Usable Authentication & Passwords

Top 10 Common Chosen Passwords

1. password
2. 12345
3. 12345678
4. abc123
5. qwerty
6. monkey
7. letmein
8. dragon
9. 111111
10. baseball

Password Guidelines

In order to protect your security, Intel has certain rules for choosing passwords. Please read the following rules so that you will know how to choose a good password:

The following rules apply to all passwords:

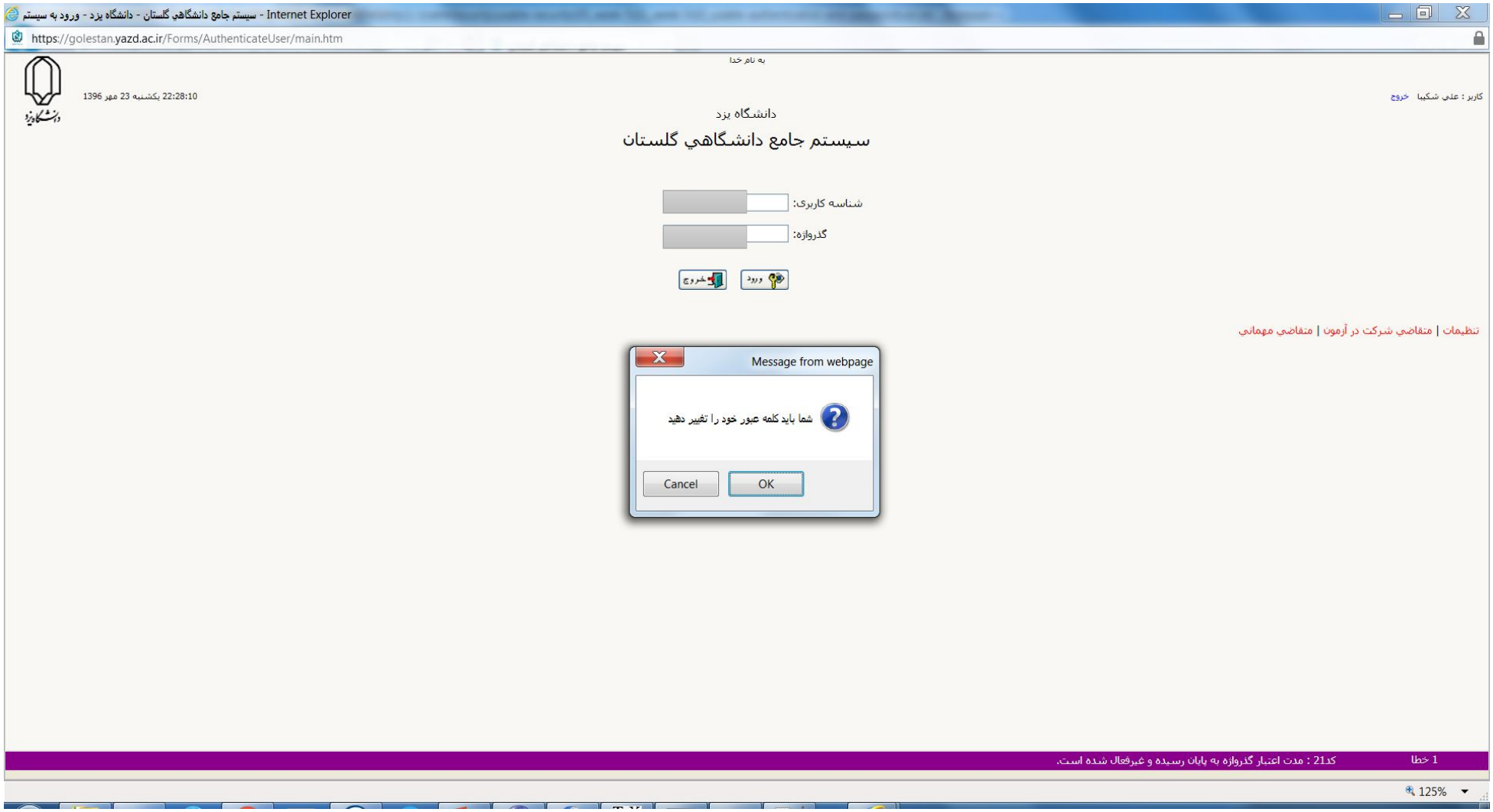
- The password must be at least eight characters long, and can contain letters, numerals, and punctuation.
- It cannot contain spaces.
- It must contain at least one alpha character [a-z; A-Z].
- It cannot contain your login ID.
- The first eight characters cannot be the same as your previous password.
- Passwords are treated as case sensitive.

Examples of strong passwords:
(The following is for example purposes only. Do not use any of these examples as your actual password.)

- Use a name, modified slightly, like "Bob*1Smith" or "Bobby$123"
- Use a phrase you can remember, like "hello world" modified to "hello1@World2"
- "ttL*hi?wur5" (contains lower case letters, capital case letters, special characters, and numbers)

Thank you for supporting your security by following these password guidelines. If you have any questions about these password guidelines, please contact Technical Support.

By submitting a support request you may be contacted by Intel or an Intel authorized reseller.


