Sichere Passwörter

Digitale Selbstverteidigung

Gefahren aus dem Internet

Gunter Bauer
https://cryptoparty.at/graz

30.11.2017


DAS PERFEKTE
PASSWORT

DAS PERFEKTE PASSWORT

Kurzes, einfaches Passwort

Beispiel: „321“

Kombinationen	**27 (3^3)**
Hackzeit$_{1)}$	**<1 Sekunde**

Kurzes, komplexes Passwort

Beispiel: „nG4"

Kombinationen	**238.328 (62^3)**
Hackzeit[1)]	**<1 Sekunde**

Langes, einfaches Passwort

Beispiel: „123231332121"

Kombinationen	**531.441 (3^{12})**
Hackzeit$_{1)}$	**<1 Sekunde**

Langes, komplexes Passwort

Beispiel: „1AhU8p0i4fG2"

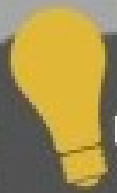
Kombinationen >3 Trilliarden (62^{12})
Hackzeit[1)] >3 Jahre

Sichere Passwörter leicht gemacht

Einen einfach zu merkenden Satz auswählen: Ich liebe meine Katze über alles.

Einzelne Buchstaben wählen (z.B. erster & letzer): Ih le me Ke uer as.

Großbuchstaben, Satz- und Sonderzeichen einfügen: !hLCMeKeUErA5.[2)]



Nach nur 5-maliger Eingabe des neuen, sicheren Passwortes bleibt meist auch schon das Tipp-Muster in Erinnerung.

„!hLCMeKeUErA5.":

Kombinationen	>5 Quadrilliarden (96^{14})
Hackzeit[1)]	>5,9 Millionen Jahre

Kriterien für ein gutes Passwort

- Muß lang genug sein (8-15 Zeichen)
- Mindestens 2 Buchstaben (GROSSBUCHSTABEN und kleinbuchstaben)
- Mindestens 2 Zahlen oder Sonderzeichen (nicht am Anfang und Ende)
- Muß gut zu merken sein
- Muß gut zu einzutippen sein
- Darf keine erkennbare Systematik enthalten
- Darf kein Wort einer bekannten Sprache sein
- (((Muß regelmäßig geändert werden)))

Verfahren zur Passwort-Generierung

- Nicht das Passwort merken,
- Sondern die **Methode der Entstehung** merken

•Akronym-Methode

•Doppelwort-Methode

•Collage-Methode

•Zufall-Methode

•Bernhards Rechnungs-Methode

Akronym-Methode

- Satz bilden
  - z.B. Liedertext, Buchtitel, Buchanfang, Gedicht, …
- Verwendet werden Anfangs- oder Endbuchstaben
- Ergänzen mit Ziffern oder Sonderzeichen

Akronym-Methode

- **Man bildet einen Satz und verwendet als Passwort die Anfangs- oder auch Endbuchstaben.**
  - MbeSuvaPdAoaE
  - MbeS&vaPdAoaE
- **Wie war zu Köln es doch vordem mit Heinzelmännchen so bequem**
  - WwzKedvmHsb
- **Mein kleiner grüner Kaktus steht draußen am Balkon**
  - MkgKsdaB1934

Akronym-Methode

Von 9 bis 12 : Rauchen verboten

- V9b10:Rv

3 + 7 = 10

- 3+Sieben=1()
- 3+7ist1()

Hugo Portisch: Aufregend war es immer 2015

- HP:Awei2015

Vea Kaiser: Blasmusikpop oder Wie die Wissenschaft in die Berge kam

- VK:BoWdWidBk

Doppelwort-Methode

- 2 Wörter (oder mehr)
- Verkürzt, verschachtelt oder mit Sonderzeichen versehen

Bsp.:

- **Stan Laurel & Oliver Hardy**
  - StLa&OlHa
- **Durch dick und dünn**
  - Dud1+due
- **Morgenstund hat Gold im Mund**
  - MosthaGo>>Mu

Collage-Methode

- Wort in 1 oder 2 Sprachen übersetzen
- Daraus Buchstaben entnehmen
- Mit Ziffern und Sonderzeichen verbinden

Bsp.:

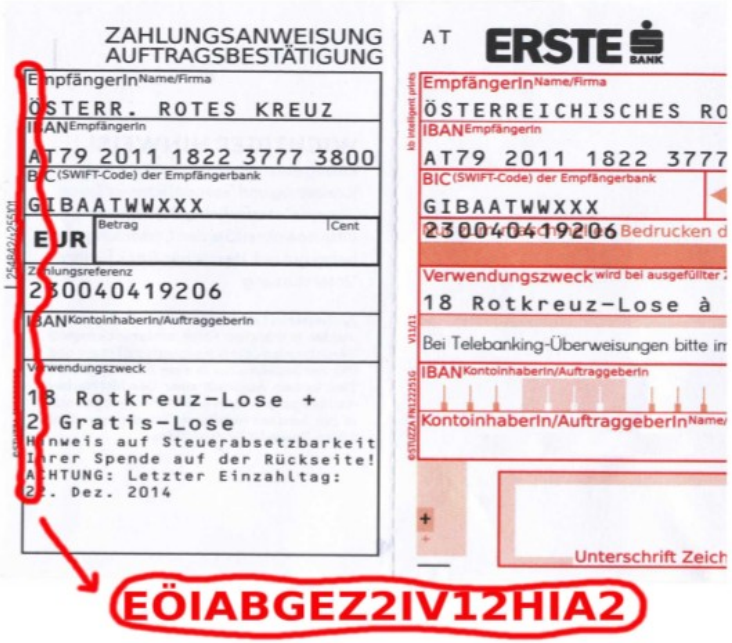
- **house Haus 99** (ist eine Hausnummer)
  - hou:99Hau
- **Pferd horse cheval**
  - P:rs$val

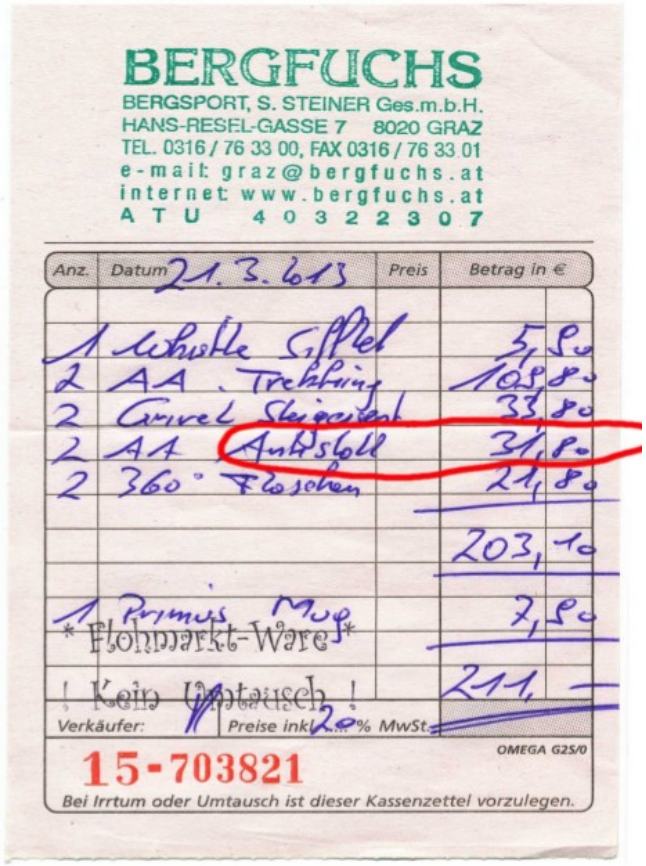
Zufall-Methode

- 8 zufällige Zeichen (ein Kind würfelt)
- Ist aber schwer zu merken
- Tipp: einüben mit Bildschirmschoner

Bernhards Verschleierungs-Methode

Verschleiern auf Papier





3.) Welche Methoden/Hilfsmittel gibt es?

Software-Unterstützung: KeePass

- Gibt es für sehr viele Betriebssysteme (auch Smartphones)
- Ist Open Source
- Enthält auch Passwort-Generator
- Man muss sich nur noch ein Master-Passwort merken
- Das sollte unbedingt gesichert werden und auf mehreren sicheren Datenträgern aufbewahrt werden !

Weblinks zu KeePass

- http://keepass.info/features.html
- http://keepass.info/ratings.html

- **Download**: https://www.keepassx.org/downloads

Warum ist KeePass sicher (Untersuchung der Europäischen Komission)?

- https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/DLV%20WP6%20-02-%20Summary%20of%20the%20evaluation%20of%20results%20_KeePass_published.pdf

Anleitungen:

- http://www.wintotal.de/keepass-passwort-safe-mit-datenbank/
- http://www.hp-scheel.de/seminar/keepass_bedienungsanleitung.pdf
- https://support.uni-landau.de/pics/keepass_win.pdf
- http://passwortbibel.de/keepass-2-password-safe
- http://www.gerold-dreyer.de/Homepage/Anleitungen/Gebrauchsanleitungen%20zu%20Programmen/keepass/materialien/keepass.doc

Passwort-Strategie

Überlegen:

- Wo benutzt man welche Passwörter ?
- Was will man unbedingt mobil (am Handy/Tablet) machen ?
- Wie synchronisiere ich die Passwörter ?
- Wie & wo sichere ich die Passwort-Dateien und das Master-Passwort ?

Anhang

Webseiten mit Passwortcheck:

- https://www.passwortcheck.ch/passwortcheck/passwortcheck
- http://www.browsercheck.pcwelt.de/passwortstarke-messen
- https://howsecureismypassword.net