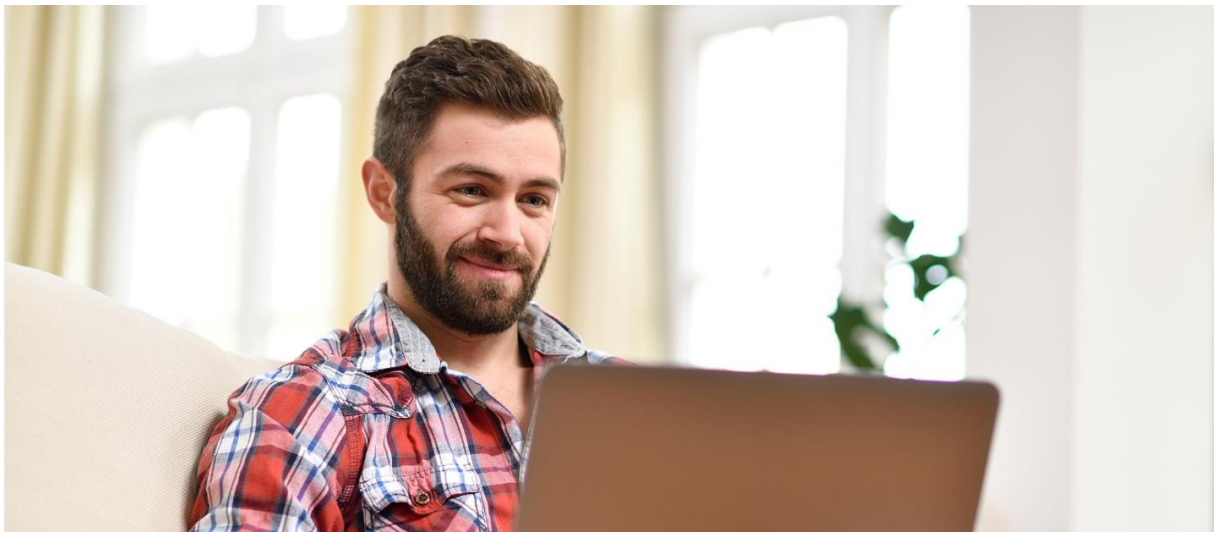


Sicher im Internet unterwegs: 7 einfache Tipps

Hacker, Betrüger und Viren: Im Netz lauern viele Gefahren. Seit Corona nehmen die Angriffe von Kriminellen sogar noch zu. Wer die Risiken und Einfallstore kennt, kann sich besser schützen. Wir geben euch 7 effektive und einfache Tipps für mehr Sicherheit im Netz.

1. Macht es Angreifern schwer: Komplett verhindern könnt ihr nicht, dass ihr ins Visier von Hackern gelangt. Das geht nämlich ganz schnell: Beim Surfen könnt ihr auf **Webseiten** stoßen, die geknackt und mit einem Schadcode versehen sind. Dann fangt ihr euch mit dem Öffnen dieser Internetseite einen **Schädling** ein. Auch durch das Herunterladen von Daten - beispielsweise PDF-Downloads wie Checklisten oder kostenlose Programme wie PC-Spiele - kann ein Schadprogramm auf euren Rechner kommen. Deshalb gilt zunächst grundsätzlich:

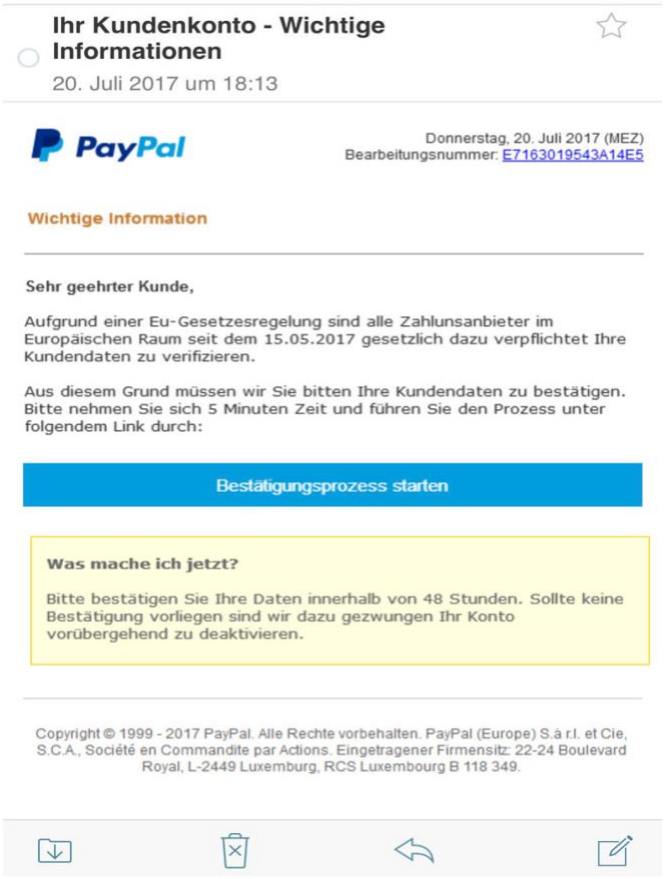
- Euer Betriebssystem sollte immer auf dem aktuellen Stand sein! Dabei hilft euch die **automatische Updatefunktion**
- Installiert dringend eine **Antiviren-Software** mit automatischem Update zur Erkennung neuer Schädlinge