سیستم جامع دانشگاهی گلستان - دانشگاه یزد - ورود به سیستم - Internet Explorer
https://golestan.yazd.ac.ir/Forms/AuthenticateUser/main.htm
به نام خدا
22:28:10 یکشنبه 23 مهر 1396
کاربر : علی شکیبا خروج
دانشگاه یزد
سیستم جامع دانشگاهی گلستان
شناسه کاربری:
گذروازه:
ورود
خروج
تنظیمات | متقاضی شرکت در آزمون | متقاضی مهمانی
Message from webpage
شما باید کلمه عبور خود را تغییر دهید
Cancel
OK
1 خطا
کد21 : مدت اعتبار گذروازه به پایان رسیده و غیرفعال شده است.
125%

2. Related work

Section: Choose

Since the expansion of the Internet and increased online activities, users have been challenged by both the explosion of numbers of passwords and the length requirement of passwords. A recent study by Microsoft Research (Florencio and Herley, 2007) shows that the average Web user has about 25 accounts that require passwords and has 6.5 passwords, each of which contains mostly lower case letters with an average bitstrength of 40.54 bits. In addition, passwords are re-used and forgotten very often, confirming the convention wisdom. An online experiment conducted by Carnegie Mellon University (Shay *et al.*, 2014) evaluates the password policy for a security/usability tradeoff. The study reveals that adding requ

Xiaoying Yu, Qi Liao, (2016) "User password repetitive patterns analysis and visualization", Information & Computer Security, Vol. 24 Issue: 1, pp.93-115, https://doi.org/10.1108/ICS-06-2015-0026

guessed passwords, and that certain combi

traditional complex policy.

Traditionally, metrics such as Shannon entropy and guessing entropy have been used to analyze the security of passwords. For exampl

various password creat

cracking over a real-w

a secure system, adapti

Information and Computer Security

ISSN: 2056-4961
Previously published as: Information Management & Computer Security
Online from: 2015
Subject Area: Information & Knowledge Management

Accepted Articles | Current Issue | Available Issues | Most Cited | Most Read | ToC Alert | RSS | Add to favorites

Clarivate Analytics
Emerging Sources Citation Index
Scopus
Publish open access in this journal

Through analyzing 70 r

guessing difficulty of sk

(Dell'Amico *et al.*, 2010

dictionary attacks, dictionary mangling and Markov chain techniques. All attack techniques are affected by

Password Attacks

- Human
- Brute force
- Common word
- Dictionary words

Password Security

Type	Password	Method	Time	Security level
6 random characters	jskerv	Brute-force	1 month	risky
6 random characters with numbers	ergs43	Brute-force	8 months	Low risk
6 random characters with mixed case, symbols and numbers	J4fS<2	Brute-force	219 years	Secure for life
6 character common word	orange	Common words	3 minutes	useless
6 character uncommon word	woosaa	dictionary	1 hour 22 minutes	useless

https://www.baekdal.com/insights/password-security-usability

Password Security

Type	Password	Method	Time	Security level
2 common word password	alpine fun	Common word	2 months	Low risk
3 common word password	this is fun	Common word	2,537 years	Secure forever

https://www.baekdal.com/insights/password-security-usability

Password Security

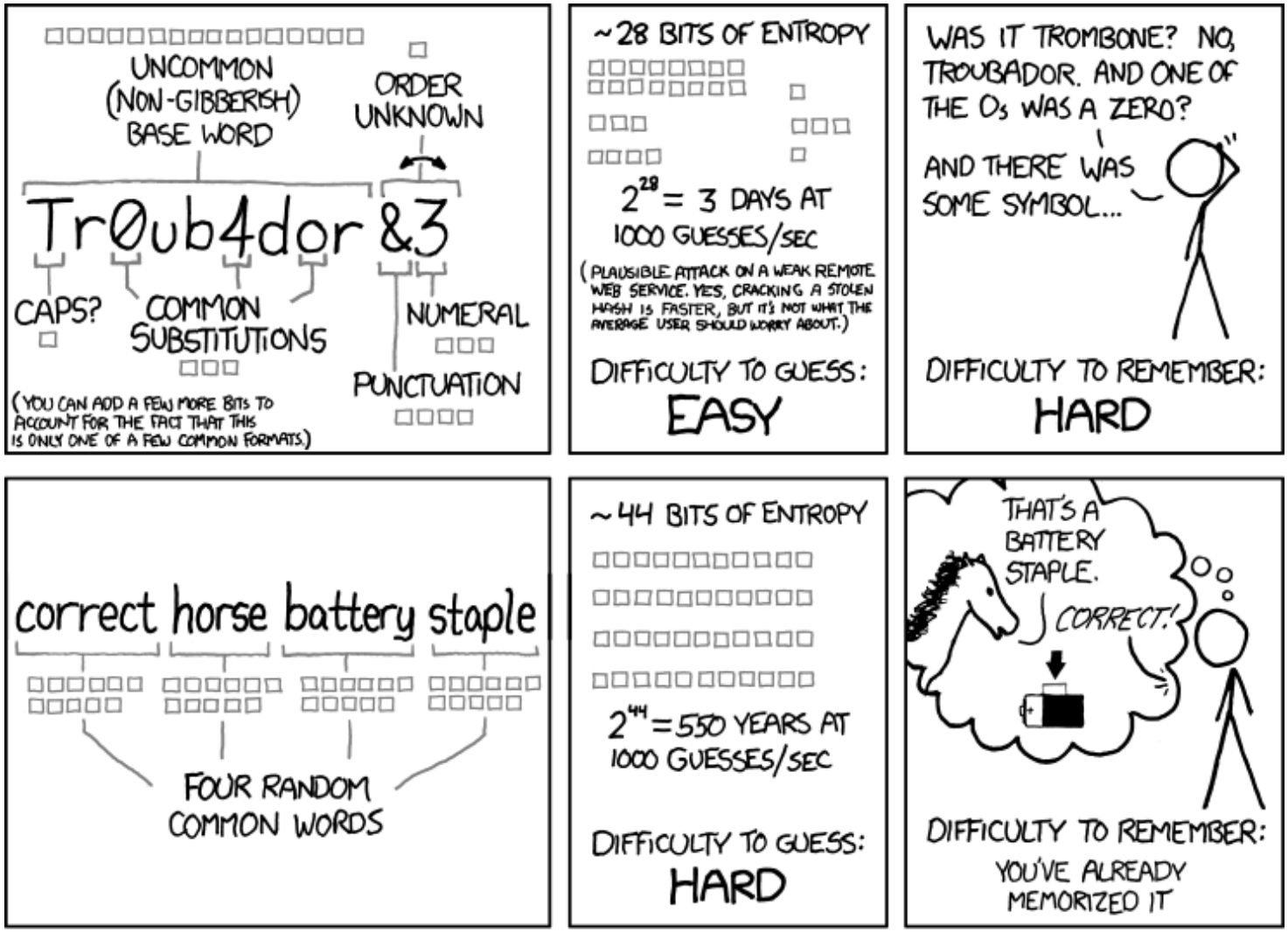
Type	Password	Method	Time	Security level
3 uncommon word password	fluffy is puffy	Dictionary	39,637,200 years	Secure forever
5 uncommon word password	du-bi-du-bi-dub	Brute-force	531,855,448,467 years	Secure forever

