Wie surfe ich sicher im Netz?

Ein Demo-Workshop zur Praxis

Neko

13.10.2012

Gliederung

- 1. Wahl des Browsers
- 2. Abzudeckende Sicherheitsaspekte
- 3. Vorführung einer Musterkonfiguration
- 4. Verhalten im Internet
- 5. Fragen und Antworten

1. Wahl des Browsers

- Mehrere Browsermöglichkeiten:

  IE, Chrome, Opera, Firefox, Chromium

- Browser mit geschlossenen Quellen:

➔ Man weiß als Benutzer nie genau, was der Browser tut.

➔ Fehlerbehebung dauert länger, da weniger Leute daran arbeiten können

2. Abzudeckende Sicherheitsaspekte

- HTTPS
- HTTP Referer
- User Agent
- Cookies
- JavaScript
- User Tracking

2. Abzudeckende Sicherheitsaspekte → HTTPS

- HTTP-Übertragungen unverschlüsselt
- ➔ Abhören der Verbindung in offenen Netzwerken möglich
- Aber: Auch Phishing-Sites verwenden HTTPS!
- Aber: Auch seriöse Seiten verwenden unsignierte Zertifikate

2. Abzudeckende Sicherheitsaspekte → HTTP Referer

- Referrer zeigt an, über welche Seite man gekommen ist
- Eigentlich keine Sicherheitslücke, aber Es verbreitet Informationen über einen im Netz.

2. Abzudeckende Sicherheitsaspekte → User Agent

- Useragent verrät unter anderem, welchen Browser und welches Betriebssystem man verwendet.
- Wie Referrer keine Sicherheitslücke, aber man selbst ist kein öffentlicher Rundfunk.

2. Abzudeckende Sicherheitsaspekte → Cookies

- Cookies dienen dazu Anmeldeinformationen und Nutzereinstellungen auf der Seite zu speichern.
- Werden häufig dazu eingesetzt Surfverhalten zu protokollieren

2. Abzudeckende Sicherheitsaspekte → JavaScript

- Werkzeug zum erstellen dynamischer und interaktiver Webinhalte
- Kann ungehindert bestimmte Systeminfomationen auslesen.

2. Abzudeckende Sicherheitsaspekte → User Tracking

- Kann nur durch die Wahl der Internetdienste verhindert werden, keine eigentliche Sicherheitslücke des Computers.
- Direkte Kontakte mit großen Suchmaschinen (Google, Yahoo, Bing,…) vermeiden, da diese am meisten tracken.

