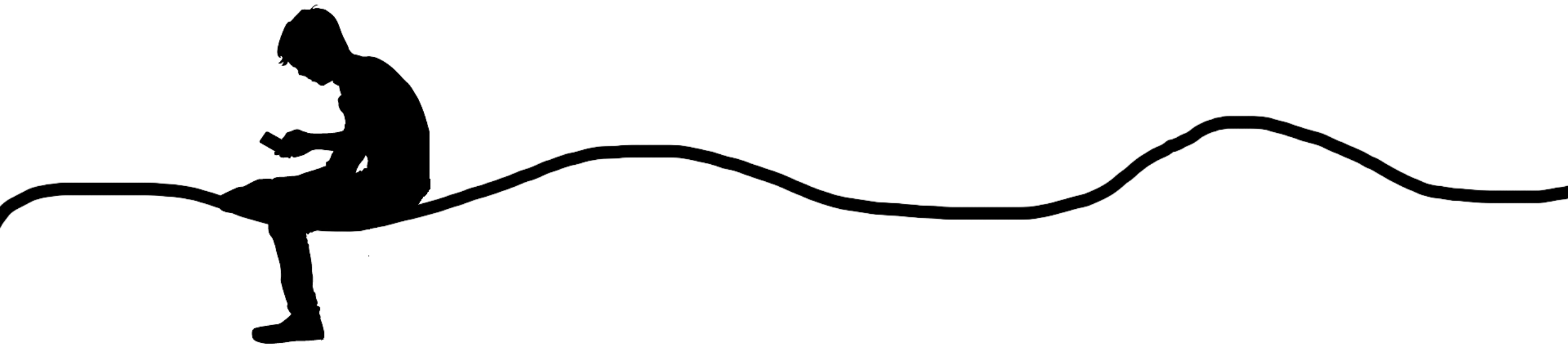
RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SEM-M01

Measuring the Rationality of Security Behavior

Elissa Redmiles

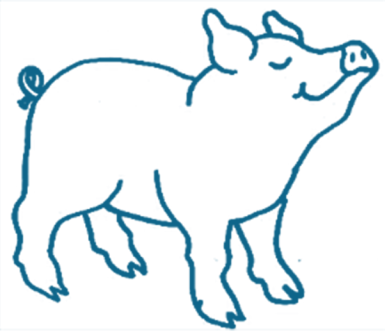
PhD Candidate, University of Maryland
eredmiles@cs.umd.edu



People must make a variety of security decisions

The decisions they make may app[illegible]rrational

Do users behave insecurely because they don't care, behave randomly, or because it's not worth it?



The user is going to pick
dancing pigs over **security** every time.

-- McGraw and Felten / Schneier

The user is rationally ignoring security advice
because **the costs outweigh the benefits.**

-- Herley, 2009

Controlled experiments to measure degree of rationality

Online experimental system: simple bank account
Account holds study compensation
Account has explicit risk of being hacked

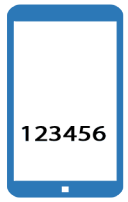
At the end of the study, you will be compensated with the amount of money left in your study bank account. You begin the study with $5 in your bank account. You must login once a day, otherwise you will lose all of the money in your account. If you are hacked, you will also lose all of the money in your account.

Studies indicate that 20% of users will have their study accounts hacked over the course of the study.

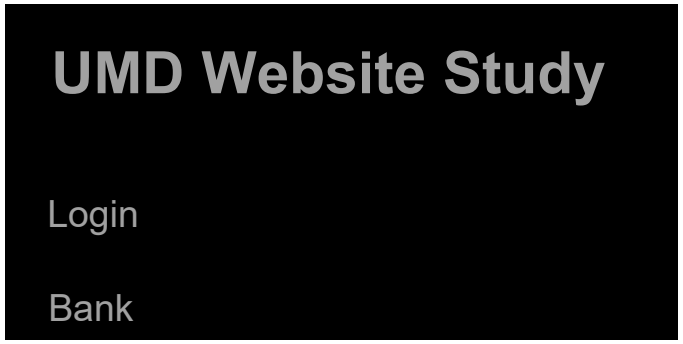
H = 1%, 20%, or 50%

Controlled experiments to measure degree of rationality

Online experimental system: simple bank account
Account holds study compensation
Account has explicit risk of being hacked



