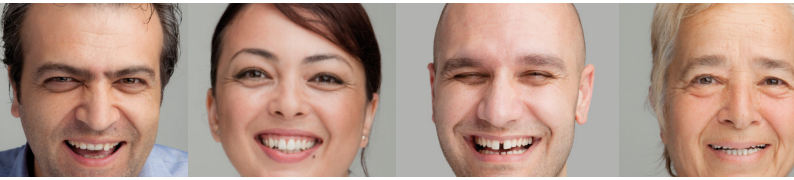
Bundesministerium
für Wirtschaft
und Technologie

WIRTSCHAFT.
WACHSTUM.
WOHLSTAND.

Kennen Sie die schon? Grundregeln für eine sichere Identität im Netz

Eine gemeinsame Empfehlung der Mitglieder der IT-Gipfel Arbeitsgruppe 4 „Vertrauen, Datenschutz und Sicherheit im Internet“

Nationaler IT Gipfel
München 2011



Grundregeln für eine sichere Identität im Netz

Eine sichere Identität im Netz beruht auf einigen allgemeinen Grundsätzen, die immer wieder zum Tragen kommen, egal ob man sich in sozialen Netzwerken bewegt oder ob man Online-Banking betreibt. Deshalb empfehlen wir, (immer) folgende Grundregeln zu beachten:

1. Sichern Sie Ihren Rechner durch **Firewall, Virenscanner, Anti-Spywareprogramm** und **Filtersoftware**. Führen Sie regelmäßig Sicherheitsupdates für diese Programme durch.

2. Benutzen Sie ein sogenanntes **Starkes Passwort**, das heißt, wählen Sie keine Namen von Freunden, Haustieren oder Ähnlichem, am besten benutzen Sie gar kein „normales“ Wort. Das Passwort sollte mindestens acht Zeichen lang sein, wechseln Sie zwischen Groß- und Kleinschreibung, Sonderzeichen und Ziffern. Um sich ein abstraktes Passwort zu merken, denken Sie sich eine Eselsbrücke bzw. einen Satz aus wie zum Beispiel: Wie soll ich mir 5 Passwörter merken? Das Passwort lautet in diesem Fall: Wsim5Pm? Wichtig ist, dass Sie Ihr Passwort nie weitergeben und nicht notieren. Außerdem sollten Sie es regelmäßig wechseln, am besten alle sechs Monate.

3. Verwenden Sie **verschiedene Benutzerprofile** (Accounts) für unterschiedliche Angebote im Netz. So sollten Sie nicht den gleichen Benutzernamen (Mit-

gliedsnamen, Nickname ...) bzw. das gleiche Passwort bei Ihrem E-Mail-Konto, Ihrem sozialen Netzwerk und/oder Ihrem Online-Bankkonto verwenden. Wählen Sie einen Benutzernamen, der nicht zu viel über Sie verrät, wie dies beispielsweise bei Petra1990 der Fall ist. Überprüfen Sie die **Einstellungen** Ihrer unterschiedlichen Benutzerkonten: Was wird gespeichert? Was ist auch für andere sichtbar?
So kann durch eine falsche Voreinstellung zum Beispiel Ihr Merkzettel für weitere Einkäufe auf einer Plattform öffentlich einsehbar sein. Achten Sie darauf, dass Ihre Einstellungen so gespeichert sind, dass Ihr Profil nicht über eine Suchmaschine gefunden werden kann, wenn Sie dies nicht wollen.

4. Legen Sie auf Ihrem Rechner **verschiedene Benutzerkonten** an, von denen nur eines mit Administratorenrechten ausgestattet ist. Nutzen Sie zum allgemeinen Surfen, Spielen usw. dann das Benutzerkonto ohne Administratorenrechte.

5. Stellen Sie sicher, dass Kommunikationsschnittstellen wie WLAN, Bluetooth usw. an Ihren **mobilen Geräten** abgestellt sind, wenn sie nicht genutzt werden. Grundsätzlich sollten mobile Geräte mit einem Passwort geschützt sein.

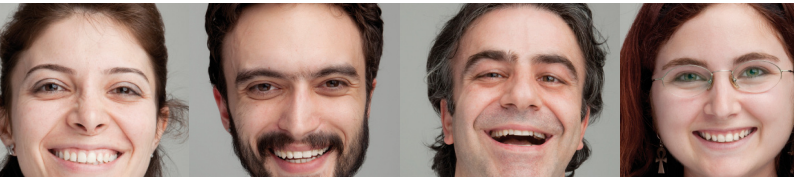
6. Seien Sie vorsichtig bei **Downloads** im Internet und folgen Sie nicht einfach jedem Weblink, der Ihnen zugeschickt wird und beispielsweise einen Gewinn oder Ähnliches verspricht.

7. Achten Sie bei **E-Mails** darauf, ob Sie den Absender wirklich kennen. Lassen Sie sich bei Ihren E-Mails den Dateityp anzeigen, so können Sie verdächtige Dateien wie beispielsweise .com, .exe, .bat, .do*, .xl*, .scr oder .vbs erkennen und nicht öffnen.

