ZVEI: Die Elektroindustrie

Digitale Gesellschaft:
Wie bewege ich mich sicher im Netz?

Internet über alle möglichen Endgeräte wie Smartphone, Tablet, Smart-TV – das bringt viele Vorteile und erleichtert den Alltag. Etwa bei der Kommunikation mit Freunden in sozialen Netzwerken oder durch Online-Shopping bequem von zu Hause aus. Bei vielen dieser Vorgänge spielen persönliche Daten eine Rolle.

Klar ist, dass die Nutzung des Internets grundsätzlich mit einer gewissen Transparenz der persönlichen Daten einhergeht, allerdings gibt es auch Schutzmechanismen, etwa durch die Einrichtung von Passwörtern sowie den sorgsamen Umgang mit den persönlichen Daten. Die richtige Wahl der Passwörter spielt eine wesentliche Rolle, um einem Missbrauch der eigenen Daten durch Dritte vorzubeugen.

1. Tipps für ein sicheres Passwort

Zunächst sollte bei der Wahl des Passworts kein real existierendes Wort benutzt werden.

Das beste Passwort besteht aus einer zufälligen Kombination aus allen möglichen Zeichen und Sonderzeichen der Tastatur wie z. B. **Ia?li7849!$**

Kombinationen aus Buchstaben und Zahlen, wie z. B. IFA2015, sind grundsätzlich etwas sicherer, aber immer noch sehr leicht zu knacken.

Folgende Tipps für sichere Passwörter ermöglichen einen sehr großen Schutz:

- **Wort zufällig wählen**
- **Passwort regelmäßig ändern**
- **Passwort nicht auf der Festplatte speichern**
- **möglichst viele unterschiedliche Zeichen sowie Sonderzeichen verwenden**
- **auf Namen als Passwörter verzichten**

Mit einer Eselsbrücke kann man sich selbst die schwierigsten Passwortkombinationen leicht einprägen. Man sollte sich zunächst einen Satz ausdenken, der dann verkürzt in Buchstaben und Zahlen dargestellt werden kann: **„#Die IFA 2015 bringt viel Neues!"** wäre **#dI15bvN!**

2. Umgang mit sozialen Netzwerken

Beim Umgang mit sozialen Netzwerken wie Facebook etc. sollte Folgendes beachtet werden:

- **Persönliche Informationen nur zurückhaltend preisgeben**
  Es sollte vorab kritisch überprüft werden, was öffentlich zugänglich gemacht werden soll und bedacht werden, dass z. B. Arbeitgeber bei Bewerbungen oft im Internet, gerade auch bei sozialen Netzwerken recherchieren.

- **Privatsphäre-Einstellungen prüfen und individuell anpassen**
  In den Optionen kann oftmals eine eingeschränkte Sichtbarkeit von Bildern und Informationen einstellen, d. h. nur bestimmte Personen (etwa Freunde aus dem Netzwerk) können die entsprechenden Bilder und Informationen sehen.

Kontakt:
Carine Lea Chardon
Digitale Gesellschaft
Telefon: +49 69 6302-260
E-Mail: chardon@zvei.org

Version: 1.0 zur IFA 2015

Stand: September 2015

Autorin:
Alexa Sophia Christ
Referentin Medienpolitik

- **Nur Kontakte bestätigen, die auch im realen Leben bekannt sind**
  Kriminelle sammeln `Freunde`, um Informationen zu bekommen, z. B. wann jemand im Urlaub ist und somit das Haus leer steht.

- **Links nicht wahllos anklicken**
  Soziale Netzwerke werden verstärkt dazu genutzt, um Phishing zu betreiben, d. h. Passwörter abzugreifen. Die Zieladresse könnte eine gefälschte Startseite eines sozialen Netzwerks sein. Wenn dort dann Benutzername und Kennwort eingegeben werden, werden die Daten direkt an die Betrüger weitergeleitet.

- **Nie die eigene Telefonnummer im Profil hinterlegen oder herausgegeben**
  Aktuell sind z. B. Betrüger bei Facebook unterwegs, die Profile hacken oder nachbauen, und die Telefonnummer erfragen, um diese dann zum Bezahlen von Interneteinkäufen zu benutzen, bei denen sich der Käufer mit seiner Telefonnummer identifizieren muss.

3. Schutz vor Spam-Mails

Unerwünschte Werbe-E-Mails, auch Spam genannt, sind nicht nur störend, sondern können auch gefährlich werden. Viele E-Mails mit Dateianhang enthalten Schadprogramme wie Viren oder Trojaner. Grundsätzlich empfiehlt es sich, den Anhang einer E-Mail vor dem Öffnen mittels eines Virenscanners, der sich stets auf dem neuesten Stand befinden sollte, zu überprüfen.

Einige Viren können aber bereits durch das bloße Aufrufen einer infizierten E-Mail gestartet werden. Um dies zu verhindern, sollte in den Einstellungen des E-Mail-Programms die Funktion „Java Script erlauben“ deaktiviert werden.

Nachrichten, die auf den ersten Blick z. B. durch die Betreffzeile als Spam zu identifizieren sind, sollten sofort gelöscht und keinesfalls beantwortet werden. Zudem sollte eine geeignete Anti-Spam-Software installiert werden.

Da Software immer intelligenter wird, sind viele Anti-Spam-Filter in der Lage, fast ohne Zutun des Benutzers zu lernen, bei welchen E-Mails es sich um Spam handelt und welche seriös sind. Entgeht eine Nachricht dem Spam-Filter einmal, kann sie vom Benutzer ganz einfach entsprechend markiert werden Auf diese Weise passen sich die Filter an die neue Bedrohung an.

4. Was muss ich beachten wenn ich mit meinem Smartphone im Urlaub bin? [1]

Vor der Abreise:

- Gerätenummer (15-stellig), SIM-Code und Provider-Hotline notieren
- Sicherheitssoftware installieren, z. B. mit Virenschutz, Sperrfunktion
- Kosten für mobiles Internet bzw. Datenroaming im Ausland abklären
- Sicherungskopien aller Daten anlegen
- PIN- und SIM-Code gut merken

Am Urlaubsort:

- unverschlüsselte WLAN-Verbindungen meiden
- WLAN-Sicherheitscode vom Hotel geben lassen
- vertrauliche Daten nur über verschlüsselte Verbindungen senden (https://…)

Bei Verlust:

- Smartphone anrufen, vielleicht meldet sich der Finder
- Ortung, Sperrung, Datenfernlöschung
- Passwörter für soziale Netzwerke, E-Mail-Programme und Online-Shops ändern
- Diebstahl bei der Polizei melden

[1] Quelle: https://www.sicher-im-netz.de/downloads/endlich-urlaub

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Lyoner Straße 9 • 60528 Frankfurt am Main • Telefon: +49 69 6302-0 • Fax:+49 69 6302-317 • E-Mail: zvei@zvei.org • www.zvei.org