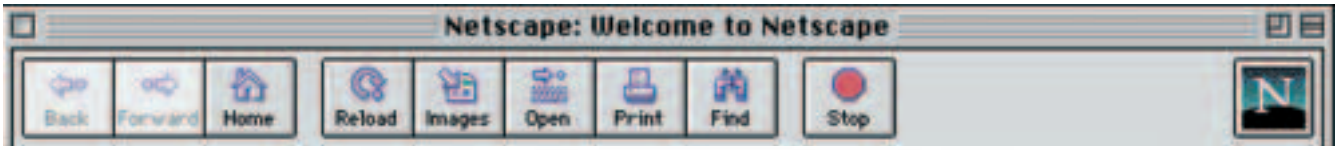


Internet

Access denied, login failed, forgotten your password?

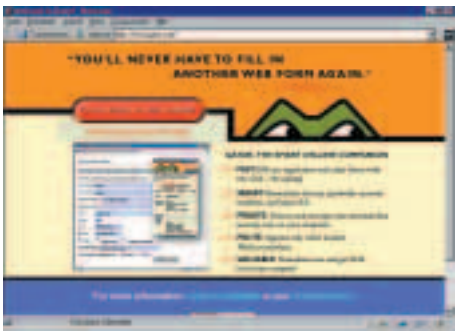
Im Dschungel der Passwörter

Internet ist immer mehr auch Business. Kaum erstaunlich, dass sich eine wachsende Zahl von Websites in irgendeiner Art mit Passwörtern und Zugriffscodes abschirmen, um bei Inanspruchnahme eines Dienstes oder eines Downloads am Ende absahnen zu können. So kommt es auch, dass User schnell einmal ein Dutzend oder mehr verschiedene Codes auswendig lernen sollten. Nach einer langen Surfnacht oder in der Sommerhitze kann es schon einmal vorkommen, dass man da steht wie der sprichwörtliche Esel am Berg: Login failed... Acces denied... please repeat your user name and password... Nach dem dritten oder vierten missglückten Anlauf haut es manch einem den Deckel ab. Immerhin ist dies weniger peinlich als am Bancomat oder am EC-Terminal ganze Schlangen von Ungeduldigen hinter sich zu wissen. Mehr oder weniger intensive Flüche, die meist mit «sh..» [englisch] oder «Sch...» [deutsch] beginnen, sind in der Regel nicht auszuschliessen. Um die kleinen grauen Zellen anzuregen, gibt es die Lösung, viel Fisch zu essen. Um des Dschungels Herr zu werden und als Vorsichtsmassnahme gegen Nervenzusammenbrüche gibt es aber auch einige ganz einfache Regeln. Hier meine Tipps.

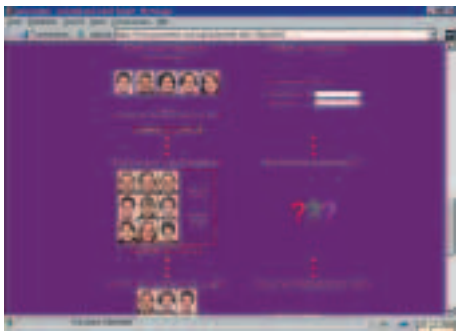
Thomas Vauthier
th.vauthier@bluewin.ch

Methodisch bleiben

Geschlossene Foren, Abonnemente, Mailing-Lists, Downloads, Online-Einkäufe... Auch der zurückhaltendste Internetbenutzer kommt schnell einmal auf ein Dutzend oder mehr Adressen, die nur mit Passwort oder Code zugänglich sind. Am einfachsten wäre es natürlich, einen universalen Schlüssel zu haben. Gut, damit gäbe es ein Risiko, dass im Fall der Entdeckung ein Unbefugter Zutritt zu all Ihren bestgehüteten Sites hätte. Trotzdem, aus Angst zu vergessen, wählen viele aber zu einfache Passwörter. Dies hat zwei Nachteile: Auf gewissen Websites, bei denen mehrere Millionen von Benutzern angemeldet sind, sind viele Möglichkeiten schon vergeben. In solchen Fällen online zu hirnen und andere einfache Kombinationen zu finden, ist oft ganz schön schwierig und ist (selbst erlebt!) auch so stressig, dass man in der Verzweiflung dann irgendein Passwort wählt, Hauptsache, es wird akzeptiert. Eben dieses hat man aber spätestens beim nächsten Einloggen mit Sicherheit schon wieder vergessen, weil in der Aufregung nirgends notiert.



