Office on the Spot
Support Service Solutions
Iris Weinig

Georg-Ohm-Str. 14, 65232 Taunusstein
+49 / 6128 / 8606151
+49 / 176 / 54060303
info@office-on-the-spot.de
www.Office-on-the-Spot.de
www.facebook.com/officeonthespot

18. April 2014

Tipps für sichere Passwörter

Mit Passwörtern schützen Sie Ihre Daten im Internet und auf Ihrem PC – aber schlechte Zugangsdaten sind in etwa so nützlich wie ein Tresor aus Holz. Ich habe Ihnen Tipps zusammengestellt, um Ihnen bei der Passwortwahl zu helfen.

Das Internet funktioniert nicht ohne Passwörter. Es fängt an beim E-Mail-Postfach, geht über Amazon und andere große Versandhäuser und endet beim Zugang für das Online-Banking. Um bei den unterschiedlichen Diensten abgesichert zu sein, sollten Sie für jeden Anbieter ein anderes Passwort benutzen – aber wer kann sich schon derart viele Passwörter merken? Noch dazu sollten diese möglichst kompliziert und damit noch schwieriger einzuprägen sein.

Ihre E-Mail-Adresse ist ALLES!

Schützen Sie Ihr E-Mail-Postfach ganz besonders gut, denn darüber lassen sich viele Passwörter für andere Seiten ergaunern. Wenn es Ihr E-Mail-Anbieter zulässt, nutzen Sie eine Zwei-Wege-Authentifizierung, so dass Sie sowohl eine Bestätigung per Passwort als auch per Handy (z. B. http://web.de/magazine/schlagwort/handy) oder Festnetztelefon benötigen, um sich anzumelden. Sicherer geht es heutzutage nicht – für alle anderen Fälle empfehlen sich die http://web.de/magazine/schlagwort/tipps für mehr Sicherheit im Internet.

Facebook-Schutz

Angesichts der mitunter wichtigen persönlichen Daten, die bei Facebook gespeichert sind, ist ein gutes Passwort auch hier sehr wichtig.

Problematisch ist die Funktion „Anmelden mit Facebook“, die mittlerweile auf vielen Webseiten zur Verfügung steht. Hier sparen Sie sich zwar das Anlegen neuer Accounts, sollte jedoch jemand ihr Facebook-Passwort stehlen, hat er damit auch Zugriff auf andere Dienste. Für einen guten Schutz gehen Sie auf „Kontoeinstellungen / Sicherheit / Anmeldebestätigung (Mitte)“. Sobald Sie diese Bestätigung aktivieren, führt Sie ein Assistent durch die Funktion. Sie bekommen damit in Zukunft immer einen Code auf Ihr Handy gesendet, sobald sich jemand von einem unbekannten Gerät bei Facebook anmeldet.

Online-Banking mit TAN-Generator

Papierlisten sind nicht wirklich sicher, ein Zufallsgenerator arbeitet besser. Möglicherweise bekommen Si einen solchen TAN-Generator kostenlos von Ihrer Bank gestellt. Ist das nicht der Fall, können Sie ihn sich für etwas 15 Euro kaufen. Danach müssen Sie Ihrer Bank dies natürlich mitteilen. Beim Online-Banking werden Sie damit in Zukunft einen individuellen Code auf Ihrem Monitor sehen, über den der TAN-Generator eine zufallsgenerierte TAN erstellt.

Android-Manager für Passwörter

Wenn Sie für allerlei Logins unterschiedliche Passwörter nutzen, vergessen Sie einige davon möglicherweise wieder. Helfen kann die App „Keepassdroid“ für Smartphones oder Tablets mit Android. Damit können Sie alle Passwörter abspeichern und anschließend mit einem sicheren Kennwort schützen, so dass nur Sie Zugriff darauf erhalten. Die Verschlüsselung ist praktisch nicht zu knacken. Aber: Sie müssen natürlich ein sehr sicheres Passwort wählen, denn sonst ist auch der sicherste Safe schnell geöffnet.

Passwörter mit Android sichern

Um Ihre Passwörter auch über längere Zeit – wie etwa nach einem Reset des Smartphones – zu sichern, können Sie diese ins Internet auslagern. Bei Android ab Version 4.0 gehen Sie über „Einstellungen / Sichern & Zurücksetzen / Meine Daten sichern“. Dort richten Sie das sogenannte Sicherheitskonto ein und aktivieren die automatische Wiederherstellung. Die Funktion ist allerdings mit Vorsicht zu genießen, da unklar ist, welche Daten Google tatsächlich speichert. Für einen einfacheren Umgang mit Website-Logins ist dieser Vorgang jedoch ebenso empfehlenswert wie sicher.

Passwörter online für den PC sichern

Lastpass ist ein Onlinedienst, der sich Ihre Passwörter merkt und diese auf Wunsch bei ausgewählten Webseiten einträgt. Praktisch daran ist, dass Sie so natürlich auch komplexe Passwörter wählen können, da Sie sich diese nicht mehr merken müssen. Ein einziges Passwort müssen Sie sich aber trotzdem einprägen: das Master-Passwort für *Lastpass*. Die Erweiterung steht für alle modernen Browser zur Verfügung – allerdings ist nicht ganz klar, was passieren wird, wenn der Dienst in einigen Monaten abgeschaltet wird.

Warum nicht gleich einen Satz?

Ein Satz ist mitunter einfacher zu merken als ein langes Passwort – insbesondere, wenn dieses Kennwort *oW9#QxtiH* oder ähnlich lautet. Ein Sprichwort hingegen – „Früher war alles besser“ – kann einfach um eine Zahl und ein Sonderzeichen erweitert werden („Früher war alles besser 92§“), um maximalen Schutz zu bieten. Das Sprichwort selbst ist natürlich sehr einfach zu merken, so dass Sie sicher nur noch die Zahl und das Sonderzeichen einprägen müssen.

Abkürzungen mit Bedeutung

Die erwähnten Sätze können Sie auch mittels Ihrer Anfangsbuchstaben abkürzen. „Fwab92§“ als Beispiel ist ebenfalls sicher, aber deutlich kürzer. Nutzen Sie dabei jedoch stets Sonderzeichen, die international funktionieren. Deutsche Umlaute (ä, ö, ü, ß) eignen sich also nicht unbedingt, da Sie diese schlichtweg nicht an allen Computern eingeben können.

Verzichten Sie im Zweifelsfall auf Komfort

Alle modernen Browser verfügen inzwischen auch über automatische Passwortspeicher. Leider sind aber gerade ältere Versionen dieser Browser anfällig für Viren, die genau diese Passwörter auslesen können. Außerdem existieren auch völlig legale Tools – wie der „*Internet Password Breaker*“ von *Elcomsoft* -, die dieselbe Funktion erfüllen. Sie dürfen diese Möglichkeit also nutzen, aber achten Sie darauf, Ihren Browser stets auf dem neuesten Stand zu halten.

Und noch ein paar kleine Tipps zur leichteren Handhabung:

- **Keine leicht zu erratenden Begriffe** (Name, Geburtsdatum, Hobby, Haustier etc.) wählen
- **Mindestens 10 Zeichen** verwenden, inkl. Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
- **Kein vorhandenes Passwort** mehrfach verwenden, z. B. für mehrere Benutzerkonten!
- Prägen Sie sich einen **Satz** ein und verwenden Sie davon alle ersten Buchstaben sowie alle Ziffern und Sonderzeichen als Passwort – z. B. so:
  Beispielsatz: "Vor 3 Jahren, es war am 5. Mai, fuhr ich nach Thailand."
  Passwort: "V3J,ewa5.M,finT."