8. Geben Sie keine **sensiblen Daten** an, wie PIN, TAN oder Kennwörter, wenn Sie per E-Mail dazu aufgefordert werden. Seriöse Anbieter werden dies in der Regel nicht verlangen. Beim Online-Bezahlen sollten Sie darauf achten, dass es sich um eine **verschlüsselte Verbindung** handelt. Dies können Sie an den Buchstaben „https“ in der Adresszeile und einem Schloss- oder Schlüsselsymbol erkennen. Viele sicher verschlüsselte Seiten haben die Adresszeile grün hinterlegt.

9. Seien Sie vorsichtig, wenn Sie Daten von fremden USB-Sticks, CDs oder DVDs herunterladen. Überprüfen Sie die Daten erst durch ein **Virenschutzprogramm**. Dies gilt auch für „leere“ Memory Sticks, die Sie als Werbegeschenk erhalten haben.

10. Wenn Sie **öffentliches WLAN** nutzen und beispielsweise in einem Café über dessen WLAN-Verbindung ins Internet gehen, übertragen Sie dort keine sensiblen Daten. Das heißt, tätigen Sie dort nicht Ihre Bankgeschäfte, kaufen Sie nicht online ein und übermitteln Sie nicht Ihre Kreditkartennummer.



11. Nutzen Sie, wo es möglich ist, den neuen **elektronischen Personalausweis (nPa)** oder eine vergleichbare sichere Identität.

12. **Löschen** Sie **Accounts** von Diensten, die Sie endgültig nicht mehr verwenden wollen. Sperren Sie Ihren Account, wenn Sie den Eindruck haben, dass Dritte sich Zugang dazu verschafft haben.

13. **Datensparsamkeit:** Geben Sie im Netz nur so viel von sich preis, wie für den jeweiligen Dienst erforderlich ist. Dies gilt insbesondere für soziale Netzwerke. Bedenken Sie: **Das Internet vergisst nichts!** Überprüfen Sie regelmäßig mit einer Suchmaschine, welche Informationen über Sie im Netz verfügbar sind.

14. Achten Sie auf die geltende **Datenschutzerklärung** des jeweiligen Anbieters, bevor Sie sich registrieren. Fragen Sie im Zweifelsfall nach, was mit Ihren Daten geschieht.

15. Sie haben das **Recht** an **Ihren eigenen Bildern!** Wenn jemand unerlaubt Bilder von Ihnen ins Netz gestellt hat, können Sie verlangen, dass er diese löscht. Das gilt auch umgekehrt: Sie sollten auch keine Fotos veröffentlichen, ohne vorher zu fragen.

Wir über uns

Die Grundregeln für eine sichere Identität im Netz sind eine Empfehlung der Mitglieder der IT-Gipfel Arbeitsgruppe 4 „Vertrauen, Datenschutz und Sicherheit im Internet“. Der Nationale IT-Gipfel ist ein vom Bundesministerium für Wirtschaft und Technologie ausgerichteter und seit 2006 jährlich stattfindender Kongress, der Konzepte entwickelt, wie die Bundesrepublik Deutschland als IT-Standort gestärkt werden kann. Unter der Federführung des Bundesministeriums des Innern (BMI) und des Unternehmens Giesecke & Devrient werden konkrete Projekte zu den Themenbereichen „Sichere Identitäten im Internet“ und „Cloud Computing“ erarbeitet.

AG 4-Mitglieder

- 1&1 Internet AG
- BITKOM e. V.
- Bundesamt für Sicherheit in der Informationstechnik
- Bundesbeauftragter für den Datenschutz
- Bundesministerium des Innern
- Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz
- Bundesverband Deutscher Banken e. V.
- Deutsche Post AG
- Deutsche Telekom AG
- Deutschland sicher im Netz e. V.
- eBay GmbH
- eco – Verband der deutschen Internetwirtschaft e. V.
- Fraunhofer Research Institution AISEC
- Giesecke & Devrient GmbH
- Hewlett-Packard GmbH
- LVM Versicherung
- Microsoft Deutschland GmbH
- secunet Security Networks AG
- Verbraucherzentrale Bundesverband e. V.
- Vodafone D2 GmbH
- VZ Netzwerke Ltd

Kontakt

Deutschland sicher im Netz e. V.
Albrechtstraße 10 a, 10117 Berlin
Tel. +49 (0) 30 27576-310
Fax +49 (0) 30 27576-51310
info@sicher-im-netz.de
www.sicher-im-netz.de

Schirmherschaft

Bundesministerium des Innern

DEUTSCHLAND DsiN.de SICHER IM NETZ

Herausgeber
Bundesministerium
für Wirtschaft und
Technologie (BMWi)
Öffentlichkeitsarbeit
10115 Berlin
www.bmwi.de

Stand
November 2011

Druck
Kriechbaumer, Taufkirchen

Gestaltung und Produktion
PRpetuum GmbH, München

Bildnachweis
iStock