https://www.baekdal.com/insights/password-security-usability

Password Security

No of attacks	Password	Time	Security level
100 times per sec	alpine fun	2 months	Low risk
1 time every 5 sec	alpine fun	63 years	Secure
1 time every 5 sec with a 1 hour penalty period after 10 attempts	alpine fun	1,889 years	Secure forever

https://www.baekdal.com/insights/password-security-usability



https://xkcd.com/936/

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.

Conclusions

- Password systems would be more secure if passwords were more usable
  - Human reasons
  - Computational reasons
- Why haven't we fixed this?

Two-Factor Authentication

Two-Factor Authentication (TFA)

- Password + one time unique code
- Generated by
  - Device
  - Email
  - Text
  - App

Security of TFA?

- More secure
- Stops most hacking attacks
- Users perceive it as more secure

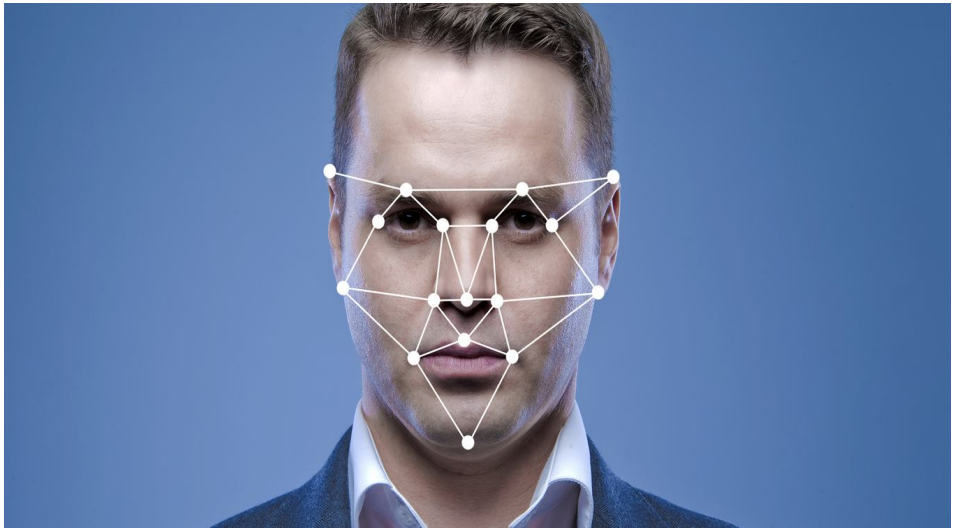
Usability of TFA

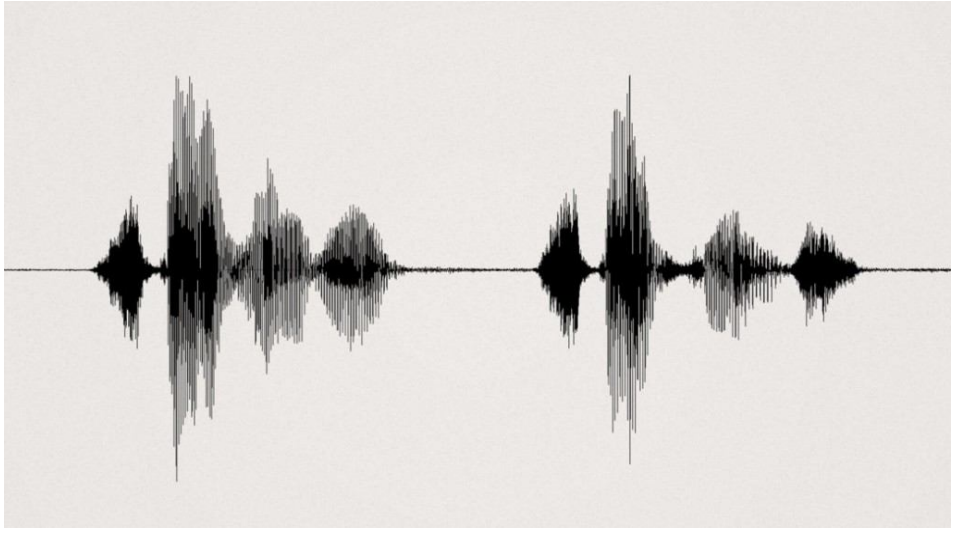
- Research says:
  - Speed: slower
  - User preference:
    - Felt less usable
    - Less convenient
    - Harder to use

Conclusions

- More secure, less usable

Biometrics





Without Biometrics

Fingerprint Recognition

Face Recognition

Voice Recognition

Analyzing Usability

Voice Recognition

- Speed
  - Medium
- Efficiency
  - Medium
- Learnability
  - Easy
- Memorability
  - Easy

Facial Recognition

- Speed
  - Medium
- Efficiency
  - Medium
- Learnability
  - Easy
- Memorability
  - Easy

Fingerprint Recognition

- Speed
  - Fast
- Efficiency
  - Good
- Learnability
  - Easy
- Memorability
  - Easy

