Smartphone

Im Alltag

by Klaus-Dieter Göritz

Smartphone im Alltag 6Uh = 3 Termine

- **Grundlagen des Smartphones und Internets** (Umgangserfahrung erfassen)
- **Nutzerprofile bei Versicherungen, Banken einrichten und verwalten**
- **Nutzerprofile bei Online-Shops einrichten und verwalten**
- **Sicher online bestellen**
- **Mobile Bezahlmethoden sicher nutzen**

Grundlagen Smartphone, Internet

1. Das Smartphone verstehen:

- Betriebssystem (Android/iOS)- Sperrbildschirm, Startbildschirm, Apps, Benachrichtigungen.
- Geräteübersicht-Tasten, Anschlüsse, Display.
- Einstellungen und Personalisierung (WLAN, mobile Daten).

2. Grundlagen des Internets:

- Was ist das Internet? Browser und Suchmaschinen.
- Wichtigkeit einer stabilen Internetverbindung.
- Einführung in sicheres Surfen.

3. E-Mail-Adresse und App-Stores:

- Einrichtung und Verwaltung einer E-Mail-Adresse auf dem Smartphone.
- Herunterladen und Installieren von Apps aus dem Google Play Store / Apple App Store.

Sicher im Internet

Im digitalen Alltag ist Vorsicht geboten.

Technische Sicherheit

- **Updates regelmäßig installieren:** Halte dein Betriebssystem, Browser und Apps immer aktuell.
- **Virenschutz & Firewall aktivieren:** Nutze eine zuverlässige Antivirensoftware und aktiviere die Firewall.
- **Browser absichern:** Deaktiviere unnötige Erweiterungen und passe Datenschutz-Einstellungen an.

Passwortschutz

- **Starke Passwörter verwenden:** Nutze lange, komplexe Passwörter mit Zahlen, Sonderzeichen und Groß-/Kleinschreibung.
- **Zwei-Faktor-Authentifizierung (2FA):** Aktiviere sie überall, wo möglich – z. B. bei E-Mail, sozialen Netzwerken und Online-Banking.

Vorsicht bei E-Mails & Downloads

- **Phishing erkennen:** Misstraue E-Mails mit unbekannten Absendern, seltsamen Links oder Dateianhängen.
- **Downloads nur von vertrauenswürdigen Quellen:** Am besten direkt von der Herstellerseite.

Sicher im Internet

Sicher surfen

- **HTTPS beachten:** Achte auf das Schloss-Symbol in der Adressleiste – es zeigt eine verschlüsselte Verbindung.
- **Öffentliches WLAN meiden:** Nutze kein Online-Banking oder Shopping über offene Netzwerke. Wenn nötig, verwende ein VPN.

Datenschutz & Verhalten

- **Persönliche Daten sparsam teilen: Gib nur das Nötigste preis – besonders in sozialen Netzwerken.**
- **Datensicherung: Erstelle regelmäßig Backups auf externen Speichermedien.**

Empfehlung: Bürgerbroschüre des BSI

Nutzerprofile bei Versicherungen, Banken

Sinn und Zweck von Online-Portalen bei Versicherungen, Banken:

- Vorteile der digitalen Verwaltung (Dokumente bzw. Konten einsehen, Änderungen vornehmen, Schaden melden, Finanzen verwalten, Überweisungen tätigen, online bezahlen, mobil bezahlen).

Registrierung und Login bei Versicherungs-, Bankportalen:

- Schritt-für-Schritt-Anleitung zur Erstellung eines Nutzerprofils.
- Sicherer Umgang mit Zugangsdaten.

Wichtige Funktionen im Versicherungs-, Bankportal:

- Vertragsübersicht.
- Änderung von persönlichen Daten.
- Schadensmeldung und Statusabfrage.
- Kommunikation mit der Versicherung, Bank.

Datenschutz und Sicherheit:

- Was ist Datenschutz?
- Rechte der Nutzer.
- Umgang mit persönlichen Daten.

Online-Shops mit oder ohne Kundenprofil – was ist erlaubt und sinnvoll?