Users make a security choice: enable/don't enable 2FA
2FA lowers risk of hacking
Increases cost (time and effort) to complete study



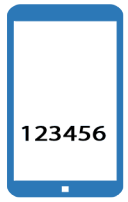
Would you like to enable two factor authentication using your phone number?
Two factor authentication will protect you from hacking 90% of the time.

P = 50% or 90%

Use Two Fac Continue Without Two Fac

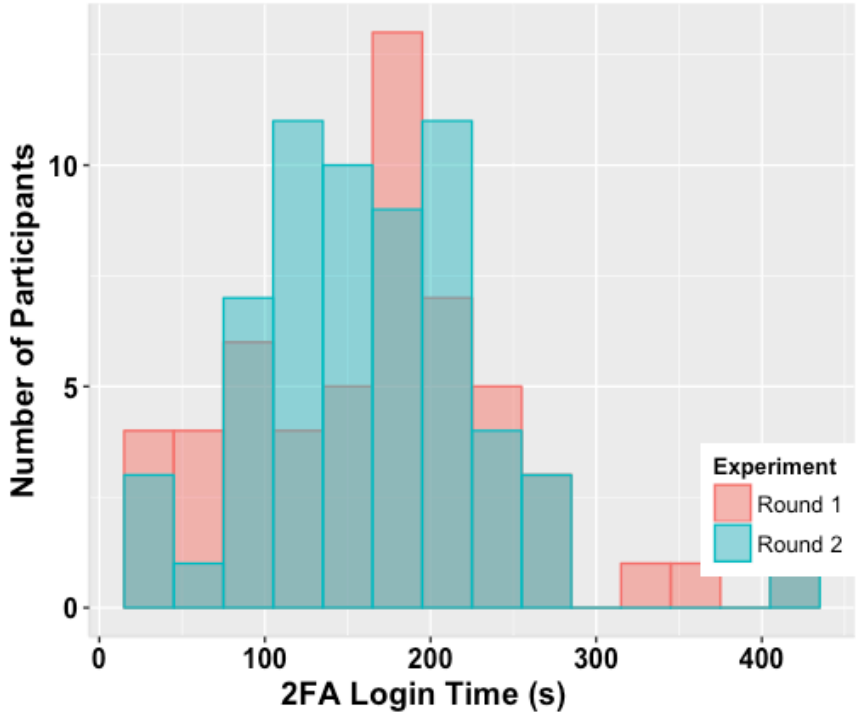
Controlled experiments to measure degree of rationality

Online experimental system: simple bank account
Account holds study compensation
Account has explicit risk of being hacked

