



**RSA**Conference2019

San Francisco | March 4–8 | Moscone Center

**BETTER.**

SESSION ID: HUM-F01

# Designing Effective Security UX: If It's Not Usable, It's Not Secure

**Ranjeet Kumar, Tayi**

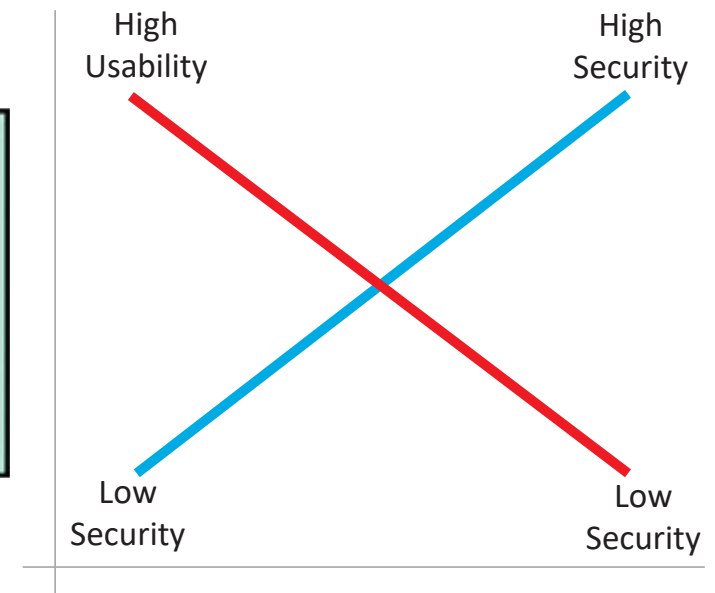
UX lead (Data Security Group)

Informatica

@ranzeeth

#RSAC

# Security and Usability: Are they opposite?





security



privacy





security



privacy



Confidentiality



Integrity



Availability



Data Usage



Fair Information Policy Practice



# Usability



Effectiveness



Efficiency



Accuracy



Learnability



Memorability



Satisfaction



Security / Privacy



Usability



Usable Security & Privacy





Security / Privacy



Usability



Usable Security & Privacy

## Human Factors

Humans are a secondary constraint to Security and Privacy constraints

Humans are a primary constraint, Security and Privacy rarely considered

Humans Factors and Security are both primary constraints

Human considered primarily in their role as adversaries / attackers

Concerned about human errors but not human attackers

Concerned about both normal users and adversaries

Involves threat models

Involves task models, mental models, cognitive models

Involves threat models and task models, mental models, etc.

Focus on security metrics

Focus on usability metrics

Considers usability and security metrics together

Focus on security testing

Focus on user studies

User studies often involve deception + adversary

# 5 Key approaches to make usable privacy and security BETTER.

1



Understanding  
the Users,  
Context, and  
Purpose

2



Analyze the  
Risks  
Involved

3



Reducing User  
Burden

4



Educating the  
User

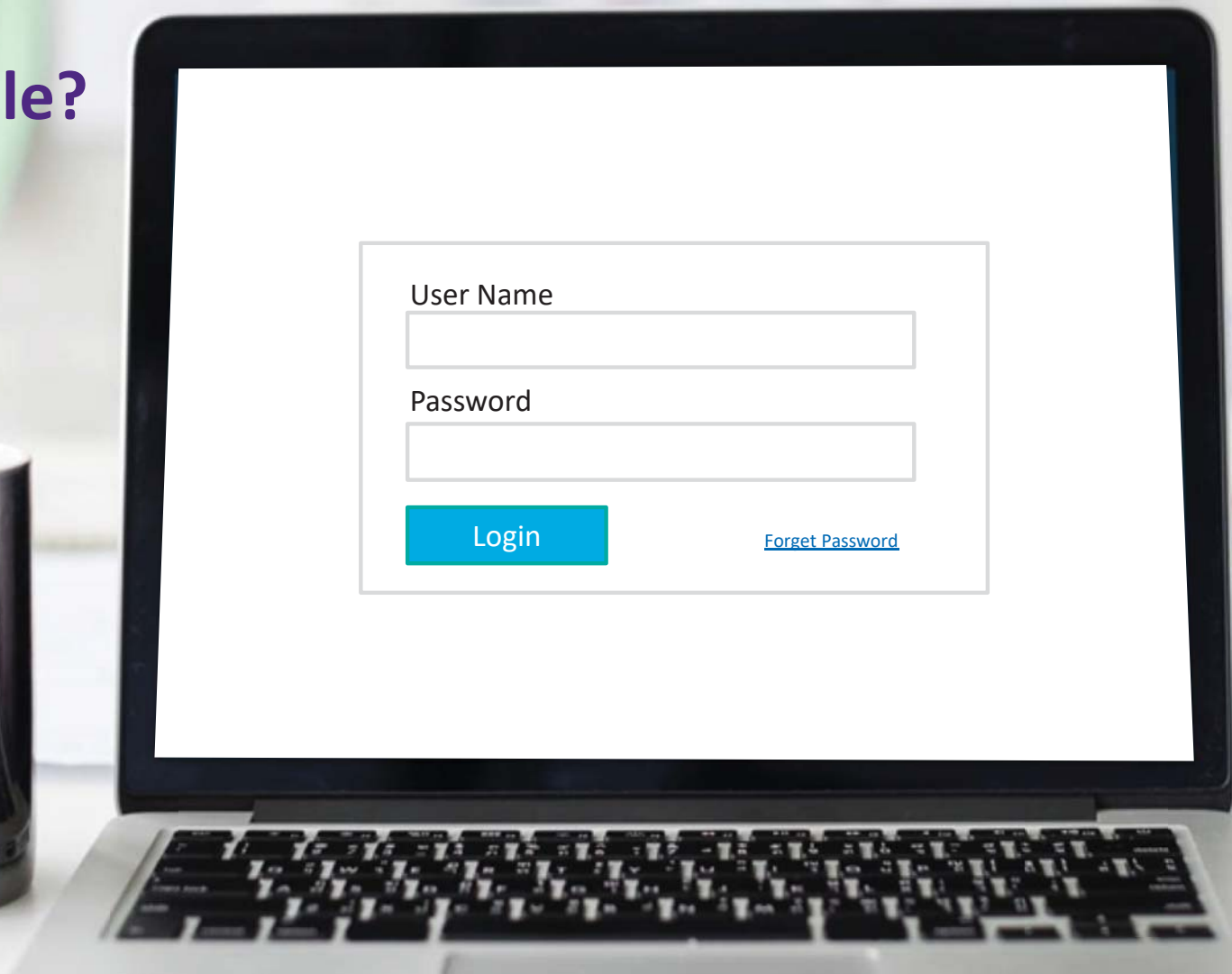
5



Measuring  
Security and  
Usability



Does this  
look simple?

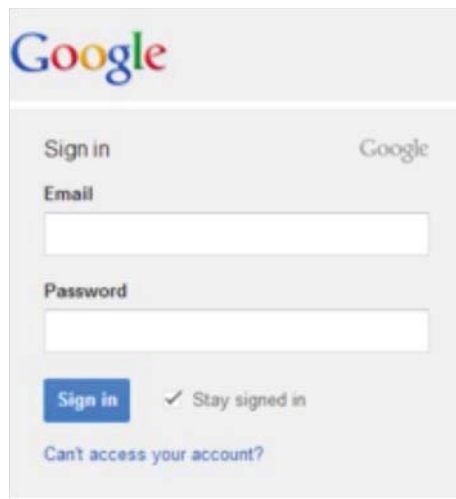


User Name

Password

Login

[Forget Password](#)



Google

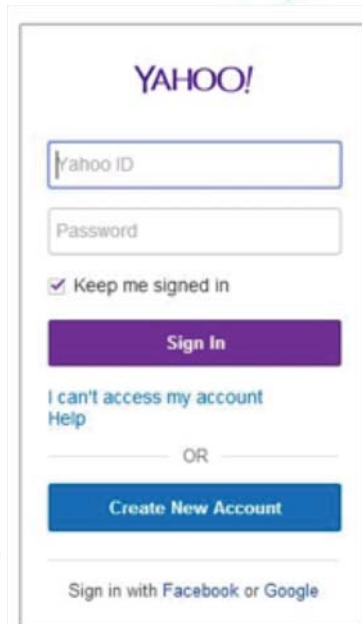
Sign in

Email

Password

[Sign in](#) ☒ Stay signed in

[Can't access your account?](#)



YAHOO!