Mit Kundenprofil-Vorteile für Händler:

- **wiederkehrende Kundenbindung**
- **Personalisierte Angebote**
- **Vereinfachte Bestellprozesse**

Rechtliche Anforderungen:

- **Ein Kundenkonto bedeutet die Verarbeitung personenbezogener Daten (Name, Adresse, E-Mail etc.).**
- **Laut DSGVO ist eine freiwillige Einwilligung erforderlich.**
- **Die Einwilligung muss nachweisbar und widerrufbar sein.**

Online-Shops mit oder ohne Kundenprofil – was ist erlaubt und sinnvoll?

Ohne Kundenprofil: Gastbestellung

Vorteile für Kunden:

- **Schnellere Bestellung ohne Registrierung**
- **Weniger Datenverarbeitung**
- **Höhere Datenschutzfreundlichkeit**

Rechtliche Einschätzung:

- **Die Datenschutzkonferenz (DSK) empfiehlt grundsätzlich die Möglichkeit eines Gastzugangs.**
- **Das Prinzip der Datenminimierung (Art. 5 Abs. 1 c DSGVO) spricht für die Gastbestellung.**
- **Gerichte wie das LG Hamburg haben aber Ausnahmen zugelassen, z. B. bei Fachhändlern mit besonderen Anforderungen.**

Fazit: Was gilt für Shop-Betreiber?

- **Ein verpflichtendes Kundenkonto ist nicht grundsätzlich verboten, aber nur zulässig, wenn es für die Vertragserfüllung erforderlich ist.**
- **Ein Gastzugang sollte angeboten werden, sofern keine zwingenden Gründe dagegen sprechen.**
- **Händler müssen transparent darlegen, warum ein Kundenkonto notwendig ist – sonst drohen Abmahnungen.**
- **Wenn du selbst einen Shop betreibst oder planst, kann ich dir helfen, die passende Strategie zu entwickeln – rechtssicher und kundenfreundlich. Oder möchtest du wissen, welche bekannten Shops Gastbestellungen erlauben?**

Online-Shops mit oder ohne Kundenprofil – was ist erlaubt und sinnvoll?

Fazit: Was gilt für Shop-Betreiber?