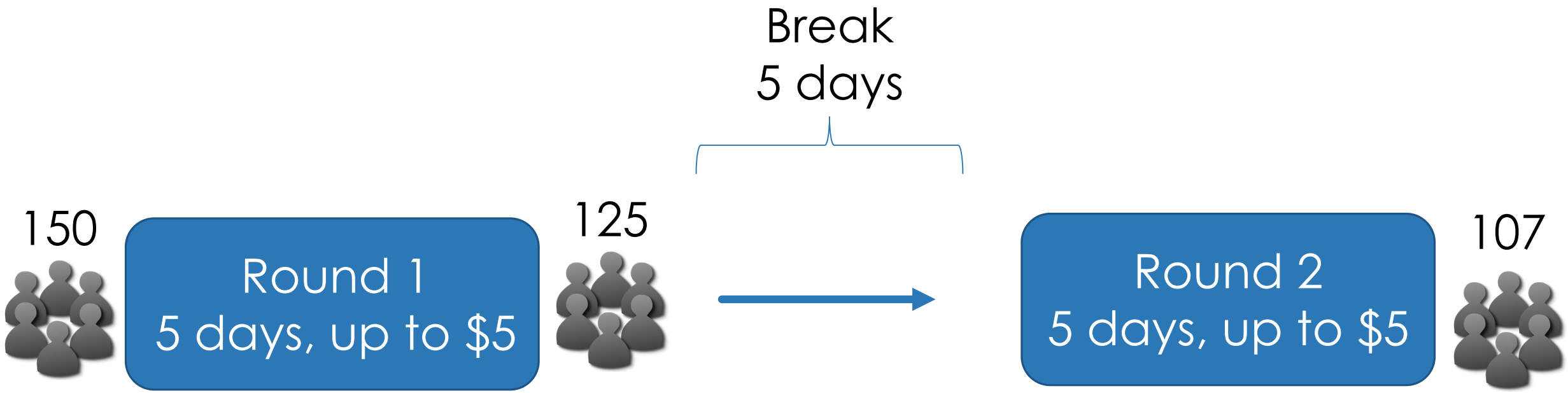


Users make a security choice: enable
2FA lowers risk of hacking
Increases cost (time and effort) to comple

Participants stand to lose money
Amazon Mechnical Turk (Crowd Worker) participants
Earn money from small time increments



Observed 2FA behavior twice to account for learning



RSAConference2019

Only 52% of participants enabled 2FA

After being shown risk & protection information

Rational behavior: benefit of behavior outweighs cost

Cost of 2FA

<

Protection offered by 2FA

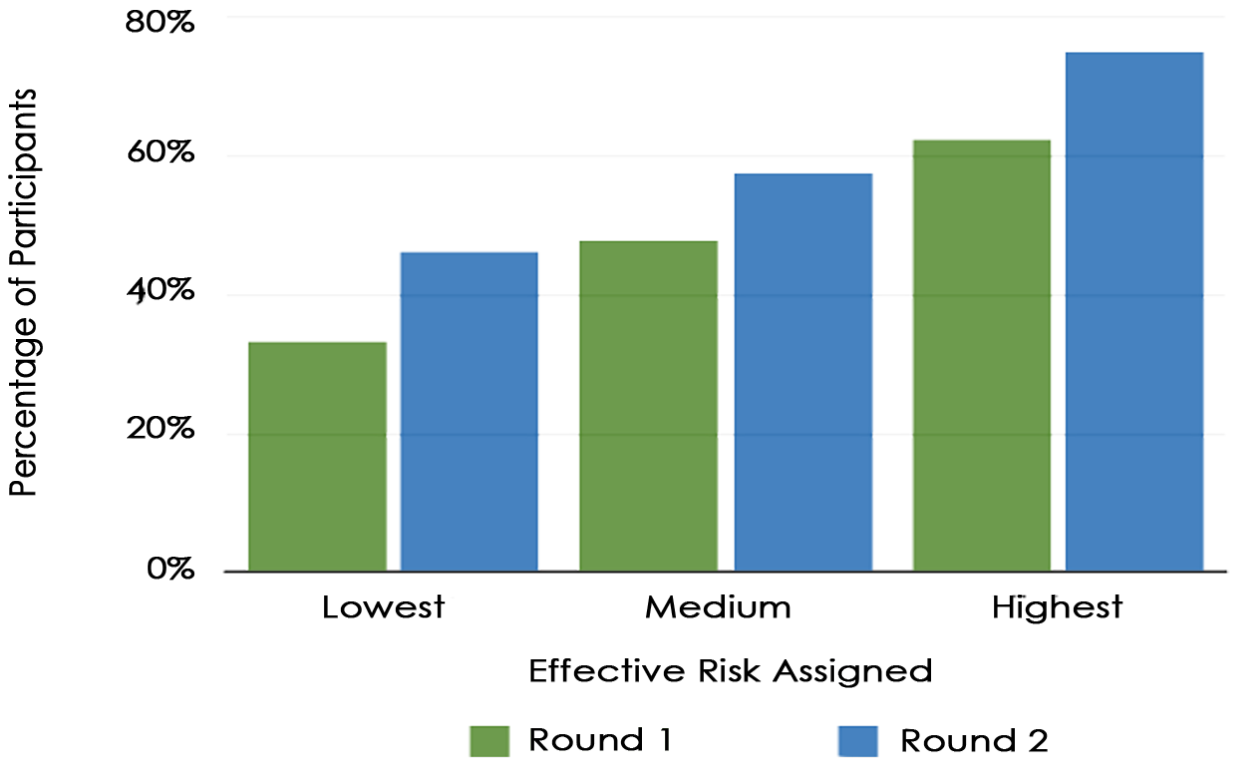
48% strictly rational with no experience

