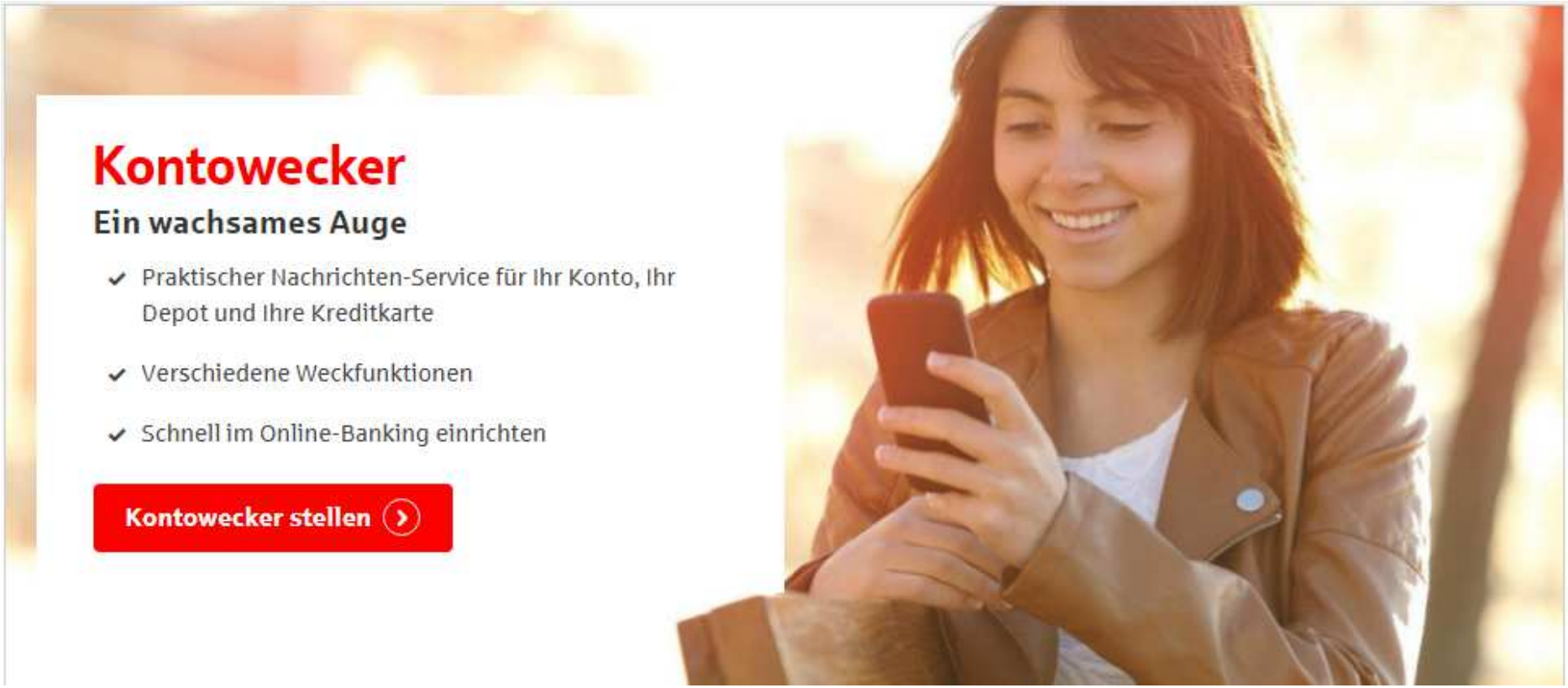
S-pushTAN-App

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

Fürstenfeldbruck

7. Kontowecker



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 nützen zu können, bitten wir Sie Ihre Daten bei folgendem Link zu bestätigen:

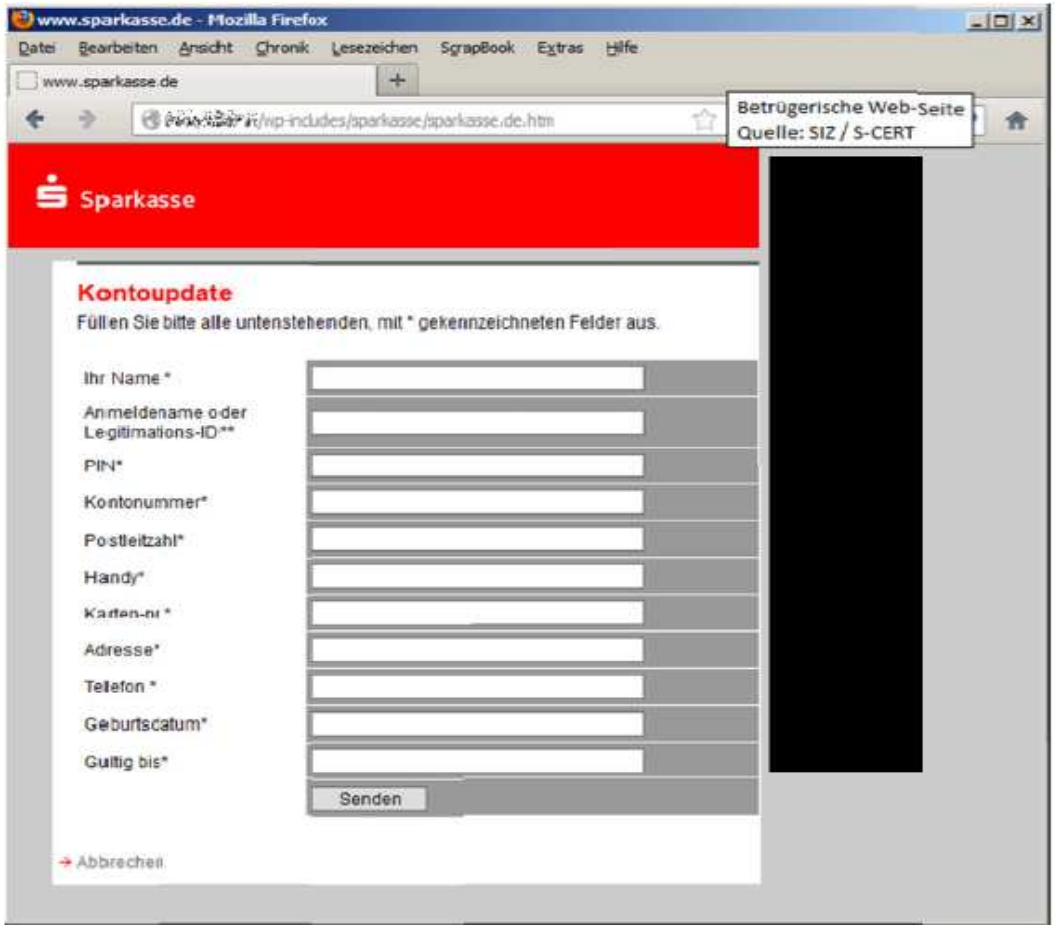
Sparkasse Online-Konto Aktualisierung: klicken Sie hier

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…)

Betreff: Rechnung #4969379_M_53128301_O_70_5292
Datum: Wed, 04 Jun 2014 11:53:40 +0200
Von: Vodafone Service <adkofc>
An: [redacted]

Betrügerische E-Mail
Quelle: SIZ / S-CERT

Ihre neue Rechnung als PDF

Ihre Kundennummer: 14074773
04.06.2014

Guten Tag!

Ihre Rechnung vom 04.06.2014 ist hier im Anhang als PDF-Datei für Sie. Falls Sie die Datei auf Ihrem Handy nicht öffnen können, versuchen Sie es bitte an Ihrem PC.

250708_W_4717874_I_81_9869.pdf

Die Gesamtsumme beträgt **351,37 Euro** und ist am 06.06.2014 fällig.

Jetzt noch übersichtlicher: Ihre Online-Rechnung im neuen Design. Sie finden Ihre Rechnung in MeinVodafone unter Rechnung > Aktuelle Rechnung. Dort können Sie Ihre Rechnung auch als PDF herunterladen und drucken. Ihre Rechnungen der letzten 24 Monate finden Sie unter "Alle Rechnungen".

Viele freundliche Grüße
Ihr Vodafone-Team

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.)

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 ZIPFER

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 Zahlen 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 klauen. „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 aussuchen. „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.

> **„Wenn von 50 Angerufenen einer mitmacht, ist das für die schon ein Erfolg.**
>
> Polizeisprecher Günther Findl

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 können, „dann übernehmen sie die Steuerung des Computers", so Findl. Die letzte Stufe sei schließlich, dass der Cyber-Eindringling nach Kontodaten, am 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".