Analyzing Security

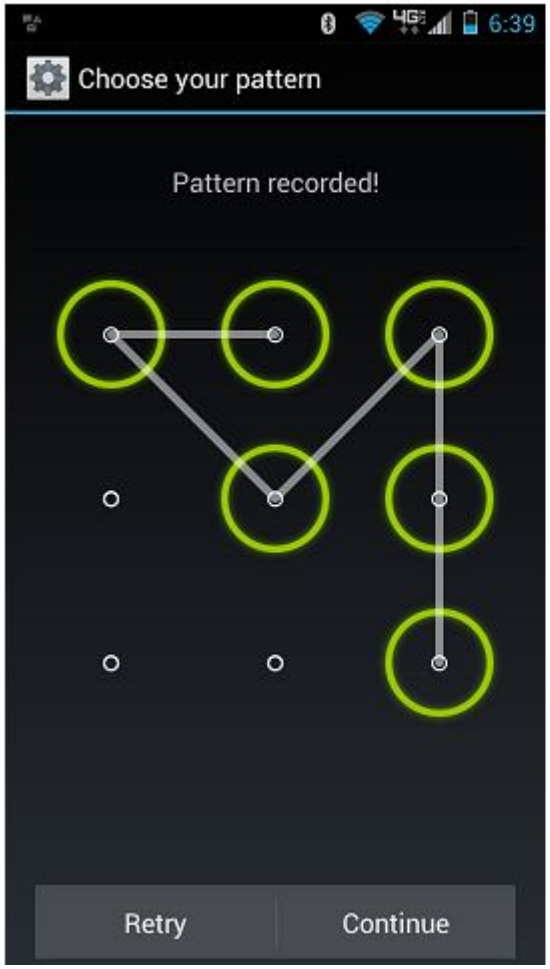
- Who can access the device?
- How easily can they replicate the biometric input?

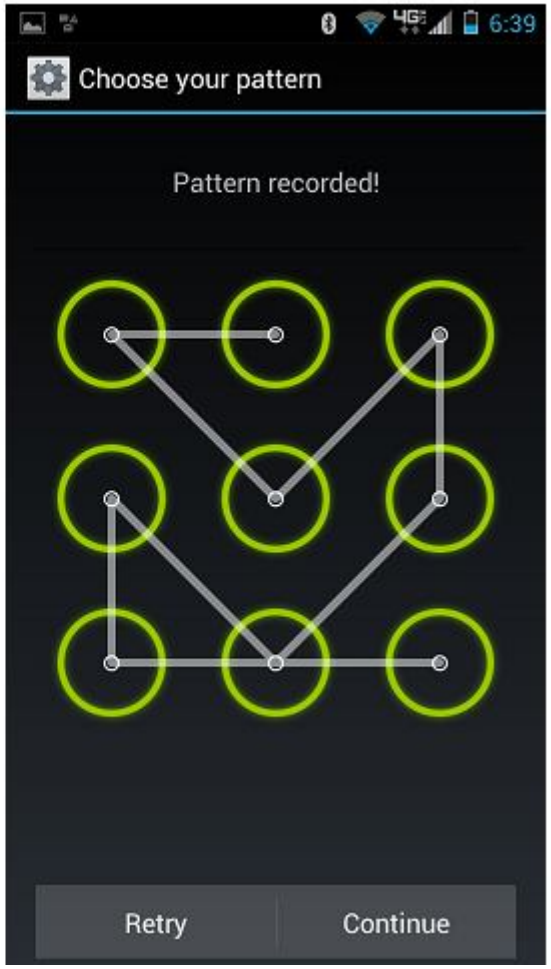
Conclusions

- Biometrics are easy & relatively secure
- Common on mobile devices but work anywhere
- Compare usability

Gesture-based Authentication

Keypad Gestures





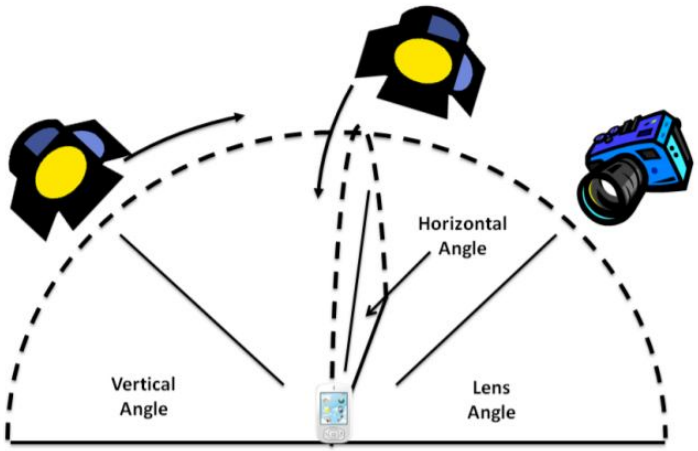
Free Gestures

Napa Sae-Bae, Kowsar Ahmed, Katherine Isbister, and Nasir Memon. 2012. Biometric-rich gestures: a novel approach to authentication on multi-touch devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '12). ACM, New York, NY, USA, 977-986. DOI: http://dx.doi.org/10.1145/2207676.2208543

Benefits

- Gestures
  - users enjoy (easy, fun, etc.)
  - tend to be more secure
- Users prefer gestures to passwords
- Gestures are faster than passwords & are less error prone

Case Study: Smudge Attacks

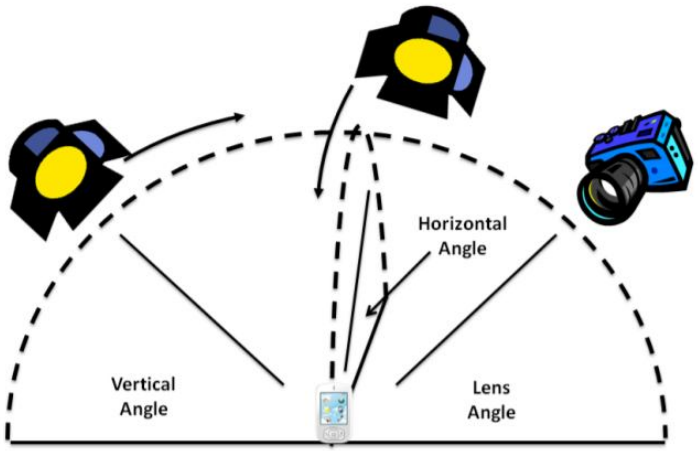


Experiment 1: Ideal Collection

Figure 5: Phone A, from Experiment 1, where the pattern is entered with normal touches. Notice that the directionality of the pattern can be determined at ever direction change.