61% strictly rational once familiar with the system

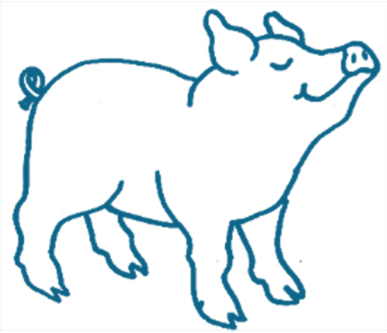
Significant ($p<0.001$), medium ($V=0.578$) learning effect

Users with more experience, skill & risk are more rational

Higher internet skill 15% more likely to behave rationally



People are not perfectly rational, but is their behavior random?



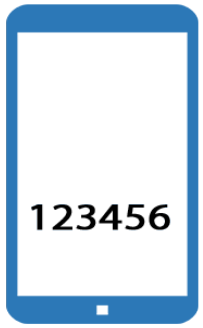
The user is going to pick
dancing pigs over **security** every time.

-- McGraw and Felten / Schneier

The user is rationally ignoring security advice
because **the costs outweigh the benefits.**

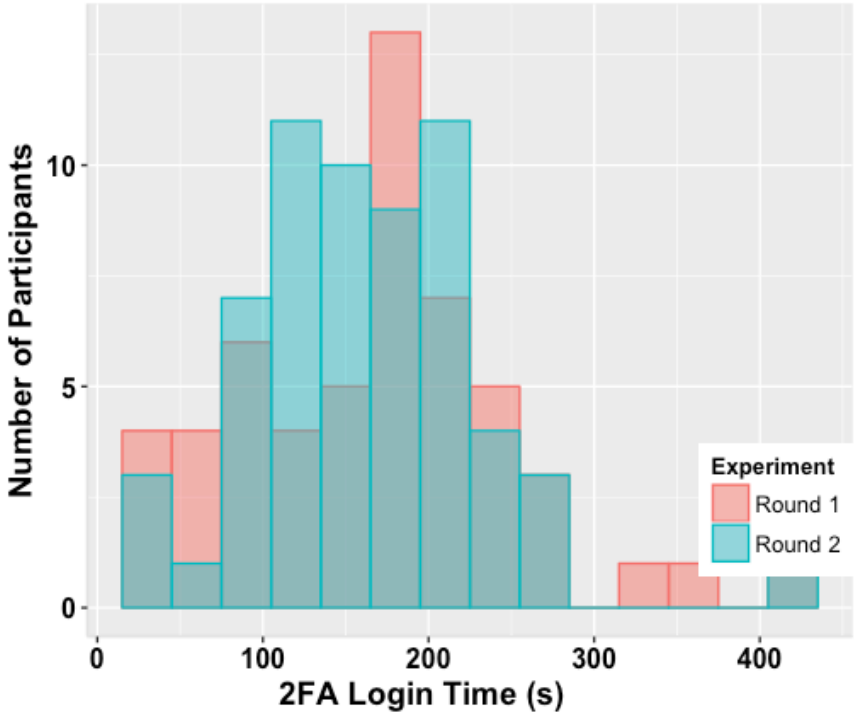
-- Herley, 2009

Testing the bounded rationality hypothesis: is there a consistent pattern in security behavior?