Yahoo ID

Password

☒ Keep me signed in

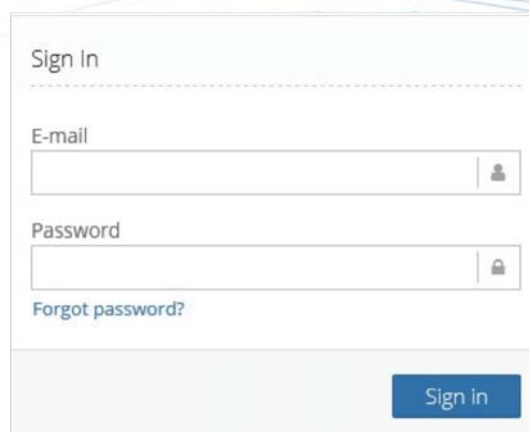
[Sign In](#)

[I can't access my account](#)  
[Help](#)

OR

[Create New Account](#)

[Sign in with Facebook or Google](#)



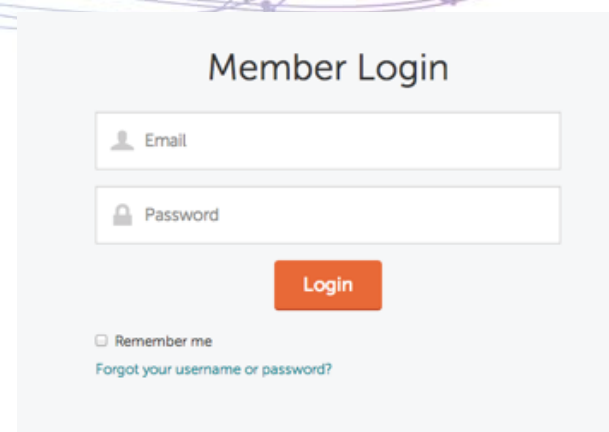
Sign In

E-mail

Password

[Forgot password?](#)

[Sign in](#)



Member Login

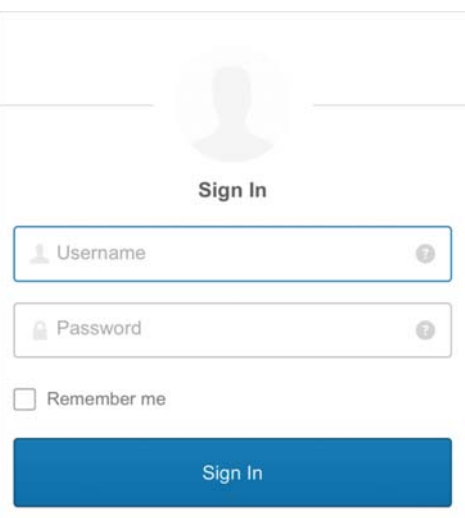
Email

Password

[Login](#)

☐ Remember me

[Forgot your username or password?](#)



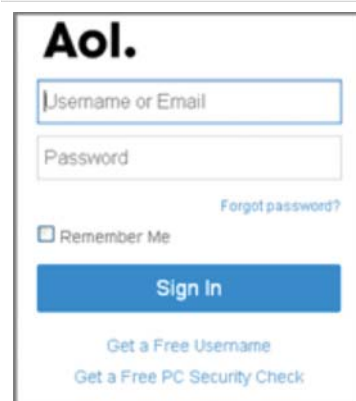
Sign In

Username

Password

☐ Remember me

[Sign In](#)



Aol.

Username or Email

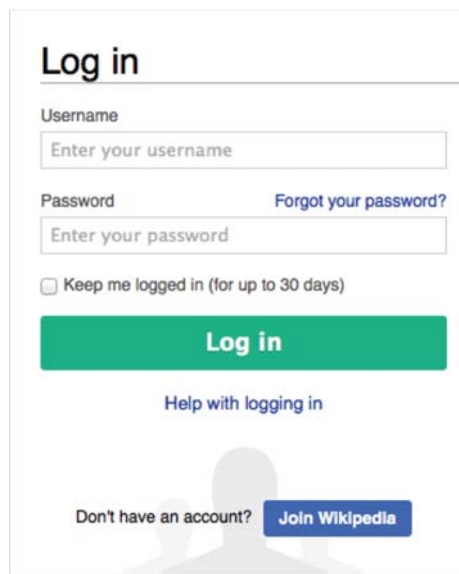
Password

[Forgot password?](#)

☐ Remember Me

[Sign In](#)

[Get a Free Username](#)  
[Get a Free PC Security Check](#)



Log in

Username

Enter your username

Password

[Forgot your password?](#)

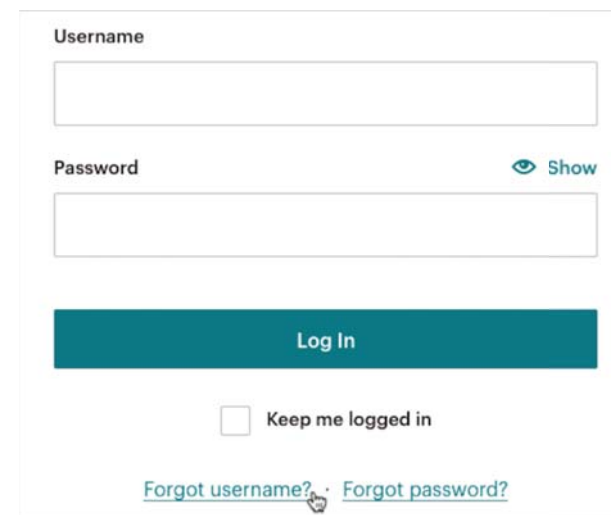
Enter your password

☐ Keep me logged in (for up to 30 days)

[Log in](#)

[Help with logging in](#)

Don't have an account? [Join Wikipedia](#)



Username

Password

[Show](#)

[Log In](#)

☐ Keep me logged in

[Forgot username?](#) [Forgot password?](#)

The following rules apply to all passwords:

- The password must be at least 8 characters long.
- The password **must** contain at least:
  - one alpha character [a-zA-Z];
  - one numeric character [0-9];
  - one special character from this set:  
! @ \$ % ^ & \* ( ) - \_ = + [ ] ; ' " , < . > / ?
- The password **must not**:
  - contain spaces;
  - begin with an exclamation [!] or a question mark [?];
  - contain your login ID.
  - Contain your registered email address
- The password cannot contain repeating character strings of 3 or more identical characters. E.g. "1111" or "aaa"
- The sequence of the first 3 characters cannot be in your login ID.
- The first 8 characters cannot be the same as in your previous password.
- Passwords are treated as case sensitive.

Password

.....

Incorrect username and/or password. You modified your password 241 days ago.

• Must contain at least 14 characters

• Must not end with a digit

• Must not start with a digit

• Must meet at least 3 of the following requirements:

• Must contain at least 1 digit

• Must contain at least 1 lowercase letter

• Must contain at least 1 special character

• Must contain at least 1 uppercase letter

• Must contain at least 1 Unicode character

✓ Must not contain 3 or more identical characters in a row

✓ Must not contain any part of your username

Password

.....