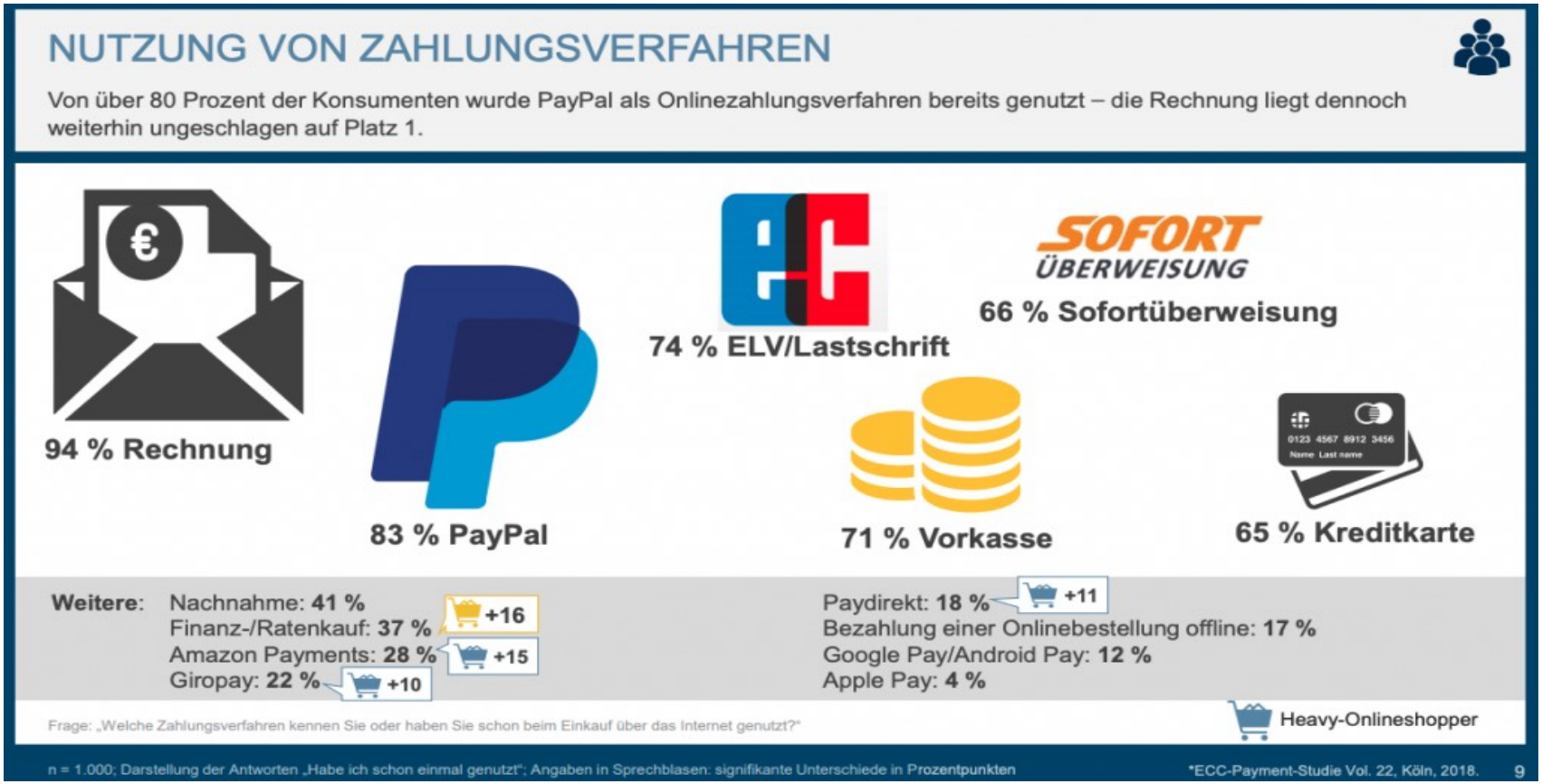
- Ein verpflichtendes Kundenkonto ist nicht grundsätzlich verboten, aber nur zulässig, wenn es für die Vertragserfüllung erforderlich ist.
- Ein Gastzugang sollte angeboten werden, sofern keine zwingenden Gründe dagegen sprechen.
- Händler müssen transparent darlegen, warum ein Kundenkonto notwendig ist – sonst drohen Abmahnungen.
- Wenn du selbst einen Shop betreibst oder planst, kann ich dir helfen, die passende Strategie zu entwickeln – rechtssicher und kundenfreundlich. Oder möchtest du wissen, welche bekannten Shops Gastbestellungen erlauben?

Rabattsysteme Großverkäufer

Rabattsysteme sind Strategien, die Unternehmen einsetzen, um den Verkauf ihrer Produkte oder Dienstleistungen zu fördern. Sie bieten Preisnachlässe, die entweder direkt beim Kauf oder später als Bonus oder Cashback gewährt werden.

- **Bonussysteme: Kunden sammeln Punkte (z. B. Payback, Miles & More), die später gegen Prämien oder Rabatte eingelöst werden können.**
- **Cashback-Systeme: Ein Teil des Kaufpreises wird nachträglich zurückerstattet.**
- **Automatische Rabatte: Direkt im Warenkorb oder an der Kasse abgezogen, oft bei Online-Shops.**
- **Eigene Apps: Verkaufseinrichtungen richten zunehmend mehr eigene Apps zur Kundenbindung über Angebotspreise ein.**

Bezahlsysteme im Internet



Online/Mobile Bezahlmethoden

Überblick über Bezahlmethoden:

- **Kreditkarte, PayPal, Lastschrift, Sofortüberweisung.**
- **Mobile Bezahldienste (Google Pay, Apple Pay, PayPal, Bankabhängige).**

Einrichten und Nutzen von PayPal/Kreditkarte auf dem Smartphone:

- **Schritt-für-Schritt-Anleitung zur Einrichtung.**
- **Sichere Anwendung im Online-Shop.**

Einführung in Google Pay/ Apple Pay/ PayPal :

- **Voraussetzungen und Einrichtung.**
- **Kontaktloses Bezahlen im Geschäft.**

Sicherheit bei mobilen Zahlungen:

- **Zwei-Faktor-Authentifizierung.**
- **Umgang mit sensiblen Daten.**
- **Was tun bei Verdacht auf Missbrauch?**