Aviv, Adam J., et al. "Smudge Attacks on Smartphone Touch Screens." WOOT 10 (2010): 1-7. https://www.usenix.org/legacy/event/woot10/tech/full_papers/Aviv.pdf

Case Study: Smudge Attacks

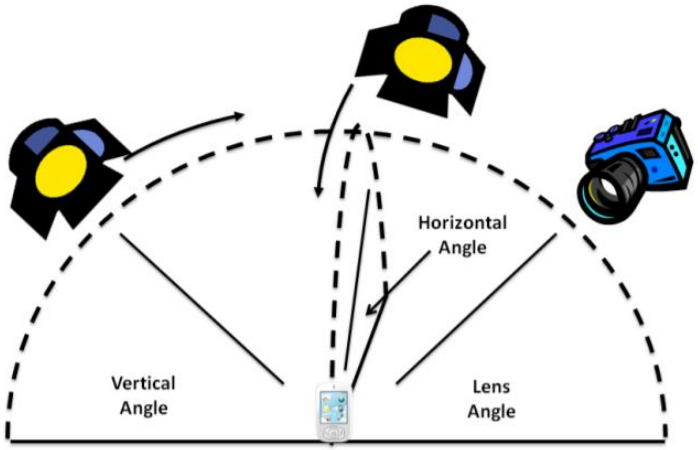


Experiment 1: Ideal Collection

Figure 7: Phone from Experiment 1: One stroke of the pattern, |84|, is lost due to the camera or lighting angle. The contrast has been adjusted.

Aviv, Adam J., et al. "Smudge Attacks on Smartphone Touch Screens." WOOT 10 (2010): 1-7. https://www.usenix.org/legacy/event/woot10/tech/full_papers/Aviv.pdf

Case Study: Smudge Attacks



Experiment 2: Simulated Usage

Figure 8: Phone from Experiment 2: With this usage condition (dot and streaks, under), the pattern is nearly all lost. The contrast has been adjusted.

Aviv, Adam J., et al. "Smudge Attacks on Smartphone Touch Screens." WOOT 10 (2010): 1-7. https://www.usenix.org/legacy/event/woot10/tech/full_papers/Aviv.pdf

Case Study: Smudge Attacks

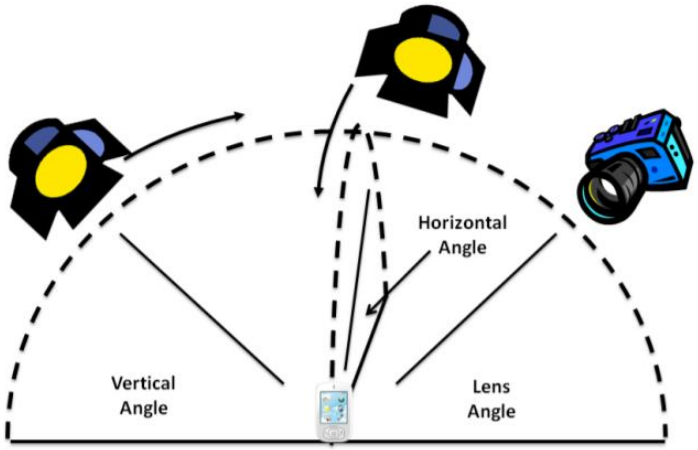


Figure 6: Phone from Experiment 3, where the phone was wiped, placed (and replaced) in a pocket. Unlike Phone A from Fig. 5, some directionality is lost in the upper left portion of the pattern.

Experiment 3: Removing Smudges

Aviv, Adam J., et al. "Smudge Attacks on Smartphone Touch Screens." WOOT 10 (2010): 1-7. https://www.usenix.org/legacy/event/woot10/tech/full_papers/Aviv.pdf

Multiple Phones

- Clean, normal password
- Clean, light password
- Dirty

Results

- Easy to retrieve at least some information about password from smudges
- Clean screens are easier to work with, but even on dirty screens, a lot of password info can be found

Conclusions

- Interesting attack on non-traditional authentication
- Human-based with a twist