Show password

Password must contain numbers

Password must contain uppercase letters

Password must have at least one @#\$ symbol

Length must be greater than 8 characters

Password should not contain strings

Password must not contain repetitions

The following rules will be verified once the password character

• Must not contain words from the list of disallowed words

• Must differ from your current password by more than the last

• Must not repeat any of your previous 24 passwords

- Contain from 8 to 16 characters
- Contain at least 2 of the following 3 characters: uppercase alphabetic, lowercase alphabetic, numeric
- Contain at least 1 special character (e.g., @, #, \$, %, & \*, +, =)
- Begin and end with an alphabetic character
- Not contain spaces
- Not contain all or part of your UserID
- Not use 2 identical characters consecutively
- Not be a recently used password

The value in the field "New Password" is invalid. Please refer to the password rules.

- It must contain between 8 and 20 characters. Use only characters from the following set: ! # \$ % & ( ) \* + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ] \_ ` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
- It must contain at least 1 lowercase letter(s) (abcdefghijklmnopqrstuvwxyz).
- It must contain at least 1 capital letter(s) (ABCDEFGHIJKLMNOPQRSTUVWXYZ).
- It must contain at least 1 numeric character(s) (0123456789).
- It must not contain more than 2 identical consecutive characters (AAA, iiiii, \$\$\$\$\$ ...).
- It must not contain your user name.
- It must not contain your email address.
- It must not contain your first name.
- It must not contain your last name.

password  
123456

## 2018's Worst Passwords

- 1.123456
- 2.password
- 3.123456789
- 4.12345678
- 5.12345
- 6.111111
- 7.1234567
- 8.sunshine
- 9.qwerty
- 10.iloveyou

SplashData

## STEP 2: Password

Password

3rd

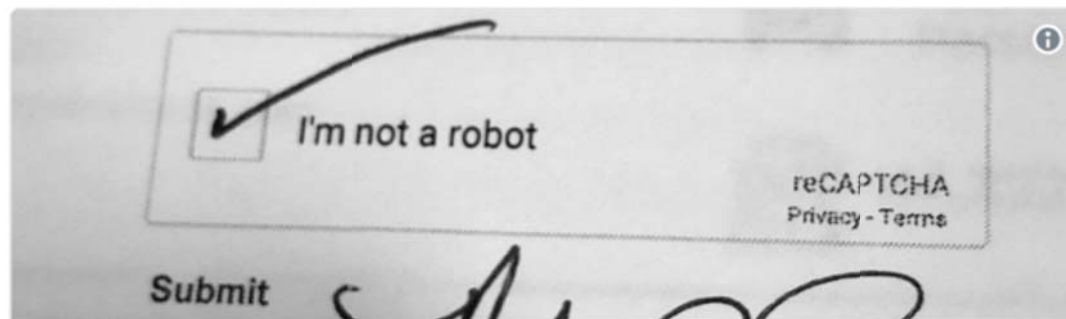
7th

8th

Please enter the **third**, **seventh** and **eighth** characters from your password.

Login

[Forgot your password?](#)



**Marci Robin** ✓  
@MarciRobin



I bought a car today, and the dealership had me check off — with a pen, on paper — that I'm not a robot.

♥ 82.4K 6:38 PM - May 19, 2018

💬 27.4K people are talking about this





# 1. Understanding the user, context, and purpose



- Know your users. Each user is different including their skills, behaviors and user journeys.
- Know your user context. Environmental, physiological, and situational concerns that influence them.
- What is their purpose? Why are they doing? What are their goals and motivations?
- Identify, Authenticate and Authorize the right user.