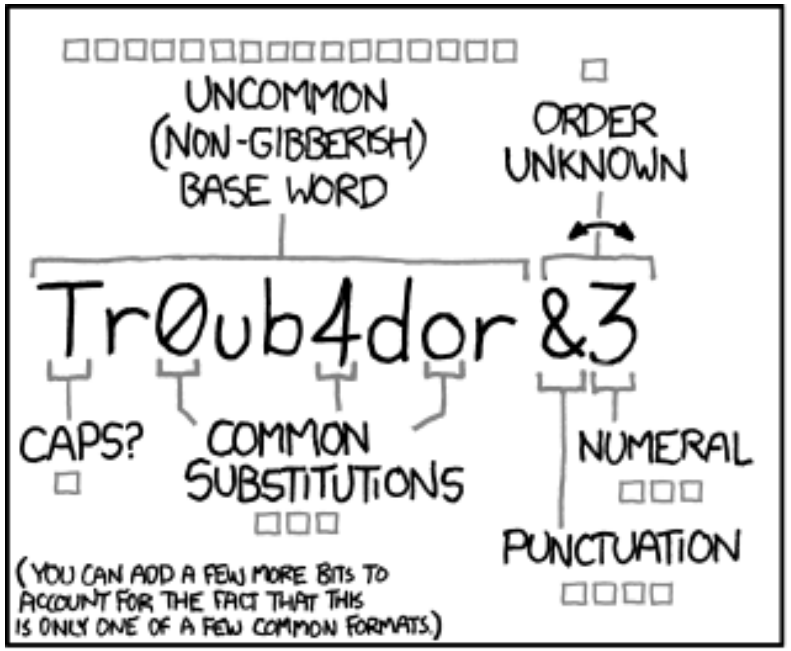
3. Musterkonfiguration

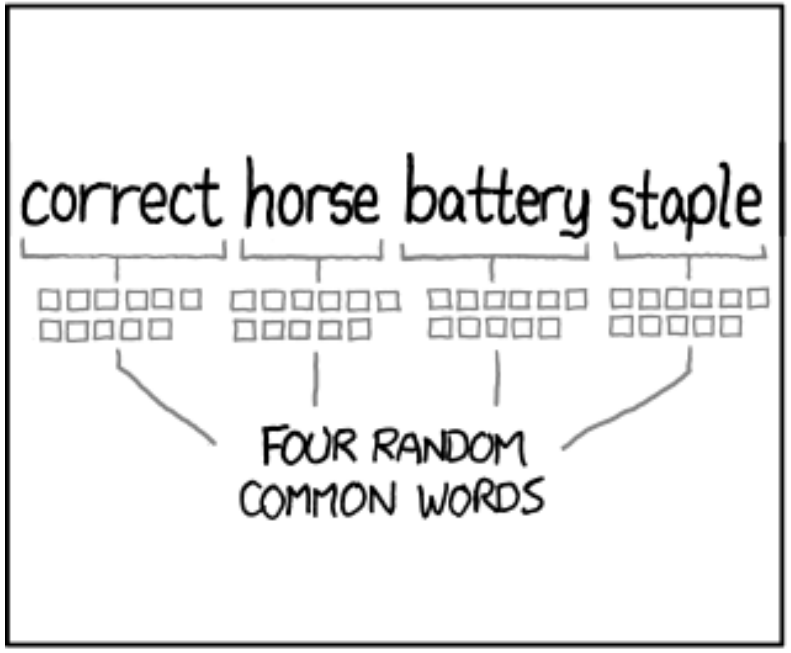
4. Verhalten im Internet

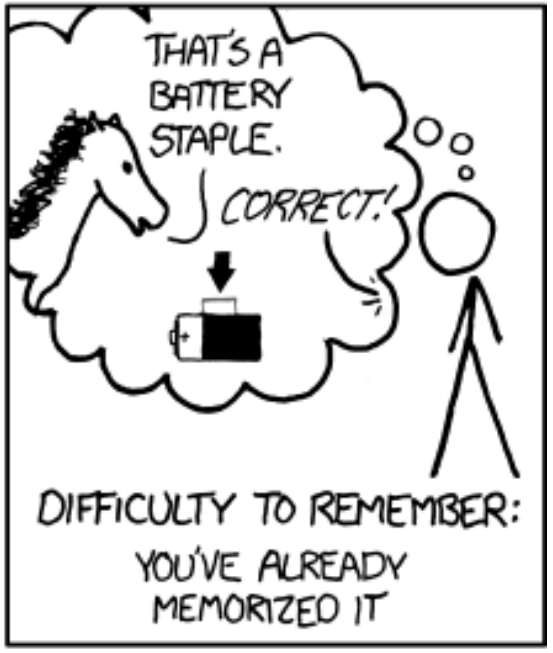
- Mindestens genauso wichtig wie ein wohlkonfigurierter Browser.
- Betrifft nicht nur den Umgang mit dem Browser und dem Internet, sondern auch Emails.
- Durch falsches Verhalten kann man sich auch strafbar machen.

4. Verhalten im Internet → Browsing

- Wann immer möglich HTTPS verwenden
  - Aber Achtung bei fehleraften Zertifikaten
- Persönliche Daten gehören nicht ins Internet
- Keine zusätzlichen Toolbars oder Smileypäckchen installieren
- Starke Passwörter verwenden







THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

4. Verhalten im Internet
→ Emails

- Glaubt keinen Mails die euch Gewinne oder Geld versprechen.
- Folgt niemals Aufforderungen eure Logininformationen oder Kreditkartennummern weiterzugeben.