

INITIATIVE D21
Gemeinsam für die Digitale Gesellschaft

Eine Studie der Initiative D21, durchgeführt von TNS Infratest.

Online - Banking 2014 Sicherheit zählt!

Wünsche und Anforderungen
an Bankgeschäfte im Internet



Mit freundlicher Unterstützung von:

FIDUCIA
Ihr IT-Partner

Inhalt

Vorwort	3
<hr/>	
Zentrale Ergebnisse im Überblick	4
<hr/>	
Kapitel 1. Anforderungen an das Online - Banking	5
Kapitel 2. Sicherheit beim Online - Banking	11
Kapitel 3. Mobile - Payment	18
Kapitel 4. Gerätenutzung beim Online - Banking	21
<hr/>	
Methodensteckbrief	22
<hr/>	
Impressum	23

Sicherheit hat keinen Preis

Wie selten zuvor sind Schutz und Sicherheit persönlicher Daten in den zurückliegenden Monaten in den Fokus der öffentlichen Wahrnehmung gerückt. Die Bandbreite der Themen reicht von den Enthüllungen Edward Snowdens über millionenfach gehackte E-Mail-Konten bis hin zur jüngsten als „Heartbleed“ bezeichneten Sicherheitslücke eines bestimmten SSL-Verschlüsselungsverfahrens. Grund genug also zu erfahren, welche Wünsche und Anforderungen die Internetnutzer in dieser Zeit an das Online-Banking haben. Denn eines ist klar: Bei kaum einem anderen Thema reagieren die Menschen so sensibel wie bei ihren Finanzangelegenheiten.

Sicherheitsbedürfnis stagniert auf hohem Niveau

Bereits zum sechsten Mal hat die Fiducia daher gemeinsam mit der Initiative D21 die Marktforscher von TNS Infratest beauftragt, sich in der „Internetgemeinde“ zum Online-Banking umzuhören. Und wie die jetzt vorgelegte, repräsentative Befragung ergab, erledigen rund 75 Prozent der über 14-jährigen Internetnutzer ihre Bankgeschäfte über das weltweite Datennetz, etwa 19 Prozent lehnen dies bewusst ab. Hauptgrund hierfür sind Sicherheitsvorbehalte, wengleich nur knapp zwei Prozent der Befragten angaben, durch Betrug im Online-Banking einen finanziellen Schaden erlitten zu haben.

Grundsätzlich überrascht es kaum, dass die Themen Sicherheit und Datenschutz sowohl bei den Nutzern als auch bei jenen, die Online-Banking ablehnen, ganz oben auf der Anforderungsliste zu finden sind, und zwar auf nahezu unverändert sehr hohem Niveau. Daher erstaunt es umso mehr, dass die Bereitschaft nach wie vor gering ist, für sichere Transaktionen im Online-Banking einen gewissen Betrag zu bezahlen. So ist über die Hälfte der Internetnutzer davon überzeugt, dass dies ein kostenloses Angebot der Kreditinstitute sein sollte. Für sie hat die Sicherheit im Online-Banking somit keinen Preis.

Smartphone und Tablet auf dem Vormarsch

Internetfähige mobile Endgeräte, so genannte mobile Devices, verändern das Verhalten der Verbraucher grundlegend – auch beim Online-Banking. Wie die Studie zeigt, wird dieser Trend vorwiegend von den Jüngeren zwischen 14 und 34 Jahren getragen. Von den über 55-jährigen greift aktuell nur jeder zehnte Online-Banker über ein Smartphone auf sein

Konto zu. Diese Gruppe erledigt ihre Bankgeschäfte dann doch noch lieber vom heimischen PC.

Über das Online-Banking hinaus sehen wir für den „Alleskönner“ Smartphone aber noch weiteres Potenzial: das bargeldlose Bezahlen. Mobile-Payment lautet hier das Stichwort, ein Verfahren, das sich in den USA, Afrika oder in Asien bereits etabliert hat, das in Deutschland aber noch in den Kinderschuhen steckt. Dies zeigt auch die Befragung, denn nur knapp fünf Prozent gaben an, ein solches System zu nutzen. Einsatzmöglichkeiten werden hier vor allem beim Bezahlen an der Ladenkasse gesehen, aber auch beim Kauf von Tickets oder sonstiger Waren am Automaten. Allerdings hat ein gutes Drittel der Befragten bisher überhaupt noch nichts über Mobile-Payment gehört. Dennoch: Sollte sich ein Verfahren auf diesem Sektor durchsetzen, das sowohl bei Kunden als auch bei den Händlern auf breite Akzeptanz stößt, bieten sich insbesondere für die Volksbanken und Raiffeisenbanken oder auch die Sparkassen große Chancen. Denn, so ein weiteres Ergebnis der Studie, in puncto Sicherheit genießen die Kreditinstitute als Anbieter und Abwickler von Mobile-Payment den größten Vertrauensvorsprung bei den Onlinern.

Für die Fiducia als IT-Dienstleister einer großen Bankengruppe, dessen zentraler Markenwert „Sicherheit“ ist, bildet die jetzt vorgelegte 6. Auflage der Studie „Online-Banking 2014 – Sicherheit zählt!“ wieder eine wichtige Momentaufnahme. Zudem engagiert sich die Fiducia unter anderem im Gesamtvorstand seit vielen Jahren aktiv in der Initiative D21, um den Wandel zur digitalen Gesellschaft aktiv zu begleiten. Die gemeinsame Studie liefert damit auch Wirtschaft und Politik eine solide Faktenbasis zu Anforderungen, Wünschen und Befürchtungen der Bürgerinnen und Bürger bei einer der vielleicht sensibelsten digitalen Anwendungen überhaupt: den Bankgeschäften über das Internet.

Jens-Olaf Bartels

Mitglied des Vorstands Fiducia IT AG

Mitglied des Gesamtvorstands
der Initiative D21



Zentrale Ergebnisse im Überblick



Sicherheit und Datenschutz sind unverändert die wichtigsten Anforderungen sowohl der Nutzer als auch der Nutzungsplaner an das Online - Banking.

76%

Sicherheitsvorbehalte sind die größten Barrieren für die Nutzung von Online - Banking. Hauptgrund für die Ablehnung ist die Angst vor Betrug (sagen 76 Prozent der Online - Banking - Ablehner).

Sicherheitsmaßnahmen stoßen auf große Zustimmung, neben den bereits etablierten Verfahren finden auch neue Varianten wie Tages- und Auslandslimits oder SMS - Benachrichtigungen Anklang.



Nach wie vor erwartet über die Hälfte der Internetanwender, dass sicheres Online - Banking kostenlos von den Banken zur Verfügung gestellt wird.

>50%

Sm@rt - TAN plus und mobileTAN sind die bekanntesten und am häufigsten genutzten Sicherheitsverfahren (über 50 Prozent Bekanntheit bei Internetnutzern).

69%

Die Bekanntheit von Mobile - Payment ist leicht gestiegen. Banken als Anbieter beziehungsweise Abwickler von Mobile - Payment genießen bei Nutzern und Nutzungsplanern das größte Vertrauen (69 Prozent).

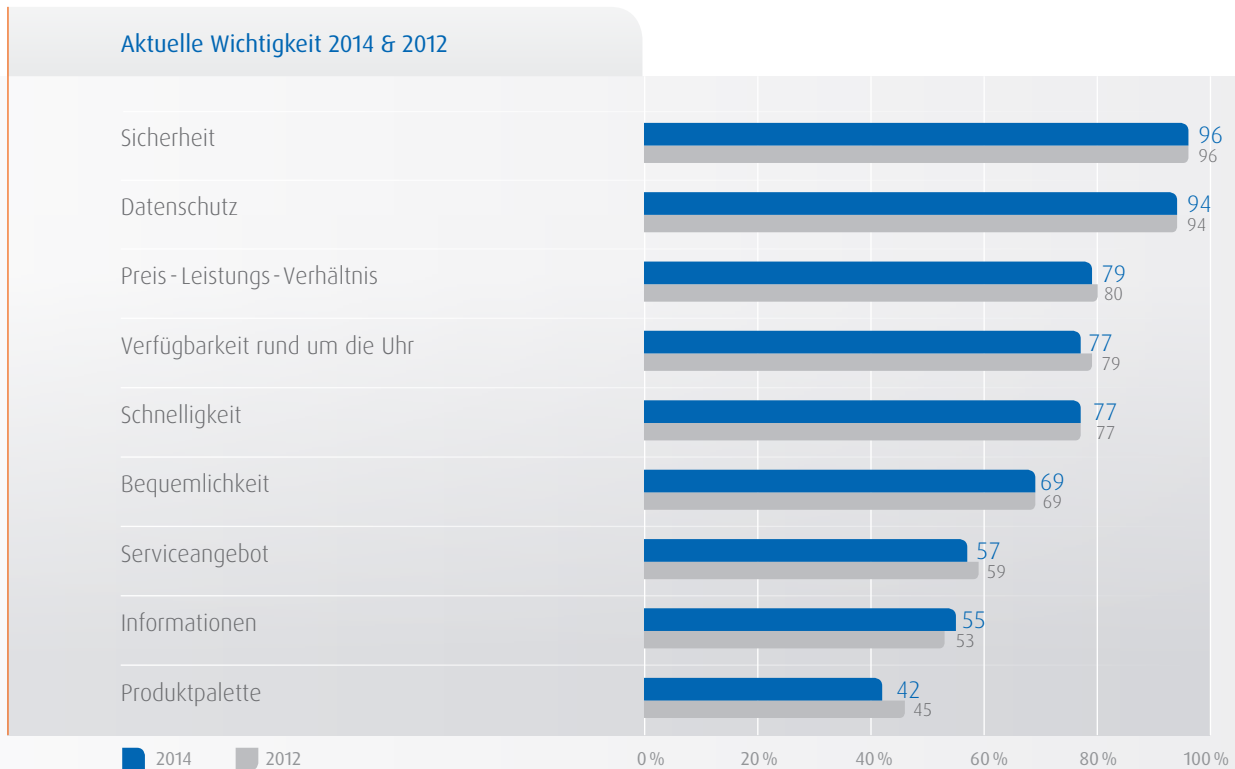
Während sich die Online - Erledigung von Bankgeschäften auf konstantem Niveau (75 Prozent der Internetnutzer) bewegt, ist der Anteil der Nutzung über mobile Endgeräte deutlich gestiegen.