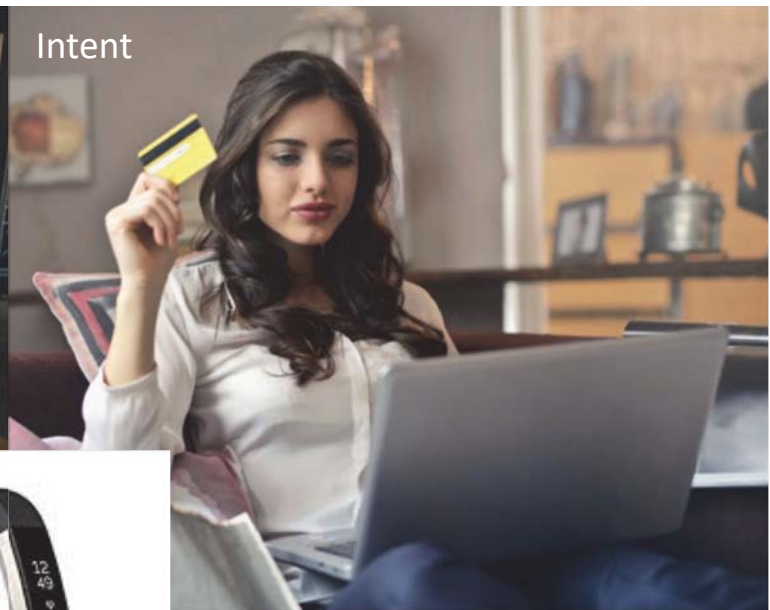
Activity



Context



Intent



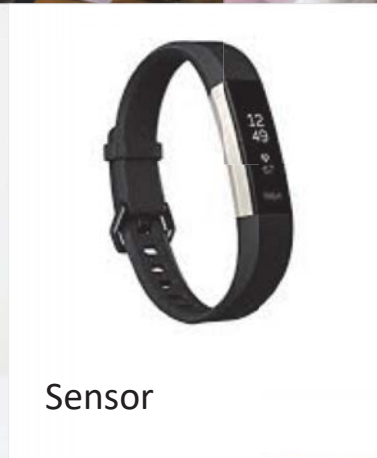
Time



Sentiment



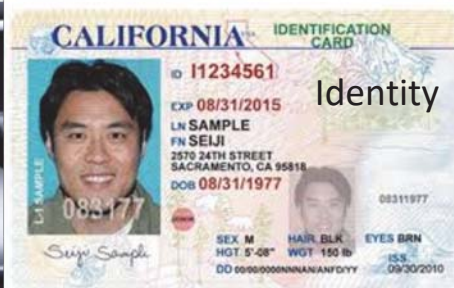
Sensor



Location



Identity



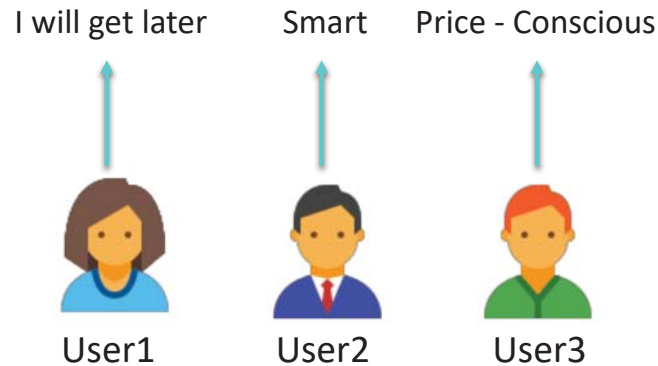
Language



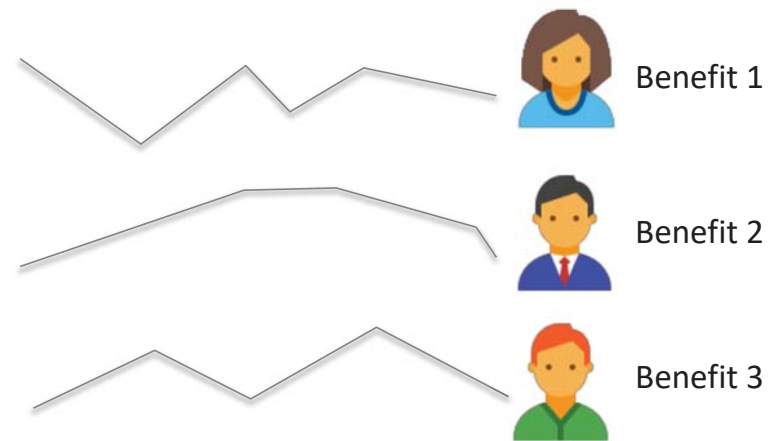
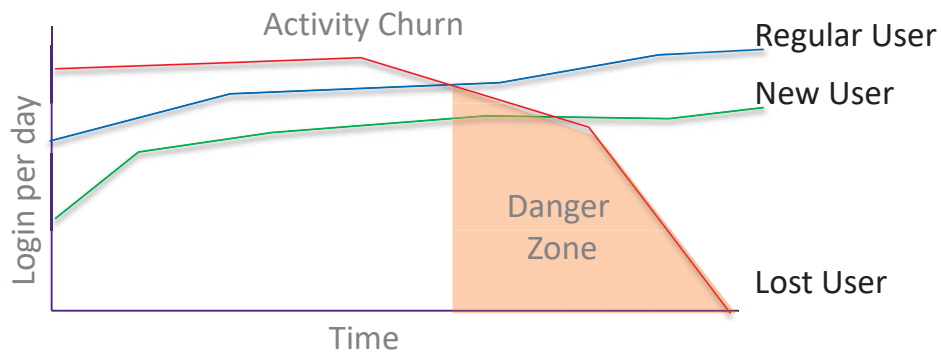
Proximity



1. Purchasing behavior
2. Benefits sought
3. Customer journey stage
4. Usage
5. Occasion or timing
6. Customer Satisfaction
7. Customer Loyalty
8. Interest
9. Engagement-level
10. User status

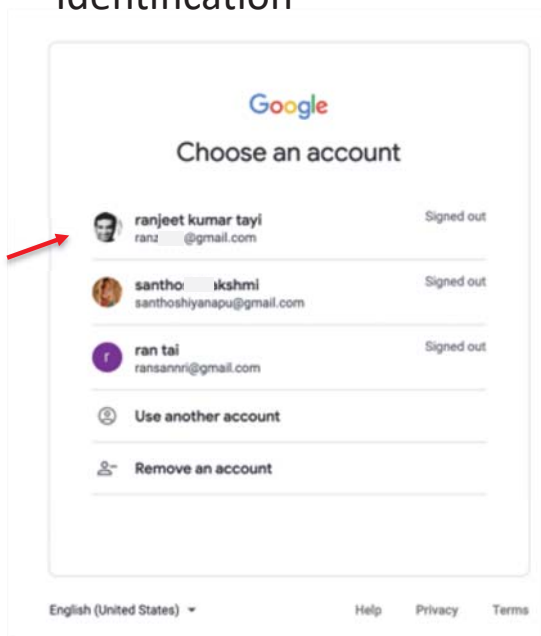


User Satisfaction










## Identification



Google

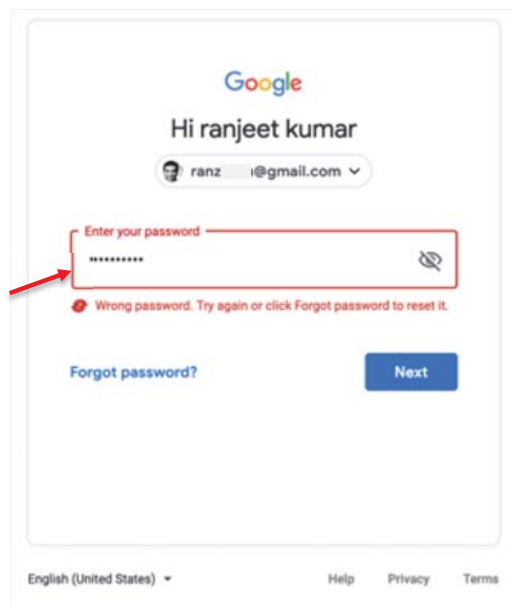
Choose an account

-  **ranjeet kumar tayi**  
ranz...@gmail.com Signed out
-  **santhosh kshmi**  
santhoshianapu@gmail.com Signed out
-  **ran tai**  
ransannri@gmail.com Signed out
-  Use another account
-  Remove an account

English (United States) ▾ Help Privacy Terms


A red arrow points to the first account entry, 'ranjeet kumar tayi'.

## Authentication



Google

Hi ranjeet kumar

 ranz...@gmail.com ▾

Enter your password

.....

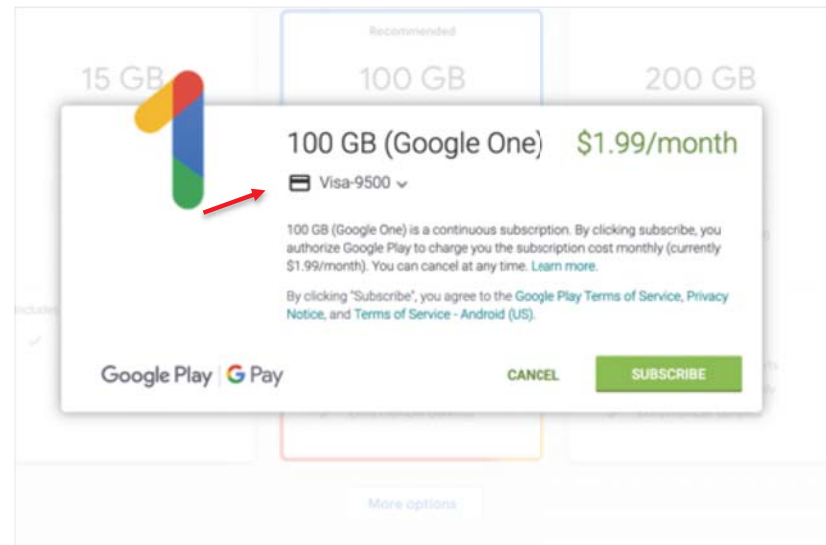
Wrong password. Try again or click [Forgot password](#) to reset it.

[Forgot password?](#) [Next](#)

English (United States) ▾ Help Privacy Terms

A red arrow points to the password input field.


## Authorization



15 GB 100 GB 200 GB


Recommended

100 GB (Google One) \$1.99/month

 Visa-9500 ▾

100 GB (Google One) is a continuous subscription. By clicking subscribe, you authorize Google Play to charge you the subscription cost monthly (currently \$1.99/month). You can cancel at any time. [Learn more](#).

By clicking "Subscribe", you agree to the [Google Play Terms of Service](#), [Privacy Notice](#), and [Terms of Service - Android \(US\)](#).

Google Play  [CANCEL](#) [SUBSCRIBE](#)

[More options](#)

A red arrow points to the Google One logo.

## 2. Analyze the risks involved



- Analyze different risks and impacts. Accuracy and understandability are key.
- Create a threat model and stack rank risks for mitigation.
- Communicate at the right level (right abstraction/aggregation based on target audience/role)
- Intuitive colors, icons & metaphors to communicate risks.

