Ideen und Konzepte der Informatik

Sicherheit und Privatheit

Praktische Tipps

Kurt Mehlhorn

Überblick

- Sicherheit: Schutz von Geräten und Daten gegen Missbrauch.
  - Passwörter und Absperren von Geräten
  - Back-Ups (Datensicherung)
  - Soziale Attacken, Phishing
- Privatheit: Wer darf was über Sie wissen?
- Ich bin nicht paranoid bezüglich Sicherheit und Privatheit, aber vorsichtig. Ich werde immer vorsichtiger (Missbrauch einer Kreditkarte, Einbruch in mein Opodokonto, Erlebnis diese Woche, verschärfte Maßnahmen meiner Bank, Microsoft, Google,…).

Sicherheit

Eine Kette ist nur so stark wie ihr schwächstes Glied.

Passwörter I

- Für meine Anwendungen (Banken, Internetstores, Zeitungen, GPSies, Datenbank des Fachbereichs, ….) habe ich Passworte unterschiedlicher Qualität benutzt. Für wichtige Dienste (hoher Schaden) jeweils ein eigenes Passwort. Für unwichtige Dienste (kleiner Schaden) einige wenige Passworte. Alle Passworte sind 8 Zeichen oder länger. Wichtige Passworte sind 12 und mehr Zeichen.
- Unterscheidung wichtig/unwichtig ist NICHT sinnvoll!
- Alle neuen Passworte sind zufällige Worte aus 16 Buchstaben, z.B. L5RxH.!dnB5Deakx
- https://sec.hpi.de/ilc/search?lang=de, Liste von kompromittierten Passwörtern.

Passwörter II

- Ich benutze einen Passwortsafe (Keepassx, Strongbox, Browser), den ich zwischen meinen verschiedenen Geräten automatisch synchronisiere.
- Dafür benutze ich ein langes Passwort (14 Zeichen). Vorsicht: in machen Browsern kann man den Passwortschutz für den Safe abstellen.
- Das Passwort für den Passwortsafe ist im Safe des Instituts hinterlegt.
- Zweifaktorauthorisierung, wenn immer möglich.

Absperren von Geräten

- Meine Geräte werden gesperrt, wenn ich sie 60 Sekunden nicht benutze. Will garantieren, dass Rechner gesperrt ist, wenn ich ihn verliere.
- Iphone, Ipad: 6stelliger Code, 3mal falscher Code führt zum Löschen aller Inhalte.
- Notebook: Passwort mit 12 Zeichen.
- WLAN zu Hause: Passwort mit 12 Zeichen.

Datensicherung (Back-Up)

- Machen Sie regelmäßig eine Datensicherung auf ein Medium, das getrennt von ihrem Rechner ist.
- KM in der Arbeit: automatisch, immer wenn ich mehrere Stunden im Büro bin.
- KM zu Hause (bis 2019): wöchentlich oder bei Bedarf öfter auf Festplatte, die ich nur dazu mit dem Rechner verband. Ich habe keinen Desktop mehr zu Hause.
- Telefon und Tablet: regelmäßig und automatisch in der Cloud.

Weitere Maßnahmen

- HTTPS Everywhere
- Vorsicht beim Öffnen von Attachments und Verfolgen von Links. Besondere Vorsicht, wenn Absender oder Webseite unbekannt. Phishing Angriff.
- Aktueller Virenscanner, aktuelle Version des Betriebssystems und aller Programme (automatische Updates).
- 10 goldene Regeln für Computersicherheit.

Privatheit

Wer darf was über mich wissen?

- Auch scheinbar nichtssagende Informationen ergeben in der Masse ein Bild.
- Tips zum Umgang mit Privatheit.

Privatheit

Wer darf was über mich wissen?

Im Internet scheint vieles umsonst (Suchmaschinen, soziale Netzwerke, Streamingdienste). Es gibt aber wenig umsonst im Internet. In der Regel zahlen wir

- mit Daten, die eine gezieltere Werbung erlauben, oder
- mit erhöhter Verwundbarkeit/Beeinflussbarkeit.

Das Internet vergisst nicht. Was wir heute lustig finden, finden wir in 10 Jahren vielleicht peinlich.