Darüber hinaus gilt im Speziellen:

- Ladet Apps oder Programme nur aus seriösen Quellen, z. B. dem App-Store herunter

2. Achtung vor Schädlingen via E-Mail: Für Kriminelle ist euer E-Mail-Posteingang ein beliebtes Einfallstor. Sie ahmen renommierte Unternehmen so präzise nach, dass ihr die Masche schwer erkennen könnt. Inhalte der Mails sind meist dringende Hinweise zur Sicherheit eures Kontos oder der **Zahlungsverzug** einer angeblichen Rechnung, manchmal auch Rabattaktionen und Ähnliches. Die Täter versuchen über Termine, Androhung von Kontoschließungen und Ähnlichem euch unter Druck zu setzen. Ihr Ziel ist, euch zum Öffnen eines Links oder der Eingabe eurer Daten zur Kontoverifizierung zu bringen. Allein dieses sehr **druckvolle Vorgehen** ist also ein **erster Hinweis** für euch.

Das Öffnen einer verseuchten **E-Mail** ist meist nicht schädlich, denn die **Schadsoftware** versteckt sich im Anhang oder Link. Sobald ihr diesen anklickt, habt ihr die Schädlinge auf eurem Computer. Cyberkriminelle können dann Daten und Passwörter abschöpfen.


Ihr Kundenkonto - Wichtige Informationen

20. Juli 2017 um 18:13

PayPal

Donnerstag, 20. Juli 2017 (MEZ)
Bearbeitungsnummer: E7163019543A14E5

Wichtige Information

Sehr geehrter Kunde,

Aufgrund einer Eu-Gesetzesregelung sind alle Zahlunsanbieter im Europäischen Raum seit dem 15.05.2017 gesetzlich dazu verpflichtet Ihre Kundendaten zu verifizieren.

Aus diesem Grund müssen wir Sie bitten Ihre Kundendaten zu bestätigen. Bitte nehmen Sie sich 5 Minuten Zeit und führen Sie den Prozess unter folgendem Link durch:

Bestätigungsprozess starten

Was mache ich jetzt?

Bitte bestätigen Sie Ihre Daten innerhalb von 48 Stunden. Sollte keine Bestätigung vorliegen sind wir dazu gezwungen Ihr Konto vorübergehend zu deaktivieren.

Copyright © 1999 - 2017 PayPal. Alle Rechte vorbehalten. PayPal (Europe) S.à r.l. et Cie, S.C.A., Société en Commandite par Actions. Eingetragener Firmensitz: 22-24 Boulevard Royal, L-2449 Luxemburg, RCS Luxembourg B 118 349.

Beispiel für eine schädliche E-Mail

So beugt ihr vor:

- Seid immer wachsam bei **E-Mail-Anlagen**!
- Öffnet weder diese noch klickt auf **Links** von **unbekannten Absendern**
- Dies gilt ganz besonders, wenn sie versuchen, euch unter **Druck** zu setzen
- Schützt euren privaten Account: Arbeitet über mindestens **zwei E-Mail Accounts**: Einen für wichtige und persönliche Angelegenheiten und einen für die Registrierung von Newslettern, zum Shoppen und allgemeinen Internetdiensten So haltet ihr euren privaten Account weitgehend von Spam frei.