### Top Users

Daan Lindhout	12	<div><div></div><div></div><div></div></div>
Adams Smith	11	<div><div></div><div></div><div></div></div>
Mike Ben	10	<div><div></div><div></div><div></div></div>
Jonathan Adams	9	<div><div></div><div></div><div></div></div>
Mallory Hill	8	<div><div></div><div></div><div></div></div>



### Sensitive Records

Observed: 6.2K | Expected 120

### Sensitive Fields

Observed: 113 | Expected 20

### Data Domains

Observed: 17 | Expected 3

### Location

Observed: Boston, USA

### Sensitive Events

Observed: 28 | Expected

### Time of Day

Observed: 10:10PM

### Data Stores

Observed: 2 | Expected 1

### Day of Week

Observed: Sunday

### Unexpected Data Store

Observed: Oracle\_CRM

80

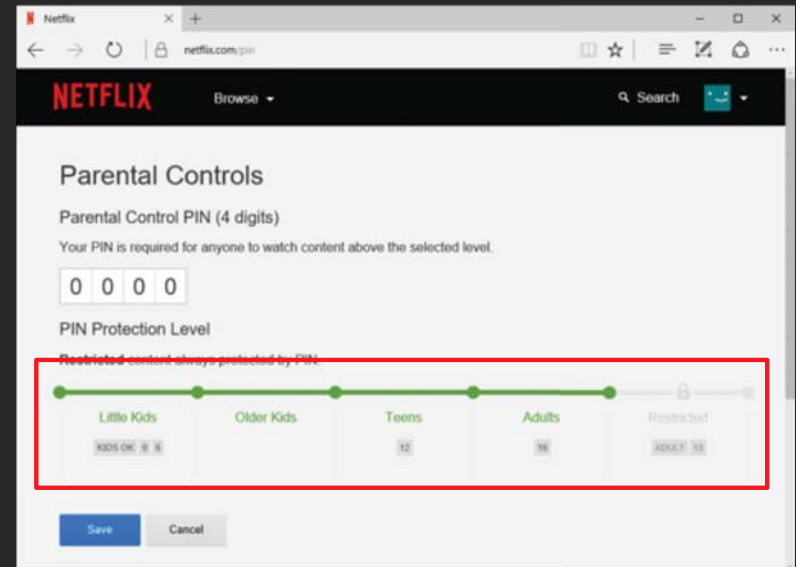
**Adam Smith**

Director, Sales  
Redwood City, USA

Risk Score: 80

Anomaly Detection:








## Security Checkup

2 issues found

### Recent security events

#### New sign-in on Windows


 Near Fremont, CA, USA  
February 17, 6:41 PM

Was this you?

No, it wasn't me

Yes

#### New sign-in on Motorola moto g(6)

 Near Fremont, CA, USA  
February 17, 1:38 PM

Was this you?

No, it wasn't me

Yes

Show others (3)

 Your devices  
4 signed-in devices

 Sign-in & recovery  
4 verification methods

 Third-party access  
6 apps with access to your data

[Continue to your Google Account](#)

Your Credit Score



#RSAC

Take a look at your credit factors to see how you could improve.

#### Hard inquiries

●○○ LOW IMPACT

1

Number of times you've applied for credit

[View details →](#)

#### Total accounts

●○○ LOW IMPACT

9

Total open and closed accounts

[View details →](#)

#### Credit age

●●○ MEDIUM IMPACT

2 YRS 11 MOS

Average age of your open accounts

[View details →](#)

#### Derogatory marks

●●● HIGH IMPACT

0

Collections, tax liens, bankruptcies or civil judgments on your report

[View details →](#)

#### Credit card use

●●● HIGH IMPACT

4% ↑

How much credit you're using compared to your total limits

[View details →](#)

#### Payment history

●●● HIGH IMPACT

100%

Percentage of payments you've made on time

[View details →](#)



⚠ Not secure example.com



🔒 Secure https://www.example.com

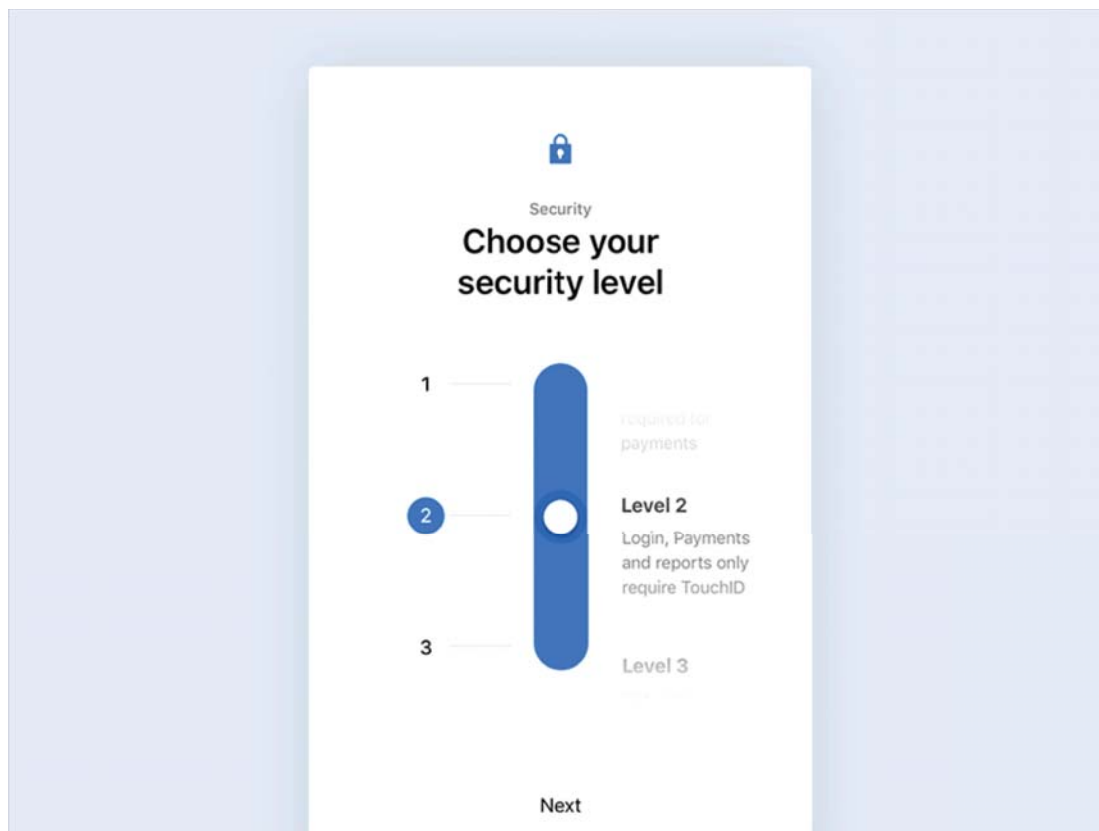
RSA<sup>®</sup>Conference2019





### 3. Reducing user burden

- Provide flexibility but Don't overwhelm.
- Provide good defaults with the right level of protection. (80/20 rule)
- Understandable levers (what can you control, how and impacts?)
- Provide right security controls with good error handling and protection.



A security level selection interface. At the top is a blue padlock icon and the word "Security". Below is the heading "Choose your security level". A vertical blue slider is positioned between three levels. Level 1 is at the top, Level 2 is in the middle with a white circle, and Level 3 is at the bottom. To the right of the slider, text describes each level: Level 1 is "required for payments", Level 2 is "Login, Payments and reports only require TouchID", and Level 3 is "Login, Payments and reports only require TouchID". At the bottom is a "Next" button.

Security

### Choose your security level

1 — required for payments

2 — Level 2  
Login, Payments and reports only require TouchID

3 — Level 3  
Login, Payments and reports only require TouchID

Next



A checkout summary and action area. It shows the subtotal for one item as \$14.19. There is a checkbox for "This order contains a gift". Below are three buttons: "Proceed to checkout", "or 1-Click Checkout", and "Buy all items with 1-Click" which includes a 1-Click icon.

