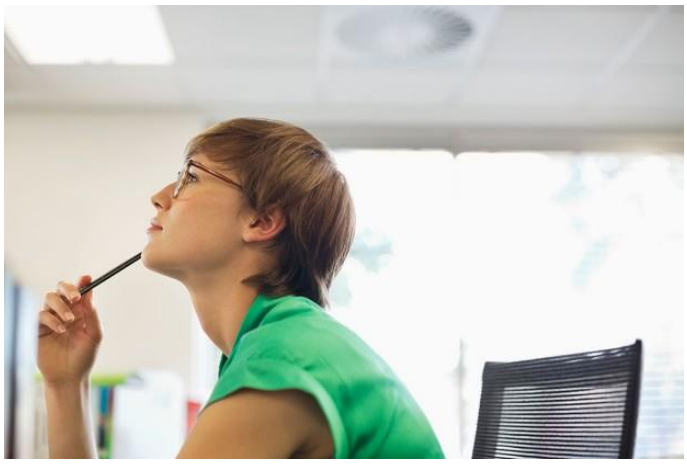
IT - News im Februar 2015

Komfort und Sicherheit beim Umgang mit Log-ins



Sichere Log-ins setzen unter anderem viele sichere Passwörter voraus: Um sich die merken zu können, ist der gute alte Zettel nicht die schlechteste Methode.

Mail-Konten, Netzwerke, Shops und Internetnutzer gehen in der Fülle von Konten unter. Alle Log-in-Daten individuell und sicher zu gestalten, ist eine Herausforderung. **Sich alle zu merken, fast unmöglich.**

Viele Browser wollen es den Nutzern leicht machen. Sie speichern auf Wunsch Benutzernamen und Passwörter für Internetseiten und -dienste ab. Grundsätzlich ist das kein Problem. Allerdings darf man dann nicht vergessen, regelmässig Updates zu installieren und den Virenschutz aktuell zu halten. *«**Wenn man da ein bisschen nachlässig ist, kann es passieren, dass sich ein Trojaner installiert und die Benutzerdaten abgreift**».*

Skeptisch sollte man sein, wenn Log-in-Daten nicht auf der Festplatte, sondern auf Servern abgelegt werden. Das mag sicher sein, ist aber nicht wirklich zu überprüfen. ***«Die Verwaltung unterschiedlicher komplexer Passwörter durch den Browser ist aber immer noch deutlich sicherer, als wenn man immer das gleiche Passwort verwendet.»***

1. Der beste Schutz gegen Trojaner: Papier und Stift

- Empfehlung ganz grundsätzlich auf **Papier mit Stift.** Der einfachste Weg ist, sich die Passwörter ganz klassisch aufzuschreiben. Da kann kein Trojaner drauf zugreifen. Den Zettel darf man dann natürlich nicht verlieren.
- Nutzer können die Sicherheit weiter erhöhen: Grundsätzlich gilt, dass ein Log-in-Token, also die Kombination aus User-Name und Passwort, umso schwerer zu erraten ist, je weniger Informationen über den Nutzer sie enthalten. **Idealerweise entspricht der Benutzername also nicht dem Eigennamen.**
- Unabdingbar sind sichere Passwörter, insbesondere beim zentralen E-Mail-Konto. Denn bei fast jedem Internet-Dienst lässt sich das Passwort per E-Mail zurücksetzen. Der erste wichtige Schritt ist daher, das E-Mail-Passwort besonders lang und kompliziert zu machen und es an keiner anderen Stelle zu verwenden.

2. Im Trend aber riskant sind Single-Sign-on Dienste

- Mit sogenannten Single-Sign-on-Diensten versuchen inzwischen auch viele Internetkonzerne, das Jonglieren mit Benutzerdaten überflüssig zu machen. Ein Beispiel: Man kann sich etwa mit seinem Facebook-Account **auch beim** Mail-Provider, beim Streaming-Anbieter und vielen weiteren Diensten anmelden.

- Doch Experten warnen: Das Problem bei Single-Sign-on-Diensten ist, dass man diesen Diensten sowie dem dort verwendeten Passwort auch den Zugang zu den verknüpften Accounts ermöglicht - also das eigene Risiko erhöht. Es hat nur einen geringen Bequemlichkeitsvorteil für den Nutzer, aber ein erhöhtes Risiko im Fall des Passwortverlustes daher eher zu Software-Lösungen greifen: Eine gute Kombination aus Sicherheit und Komfort bieten sogenannte Passwortspeicher. Die legen alle Log-ins verschlüsselt ab - und der Nutzer muss sich nur ein Masterpasswort merken.
- Ein relativ hohes Sicherheitsniveau bietet die sogenannte Zwei-Faktor-Authentifizierung. Bei diesem Verfahren muss der Nutzer seine Identität neben dem Log-in noch über ein zweites Merkmal nachweisen - etwa per Einweg-Code, den er aufs Handy geschickt bekommt. Viele kennen das Prinzip vom Online-Banking.