1 Anforderungen an das Online - Banking



» Wie wichtig sind Ihnen persönlich die folgenden Punkte beim Online - Banking? «



BASIS Alle Befragten 2014: n=1.001 | 2012: n=1.002 | Top2 - Werte Skala 1=unwichtig bis 5=äußerst wichtig



Sicherheit und Datenschutz sind in ihrer Bedeutung konstant geblieben!

Die Anforderungen, die an das Online - Banking gestellt werden, reichen von Sicherheitsanforderungen über die angebotenen Leistungen und ablaufenden Prozesse bis hin zu Vorteilen gegenüber klassischem Banking wie der ständigen Verfügbarkeit der Kontoinformationen im Internet und damit verknüpft der Möglichkeit, (einige) Bankgeschäfte rund um die Uhr erledigen zu können. Wie in den Vorjahren erweisen sich Sicherheit und Datenschutz als die mit Abstand wichtigsten Anforderungen, die die Onliner in Deutschland haben. Auffällig ist, dass das Sicherheitsbedürfnis ganz allgemein trotz der jüngsten Diskussionen zum Datenschutz, etwa aufgrund der als »Heartbleed« bekannt gewordenen SSL - Sicherheitslücke, konstant geblieben und nicht gestiegen ist.

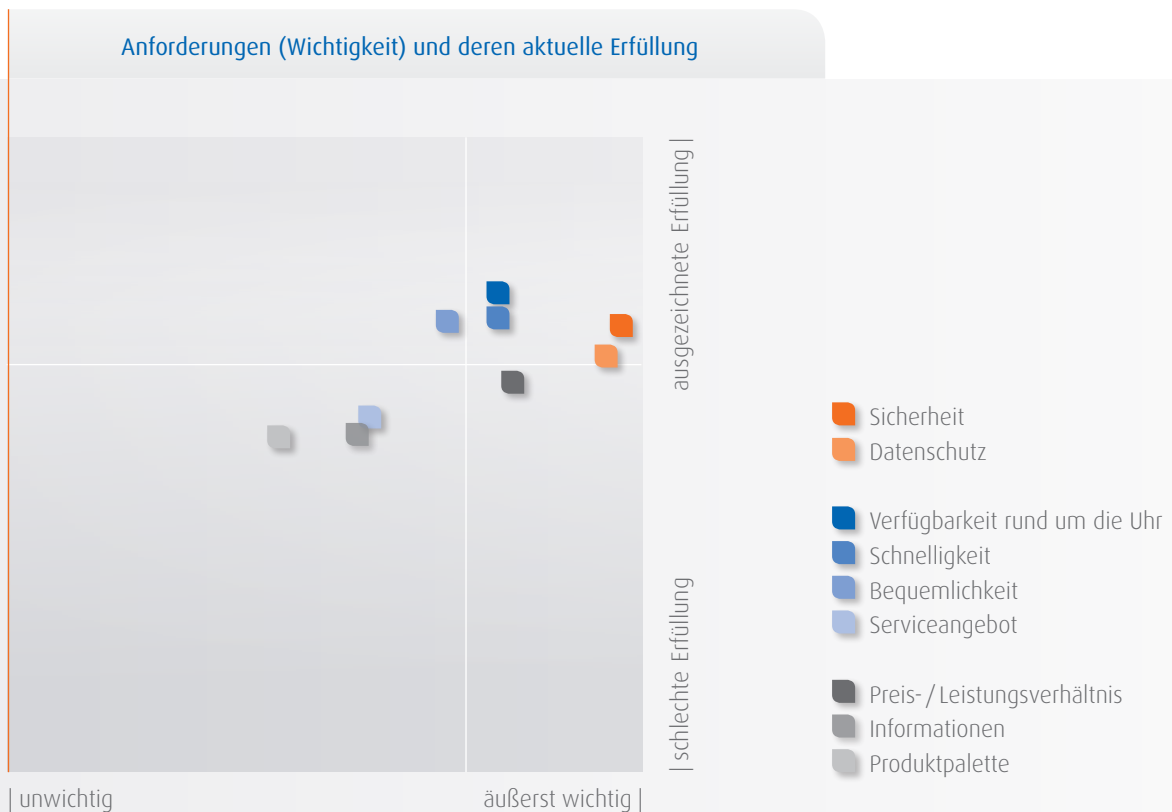
Etwas weniger wichtig sind aus Nutzersicht das Verhältnis von Preis und Leistung (79 Prozent), die Rund - um - die - Uhr - Verfügbarkeit (77 Prozent) sowie die Schnelligkeit, mit der man im Online - Banking seine Bankgeschäfte erledigen kann (77 Prozent). Das Serviceangebot als solches sowie Informationen und die Produktpalette sind dagegen für rund die Hälfte der Internetnutzer von Relevanz.

Die Abstufung der verschiedenen Aspekte ist über die letzten Jahre hinweg stabil. Dies ist ein klares Zeichen der deutschen Internetbevölkerung, dass sie die Sicherheit ihrer Daten prinzipiell über alle Produktvorteile stellt, die Online - Banking bietet.

1.1 Anforderungen und deren aktuelle Erfüllung im Online - Banking

?

» Wie wichtig sind Ihnen persönlich die folgenden Punkte beim Online - Banking? Wie gut sind die folgenden Punkte aktuell im Online - Banking erfüllt? «



BASIS Alle Befragten: n=1.001; Top2 - Werte Wichtigkeit (sehr / äußerst wichtig) und Erfüllung (sehr gut / ausgezeichnet) | Das Achsenkreuz besteht aus den durchschnittlichen Top2-Werten aller Aspekte (0 bis 100%).

i

Internetnutzer sehen noch Potenzial beim Thema Sicherheit

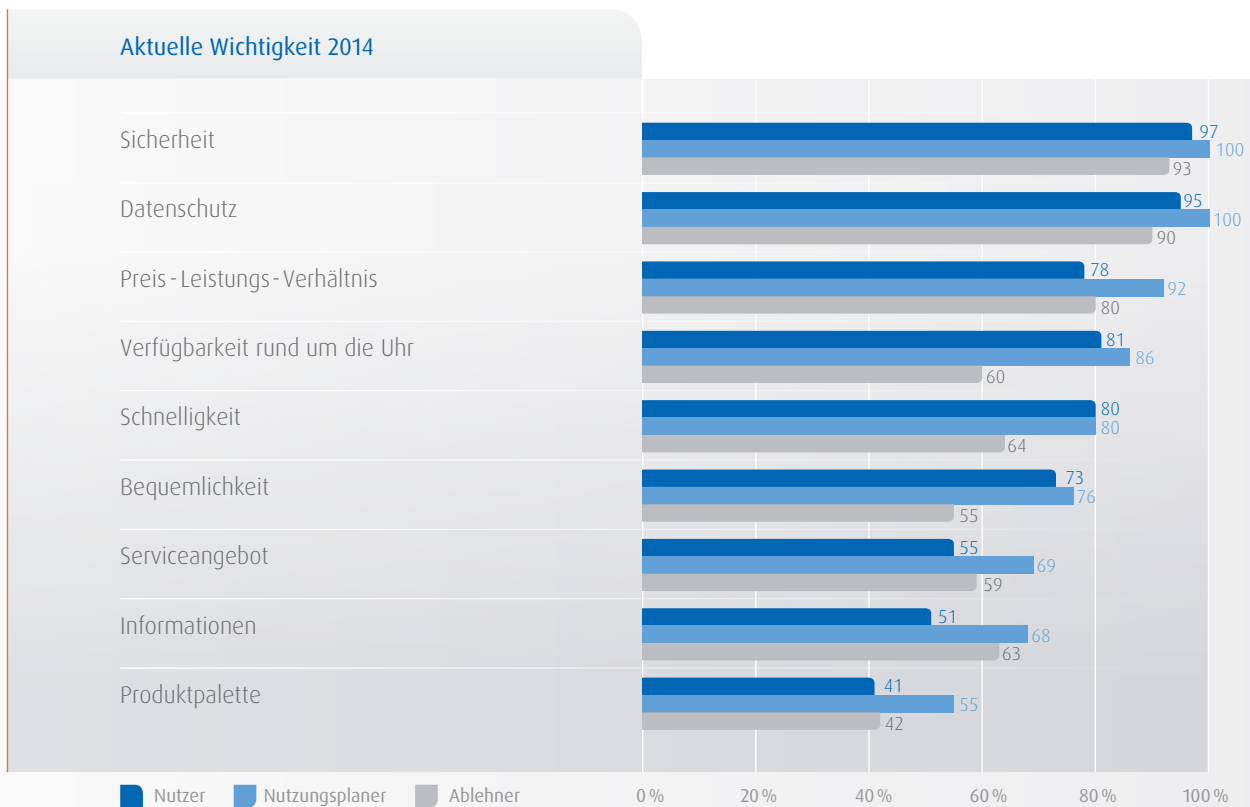
Der Abgleich zwischen der geäußerten Wichtigkeit der unterschiedlichen Aspekte und deren aktuell wahrgenommener Erfüllung im Online - Banking zeigt eine Diskrepanz auf. Sicherheit und Datenschutz werden zwar am häufigsten als wichtig eingestuft, sind aber aus Sicht der deutschen Online - Bevölkerung nicht am besten umgesetzt: Nur sieben von zehn Internetnutzern sehen ihr Bedürfnis nach Sicherheit erfüllt. Lediglich rund zwei Drittel geben an, dass der Datenschutz beim Online - Banking aus ihrer Sicht derzeit gut eingehalten wird.

Die Nutzenaspekte werden dagegen etwas besser bewertet: Verfügbarkeit, Schnelligkeit und Bequemlichkeit sind im Vergleich die aktuell am besten erfüllten Aspekte beim Online - Banking.