3. Gefälschte Links erkennen:

- Gefälschte Links in Mails oder Nachrichten führen häufig auf Seiten, die die Schadsoftware direkt auf eurem Rechner installieren
- Bei Rabattaktionen landet ihr auf einem Fake-Shop - ihr bestellt, bezahlt, aber erhaltet keine Ware
- Mails, die vermeintlich von der eigenen Bank kommen, sind eine beliebte Masche. Da wird nicht nur euer Onlinebanking-Passwort ausgespäht, sondern via erschlichener TANs das gesamte Konto geplündert.

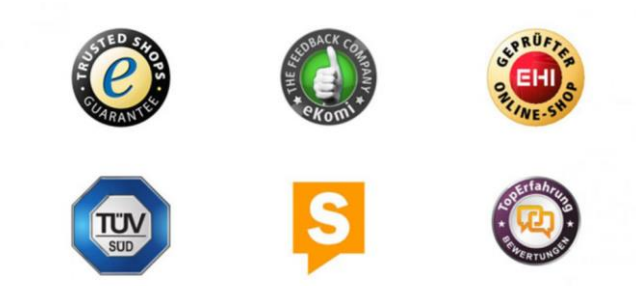
Das sind die Hinweise für euch:

- Merkwürdige oft auch kleine **Abweichungen** im Link selbst, zum Beispiel amazom.com oder amazn.com statt amazon.com. Die Phisher setzen darauf, dass ihr nur oberflächlich schaut und schnell auf den Link klickt.

- Eine prima Hilfe ist, mit der Maus über den Link zu fahren - nicht klicken-, dann seht ihr die tatsächliche Linkadresse, zu der die Verbindung aufgebaut würde, wenn ihr daraufklickt.
- Wichtig: Klickt erst dann, wenn ihr ganz sicher seid, dass der Link stimmt.
- Beginnt ein Link zu einem Online-Shop mit http:// statt https://, so ist schon das ein erster Hinweis! Alle **seriösen Online-Shops** bieten eine sichere und damit verschlüsselte **https:// Verbindung** an. Dies garantiert euch einen sicheren Austausch der eingegebenen Daten.
- Aber: http-Seiten sind nicht generell riskant. Führt eine http-Adresse nicht zu einem Online-Shop, sondern z.B. auf einen Blog, ist das unproblematisch.
- Auch darf das www. in der Adresse fehlen. Es gibt nämlich tatsächlich Seiten mit und ohne www.
- Also: Achtet darauf, dass ihr euch nur auf Internetseiten **einloggt**, die eine https.//-Verbindung anbieten UND
- Prüft die wirkliche Linkadresse, bevor ihr daraufklickt

4. Sicher online Shoppen: Onlineshopping hat gerade jetzt viele Vorteile: man meidet Menschenansammlungen, es ist bequem, weil man jederzeit und überall shoppen kann, ohne Stau, Parkplatzsuche und Warteschlangen. Auf der Suche nach dem günstigsten Produkt oder kostenlosem Versand stößt man auch oft auf unbekannte Seiten. Bevor ihr euch dort mit euren persönlichen Daten anmeldet und bestellt, solltet ihr einen unbekannten Shop sehr genau unter die Lupe nehmen: Unser **Quickcheck**:

- Hat der Online-Shop ein Gütesiegel, das ihn als sicheren Shop auszeichnet?
- Sind Versandkosten, Rücksendekosten und mögliche Zusatzkosten transparent?
- Bietet der Händler verschiedene Zahlungsmöglichkeiten an?
- Sind Angaben zum Widerrufsrecht, Rückgaberecht und der Kaufpreisrückerstattung verfügbar?
- Gibt der Händler seine vollständigen Kontakt- und Anschriftdaten an?
- Sind Informationen zum Datenschutz und Datensicherheit verfügbar?
- Ist das Impressum vorhanden und vollständig?
- Prüft, ob es im Netz Bewertungen über diesen Online-Shop gibt



Diese Siegel sind ein Zeichen für einen geprüften Shop

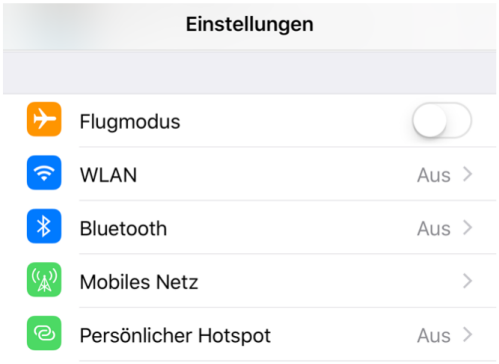
5. Vorsicht bei offenem WLAN: Ein öffentliches WLAN **ohne Passwort** ist unsicher. Alles, was ihr hierüber austauscht, kann von anderen mitgelesen werden.
Das geht:

- Nutzt im öffentlichen WLAN **nur allgemeine Internetdienste**
- Verzichtet auf alle Anwendungen oder Seiten, die ein Login benötigen und wo Kontodaten hinterlegt sind. Online-Banking sollte absolut tabu sein. Nutzt dafür besser das Funknetz des Handys, sollte es nicht warten können.

Aber auch freie WLANS **mit Passwort** sind nicht sicher, zumal häufig dasselbe Passwort allen Surfern zur Verfügung gestellt wird. Wenn ihr nicht sicher seid, fragt, wie das gehandhabt wird. Im Übrigen bieten viele Smartphones einen Hotspot an. Wollt ihr also mit dem Rechner ins Netz, baut ihr über euer Smartphone eine Verbindung zum Rechner auf.

Und noch ein wichtiger Aspekt: Oft sind WLAN und **Bluetooth** dauerhaft aktiviert, weil dies bequem ist. Schaltet immer Funktionen ab, die ihr gerade nicht unbedingt braucht. Bluetooth braucht ihr nur, wenn ihr euch mit einem anderen Gerät koppeln wollt. Das könnt ihr schnell und einfach über die Einstellungen eures Mobilgeräts machen. Weiterer Vorteil: Ihr schont damit auch den Akku.

- Aktiviert WLAN und Bluetooth nur, wenn ihr diese Verbindungen braucht
- Verzichtet bei öffentlichen WLAN-Verbindungen auf den Aufruf von Anwendungen oder Seiten, die ein Login benötigen



Aktivieren Sie WLAN und Bluetooth nur, wenn Sie diese Verbindungen benötigen

6. Eigenes WLAN sichern: Gerade wer im Haushalt mehrere Personen oder Endgeräte hat, schätzt auch zu Hause ein komfortables WLAN. Das gibt es zu beachten, damit es sicher ist:

- Das WLAN ist meist mit dem **Produktnamen** vorbelegt. Bitte ändert diesen, denn er informiert einen potenziellen Angreifer über Schwachstellen.
- Verwendet **lange und komplexe Passwörter**. Das ist beim ersten Einloggen zwar umständlich, gibt euch aber einen Vorsprung an Sicherheit. Und: Die meisten Geräte bieten an, sich das Passwort "zu merken". Für einen Angreifer ist jedes zusätzliche Zeichen eine weitere Hürde.
- So manche neuen Router haben voreingestellt, dass sie automatisch ein freies WLAN anbieten. Prüft also die Werkseinstellungen eures Routers und deaktiviert diese Funktion. Sonst nutzen Nachbarn oder Passanten euren Router, um ins Netz zu gehen.

7. Richtiger Umgang mit der Cloud: Cloud Lösungen sind wirklich komfortabel. Über sie habt ihr von überall auf der Welt und von jedem Endgerät aus Zugriff auf eure Daten und ein Backup dazu. Google bietet Google Drive an, Amazon den Amazon Drive, bei Apple gibt's die iCloud und bei Microsoft das OneDrive. Somit haben Computerbesitzer zusätzlichen freien Speicherplatz - in den Basisversionen sogar meist kostenfrei.

Nachteil: **Cloudserver** stehen meist in USA oder Kontinenten außerhalb der EU. Damit gelten für diese Dienste nicht die strengen europäischen Datenschutzregelungen. Speichert deshalb dort keine Daten, die dem Datenschutz unterliegen. Allgemeine und **nicht personenbezogene** oder **vertrauliche** Daten wie Musik oder E-Bücher sind unkritisch. Für alle anderen Daten sucht euch einen Anbieter aus der EU. Sie sind an die Datenschutzregelungen der EU gebunden und haben weitere **Sicherheitseinstellungen** wie beispielsweise eine vollständige Verschlüsselung eurer Daten in der Cloud.

Noch ein letzter Hinweis: Die Daten in der Cloud aufzubewahren ist keine **Alternative** zum **klassischen Backup** auf Festplatte oder USB-Stick.

Sparkassen Versicherung