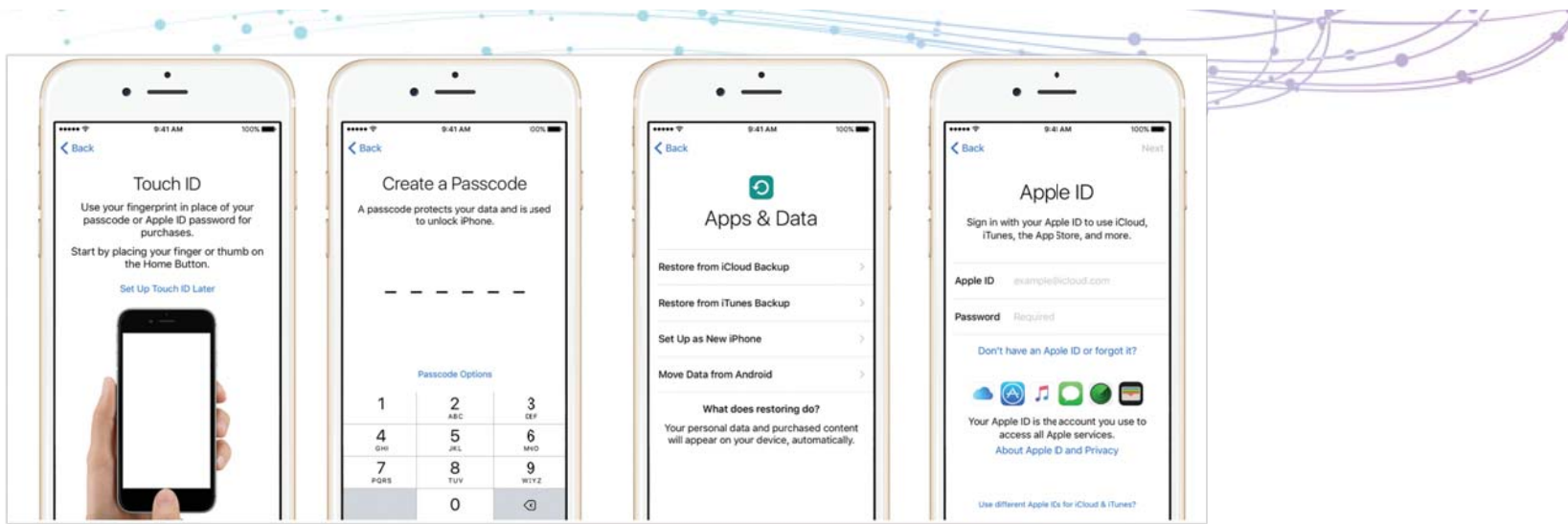
**Subtotal (1 item): \$14.19**

☐ This order contains a gift

Proceed to checkout

or 1-Click Checkout

 Buy all items with 1-Click



## Sign Out of All Devices

Are you sure you want to sign out of this Netflix account on all devices?

This may take up to 8 hours to take effect on all devices and affects all profiles in this account.

Sign Out

Cancel

mail.google.com says:

It seems like you forgot to attach a file.

You wrote "I have attached" in your message, but there are no files attached. Send anyway?

Cancel

OK

## Error

somemail@gmailcon



Did you mean somemail@gmail.com?

Phone Numeber

( ) -

Creadit Card Number

- - - -

Date

mm/dd/yyyy

SSN

- - -



## 4. Educating the user



- Integrated training to understand the impact.
- Provide the right affordances that signal the parts that are relevant to security.
- Provide transparency and clarity of what data is collected, for what purpose and what users get out of it.
- Use simple vocabulary to communicate errors, warnings, help, etc.



## Get started with a free account

Find your people. Engage your customers. Build your brand. Do it all with Mailchimp's marketing tools. Already have an account? [Log in](#)

Email

ExcitedNewUser@Yay.com

Username

ExcitedNewUser

Password

Show

- One lowercase character
- One uppercase character
- One number
- One special character
- 8 characters minimum

Get Started!

By clicking this button, you agree to Mailchimp's [Anti-spam Policy & Terms of Use](#).

#RSAC

Password

Hide

- One lowercase character
- One uppercase character
- One number
- One special character
- 8 characters minimum



Password

Hide

Great1

- One lowercase character
- One uppercase character
- One number
- One special character
- 8 characters minimum



Requirements update as you type

Password

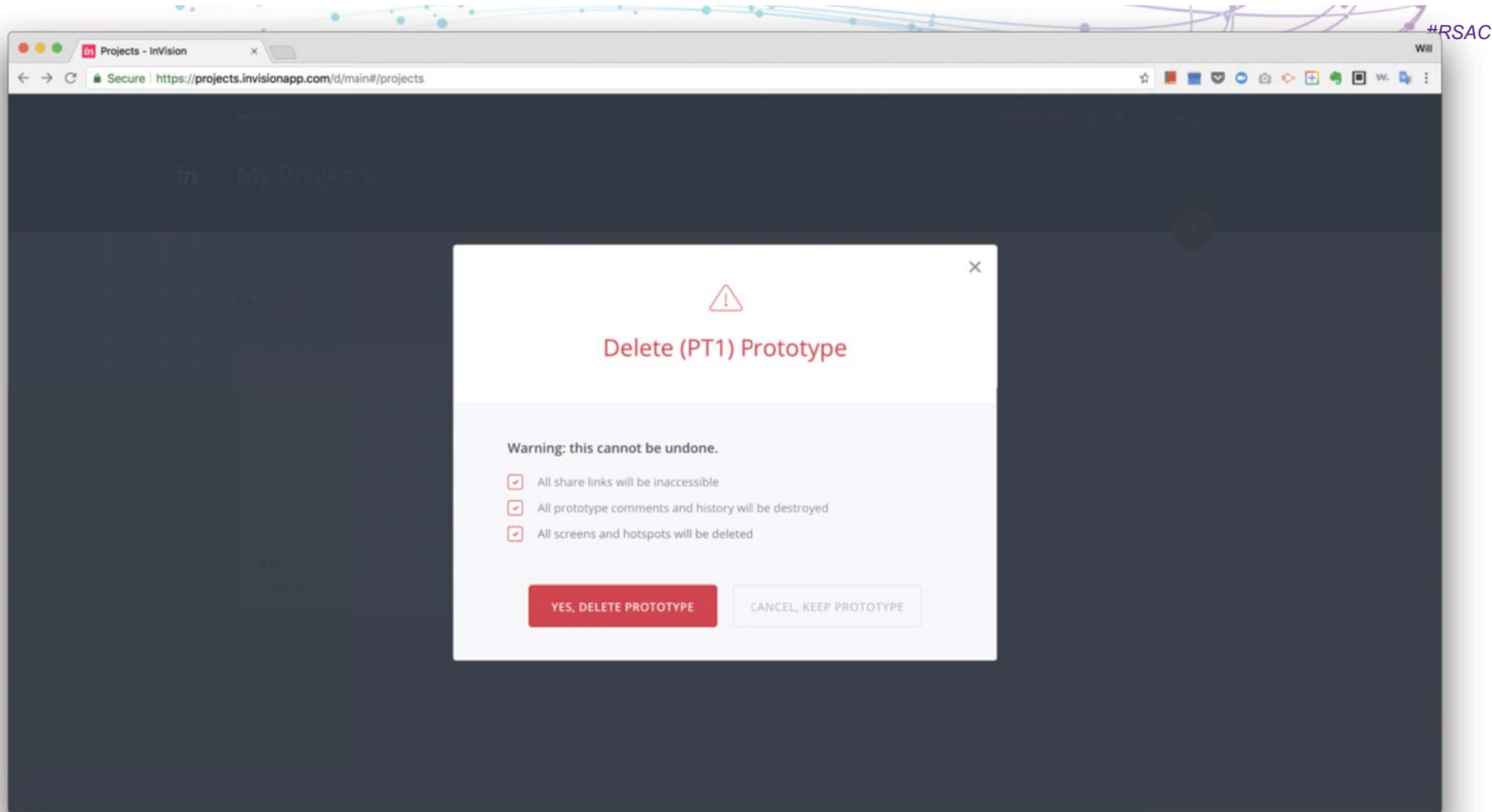
Hide

Great123!