1.2 Aktuelle Anforderungen bei Online - Banking - Nutzern, Nutzungsplanern und Ablehnern



»Wie wichtig sind Ihnen persönlich die folgenden Punkte beim Online - Banking?«



BASIS Online - Banking - Nutzer: n = 755 | Nutzungsplaner: n = 47 | Online - Banking - Ablehner: n = 184 | Top2 - Werte Skala 1 = unwichtig bis 5 = äußerst wichtig

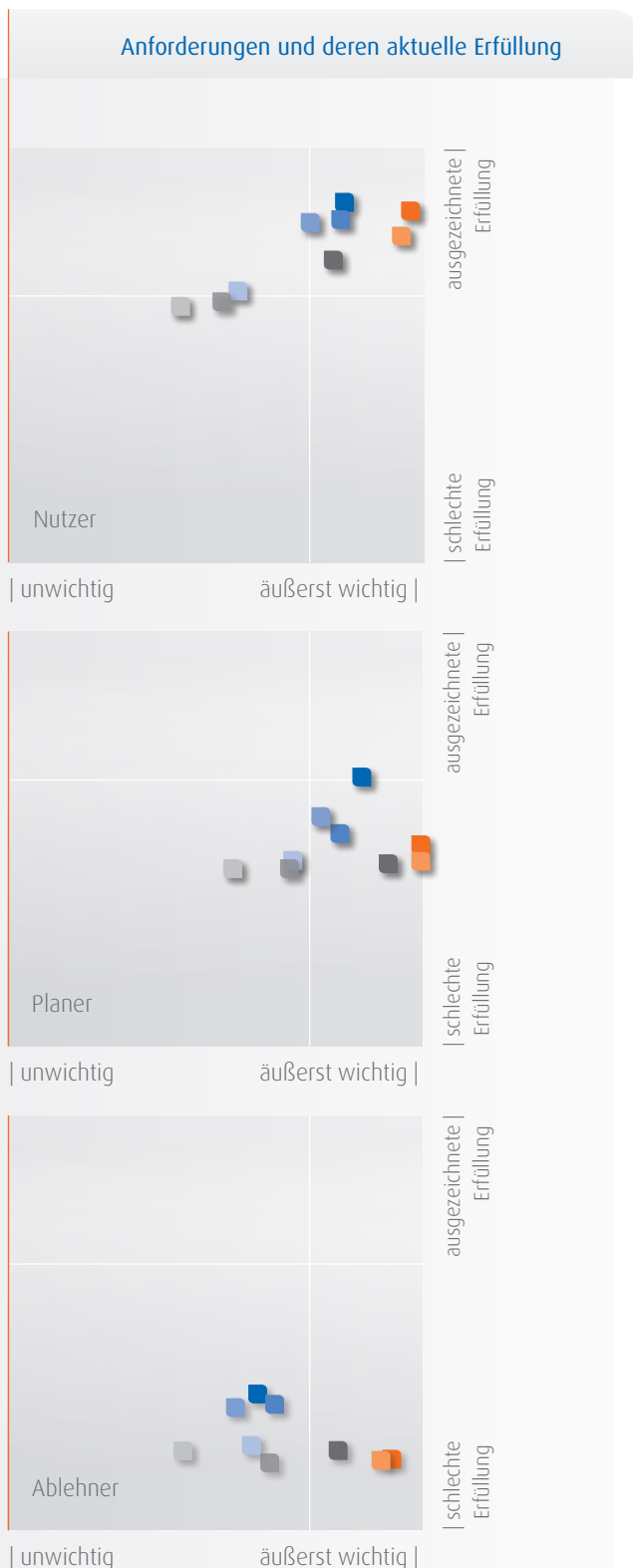
Für Nutzer, Nutzungsplaner und die aktuellen Ablehner von Online - Banking sind die abgefragten Aspekte unterschiedlich relevant. Für diejenigen, die planen, künftig Online - Banking zu nutzen, liegen Sicherheit und Datenschutz mit 100 Prozent auf Platz eins der Wichtigkeit. Dies ist ein klares Indiz dafür, dass Sicherheit und Schutz der individuellen Daten die Haupt - Barriere der Nutzung darstellen. An dritter Stelle steht (wie bereits 2012) das Verhältnis von Preis und Leistung.

Die Ablehner von Online - Banking schreiben den Nutzenaspekten des Services wie der Rund - um - die - Uhr - Verfügbarkeit oder der Schnelligkeit nur unterdurchschnittliche Relevanz zu. Doch gerade diese Bereiche sind nach den Sicherheitsaspekten für die Nutzer selbst am wichtigsten.

1.3 Anforderungen und deren aktuelle Erfüllung im Online - Banking bei Nutzern, Nutzungsplanern und Ablehnern



» Wie wichtig sind Ihnen persönlich die folgenden Punkte beim Online - Banking? Wie gut sind die folgenden Punkte aktuell im Online - Banking erfüllt? «



Online - Banking - Nutzer sehen ihre Sicherheitsanforderungen aktuell weitgehend erfüllt!

Die Online - Banking - Nutzer schätzen das Thema Sicherheit nicht nur als wichtig ein, sondern sehen es im Online - Banking im Vergleich zur Gesamtheit der Internetanwender (siehe 1.2) auch stärker erfüllt.

Für die Ablehner sind Sicherheit und Datenschutz zwar auch die wichtigsten, zugleich jedoch die am schlechtesten umgesetzten Anforderungen an das Online - Banking. Sicherheitsvorbehalte erweisen sich damit als Hauptbarrieren der Nutzung. Hier könnte im ersten Schritt bereits eine stärkere Kommunikation sicherer Verfahren helfen, aktuelle Ablehner zur Nutzung von Online - Banking zu bewegen.

- Sicherheit
- Datenschutz
- Verfügbarkeit rund um die Uhr
- Schnelligkeit
- Bequemlichkeit
- Serviceangebot
- Preis- / Leistungsverhältnis
- Informationen
- Produktpalette

BASIS Online - Banking - Nutzer: n = 755 | Nutzungsplaner: n = 47 | Online - Banking - Ablehner: n = 184

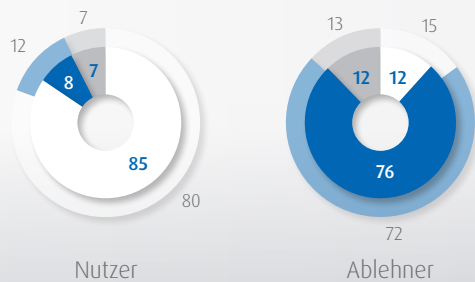
Dargestellt sind Top2 - Werte Wichtigkeit (sehr / äußerst wichtig) und Erfüllung (sehr gut / ausgezeichnet) | Das Achsenkreuz besteht aus den durchschnittlichen Top2 - Werten aller Aspekte (0 bis 100%).

1.4 Angst vor Betrug als Barriere?



» Hält Sie die Befürchtung, beim Online-Banking betrogen zu werden, derzeit von Transaktionen im Internet ab? «

Angst vor Betrug Nutzer/Ablehner 2014 & 2012



» 8 % der Online-Banking Nutzer handeln vorsichtiger aus Angst vor Betrug. «

Angst vor Betrug nach Geschlecht 2014



2014
2012

■ Ja
 ■ Nein
 ■ Weiß nicht / keine Angabe

BASIS Alle Befragten 2014: n=1.001 | Frauen: n=483 | Männer: n=518 | Online-Banking-Nutzer: n=755 | Online-Banking-Ablehner: n=184 | 2012: Online-Banking-Nutzer: n=786 | Ablehner: n=158

» 76 % der Online-Banking-Ablehner nennen Angst vor Betrug als Barriere. «

Die Angst der Ablehner vor Betrug im Online-Banking ist 2014 leicht auf 76 Prozent gestiegen (2012: 72 Prozent). Weniger ängstlich dagegen sind die Nutzer: Nur acht Prozent geben an, dass sie Betrug befürchten und deshalb Transaktionen im Internet momentan meiden, d.h. aktuell auf die Nutzung von Online-Banking verzichten. 2012 waren dies noch zwölf Prozent.

1.5 Mögliche Motivatoren für zukünftige Online - Banking Nutzung



» Welche der folgenden Leistungen könnte Sie dazu bewegen, künftig Online - Banking zu nutzen? «

Motivatoren 2014



BASIS Online - Banking - Ablehner: n=184

55 Prozent derjenigen, die einer Online - Banking - Nutzung ablehnend gegenüberstehen, geben an, dass nichts sie zu einer Nutzung bewegen kann. Für die übrigen 45 Prozent aktueller Ablehner wurden hingegen mögliche Motivatoren für eine künftige Nutzung ermittelt.

Der am häufigsten genannte Ansatz ist die Entwicklung ganz neuer Sicherheitsverfahren. Auch die zweit- und dritthäufigsten Beweggründe sind Sicherheitsaspekte. Sowohl eine Sicherheitsgarantie der Bank als auch eine ausführliche Aufklärung über Sicherheitsmaßnahmen könnten

die Betroffenen vom Online - Banking überzeugen. Weit weniger Umstimmungspotenzial besitzen die Erhöhung der Benutzerfreundlichkeit und eine Einführung in die Funktionsweise des Online - Bankings.

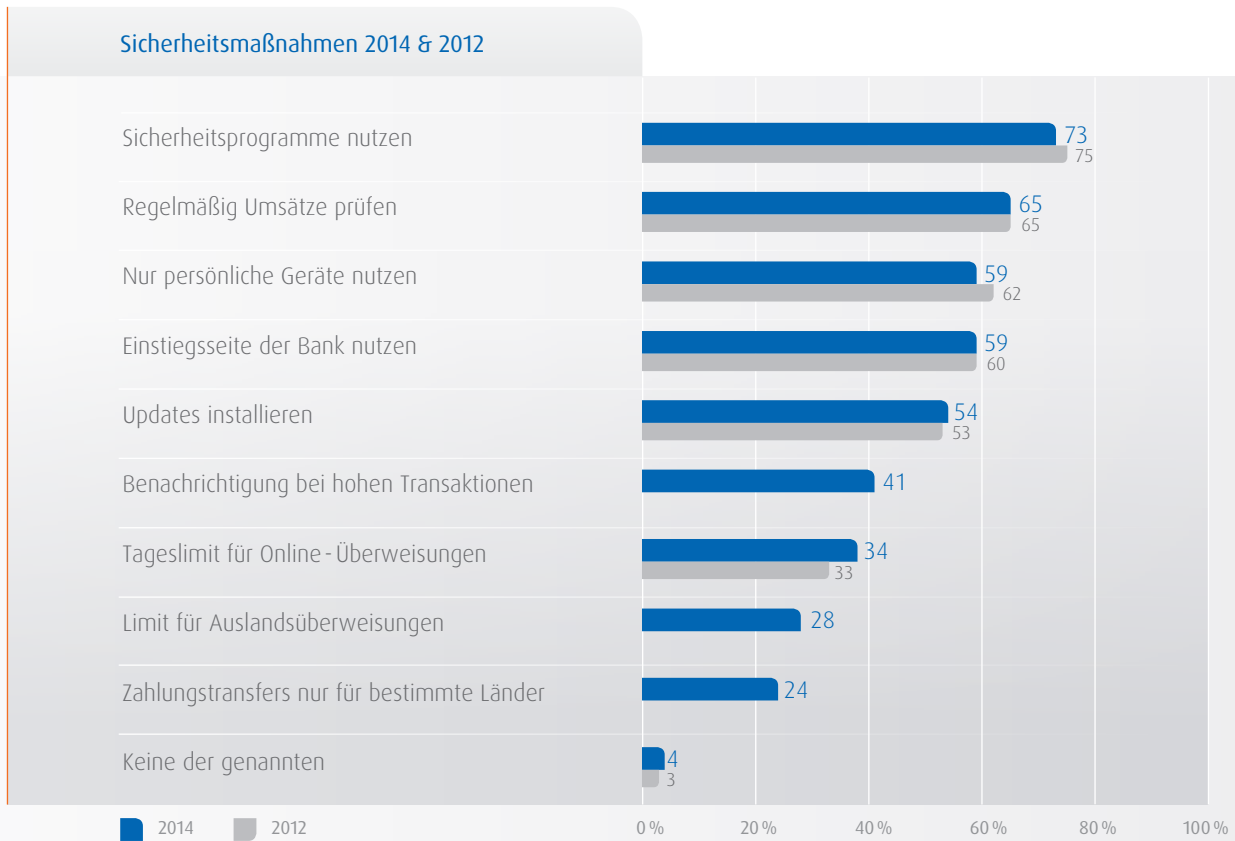
Zusammenfassend könnten erweiterte Sicherheitsmaßnahmen und deren stärkere Kommunikation maßgeblich dazu beitragen, aktuelle Ablehner von der Nutzung des Online - Bankings zu überzeugen.