Mobile Bezahlsysteme

- **Mobiles Bezahlen mit dem Smartphone funktioniert ähnlich wie das kontaktlose Bezahlen mit einer NFC-fähigen Bankkarte. Sie benötigen dafür eine App, mit der der Bezahlprozess an der Kasse ausgeführt wird. Diese App müssen Sie vorher entweder mit Geld aufgeladen oder mit einem anderen Zahlungsmittel verbunden haben.**

Unbedingte Voraussetztungen

Schützen Sie Ihr Gerät: Sichern Sie den Zugang zu Ihrem Smartphone oder Tablet mit einem Entsperrcode und nutzen Sie, **wenn möglich, Fingerabdruck oder Gesichtserkennung** zur Entsperrung.

Schützen Sie Ihre Zugangsdaten: Egal, ob auf dem PC oder dem Smartphone: Das größte Risiko besteht darin, dass jemand per Phishing Ihre Zugangsdaten ausspioniert. Fragt jemand per E-Mail oder Telefon nach vertraulichen Daten, geben Sie diese nicht weiter. Eine Bank fragt ausschließlich bei der Nutzung des Onlinebankings nach Ihren Passwörtern oder TANs. Ein Tipp zum Schutz gegen Phishing: Ganz sicher mit der Seite der Bank verbunden sind Sie immer dann, wenn Sie die Internetadresse selbst richtig in die Adresszeile des Browsers eingetippt haben.

Und **sind Sie unsicher**, ob z.B. die E-Mail wirklich von Ihrer Bank stammt, **fragen Sie lieber erst einmal nach,** bevor Sie irgendwelche Daten preisgeben.
Woran Sie Phishing-Versuche erkennen, erfahren Sie hier.

Halten Sie Ihr Betriebssystem aktuell: Spielen Sie Betriebssystem Updates zeitnah ein und führen Sie auch App Updates zeitnah durch. Mit diesen Aktualisierungen werden regelmäßig Sicherheitslücken geschlossen, die durch Betrüger ausgenutzt werden könnten.

Ihre Apps laden Sie bitte **nur aus den offiziellen App Stores** herunter und nicht über dritte Quellen. Aber seien Sie bitte auch hier vorsichtig, denn es gibt betrügerische Apps, die einen Bankingtrojaner beinhalten. Deshalb achten Sie am Besten auf die korrekte Schreibweise des Herstellers (z.B. „Micosoft“ statt „Microsoft“) und auch bei einer geringen Anzahl an Downloads oder Bewertungen sollten Sie aufpassen. Vorsicht ist ebenfalls bei älteren Geräten geboten - diese erhalten oft keine Betriebssystem Updates mehr. Idealerweise informieren Sie sich beim Kauf eines Gerätes über die Dauer des Supports.

Nutzen Sie Benachrichtigungsfunktionen Ihrer Banking App: Viele Banken bieten die Möglichkeit sich z.B. per SMS über Kontoveränderungen informieren zu lassen.
Bei den jeweiligen Apps können Sie einstellen, ob und ab welcher Höhe wir Sie bei Umsätzen auf Ihrem Girokonto benachrichtigen. So haben Sie auch von unterwegs Ihre Finanzen immer im Blick und können sofort reagieren, falls ein Umsatz tatsächlich mal nicht passen sollte.

Seien Sie vorsichtig mit vertraulichen Daten im öffentlichen WLAN: Erledigen Sie Ihre Bankgeschäfte nicht über ein öffentliches WLAN, sondern nutzen Sie lieber die mobilen Daten Ihres Geräts oder das heimische WLAN.

NFC-Smartphones

- **NFC** (Near Field Communication) ist eine Nahfunktechnik, um Daten über kurze Strecken zu übertragen.
- Ein **Smartphone** mit **NFC**-Chip kann dazu genutzt werden, bargeldlos zu bezahlen.
- NFC-fähiges **Android-Smartphone** mit eingerichteter Gerätesperre

Bankeigene Apps

- Sparkasse (App: Mobiles Bezahlen), Deutsche Bank (Deutsche Bank Mobile) und Volksbanken/Raiffeisenbanken haben jeweils eigene Apps, die sich in das NFC-System des Android-Smartphones einklinken.
- Voraussetzung: teilweise sollte das Bankkonto auf „Onlinebanking“ eingerichtet sein