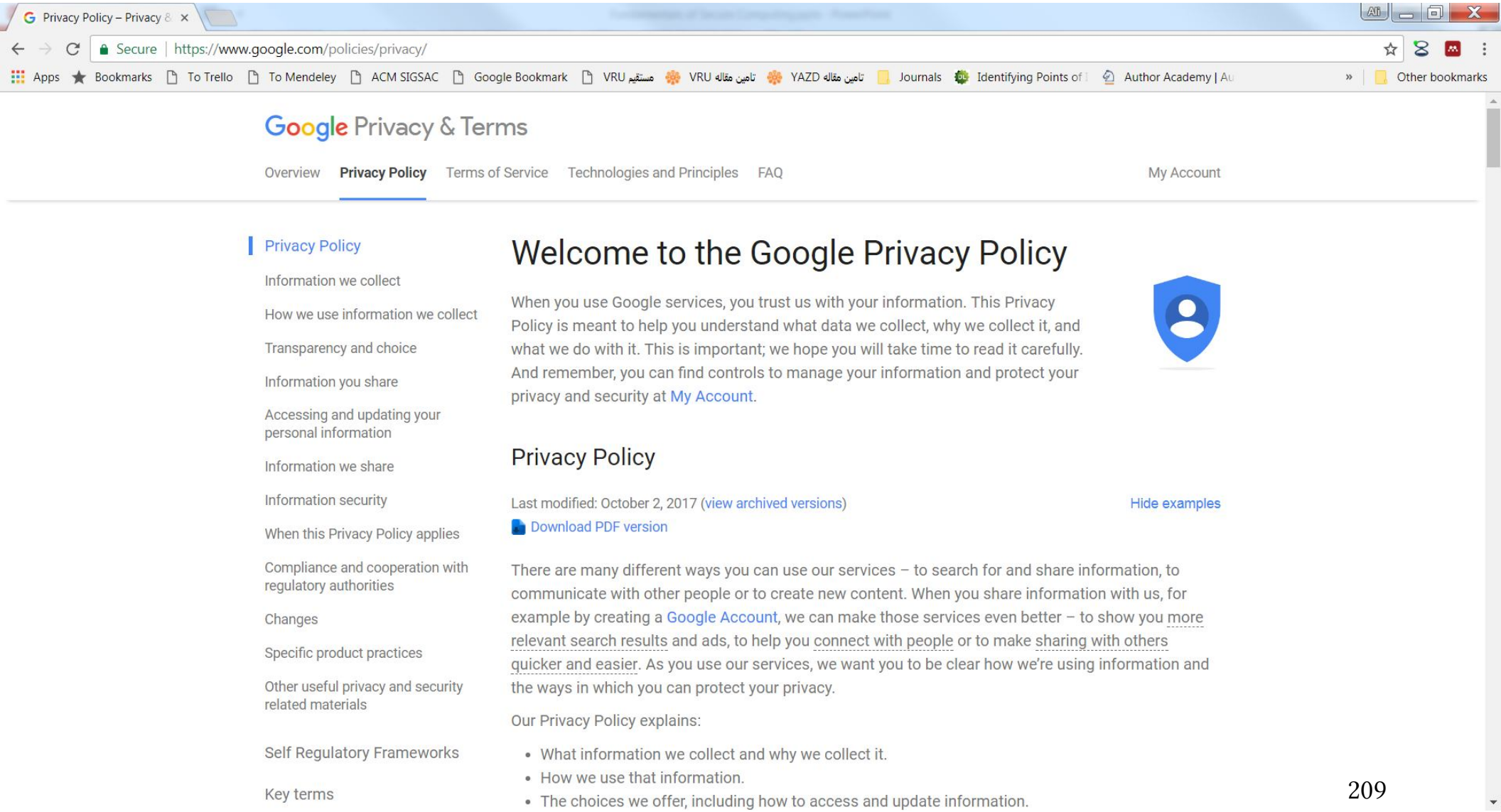
Usable Privacy Basics

Privacy is a kind of security.

- Users want to protect their information.
- Users should have the right to understand what happens with their data.
- Users should have as much control as possible over how it is used.

Privacy Policies

- Tell a user everything they need to know about how their data is collected, used & shared.
- Can be analyzed for usability.


Privacy Policy – Privacy &
Secure | https://www.google.com/policies/privacy/
Apps Bookmarks To Trello To Mendeley ACM SIGSAC Google Bookmark VRU مستقیم VRU تامین مقاله YAZD تامین مقاله Journals Identifying Points of Author Academy | Au Other bookmarks
Google Privacy & Terms
Overview Privacy Policy Terms of Service Technologies and Principles FAQ My Account
Privacy Policy
Information we collect
How we use information we collect
Transparency and choice
Information you share
Accessing and updating your personal information
Information we share
Information security
When this Privacy Policy applies
Compliance and cooperation with regulatory authorities
Changes
Specific product practices
Other useful privacy and security related materials
Self Regulatory Frameworks
Key terms
Welcome to the Google Privacy Policy
When you use Google services, you trust us with your information. This Privacy Policy is meant to help you understand what data we collect, why we collect it, and what we do with it. This is important; we hope you will take time to read it carefully. And remember, you can find controls to manage your information and protect your privacy and security at My Account.
Privacy Policy
Last modified: October 2, 2017 (view archived versions)
Hide examples
Download PDF version
There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy.
Our Privacy Policy explains:
What information we collect and why we collect it.
How we use that information.
The choices we offer, including how to access and update information.

Purpose

The purpose of this Privacy Policy is to describe how Coursera, Inc. ("Coursera," "us," "we," or "our") collects, uses and shares information about you through our U.S. online interfaces (e.g., websites and mobile applications) owned and controlled by us, including www.coursera.org (collectively referred to herein as the "Site"). Please read this notice carefully to understand what we do. If you do not understand any aspects of our Privacy Policy, please feel free to contact us at privacy@coursera.org. Your use of our Site is also governed by our Terms of Use.

What Information this Privacy Policy Covers

This Privacy Policy covers information we collect from you through our Site. Some of our Site's functionality can be used without revealing any personal information, though for features or services related to the Online Courses, personal information is required. If you do not use these specific features or services on the Site, then the only information we collect will be "Non-Personal Information" (i.e., information that cannot be used to identify you). Non-Personal Information includes information such as the web pages that you have viewed. In order to access certain features and benefits on our Site, you may need to submit "Personally Identifiable Information" (i.e., information that can be used to identify you). Personally Identifiable Information can include information such as your name and email address, among other things. You are responsible for ensuring the accuracy of the Personally Identifiable Information you submit to Coursera. Inaccurate information may affect your ability to use the Site, the information you receive when using the Site, and our ability to contact you. For example, your email address should be kept current because that is one of the primary manners in which we communicate with you.

What You Consent to by Using Our Site

Please understand that by submitting any Personally Identifiable Information to us, you consent and agree that we may collect, use and disclose such Personally Identifiable Information in accordance with this Privacy Policy and our Terms of Use, and as permitted or required by law. If you do not agree with these terms, then please do not provide any Personally Identifiable Information to us. If you refuse or withdraw your consent, or if you choose not to provide us with any required Personally Identifiable Information, we may not be able to provide you with the services that can be offered on our Site.