Ein Irrglaube

Google/Facebook wissen viel über mich, aber nur unwichtiges Zeug:

- Welche Filme mir gefallen, welche Schauspieler und Sportler ich toll finde, wann ein Geschäft geöffnet ist, wie man am schnellsten nach Wallerfangen kommt, …

Wichige Informationen behalte ich für mich:

- Mein Einkommen, meinen Intelligenzquotienten, meine politische Einstellung, …

Der digitale Fußabdruck verrät viel

We show that easily accessible digital records of behavior, Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender. The analysis presented is based on a data set of over 58,000 volunteers who provided their Facebook Likes, detailed demographic profiles, and the results of several psychometric tests. The derived model correctly discriminates between homosexual and heterosexual men in 88% of cases, African Americans and Caucasian Americans in 95% of cases, and between Democrat and Republican in 85% of cases. For the personality trait “Openness,” prediction accuracy is close to the test–retest accuracy of a standard personality test. We give examples of associations between attributes and Likes and discuss implications for online personalization and privacy.

Kosinski et al: Private traits and attributes are predictable from digital records of human behavior, PNAS 2013

Der digitale Fußabdruck verrät viel

Autoren kannten von 58.000 Freiwilligen:

- Facebook likes
- Selbstauskunft über Wohnort, politische und sexuelle Präferenzen, Persönlichkeitstest, …

Aus der Hälfte wird gelernt (siehe Einheit maschinelles Lernen)

Facebook Likes → Persönlichkeitsmerkmale

Mit der anderen Hälfte wird Qualität der Vorhersage ausgewertet.

Merkmal Intelligenzquotient

Niedrig

Sephora (Kosmetik)
I love being a mom
Harley Davidson
Lady Antebellum (Country Song Gruppe)

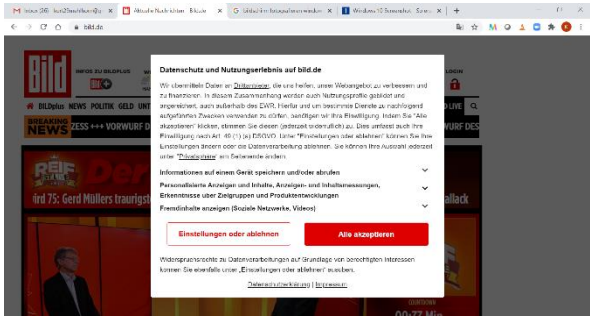
Hoch

Thunderstorms
The Colbert Report (Satire Sendung)
Science
Curly Fries

Der Artikel Kosinski et al: Private traits and attributes are predictable from digital records of human behavior, PNAS 2013 steht unter Materialien bereit.

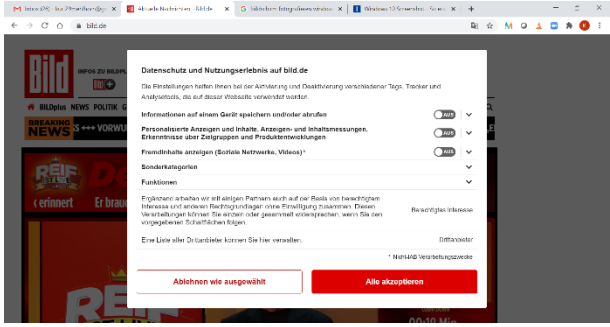
Dienste

- Ich benutze Browser, Google, WhatsApp, email (auch gmail), Dropbox.



- Browser: maximale Sicherheits- und Privatheitseinstellungen.

- Browsererweiterungen Adblock, HTTPS Everywhere, Privacy Badger (protection against trackers), Google Analytics Opt-Out, NoScript, Jumbo, opt-out on Cookies.



- Google Privatsphärecheck: habe Rechte von Google zur Auswertung meines Browserverhaltens weit möglichst eingeschränkt.

Email

- Ich signiere meine Emails. (Elektronische Unterschrift)
- Manche Emails verschlüssele ich. Wenn immer der Empfänger es so eingerichtet hat.
- Ich benutze auch gmail, obwohl ich damit Google die Erlaubnis gebe, meine emails zu lesen.
  - Soll ich Google erlauben, mein persönlicher Assistent zu werden? Das ist eine Vertrauensfrage.

Zusammenfassung

- Benutzen Sie die Segnungen des Internets bewusst.
- Treffen Sie Vorkehrungen gegen Missbrauch.
- Missbrauch bedeutet Ärger, Verlust von Zeit und/oder Geld, Ansehen, ….