2 Sicherheit beim Online - Banking

2.1 Sicherheitsmaßnahmen



» Welche der folgenden Maßnahmen kommen für Sie persönlich in Frage, um die Sicherheit beim Online - Banking zu erhöhen? «



BASIS Alle Befragten 2014 n=1.001 | 2012: n=1.002 | Mehrfachantworten möglich

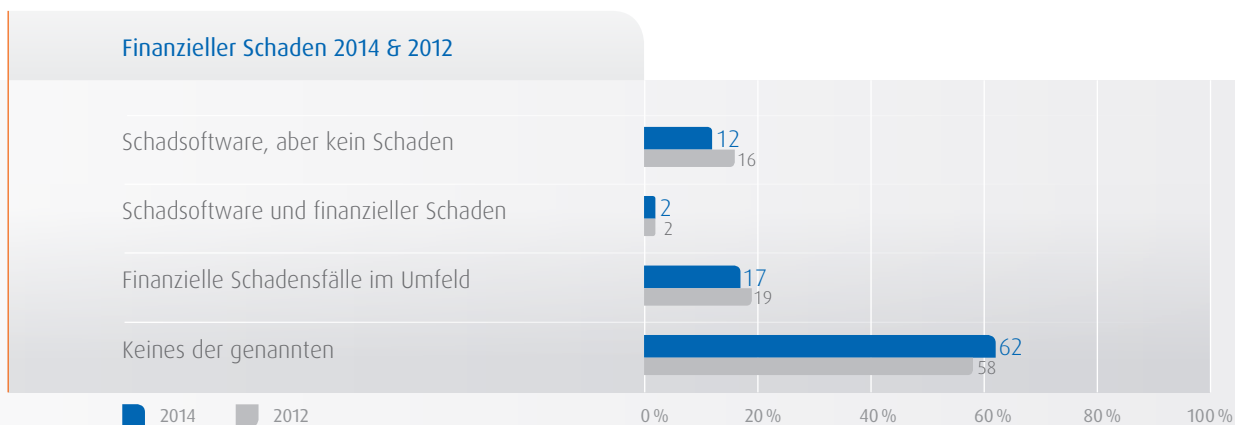
Trotz der aktuellen Diskussionen rund um das Thema Online - Sicherheit und Datenschutz ist eine Verstärkung der Sicherheitsmaßnahmen im Vergleich zu 2012 nicht erkennbar. Die Verwendung von Sicherheitsprogrammen, etwa zum Virenschutz, bleibt mit 73 Prozent auf nahezu dem gleichen Niveau wie 2012. Die ausschließliche Verwendung persönlicher Geräte ist von 62 Prozent auf 59 Prozent leicht zurückgegangen. Nach wie vor geben vier Prozent aller Befragten an, überhaupt keine Sicherheitsmaßnahmen für ihren eigenen Schutz zu ergreifen.

Insgesamt tragen allgemeine Schutzmaßnahmen (Nutzung von Sicherheitsprogrammen, regelmäßige Prüfung der Umsätze, Nutzung persönlicher Geräte und ausschließlicher Zugang über die Bank - Webseite) mehr dazu bei, die

Sicherheit beim Online - Banking zu erhöhen. Darüber hinaus ziehen die Internetnutzer auch individuelle Maßnahmen in Betracht wie den Abschluss von Versicherungen oder sogar persönliche Vereinbarungen mit der Bank. Allen voran käme hier ein SMS - Service bei ungewöhnlichen Kontobewegungen in Frage oder auch die Vereinbarung von Tages- oder Auslandslimits bei Online - Überweisungen. In der Zukunft werden diese Maßnahmen durch Systeme unterstützt, die das vollautomatische Erkennen und Unterbinden ungewöhnlicher oder dubioser Transaktionen im Online - Banking sicherstellen. Die Fiducia IT AG arbeitet derzeit an einem solchen System zur Betrugserkennung im Online - Banking. Diese so genannte » Fraud Detection « soll die Sicherheit und das Vertrauen ins Online - Banking künftig weiter erhöhen.

2.2 Finanzielle Schäden durch Online - Banking

» Ist Ihnen schon einmal ein finanzieller Schaden im Zusammenhang mit Online - Banking entstanden? «



BASIS Alle Befragten 2014: n=1.001 | 2012: n=1.002

Erklärung der wichtigsten Techniken

iTAN

Die Autorisierung einer Transaktion muss bei diesem Verfahren durch eine bestimmte (= indizierte) Transaktionsnummer (TAN) erfolgen. Dazu ist jede TAN auf der TAN - Liste, die der Kunde von seiner Bank erhält, durch eine Positionsnummer (= Index) gekennzeichnet.

Sm@rt - TAN plus

Das Verfahren stellt zwei Anwendungsmöglichkeiten zur Verfügung: mit manueller Eingabe oder mit optischer Übertragung.

Mit manueller Eingabe

Beim Sm@rt - TAN - plus - Verfahren mit manueller Eingabe schiebt der Bankkunde seine Chipkarte in einen Kartenleser (TAN - Generator) mit integrierter Tastatur. Anschließend gibt er dort manuell die Daten ein, die für die Erstellung einer TAN benötigt werden. Die Transaktion, etwa eine Überweisung, und die TAN - Übermittlung werden so in zwei Schritte zerlegt und voneinander getrennt durch-

geführt. TAN - Nummern können dadurch nicht mehr via Phishing abgefangen, willkürlich geändert oder für einen anderweitigen Überweisungsauftrag verwendet werden. Die erzeugte TAN wird nur für diesen entsprechenden Überweisungsauftrag erstellt und durch den Anwender zusätzlich kontrolliert.

Mit optischer Übertragung

Beim Sm@rt - TAN - plus - Verfahren mit optischer Übertragung der Transaktionsdaten ist die manuelle Eingabe der Auftragsdaten nicht mehr nötig. Die optische Schnittstelle im Lesegerät (TAN - Generator) liest nach dem Einschieben der Chipkarte die notwendigen Kontrolldaten vom Monitor direkt in das Lesegerät ein. Die erforderlichen Daten werden über eine animierte Grafik in die Online - Anwendung eingeblendet. Der Kunde muss daher keine Daten mehr am Lesegerät eingeben, sondern nur den Leser vor die animierte Grafik halten und anschließend die im Leser angezeigten Werte mit den Originaldaten, beispielsweise mit einer Rechnung, vergleichen. Danach werden die Anga-

Finanzielle Schäden durch Online - Banking

Lediglich knapp zwei Prozent der Befragten gibt an, beim Online - Banking schon einmal einen finanziellen Schaden erlitten zu haben. Damit liegt dieser Wert auf gleicher Höhe wie im Jahr 2012. Dennoch: Blindes Vertrauen in das digitale Bankgeschäft ist trotz der geringen Zahl an Betroffenen nicht angebracht. Denn immerhin 17 Prozent der Befragten können von finanziellen Schadensfällen in ihrem Umfeld im Zusammenhang mit Online - Banking berichten. Die Gefahr von Beeinträchtigungen ist damit zwar tendenziell über die letzten zwei Jahre gesunken, dennoch weiterhin ernst zu nehmen.



» Die Fiducia IT AG arbeitet derzeit an » Fraud Detection«, einem System zur Betrugserkennung. «

ben mit der »OK«-Taste bestätigt, und dem Kunden wird die TAN im Display des Lesers angezeigt.

mobileTAN

Hier erhält der Bankkunde die TAN zur Autorisierung seiner Transaktion per SMS auf sein Handy, zusammen mit den wesentlichen Transaktionsdaten wie Betrag und Empfängerkontonummer. Nach Prüfung der in der SMS enthaltenen Daten schließt der Kunde mit der Eingabe der TAN aus der zugesandten SMS in das Online - Formular die Transaktion ab.

HBCI

Die Autorisierung von Transaktionen erfolgt hier durch hardwaregestützte Verschlüsselungstechnik. Dazu stellt die Bank dem Kunden eine personalisierte Chipkarte aus. Der Kunde benötigt zusätzlich einen Chipkartenleser, den er an seinen Computer anschließt und eine Software, die den HBCI (Homebanking Computer Interface)-Standard unterstützt. Beim Online - Banking mit Chipkarte entfallen

die TAN - Listen, deren jeweilige Freischaltung und die Eingabe der TAN durch den Bankkunden.

