Online-Sicherheit

Sicher unterwegs im Internet mit Computer, Notebook und Co.

d·bug GmbH
Sollner Str. 71a
81479 München

Fon 0 89 / 790 10 33
Fax 0 89 / 790 42 25

Mail info@d-bug.de
Web www.d-bug.de

Montag - Freitag jeweils 09:00 - 18:00 Uhr

d·bug GmbH

Ihr kompetenter und zuverlässiger Partner in allen Fragen rund um die Bereiche IT Consulting, Business Lösungen und professionelle IT Services in München seit 1999.

Grundsätzliches zur Online-Sicherheit

Ist man früher nur bei Bedarf „online gegangen" ist der Rechner, das Notebook, Tablet oder Smartphone durch Flatrate und Co. heute praktisch „always online" und somit auch permanent Bedrohungen aus dem Internet ausgesetzt.

Welche Bedrohungen lauern online?

Die größte Bedrohung lauert dabei im Identitäts- und Datendiebstahl durch Dritte. Ihre persönlichen Benutzernamen, E-Mail Adressen, Kennwörter, Konto- und Kreditkartendaten lassen sich hervorragend zu Geld machen oder direkt missbrauchen. Auch persönliche Dokumente, die auf einem Rechner gespeichert sind lassen sich effektiv für sog. „Social Engineering" Angriffe nutzen um an diese Daten zu gelangen.

Dabei wird versucht, den Rechner mit Schädlingen zu infizieren, die diese Daten abschöpfen, der Benutzer wird durch Phishing-Mails auf betrügerische Webseiten gelockt oder die Daten werden durch Einbrüche bei Online-Dienstleistern und Webseiten erbeutet.

Wie kann man sich sinnvoll schützen?

Betrachten Sie grundsätzlich jede Information, die Sie im Internet speichern oder eingeben oder von dort erhalten als unsicher. Geben Sie bei Anmeldungen zu Diensten oder Webseiten nur die unbedingt erforderlichen Daten an und verwenden Sie für jeden Dienst und jede Seite unterschiedliche, sichere Passwörter.

Online-Sicherheit

Sicherer Umgang mit Internet, E-Mail und Co.

Nutzen Sie Verschlüsselung wo immer es geht und speichern Sie keine Zugangsdaten lokal auf Ihrem Rechner ab - zumindest nicht unverschlüsselt!

Schützen Sie Ihren Rechner vor Missbrauch durch eine Anti-Virus-Software und halten Sie das System und die gesamte installierte Software stets aktuell. Installieren Sie keine Software aus unbekannten Quellen und auch nur die Software, die Sie wirklich zum Arbeiten benötigen.

Öffnen Sie keine Anhänge aus E-Mails oder klicken Sie auf Links in E-Mails, die Sie nicht selbst angefordert oder erwartet haben. Absender lassen sich leicht fälschen und Links können auf gefälschte Webseiten führen.

Für Online-Banking sollten Sie nur eine spezielle Banking-Software und ein sicheres Authentifizierungsverfahren wie z.B. einen externen HBCI-Kartenleser verwenden.

Versenden Sie keine sensiblen Daten über öffentliche WLAN-Zugänge am Flughafen, in Bars, Hotels oder an fremden Rechnern.

Zusammenfassung der Tipps im Überblick

- stets unterschiedliche und sichere Passwörter für jeden Dienst/jede Webseite verwenden
- immer nur absolut notwendige Daten angeben
- Verschlüsselung nutzen wo immer möglich
- eigenen Rechner durch regelmäßige Software-Updates und Anti-Viren-Software schützen
- nur absolut notwendige Software aus sicheren Quellen installieren und nutzen
- nur erwartete Anhänge und Links in E-Mails öffnen
- Online-Banking nur mit spezieller Banking-Software und sicherer Authentifizierung vom eigenen Rechner
- keine sensiblen Daten über öffentliche WLANs oder fremde Rechner versenden

Fazit: Denken Sie nach bevor Sie etwas anklicken! Fragen Sie lieber vorher jemanden, der sich damit auskennt - gerne auch die d·bug GmbH! Wir helfen Ihnen gerne!