Purpose

The purpose of this Privacy Policy is to describe how Coursera, Inc. ("Coursera," "us," "we," or "our") collects, uses and shares information about you through our U.S. online interfaces (e.g., websites and mobile applications) owned and controlled by us, including www.coursera.org (collectively referred to herein as the "Site"). Please read this notice carefully to understand what we do. If you do not understand any aspects of our Privacy Policy, please feel free to contact us at privacy@coursera.org. Your use of our Site is also governed by our Terms of Use.

What You Consent to by Using Our Site

Please understand that by submitting any Personally Identifiable Information to us, you consent and agree that we may collect, use and disclose such Personally Identifiable Information in accordance with this Privacy Policy and our Terms of Use, and as permitted or required by law. If you do not agree with these terms, then please do not provide any Personally Identifiable Information to us. If you refuse or withdraw your consent, or if you choose not to provide us with any required Personally Identifiable Information, we may not be able to provide you with the services that can be offered on our Site.

example, your email address should be kept current because that is one of the primary manners in which we communicate with you.

What You Consent to by Using Our Site

Please understand that by submitting any Personally Identifiable Information to us, you consent and agree that we may collect, use and disclose such Personally Identifiable Information in accordance with this Privacy Policy and our Terms of Use, and as permitted or required by law. If you do not agree with these terms, then please do not provide any Personally Identifiable Information to us. If you refuse or withdraw your consent, or if you choose not to provide us with any required Personally Identifiable Information, we may not be able to provide you with the services that can be offered on our Site.

حریم خصوصی
Digikala Co. [IR] | https://www.digikala.com/Page/Privacy-Policy
Bookmarks | To Trello | To Mendeley | ACM SIGSAC | Google Bookmark | VRU مستقیم | VRU تامین مقاله | YAZD تامین مقاله | Journals | Identifying Points of | Author Academy | Au | bookmarklet | Other bookmarks

حریم خصوصی

دیجی‌کالا ضمن احترامی که برای حریم شخصی کاربران قائل است، برای خرید، ثبت نظر یا استفاده از برخی امکانات وب سایت اطلاعاتی را از کاربران درخواست می‌کند تا بتواند خدماتی امن و مطمئن را به کاربران ارائه دهد. برای پردازش و ارسال سفارش، اطلاعاتی مانند آدرس، شماره تلفن و ایمیل مورد نیاز است و از آنجا که کلیه فعالیت‌های دیجی‌کالا قانونی و مبتنی بر قوانین تجارت الکترونیک صورت می‌گیرد و طی فرایند خرید، فاکتور رسمی و بنا به درخواست مشتریان حقوقی گواهی ارزش افزوده صادر می‌شود، از این رو وارد کردن اطلاعاتی مانند نام و کد ملی برای اشخاص حقیقی یا کد اقتصادی و شناسه ملی برای خریدهای سازمانی لازم است. همچنین آدرس ایمیل و تلفن‌هایی که مشتری در پروفایل خود ثبت می‌کند، تنها آدرس ایمیل و تلفن‌های رسمی و مورد تایید مشتری است و تمام مکاتبات و پاسخ‌های شرکت از طریق آنها صورت می‌گیرد.

بنابراین درج آدرس، ایمیل و شماره تماس‌های همراه و ثابت توسط مشتری، به منزله مورد تایید بودن صحت آنها است و در صورتی که این موارد به صورت صحیح یا کامل درج نشده باشد، دیجی‌کالا جهت اطمینان از صحت و قطعیت ثبت سفارش می‌تواند از مشتری، اطلاعات تکمیلی و بیشتری درخواست کند.

مشتریان می‌توانند نام، آدرس و تلفن شخص دیگری را برای تحویل گرفتن سفارش وارد کنند و دیجی‌کالا تنها برای ارسال همان سفارش، از این اطلاعات استفاده خواهد کرد.

همچنین دیجی‌کالا ممکن است برای ارتباط با مشتریان، بهینه سازی محتوای وب سایت و تحقیقات بازاریابی از برخی اطلاعات استفاده کند و برای اطلاع رسانی رویدادها و اخبار، خدمات و سرویس‌های ویژه یا پروموشن‌ها، برای اعضای وب سایت ایمیل یا پیامک ارسال نماید. در صورتی که کاربران تمایل به دریافت اینگونه ایمیل و پیامک‌ها نداشته باشند، می‌توانند عضویت دریافت خبرنامه دیجی‌کالا را در پروفایل خود لغو کنند.

توجه داشته باشید که **300061930000** و **100061930000** شماره‌هایی است که دیجی‌کالا از طریق آن برای کاربران و مشتریان خود پیامک (اس ام اس) ارسال می‌کند. همچنین این شماره‌ها، سامانه ارسال پیامک است که وضعیت پردازش سفارش یا رویدادها، خدمات و سرویس‌های ویژه دیجی‌کالا را به اطلاع کاربران می‌رساند و روشن است که امکان دریافت پیام‌های شما از طریق آن وجود ندارد.

همچنین ممکن است دیجی‌کالا از طریق شماره **300061930002** برای برخی کاربران یا مشتریان خود، سوال نظرسنجی ارسال کند.

بنابراین ارسال هرگونه پیامک تحت عنوان دیجی‌کالا، با هر شماره دیگری تخلف و سوء استفاده از نام دیجی‌کالا است و در صورت دریافت چنین پیامکی، لطفاً جهت پیگیری قانونی آن را به **Info@digikala.com** اطلاع دهید.

دیجی‌کالا ممکن است نقد و نظرهای ارسالی کاربران را در راستای رعایت قوانین وب سایت ویرایش کند. همچنین اگر نظر یا پیام ارسال شده توسط کاربر، مشمول مصادیق محتوای مجرمانه باشد، دیجی‌کالا می‌تواند از اطلاعات ثبت شده برای پیگیری قانونی استفاده کند.