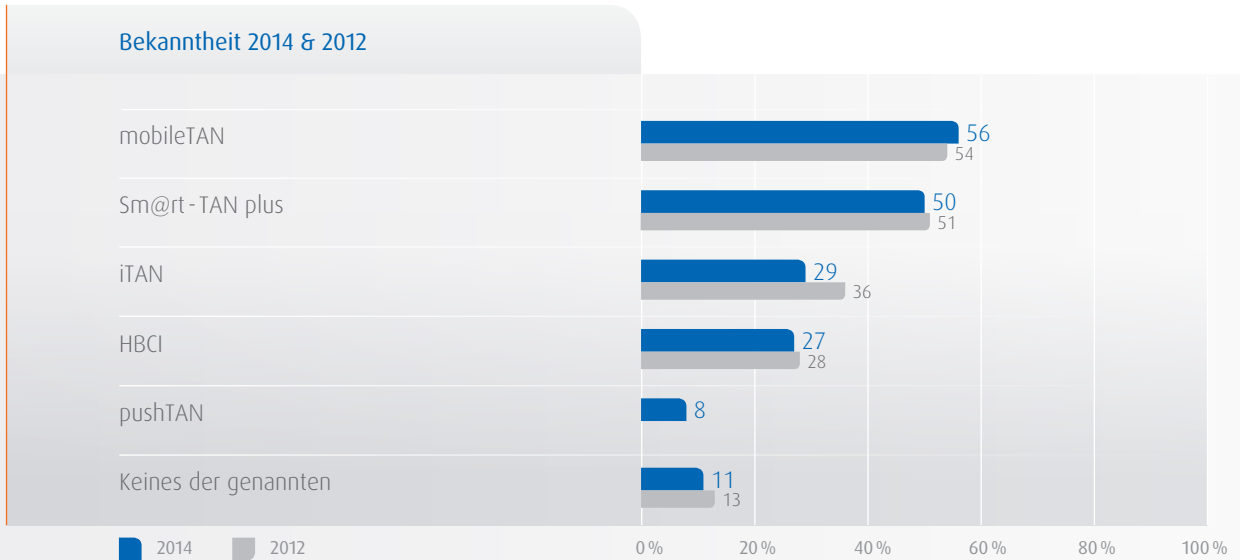
pushTAN

Das pushTAN - Verfahren erfordert neben der eigentlichen Banking - Anwendung am PC oder auf dem mobilen Endgerät eine zusätzliche App auf dem Smartphone oder anderem Gerät (z. B. Tablet). Anders als bei der mobileTAN wird die Transaktionsnummer nicht über das Mobilfunknetz übermittelt, sondern über eine verschlüsselte IP - Verbindung aus dem Rechenzentrum der Bank. Zusätzlich wird diese App mit weiteren Sicherheitsmaßnahmen gesondert gegen Angriffe geschützt. Die PushTAN - App ist unabhängig vom Online - Banking und nutzt eigene Zugangsdaten. Der Nutzer prüft wie bisher die in der App angezeigten Transaktionsdaten wie Empfänger - IBAN oder Betrag und erfasst die TAN dann in seiner Banking - Anwendung.

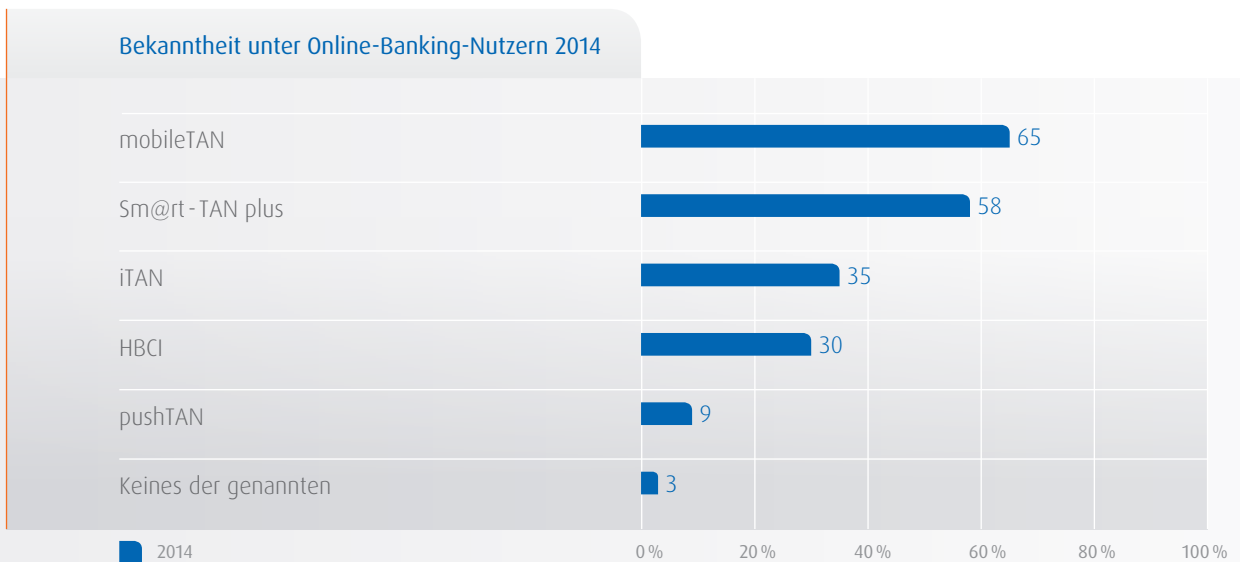
2.3 Bekanntheit von Sicherheitstechniken



» Welche der folgenden Sicherheitsverfahren beim Online - Banking kennen Sie? «



BASIS Alle Befragten 2014: n = 1.001 | 2012: n = 1.002

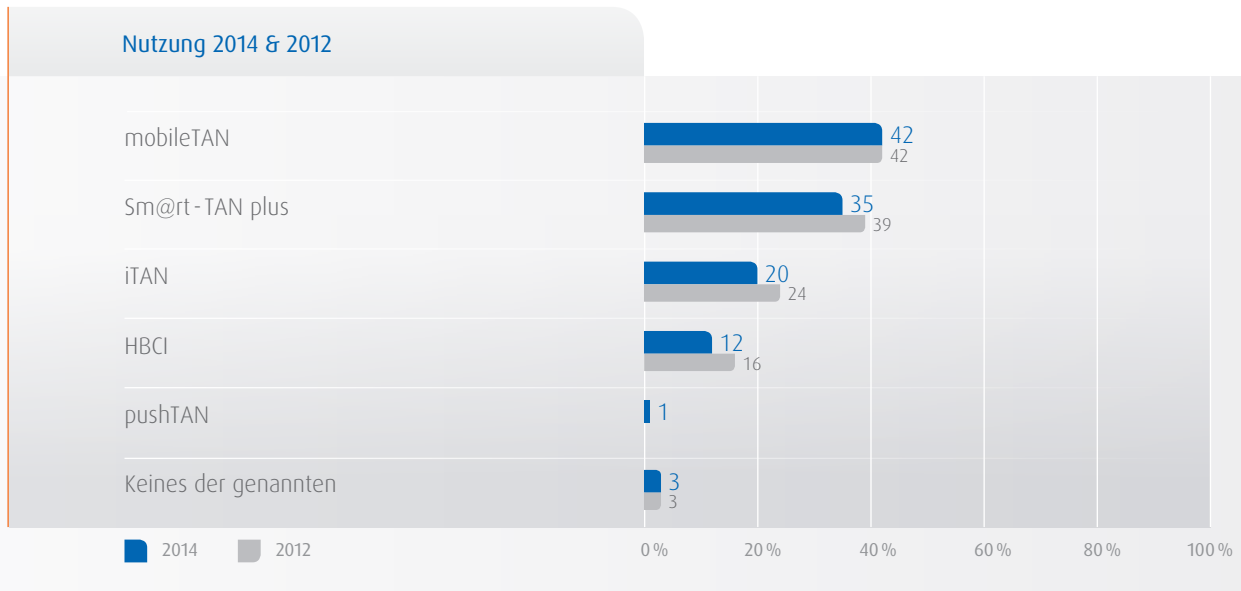


BASIS Alle Online - Banking - Nutzer (2014): n = 755

2.4 Nutzung von Sicherheitstechniken



» Welche der folgenden Sicherheitsverfahren beim Online - Banking nutzen Sie? «



BASIS Alle Online - Banking - Nutzer | 2014: n = 755 | 2012: n = 757

Die Bekanntheit der mittlerweile etablierten Verfahren Sm@rt-TAN plus und mobileTAN liegt im Vergleich zur Vorgängerstudie aus dem Jahr 2012 ungefähr auf dem gleichen Niveau (mehr als die Hälfte aller Befragten, also Nutzer und Ablehner von Online-Banking, kennt diese beiden Methoden). Im Vergleich zu 2012 verliert iTAN an Bedeutung, die Bekanntheit geht hier um sieben Prozentpunkte zurück. Ein wesentlicher Grund hierfür dürfte die Einstellung dieses Systems bei vielen Instituten Anfang 2012 sein. Das vergleichsweise neue und derzeit nur von den öffentlich-rechtlichen Kreditinstituten angebotene Verfahren »pushTAN« ist aktuell noch wenig bekannt (acht Prozent).

Betrachtet man nur die Gruppe der Online-Banking-Nutzer, so ist die mobileTAN mit fast zwei Drittel (65 Prozent) aktuell das bekannteste Sicherheitsverfahren, gefolgt von Sm@rt-TAN plus (58 Prozent). Die veraltete iTAN kennen nur noch etwas mehr als ein Drittel (35 Prozent) und HBCI Chipkarte ist immerhin 30 Prozent ein Begriff. Die vergleichsweise neue Methode via pushTAN-App ist derzeit nur neun Prozent der Online-Banking-Nutzer geläufig. Ins-

gesamt ist damit die Bekanntheit der einzelnen Verfahren unter Online-Banking-Nutzern naturgemäß etwas höher, wengleich auch hier mobileTAN und Sm@rt-TAN plus die beiden bekanntesten sind.

Die mobileTAN ist mit 42 Prozent auch das am häufigsten genutzte Verfahren unter Online-Banking-Nutzern, gefolgt von Sm@rt-TAN plus (35 Prozent). Die iTAN ist dagegen nur noch bei jedem fünften Online-Banking-Nutzer im Einsatz. HBCI Chipkarte wird von 12 Prozent verwendet. Die noch junge Methode pushTAN-App wird gerade mal von einem Prozent genutzt. Im Vergleich zu 2012 zeigt sich insgesamt über fast alle Verfahren (außer mobileTAN) ein leichter Rückgang, der auf einen insgesamt vorsichtigeren Umgang der Nutzer im Online-Banking schließen lässt.