Zweiter Nachteil: Allzu offensichtliche Passwörter sind leicht zu knacken. Wenn der Code genügend subtil gewählt wäre, z.B. aus einem Mix von Ziffern, Buchstaben und Sonderzeichen (sicher aber nicht Ihr Vorname oder die Telefonnummer der Praxis), wäre das Risiko relativ gering – wesentlich kleiner jedenfalls als bei Bank-Codes, die aus höchstens 6 Zahlen zusammengesetzt sein dürfen! Leider ist die Realität auf dem Net nicht so einfach. Verschiedene Anbieter, verschiedene Vorgaben bei den zulässigen Zeichen. Meistens sind Sonderzeichen nicht erlaubt (z.B. Akzente, #, §, ~ etc.), die schon eine gewisse Schutzwirkung hätten – manchmal nicht einmal einfache Interpunktionszeichen.



Zweitens: Ehrlich währt am längsten

Wenn bei der Anmeldung für ein Abonnement, eine Zugangsberechtigung oder anderen Online-Dienst Ihre E-Mail-Adresse verlangt wird, versuchen Sie nicht zu tricksen. Erstens wird bei den schnellen Servern die Adresse sofort nachgeprüft und wenn – ob durch Fehler oder Absicht – sie falsch ist, wird die Transaktion nicht gelingen. Geben Sie also eine gültige Mail-Adresse an. Dies lohnt sich auch aus einem anderen Grund: Manche Anbieter bestätigen Ihnen mehr oder weniger umgehend die Anmeldung per E-Mail. Um die Dienstleistung definitiv zu aktivieren, müssen Sie danach noch einmal quittieren. Und last but not least: Sollten Sie trotz aller Vorsichtsmassnahmen je Ihr Passwort verlieren, können Sie dieses meist per E-Mail wieder anfordern, unter der Voraussetzung, dass Sie dem Webmaster einen vereinbarten Sicherheitsschlüssel (z.B. Ihr Geburtsdatum) als Notidentifizierung mitgeteilt haben. Wenn Sie aber bei der E-Mail-Adresse geschummelt haben (was zwar a priori nützlich sein kann, um sich gegen Werbung, Junk-Mail oder Spams zu schützen), wird Ihnen niemand im entscheidenden Moment eine Rettungsboje zuwerfen...

Drittens: Ein nützlicher Trick

Wie bei EC-Codes oder ähnlichem sollte man Passwörter & Co. nicht an einem allzu offensichtlichen Ort notieren. Ein empfehlenswerter Kniff: Sie wählen in Ihrem Archiv ein Word-File, an das Sie sich besonders gut erinnern können, das aber nicht mehr in Gebrauch ist (darum ist es ja auch archiviert...) Mit der rechten Maustaste auf *Eigenschaften* klicken, dann auf Datei-Info. Darin steht unter *Kommentar* ein kleines Textfeld, das Sie beliebig nutzen können. James Bond lässt grüssen!

Und bevor ich es vergesse: Zwei empfehlenswerte Adressen

PassCenter (www.passcenter.com) ist ideal für eine visuelle Verwaltung von Zugangscodes. Vergessliche und Dyslektiker werden gleichermassen Freude haben, denn hier kann man alle verschiedenen Zugänge nicht mit Hilfe von Passwörtern, sondern von Passgesichtern verwalten. Nachteil: PassCenter funktioniert nur auf Englisch und jeder Zugang zu den so geschützten Sites muss via PassCenter erfolgen.

Gator (www.gator.com) verwaltet auf Ihrer Festplatte ein Plug-in, in dem die immer wiederkehrenden Angaben, die für Logins nötig sind, gespeichert sind. Wenn nun auf irgendeinem Internet-Dienst ein Formular oder Fragebogen auftaucht, erwacht der hilfreiche Alli*Gator* und füllt dies sicher, zuverlässig und automatisch aus.

Fortsetzung folgt...