

Kennworte erstellen

Posträuber Ronald Briggs und seine Komplizen überfielen 1963 noch den Zug Glasgow-London um ans große Geld zu gelangen. Moderne Gangster beschaffen sich heute vom Schreibtisch aus ihr Geld.

Wer den Schaden hat ...

Das Passwort ist der direkte Weg zu Ihren persönlichen Daten und damit zu Ihrem Geld. Mit Ihrem Passwort kann der Dieb Ihr Geld stehlen, indem er Ihre Kreditkarten benutzt und Ihr Konto leer räumt. Der Raub Ihres Passwortes ist Identitätsdiebstahl. In den Firmen drohen ebenso große Gefahren. Datenspione können direkt von zu Hause aus mit Ihrem Kennwort die Daten der Firma einsehen und schon allein mit diesem Wissen großen Schaden anrichten.

Was tun?

Nennen Sie niemandem Ihr Passwort!

Sie sollten **nie** vertrauliche Anmeldeinformationen, Benutzernamen, Passwörter und ähnliche Daten per E-Mail, Fax oder am Telefon herausgeben! Diese Art des Betrugs wird immer populärer und ist die zurzeit am häufigsten eingesetzte Methode, um Anwender zur Herausgabe vertraulicher Daten zu bewegen.

Geben Sie Passwörter nur mit der dazugehörigen richtigen Internetadresse ein! Beim Eingeben von Passwörtern im Internet muss in der Adresszeile auch die zugehörige richtige Adresse eingetragen sein. E-Mails, in denen Internetadressen stehen, niemals anklicken, auch wenn diese E-Mails noch so wichtig klingen.

Je stärker das Passwort, desto sicherer sind Sie vor Missbrauch geschützt!

Die Kunst ist es, ein Passwort festzulegen, das Sie sich leicht merken können und das gleichzeitig von Betrügern nicht einfach zu erraten oder durch Brute Force Programme gefunden werden kann. Für das Passwort **aerodynamic99** z.B. benötigt ein Brute Force Programm 3 Sekunden! Ihr Passwort muss deshalb bestimmten Anforderungen genügen:

Das Passwort sollte ...

- mindestens acht Zeichen lang sein
- kein Wort aus einer beliebigen Sprache, sondern eine willkürliche Kombination von großen Buchstaben, kleinen Buchstaben, Sonderzeichen und Ziffern darstellen
- keine Teile des Benutzernamens enthalten



Brute Force

bzw. **Methode der rohen Gewalt** ist der Fachbegriff für eine Lösungsmethode aus dem Bereich der Informatik und der Spieltheorie. Hierbei werden mathematische Probleme durch das Ausprobieren aller möglichen Varianten gelöst.



Brute Force Angriff

ist das Ausprobieren aller möglichen Passwörter durch ein Computerprogramm. Oft werden in diesen Programmen auch Wortlisten und Wörterbücher zur Passwortsuche eingesetzt.



Komplexe Passwörter kann man sich leider nur sehr schwer merken. Bewahren Sie die Notizen der Passwörter nur an einem sehr sicheren Platz auf. Zum leichteren Behalten der Passwörter kann folgender Trick angewendet werden:

Sichere Passwörter können aus den Anfangsbuchstaben der Wörter eines Satzes gebildet werden.

Jeden Morgen um 8:00 Uhr gehe ich zur Arbeit = JMu8:UgizurA

Sie können auch einen vollständigen Satz als Passwort verwenden. Niemand schreibt vor, dass Kennwörter nur aus einem Wort bestehen dürfen.

Auch wenn die Computer-Nutzung für Sie aufwändiger und umständlicher wird, sollten Sie unterschiedliche Kennwörter für verschiedene Aufgaben verwenden. Gelangt doch einmal ein Passwort in falsche Hände, kann der Betrüger nicht überall unter Ihrem Namen Schaden anrichten. Auch die regelmäßige Änderung von Kennwörtern erhöht den Schutz vor Missbrauch wesentlich.

Sichere Webseiten

Heutzutage sind die meisten Webseiten, in denen Kennwörter eingegeben werden müssen, als Sicherheitsseiten angelegt. Anstelle des Protokolls <http://> erscheint ein <https://>. Das „s“ steht für security (Sicherheit). Damit ist gewährleistet, dass in diesem Augenblick niemand Zugang zu dieser Seite hat und das das Kennwort gefahrlos übertragen wird. Optisch ist an einer gelb unterlegten Adressleiste im Browser erkennbar. Da aber nicht jeder Browser diese Kennzeichnung anwendet, ist nur das besagte „s“ im Protokoll entscheidend. Jeder, der im Internet vertrauliche Daten eingeben will, sollte vorher auf dieses Sicherheitsmerkmal achten. Im Zweifelsfall lieber nachfragen oder die Seiten neu aufrufen.

Beauftragter für Innovation und Technologie im Handel Berlin-Brandenburg
in der Bildungszentrum Handel, Wirtschaft und Verwaltung GmbH
Fürstenwalder Poststr. 86
15234 Frankfurt (Oder)

Ihr Ansprechpartner: Bernd Thiel

Fon: 0335 41302-0 Mail: bz@handel.ff.shuttle.de
Fax: 0335 41302-22 Web: www.bzh-ff.de

Die Beauftragten für Innovation und Technologie werden aufgrund eines Beschlusses des Deutschen Bundestages vom Bundesministerium für Wirtschaft und Technologie gefördert.