3. Zwei Faktoren oder ein zusätzlicher Stick bieten die grösstmögliche Sicherheit

- Damit es dort sicher angewendet werden kann, ist aber Voraussetzung, dass er sich nicht mit dem gleichen Smartphone auf der Bankseite einloggt, mit dem er auch den TAN-Code empfängt. Hat nämlich ein Angreifer den PC des Nutzers mit einer Spähsoftware infiziert, so kann er auf diesem gleichzeitig Login-Daten und den TAN-Code abgreifen, die reguläre Transaktion des Nutzers abbrechen und mit den erbeuteten Daten eine eigene Transaktion in die Wege leiten.
- Zwei Faktoren zum Einloggen bieten inzwischen zumindest auch die grossen Online-Dienste wie Apple, Google, Facebook oder Dropbox an. Das ständige Eintippen der Codes ist einigen Nutzern aber auf Dauer zu lästig. Deshalb lässt sich die Authentifizierung meist so einstellen, dass man den Zusatzcode nicht jedes Mal eingeben muss, sondern nur dann, wenn man sich von einem anderen Rechner einloggt.
- Zudem gibt es ein Verfahren, bei dem man sich mit einem kleinen USB-Stick zusätzlich legitimiert. Die Entwicklung wird von der FIDO-Allianz vorangetrieben, in der sich viele Anbieter zusammengeschlossen haben. Seit kurzem akzeptiert Google USB-Sticks, die den offenen Standard FIDO Universal 2nd Factor (U2F) unterstützen, als zweites Identifikationsmerkmal. So ein Stick kostet nur wenige Franken, funktioniert bei Google aber vorerst nur in Desktop-Chrome-Browsern.

Quelle: Bluewin

Glossar: Weitere Artikel zum Thema "Passwörter"

Die schlechtesten Passwörter

Schwache Passwörter stellen ein hohes Risiko für die Privatsphäre und die Datensicherheit dar. Dennoch werden ausgerechnet die schlechtesten Passwörter am häufigsten benutzt. Wir zeigen Ihnen, auf welche Passwörter Sie lieber verzichten sollten und wie Sie Ihre Online-Zugänge besser schützen können.

Dass man «123456» oder «Passwort» nicht als Passwörter für einen Online-Zugang verwenden sollte, dürfte mittlerweile jedem Internetnutzer klar sein. Solche Codes sind sehr einfach zu knacken und schützen deshalb Logins für E-Mail, E-Shops oder alle Webseiten nicht ausreichend. Und trotzdem werden genau solche Passwörter am häufigsten verwendet. Dies geht aus Untersuchungen von gestohlenen Zugangsdaten im Internet hervor. In unserer Bildergalerie zeigen wir, was ein sicheres Passwort ausmacht.

1. Die häufigsten Passwörter sind die schlechtesten

- Schwache Passwort-Datensätze wurden etwa nach dem Diebstahl grosser Mengen von Zugangsdaten für Adobe- und Hotmail-Konten analysiert. Die häufigsten Passwörter sind auch die schlechtesten. Das IT-Sicherheitsunternehmen SplashData veröffentlicht jährlich eine Hitliste der meistgefundenen Passwörter. In der Häufigkeitsliste ganz oben stehen auch die Passwörter «qwerty» (die ersten sechs Tasten oben links auf der englischen Tastatur), «abc123» und «111111».
- **Diese Passwörter lagen letztes Jahr in den Top Ten von SplashData.**
    1. 123456
    2. password
    3. 12345678
    4. qwerty
    5. abc123
    6. 123456789
    7. 111111
    8. 1234567
    9. iloveyou
    10. adobe123
- Die Erhebung stammt zwar bereits aus dem Jahre 2013. Da sich die Auswertungen in den letzten Jahren nicht stark unterscheiden, dürften auch dieses Jahr ähnliche Passwörter die Rangliste anführen. Eine entsprechende Top 10 wird aber frühestens im nächsten Jahr veröffentlicht. Allerdings dürfte das Passwort auf dem 10. Platz bei einer allfälligen neuen Rangliste herausfallen: «adobe123» kam im letzten Jahr in die Top Ten, weil damals eine grosse Menge an gestohlenen Zugangsdaten für Adobe-Accounts in die Analyse-Daten eingeflossen **sin**d.

2. Anspruchsvolle Passwörter wählen

- Obwohl in einschlägigen Ratgebern und von Sicherheitsfirmen immer wieder kolportiert wird, dass man sich ein schwieriges Passwort ausdenken soll und dieses möglichst nur einmal verwenden soll, halten sich anscheinend viele Internetnutzer nicht an solche Ratschläge. Deshalb hier ein paar Tipps, wie man sich ein sicheres Passwort zulegt.
- Die Grafik verdeutlicht, wie schnell ein unsicheres Passwort gehackt werden kann. Weitere Informationen dazu bietet der Datenschutz Blog von The Safe Shop. Wir zeigen Ihnen 7 Regeln, die es für ein sicheres Passwort unbedingt zu befolgen gilt.

Ein Passwort sollte:

1. **aus** Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen.
2. kein bekannter Begriff sein, also in keinem Lexikon oder sonst einer Begriffsliste vorkommen.
3. **keine** Namen, Firmenbezeichnungen oder andere Informationen beinhalten.
4. **keine** Umlaute oder andere sprachenspezifische Zeichen enthalten, damit es sich auch auf Tastaturen in anderen Ländern eintippen lässt.
5. **mindestens** 8 Zeichen, besser noch 12 oder mehr Zeichen lang sein.
6. **jeweils** nur einmal verwendet werden.
7. **komplex**, aber trotzdem gut zu merken sein. Ein beliebter Kniff dafür sind Abkürzungen, beziehungsweise die Aneinanderreihung von Anfangsbuchstaben von längeren Sätzen. Beispiel: Isfjm34LeaP! («Ich setze für jedes meiner 34 Logins ein anderes Passwort!»).

Quelle: Bluewin