Your password is secure and you're all set!



RSA<sup>®</sup>Conference2019



#RSAC

RSAConference2019

Effective May 8, 2018  
Our Privacy Policy has been updated. Click here to see a [summary of changes](#).

See a [guided tour](#) of the main changes.

## Your Privacy Matters

LinkedIn's mission is to connect the world's professionals to allow them to be more productive and successful. Central to this mission is our commitment to be transparent about the data we collect about you, how it is used and with whom it is shared.

This Privacy Policy applies when you use our Services (described below). We offer our users choices about the data we collect, use and share as described in this Privacy Policy, [Cookie Policy](#), [Settings](#) and our [Help Center](#).

 [View our Privacy Policy video](#)

### Introduction

Our registered users ("Members") share their professional knowledge and professional insights, post and view business and career opportunities. Content and data on some members ("Visitors").

We use the term "Designated Countries" to refer to countries in the European Economic Area (EEA), and Switzerland.

**Services**

This Privacy Policy applies to LinkedIn.com, LinkedIn-branded Learning and other LinkedIn-related sites, apps, communication including off-site Services, such as our ad services and the "Ag LinkedIn" plugins, but excluding services that state that they are not subject to this policy.

We have changed which LinkedIn entity acts as the data controller for the data of some of our Members and Visitors. LinkedIn Corporation will be the data controller for those who live outside of the "Designated Countries" while LinkedIn Ireland will remain the data controller for those that live in the Designated Countries. We use the term "Designated Countries" to refer to countries in the European Union (EU), European Economic Area (EEA), and Switzerland.

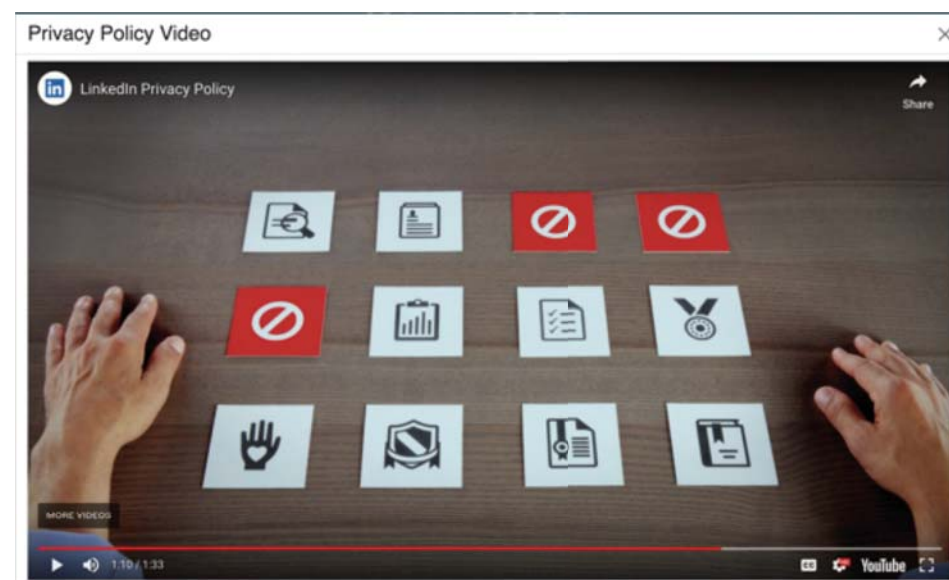
[Previous](#) [Next](#)

Table of Contents:

- [Introduction](#)
- [Data We Collect](#)
- [How We Use Your Data](#)
- [How We Share Information](#)
- [Your Choices & Obligations](#)
- [Other Important Information](#)



#RSAC



## 5. Measuring security and usability

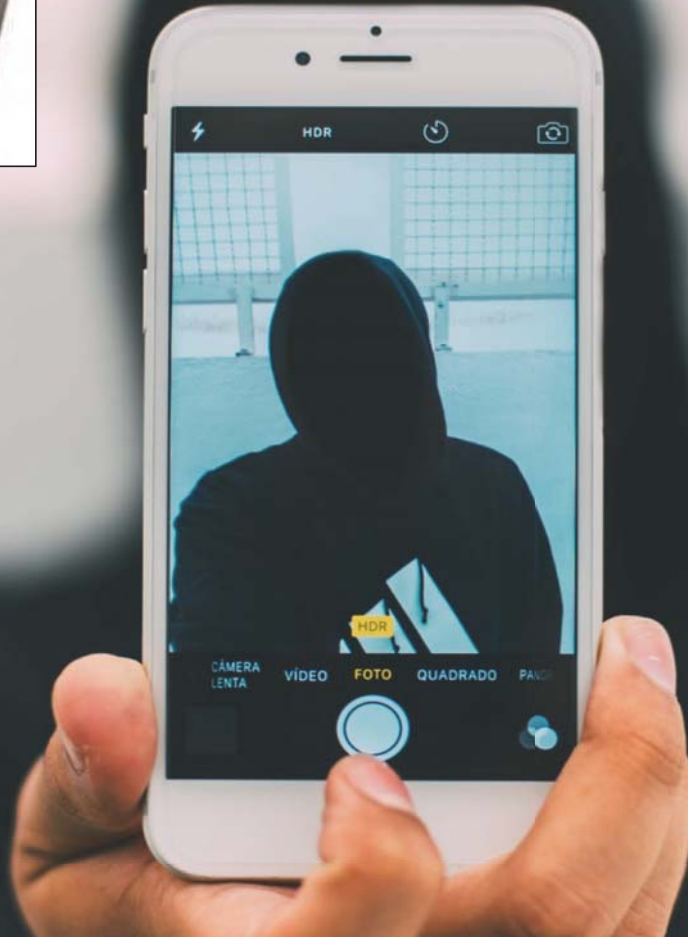


- Adversaries / Threat actors as another user persona.
- Define user journey maps even for threat actors.
- Focus on both usability metrics and security metrics together.
- Discover the right balance for usability & security based on user context.





Threat Actor  
**Persona**

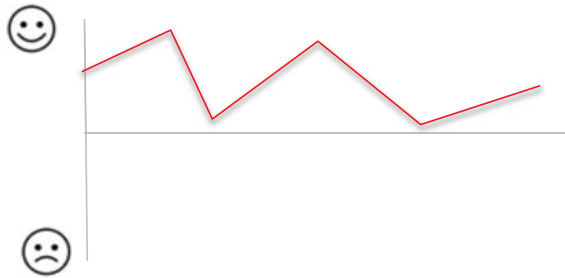


- Name: Unknown  
Occupation: Hacker  
Location: Unknown  
Age: 25-45 Years  
Goals: Hack the systems to steal sensitive information.  
Look for loopholes so that he can break things easily.  
Fear: Get arrested and go to Jail  
Motivation: To remain anonymous and illegally access confidential systems to make money or defame organizations  
Skills: Expert in hacking complex systems  
Experiments on various systems and technologies.  
Expert in hiding his identity & being anonymous.  
Tools: Multiple computers, hacking tools, debug tools, cheat code, virus generators, etc.