2.5 Risikoeinschätzung von Geräten / Zahlungsmitteln

» Wie schätzen Sie das Risiko der Nutzung folgender Geräte bzw. Zahlungsmittel beim elektronischen Bezahlen ein? «



BASIS Alle Befragten 2014: n=1.001 | 2012: n=1.002 | Top2 - Werte Skala 1=sehr gering bis 4=sehr hoch

Risikoeinschätzung von Geräten / Zahlungsmitteln

Beim Vergleich verschiedener Geräte bzw. Zahlungsmittel, über die Zahlungstransaktionen durchgeführt werden können, zeigt sich eine klare Abstufung bei den empfundenen Sicherheitsrisiken. Wichtige Einflussfaktoren sind dabei der Standort und die Art des Zugangskanals.

So erscheint einem Großteil der Bevölkerung (87 Prozent) vor allem die Nutzung öffentlicher Computer als sehr riskant. Die Möglichkeit, dass andere Personen im Nachhinein auf ihre gespeicherten Daten zugreifen, könnte ein Grund für diese Einstellung sein. Private Geräte hingegen, die einen

festen Standort haben, werden von lediglich einem Drittel (36 Prozent) der Befragten als risikobehaftet angesehen.

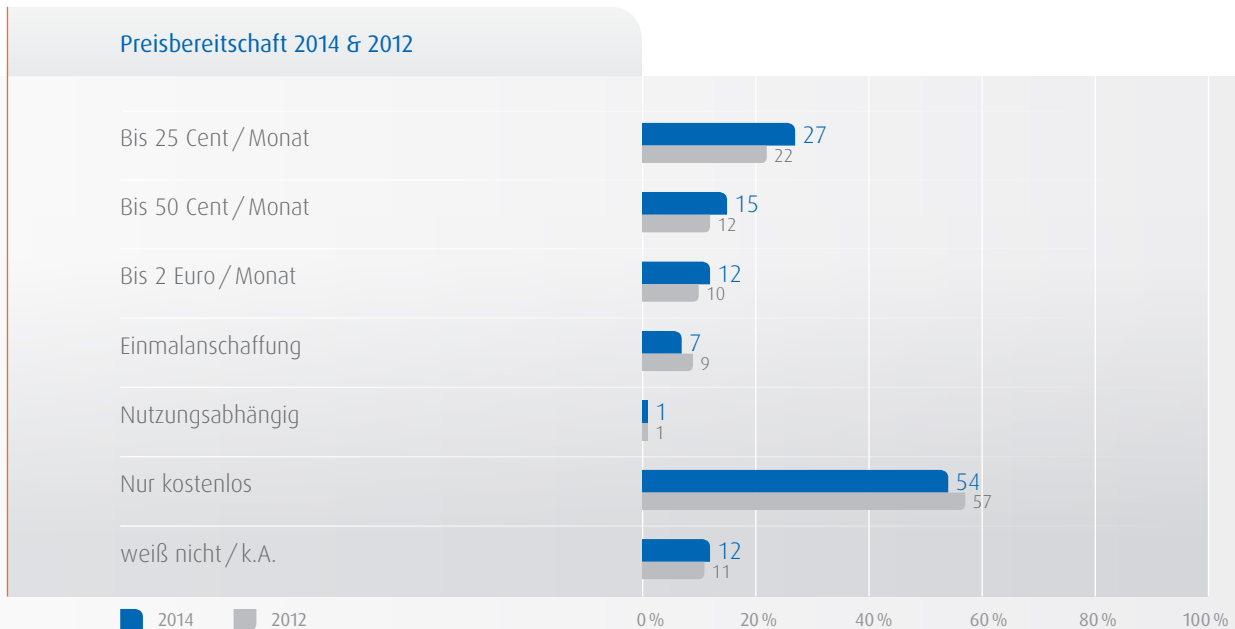
Mobile Endgeräte werden von vielen als unsicher eingeschätzt. So gehen drei Viertel der Befragten davon aus, dass Smartphones, gefolgt von Mobiltelefonen (70 Prozent) und Tablets (63 Prozent), ein erhöhtes Sicherheitsrisiko beim Online - Banking aufweisen.

Auch das Telefonbanking schätzt über die Hälfte der Online - Bevölkerung als risikobehaftet ein (53 Prozent).

2.6 Preisbereitschaft für sichere Transaktionen



» Welchen Preis würden Sie für sichere Transaktionen beim Online - Banking bezahlen? «



BASIS Alle Befragten 2014: n=1.001 | 2012: n=1.002

Als relativ sicher hingegen werden direkt durch die Banken gestellte Geräte eingeschätzt. So sehen nur etwas über ein Drittel der Befragten bei der Nutzung von Service-Terminals (36 Prozent) und Geldautomaten (38 Prozent) ein Risiko.

Bei den Zahlungsmitteln schätzt knapp die Hälfte der Internet-Nutzer (45 Prozent) die Kreditkarte als riskant ein. Demgegenüber erkennen nur knapp über ein Drittel in der Nutzung der Girocard (35 Prozent) und der Geldkarte (36 Prozent) Gefahrenpotenzial.

Preisbereitschaft für sichere Transaktionen

Die Bereitschaft, für sichere Transaktionen im Online-Banking zu bezahlen, ist wieder leicht gestiegen. So können sich über ein Drittel der Befragten vorstellen, hierfür einen gewissen Betrag zu entrichten. Bei der Frage nach der Höhe des akzeptierten Preises jedoch zeigen sich deutliche Unterschiede. Immerhin sind zwölf Prozent der Befragten bereit, zwei Euro pro Monat zu bezahlen, 15 Prozent wür-

den bis zu 50 Cent ausgeben, und für 27 Prozent wären 25 Cent pro Monat denkbar. Mit sieben Prozent ist nur ein sehr geringer Teil dazu bereit, einen einmaligen Betrag für die Sicherheit im Online-Banking zu bezahlen.

Im Durchschnitt würden die Zahlungsbereiten einen einmaligen Anschaffungspreis von 19,39 Euro akzeptieren, was ungefähr drei Euro unter der Zahlungsbereitschaft von 2012 liegt. Nach wie vor verschwindend gering ist mit etwa einem Prozent die Akzeptanz für eine nutzungsabhängige Gebühr beim Online-Banking. Hierfür wären die Nutzer bereit, etwa 13 Cent zu bezahlen.

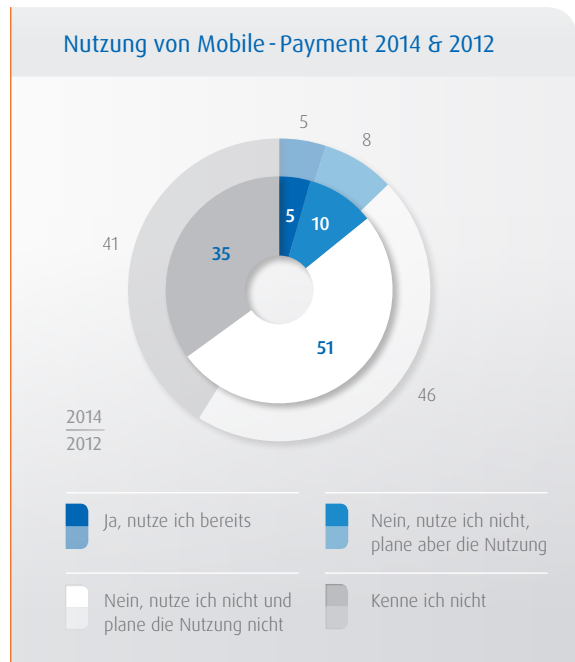
Trotz eines unverändert großen Sicherheitsbedürfnisses beim Online-Banking zeigen diese Werte, dass die »Internetgemeinde« mehrheitlich nach wie vor nicht bereit ist, in sicheres Online-Banking zu investieren. Noch immer geben 54 Prozent der Befragten an, dass sicheres Online-Banking ein Angebot sein soll, das die Kreditinstitute kostenlos zur Verfügung stellen müssen. Im Vergleich zu 2012 ist dieser Wert minimal gesunken (2012: 57 Prozent).

3 Mobile - Payment

Mobile-Payment ist eine relativ junge Entwicklung und bezeichnet die Möglichkeit, mit einem mobilen Endgerät wie Smartphone oder Tablet quasi im Vorbeigehen zu bezahlen. Ganz ohne Bankkarte oder Bargeld. Einen übergreifenden und einheitlichen technologischen Standard für ein solches System gibt es in Deutschland allerdings noch nicht. Legt man den Fokus auf den mobilen Bezahlprozess an der Supermarktkasse, so kristallisieren sich jedoch zwei Trends heraus: die Software-Lösung und die Hardware-Lösung. Bei der Software-Variante werden mittels eines Barcodes die notwendigen Informationen zwischen Händler und Kunde ausgetauscht und dann an den Zahlungsdienstleister übermittelt. Die Hardware-Lösung setzt momentan auf die Near-Field-Communication (NFC), die innerhalb einer sehr kurzen Reichweite den Austausch der relevanten Transferdaten zwischen Smartphone und PoS-Terminal ermöglicht.

Nutzung von Mobile - Payment 2012 und 2014

Während Mobile-Payment in den USA und vor allem in Asien boomt, ist dieser Trend in Deutschland noch nicht angekommen. Denn nur fünf Prozent aller Befragten geben an, Mobile-Payment bereits zu nutzen, weitere zehn Prozent planen die Nutzung. Jeder Zweite sagt hingegen, dass er mobile Bezahlssysteme aktuell weder nutzt noch den Einsatz plant. Mit 35 Prozent ist auch der Anteil derjenigen sehr hoch, die Mobile-Payment nicht kennen.