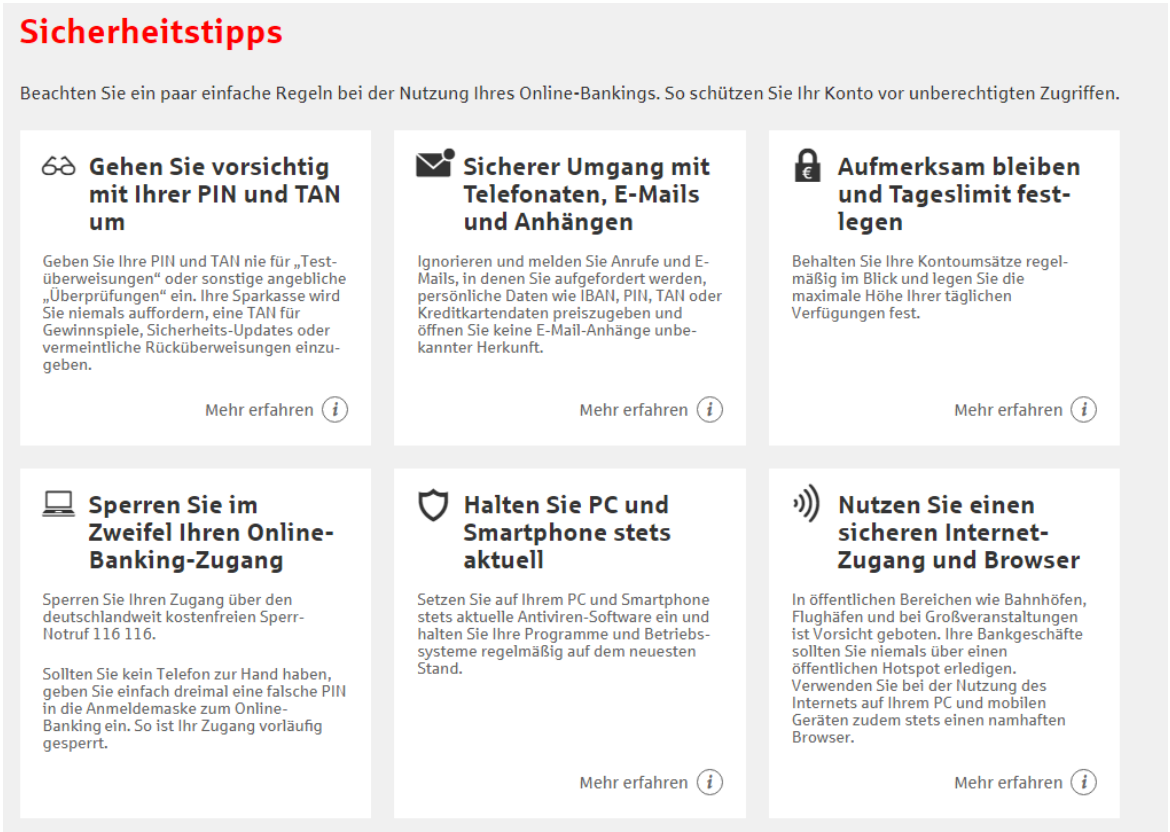
Microsoft selbst betont in diesem Zusammenhang, „dass es unter keinen Umständen technischen Support von sich aus anbietet". Jeglicher Kontakt für eine von Microsoft angebotene Supportleistung müsse vom Kunden ausgehen. Polizist Findl ergänzt außerdem, dass Angerufene „im Zweifel immer bei der Polizei nachfragen" beziehungsweise sich über die Internetseiten www.polizei.bayern.de und www.verbraucherzentrale.de über etwaige Betrugsmaschen informieren sollten. Günther Findl zufolge würde es die Anrufer auch oftmals beeindrucken, wenn man auf eine Rückrufnummer bestehe: 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 „Test-überweisungen" oder sonstige angebliche „Überprüfungen" ein. Ihre Sparkasse wird Sie niemals auffordern, eine TAN für Gewinnspiele, Sicherheits-Updates oder vermeintliche Rücküberweisungen einzu-geben.

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 unbe-kannter Herkunft.

Mehr erfahren

Aufmerksam bleiben und Tageslimit fest-legen

Behalten Sie Ihre Kontoumsätze regel-mäßig 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 Betriebs-systeme 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!