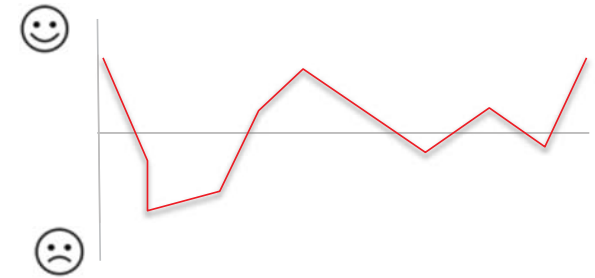
## When user...



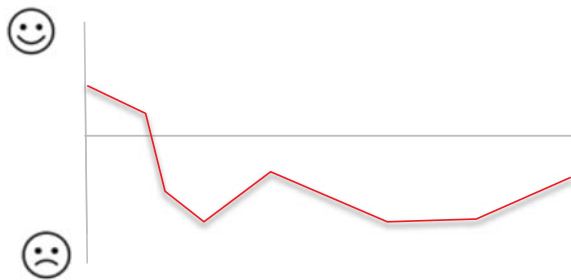
enters right user name  
and password



returns session before it  
expired



returns after session  
expired



enters right username, but  
cant recall password



account gets locked due  
to wrong password



cant recall either  
username or password

# Security and usability metrics

## Security Testing

System hardening

Application Whitelisting

Log Collection

Monitoring

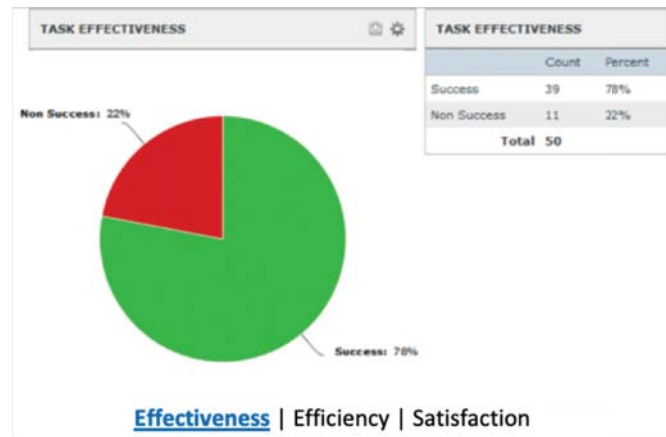
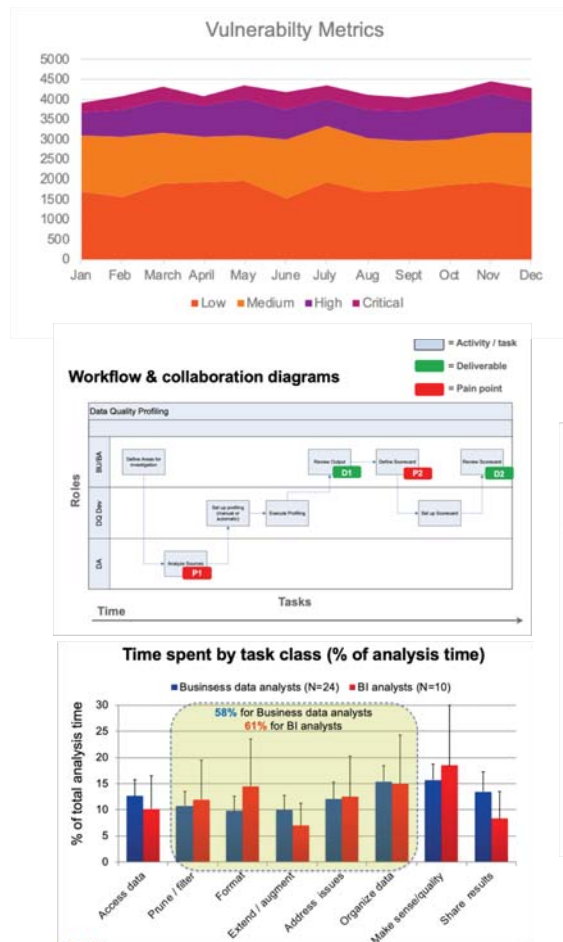
Vulnerability Scans

Unit Tests

Dynamic Analysis

Penetration Testing

Other Security Testing



## Usability Testing

Task Analysis

User Studies

Customer Journey Maps

Formative & Summative Usability Studies

Heuristic Evaluations

Eye Tracking

A/B Testing

Design Validation

Other User Studies



## Recap: Making security & privacy BETTER.

1



Understanding  
the Users,  
Context and  
Purpose

2



Analyze the  
Risks  
Involved

3



Reducing User  
Burden

4



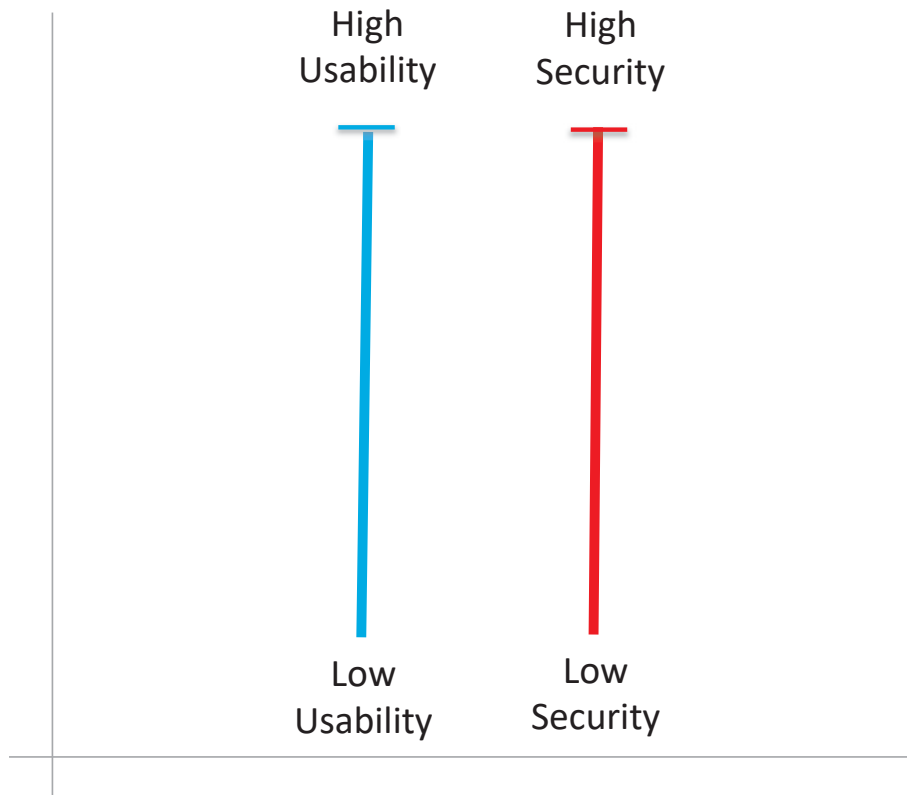
Educating the  
User

5



Measuring  
Security and  
Usability

## Finding the right balance



- Better user engagement
- Better secure apps
- Better credibility
- Better compliance
- Better brand value
- Better sales

**Consider usability  
when you invest in security.**

**If It's Not Usable, It's Not Secure**



## Apply What You Have Learned Today

- Next week you should:
  - Talk to your design team and learn more about usable security & privacy.
- In the first three months following this presentation you should:
  - Know your users, behaviors, context, journeys, and purpose.
  - Partner with your design team and do analysis on usability and security.
- Within six months you should:
  - Plan for a design thinking workshop with your design team to explore ideas and concepts to improve both usability and security.
  - Create an implementation project to implement and validate solutions.



Photos: pexels.com

Lets design things  
**BETTER.**



Ranjeet Tayi  
[www.ranjeeth.com](http://www.ranjeeth.com)

   [@ranzeeth](https://twitter.com/ranjeeth)