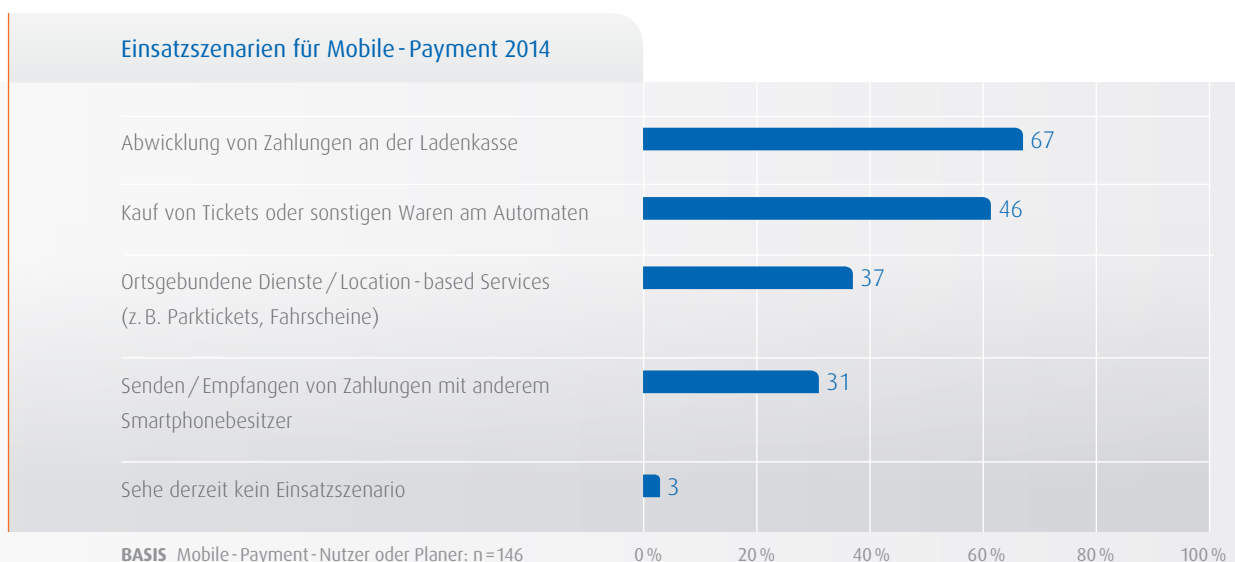
BASIS Alle Befragten 2014: n=1.001 | 2012: n=1.002

Der Vergleich mit den Befragungsergebnissen 2012 zeigt, dass sich in den vergangenen beiden Jahren wenig bei den mobilen Bezahlssystemen getan hat. Zwar ist die Bekanntheit leicht gestiegen, hingegen ist das Interesse, dieses Verfahren zu verwenden, auf niedrigem Niveau nahezu konstant geblieben.

3.1 Einsatzszenarien für Mobile - Payment 2014



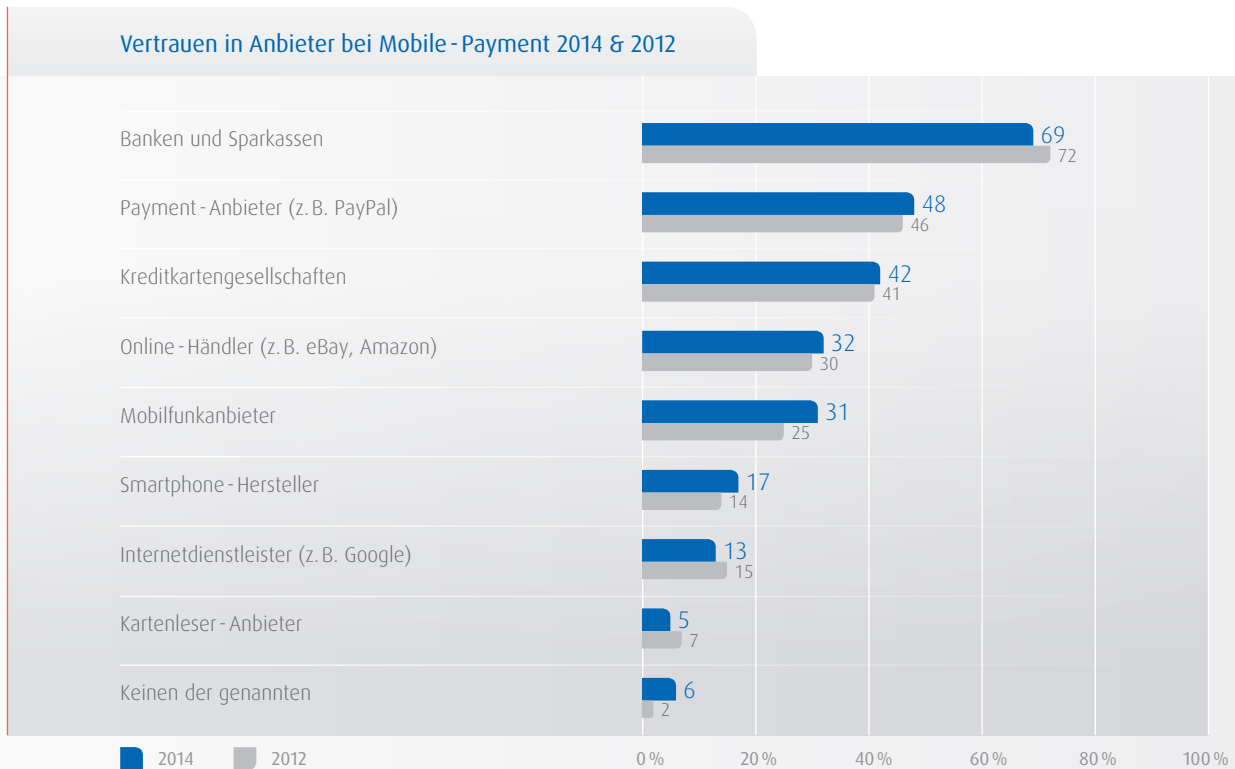
» Welche Einsatzszenarien sehen Sie für sich, Mobile - Payment zu nutzen? «



3.2 Vertrauen in Anbieter bei Mobile - Payment 2014



» Welchen Marktakteuren vertrauen Sie bzw. würden Sie vertrauen, falls Sie Mobile - Payment nutzen? «



BASIS Mobile - Payment - Nutzer oder Planer: n = 146

Einsatzszenarien für Mobile - Payment 2014

Bei der Frage nach den Anwendungsmöglichkeiten mobiler Bezahlfverfahren sehen die Nutzer von Mobile - Payment in erster Linie das Bezahlen an der Ladenkasse (67 Prozent). Ebenfalls beliebt sind der Kauf von Tickets oder sonstiger Waren am Automaten (46 Prozent) sowie die Nutzung ortsgebundener Dienste (37 Prozent).

Es fällt auf, dass sich immerhin 31 Prozent bereits vorstellen können, so genannte Peer - to - Peer - Bezahlvorgänge über ihr Smartphone abzuwickeln, also den Geldtransfer (Zahlungen senden und empfangen) zwischen Einzelpersonen, etwa bei privaten Verkäufen. Vor dem Hintergrund, dass solche Systeme im Markt derzeit nur in ersten Ansätzen und in kleineren, geschlossenen Benutzergruppen existieren, ist dies ein positives Ergebnis.

Vertrauen in Anbieter bei Mobile - Payment

Trotz des bislang niedrigen Interesses der Onliner für das Thema Mobile - Payment ist es mit Blick auf die Sicherheit eines solchen Verfahrens interessant, zu erfragen, welchen Anbietern oder Abwicklern entsprechender Systeme die Internetgemeinde in Zukunft am ehesten vertrauen würde. Hier scheint sich die Expertise der Banken beim Thema Online - Banking durchzusetzen.

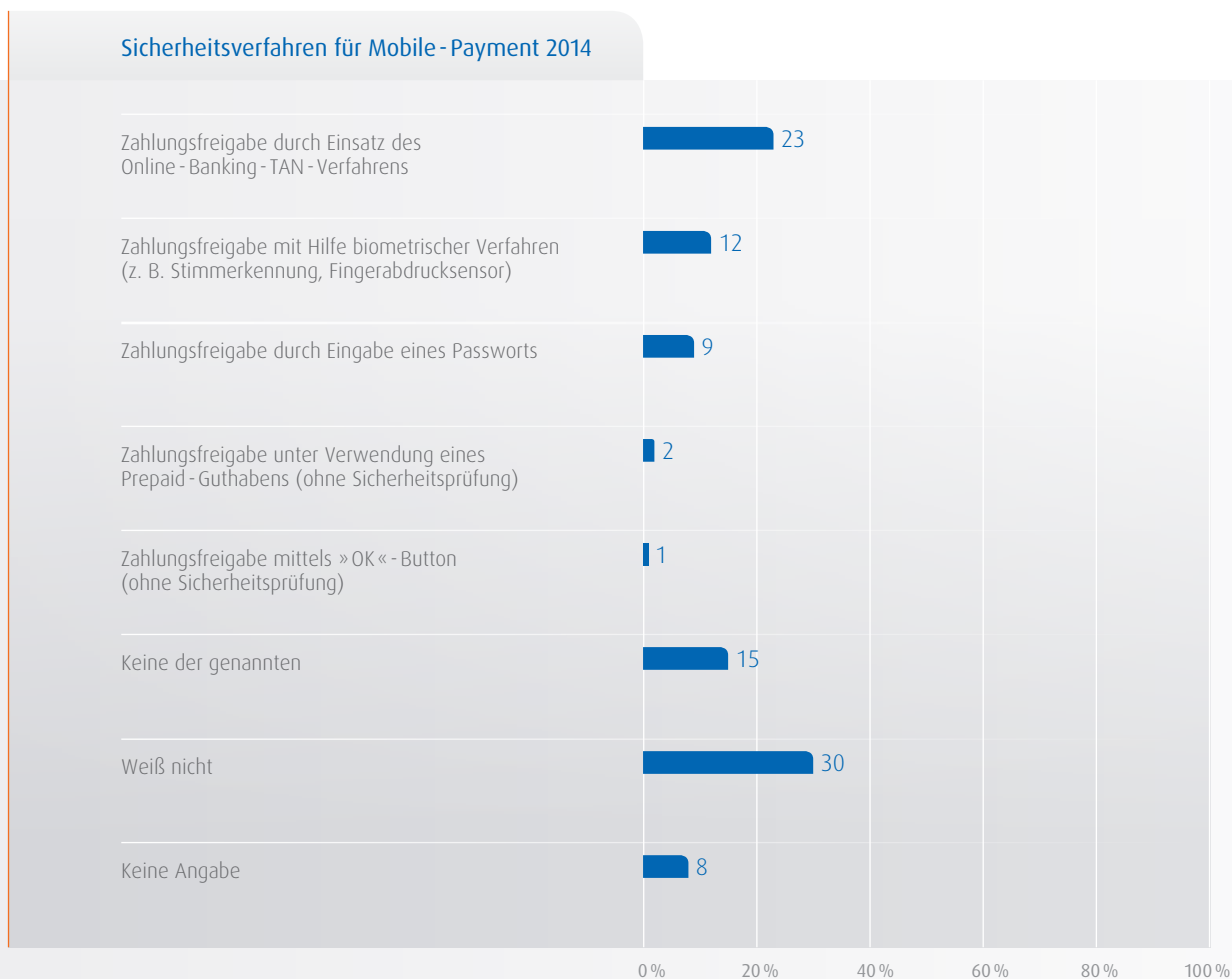
So sprechen 69 Prozent der Befragten den Geldinstituten als Intermediäre beim Mobile - Payment ihr Vertrauen aus. Allerdings ist dieser Anteil im Vergleich zu 2012 leicht gesunken. Es folgen Payment - Anbieter mit 48 Prozent und Kreditkartengesellschaften mit 42 Prozent.