حفظ و نگهداری رمز عبور بر عهده کاربران است و برای جلوگیری از هرگونه سوء استفاده احتمالی، کاربران نباید آن را برای شخص دیگری فاش کنند. دیجی‌کالا هویت شخصی کاربران را محرمانه می‌داند و اطلاعات شخصی آنان را به هیچ شخص یا سازمان دیگری منتقل نمی‌کند، مگر اینکه با حکم قانونی مجبور باشد در اختیار مراجع ذی‌صلاح قرار دهد.

دیجی‌کالا همانند سایر وب سایت‌ها از جمع آوری IP و کوکی‌ها استفاده می‌کند، اما پروتکل، سرور و لایه‌های امنیتی دیجی‌کالا و روش‌های مناسب مدیریت داده‌ها اطلاعات کاربران را محافظت و از دسترسی‌های غیر قانونی جلوگیری می‌کند.

در صورتی که تمایلی به دریافت ایمیل‌ها و خبرنامه های دیجی کالا ندارید، می توانید بر روی کلمه لغو عضویت در انتهای صفحه ایمیل کلیک کنید.

Privacy Controls

- Should data be collected or not?
- Who has permission to see it?

Going Forward

- Privacy & security are part of the same issue
- Analyzing usability is done the same way with privacy
- Keep the user in mind first

Privacy Policies & User Understanding

For users to control their privacy, they must understand privacy policies. Do they?

What We Know

- Most people do not read privacy policy.
  - about 16% said that they read them all the time.
- However, when people do read them, they do not necessarily understand them.
  - about half of the people who said they read them, said that they do not understand them.

How to Learn?

- Read privacy policies
- Discover through other sources

A quick experiment: Facebook apps

- Ask people what data they think apps can access
- Have them read privacy policy or watch a video
- Ask again

J. Golbeck, M.L. Mauriello. "User Perception of Facebook App Data Access: A Comparison of Methods and Privacy Concerns" Future Internet 2016, 8(2), 9; doi:10.3390/fi8020009

Results

- Every user underestimated what data could be accessed when they were first asked
- Every user improved after reading the privacy policy or watching the video
- The video led to greater improvements in user understanding

Implications

- Privacy policies are boring & hard to read
  - Poor usability
- They are also really important
- Are there more usable ways to convey the information in a privacy policy?

Informed Consent by Design

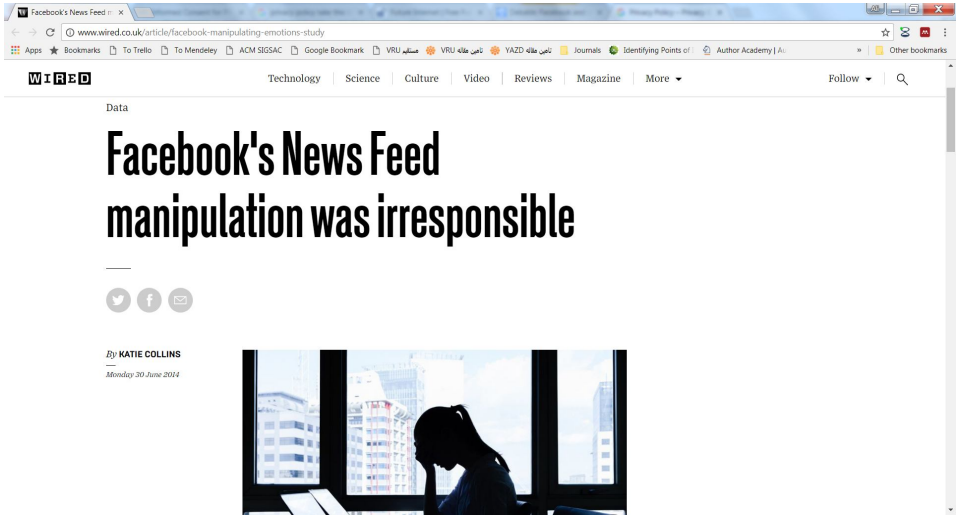
Friedman, Batya, Peyina Lin, and Jessica K. Miller. "Informed consent by design." Security and Usability (2005): 495-521

What is Informed Consent?

- Users understand what data is being collected & shared and they consent to how it is used.
- Six components
  - Disclosure
    - who, what, where, when, how
  - Comprehension
  - Voluntariness
  - Competence
  - Agreement
  - Minimal Distraction

Some Examples

- Google.com Privacy Policy
- Facebook Privacy Policy



Oh dear, Facebook. This weekend it emerged that the world's largest social network had conducted a study in which the company attempted to manipulate the emotional reaction of users by controlling the content that appeared in their News Feeds.

Conclusion

- Usable privacy requires informed consent from users
- They must understand how their data is used & agree to it being used that way
- These six components can help you analyze a system for informed consent

Five Pitfalls of Privacy

Lederer, Scott, et al. "Personal privacy through understanding and action: five pitfalls for designers." Personal and Ubiquitous Computing 8.6 (2004): 440-454.

Understanding

1. Obscuring potential information flow
2. Obscuring actual information flow

Action

3. Emphasizing configuration over action
4. Lacking coarse-grained control
5. Inhibiting established practice

Obscuring potential information flow

Obscuring actual information flow

Information Flow

- Types of information
- Kinds of observers
- Media through which info is conveyed
- Length of retention
- Potential for unintended disclosure
- Collection of metadata

Obscuring potential information flow

Obscuring actual information flow

Emphasizing configuration over action

- Privacy management should be part of natural workflow
  - Recall this same guideline about security

Lacking coarse-grained control

- Have an obvious, top-level control to turn sharing on and off

Inhibiting established practice

- What do users expect from other experiences?
  - Let them expect that here, too.
- Mental models, conventions

Conclusion

- Make it clear how information is being shared
- Make it easy & natural for users to control privacy
- Make the default practice match users' expectations

Inferring Personal Data

Assignment

- Do the same for two Privacy Policies in Farsi

That's all on the privacy.