Fremde Apps

- Comdirect, Commerzbank, BW-Bank, N26 und bald DKB: Haben Sie ein Konto bei einer der Banken, die direkt mit **Google Pay** arbeiten, funktionieren Einrichtung und Bezahlung per Android-Smartphone etwas anders – und **in der Regel nur, wenn Sie auch eine Kreditkarte** bei einer dieser Banken haben

WERO

- **Das neue europäische Bezahlsystem**
- **digitaler Zahlungsdienst**, der im Juli 2024 gestartet wurde und von der *European Payments Initiative (EPI)* betrieben wird. Ziel ist es, **eine europäische Alternative** zu Diensten wie PayPal oder Venmo zu schaffen – schnell, sicher und direkt über dein Bankkonto.

Google-Pay

- Laden Sie sich zunächst die Google Pay-**App** herunter und fügen Sie eine **Kreditkarte** hinzu.
- Im Anschluss können Sie dann via NFC **bezahlen**.

Samsung Pay

- Wenn Sie ein Samsung-**Smartphone** besitzen, können Sie die App **Samsung Pay** verwenden.
- Nach dem Hinzufügen Ihrer **Bankkarte** können Sie direkt loslegen

Apple-Pay Deutsche Bank

Apple Pay auf dem **iPhone** verwendet zum Autorisieren der Zahlung einen Fingerabdruck (Touch-ID) oder die Gesichtserkennung Face-ID

Deutsche Bank Mobile“-App öffnen und klicken Sie auf die **Apple Pay** Anzeige. Bestellen Sie in der App eine kostenfreie **Deutsche Bank** Card Virtual (Mastercard Debitkarte). Nach spätestens zwei Arbeitstagen können Sie **Apple Pay** in der „**Deutsche Bank** Mobile“-App aktivieren.

Apple-Pay Sparkasse

- Ein Apple Pay-fähiges Endgerät (iPhone)
- Eine Apple-ID
- Die Sparkassen-App (aktuellste Version)
- Ein Sparkassen-Konto mit einer Sparkassen-Card (Debitkarte), einer Sparkassen-Kreditkarte oder einer Sparkassen-Karte Basis (Debitkarte)
- Eine Freischaltung für das **Online-Banking** (mit Nutzung des Elektronischen Postfachs und pushTAN- oder chipTAN-Verfahrens)

Datensicherheit, Datenschutz

Obwohl die Begriffe oft synonym verwendet werden, verfolgen Datensicherheit und Datenschutz unterschiedliche Ziele – und beide sind essenziell für den verantwortungsvollen Umgang mit Informationen.

Datensicherheit – Schutz aller Daten

Ziel: Verhindern von Datenverlust, Manipulation oder unbefugtem Zugriff.

Maßnahmen: Firewalls, Verschlüsselung, Zugriffskontrollen, Backup-Systeme und Notfallpläne

Gilt für: Alle Daten – auch technische, betriebliche oder anonymisierte Informationen.

Beispiel: Ein Unternehmen schützt seine Server mit Firewalls und speichert Daten verschlüsselt

– das ist Datensicherheit.

Datenschutz – Schutz personenbezogener Daten

Ziel: Sicherstellen, dass persönliche Daten nur rechtmäßig verarbeitet werden.

Rechtsgrundlage: DSGVO (EU-Datenschutz-Grundverordnung) und BDSG (Bundesdatenschutzgesetz)

Gilt für: Daten, die sich auf eine identifizierbare Person beziehen (z. B. Name, Adresse, IP-Adresse)

Beispiel: Ein Online-Shop fragt nur die Daten ab, die für die Bestellung nötig sind

– das ist Datenschutz.

Datensicherheit, Datenschutz

Der Unterschied auf den Punkt gebracht

- **Datenschutz regelt, *was* mit Daten geschehen darf.**
- **Datensicherheit sorgt dafür, *dass* dabei nichts schiefgeht.**

Datensicherung

- Konten
- Berechtigungen
- Wiederherstellung, Synchronisieren
- Externe Datenträger (Festplatte, USB Stick, Cloud)
- App Sicherheit

Cloud

- Google Drive
- Hersteller Cloud
- One Drive
- Spezielle Apps