Auf den unteren Plätzen rangieren Smartphone - Hersteller (17 Prozent), Internetdienstleister (13 Prozent) und Kartenleser - Anbieter.

3.3 Bevorzugte Sicherheitsverfahren für Mobile - Payment 2014



» Welches Sicherheitsverfahren bei Mobile - Payment würden Sie persönlich für die Freigabe der Zahlung bevorzugen? «



BASIS Alle Befragten 2014: n=1.001

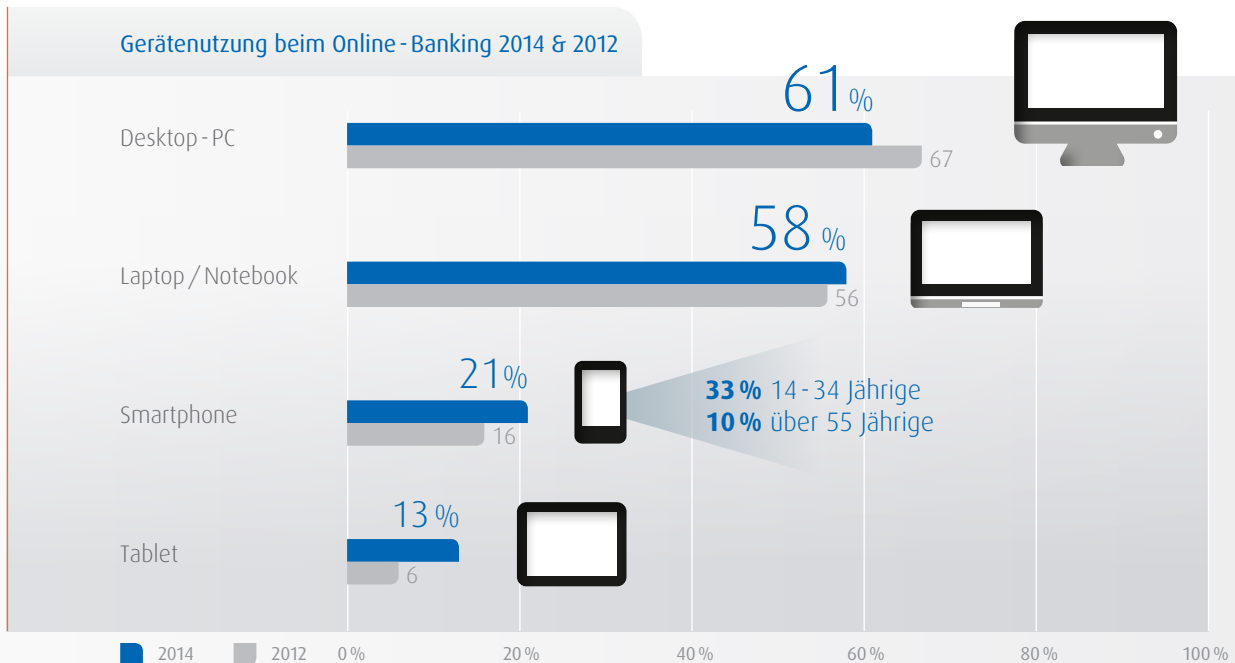
Bei der Frage nach der Sicherheit mobiler Bezahlssysteme scheint bei den Onlinern noch kein festes Meinungsbild zu existieren. So gibt jeder dritte Befragte an, nicht zu wissen, welches Sicherheitsverfahren er für die Freigabe einer Zahlung bevorzugen würde, und auch die genannten Maßnahmen finden insgesamt wenig Zustimmung.

Am häufigsten wird noch die Zahlungsfreigabe durch Einsatz des TAN-Verfahrens auf Basis des Online-Bankings genannt (23 Prozent), gefolgt von der Zahlungsfreigabe über biometrische Verfahren wie Stimmerkennung oder Fingerabdrucksensoren (12 Prozent).

Insgesamt zeigen die Ergebnisse deutlich, dass Mobile - Payment noch nicht im Bewusstsein der Internetbevölkerung angekommen ist. Dies ist auch vor dem Hintergrund zu sehen, dass bislang in Deutschland noch keine flächendeckenden und vor allem noch keine einheitlichen Systeme für das Mobile - Payment vorhanden sind – für die Konsumenten, aber vor allem für den Handel sind dies unabdingbare Voraussetzungen für die Akzeptanz eines neuen Bezahlverfahrens.

4 Gerätenutzung beim Online - Banking

» Über welche Endgeräte nutzen Sie derzeit Online - Banking? «

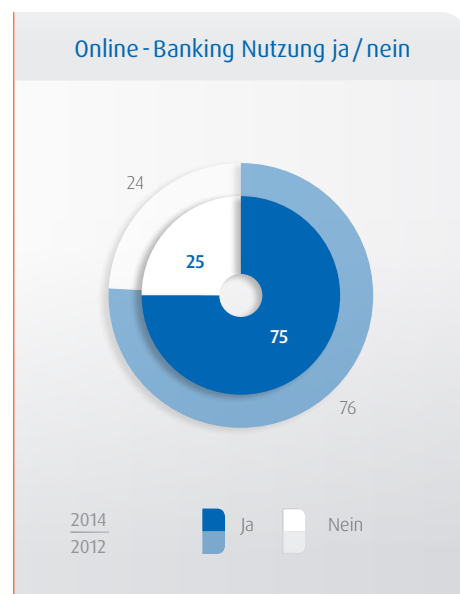


BASIS Online - Banking - Nutzer 2014: n=755 | Online - Banking - Nutzer 2012: n=757 | Online - Banking - Nutzer: 14-34 Jahre: n=266; 55 Jahre und älter: n=183

i Die Bedeutung mobiler Endgeräte steigt weiter an.

Beim Online-Banking fällt eine deutliche Verlagerung der verwendeten Geräte auf: weg vom stationären PC hin zu mobilen Endgeräten wie Smartphone oder Tablet. Erledigten 2012 noch 67 Prozent der Befragten ihre Bankgeschäfte über den Desktop-PC, so waren dies 2014 nur noch 61 Prozent. Zeitgleich haben Smartphones und Tablets an Bedeutung gewonnen. Über das Smartphone steigt die Nutzung von Online-Banking von 16 Prozent (2012) auf 21 Prozent (2014). Beim Tablet verdoppelt sich dieser Wert im gleichen Zeitraum von sechs auf 13 Prozent.

Die Nutzung mobiler Endgeräte wird stark von den jüngeren Onlinern zwischen 14 und 34 Jahren vorangetrieben. Ein Drittel in dieser Altersgruppe erledigt seine Bankgeschäfte über das Smartphone. Bei den über 55-Jährigen ist dieser Anteil deutlich niedriger – hier greift nur jeder Zehnte über dieses Medium auf sein Bankkonto zu.



BASIS Alle Befragten 2014: 1.001; 2012: n=2.002

Methodensteckbrief

Auswahl Interviews

Durchführung von 1.001 Interviews in Deutschland (2012: 1.002 Interviews).

Grundgesamtheit

Personen in Privathaushalten in Deutschland ab 14 Jahren, die das Internet regelmäßig privat nutzen.

Auswahl

Online - Panel; Daten gewichtet nach zentralen Merkmalen (Geschlecht, Alter und formale Bildung).

Repräsentative Erhebung

Auf die Grundgesamtheit übertragbar.

Erhebungsmethode

Durchführung als Onlinebefragung (computergestütztes Webinterview (CAWI), KW 15 bis KW 16 2014).

Definition Untergruppen

NUTZER	Personen, die den Dienst aktuell nutzen.
NUTZUNGSPLANER	Personen, die innerhalb der nächsten 12 Monate die Nutzung des Dienstes /des Endgeräts planen, es aktuell aber nicht nutzen.
ABLEHNER	Personen, die den Dienst nicht nutzen und die Nutzung nicht planen.

Impressum

Ansprechpartner

Fiducia IT AG
Thomas Nusche
Presse- und Öffentlichkeitsarbeit
Telefon 0721 / 40 04 44 70
thomas.nusche@fiducia.de

Initiative D21 e.V.
Lena-Sophie Müller
Geschäftsführerin
Telefon 030 / 526 87 22 52
lena-sophie.mueller@initiated21.de

Projektleitung und Redaktion

TNS Infratest GmbH
Linda Paul
Telefon 089 / 56 00 16 81
linda.paul@tns-infratest.com

TNS Infratest GmbH
Dr. Malthe Wolf
Telefon 089 / 56 00 11 33
malthe.wolf@tns-infratest.com

Herausgeber

Fiducia IT AG
www.fiducia.de

Initiative D21 e.V.
www.initiated21.de

Gestaltung und Produktion

Werkstatt für visuelle Kommunikation
Silke Wohner, Stefanie Brendle i. A.
www.werkstatt-trier.de

Druck

Schmekies, Medien & Druck
www.schmekies.de



Online-Banking 2014 Sicherheit zählt! von Initiative D21,
durchgeführt von TNS Infratest ist lizenziert unter einer
Creative Commons Namensnennung 4.0 International Lizenz.

Online - Banking 2014 – Sicherheit zählt!

Wünsche und Anforderungen an Bankgeschäfte im Internet

Als IT-Dienstleister für Volksbanken und Raiffeisenbanken entwickelt die Fiducia IT AG seit Jahren einfache, mobile und vor allem sichere Methoden für Bankgeschäfte im Internet. Zu den bekanntesten Lösungen zählen hier das Sicherheitsverfahren Sm@rtTAN plus oder die App »VR - Banking«, die aktuell auf rund 1,7 Millionen Smartphones und Tablets im Einsatz ist. Doch welche Anforderungen stellen eigentlich die Nutzer an das Online - Banking? Verändern sich diese Bedürfnisse im Zeitablauf? Und welche Rolle spielen dabei Vertrauen und Sicherheit? Antworten auf diese und weitere Fragen gibt die aktuelle Studie »Online - Banking 2014 – Sicherheit zählt!« aus der Reihe der Initiative -D21 -Studien. Sie erscheint bereits in sechster Auflage und spiegelt damit auch langfristige Trends und Entwicklungen wider.