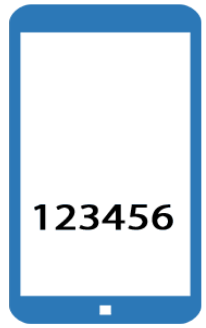
Enable 2FA

~



Costs
(time)

+



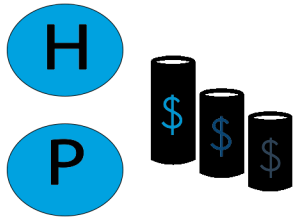
Past 2FA
Behavior

+

Demographics

Controls

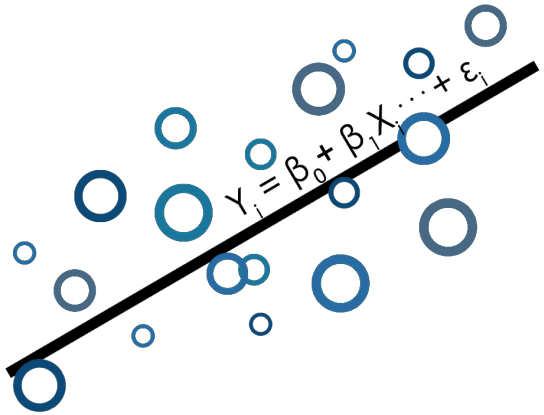
Experimental results suggest users are boundedly rational



Risk + **Account Value**

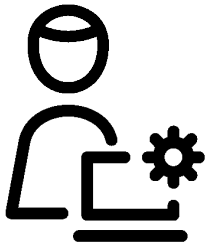
explains 9% behavior variance

Security behavior is not random
Differences in ability and account value alter behavior



People behave in ways we can model well

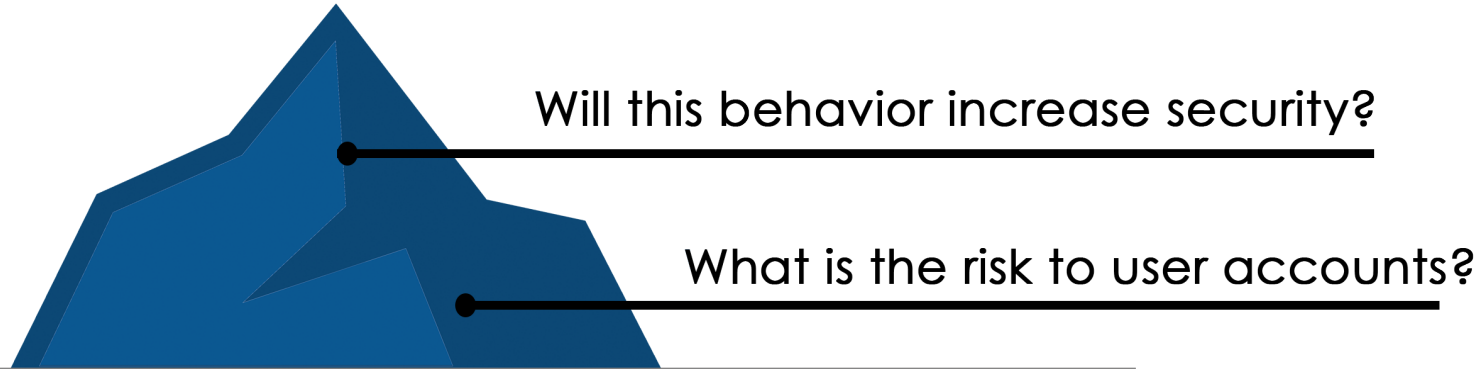
We can model human behavior well (R^2=0.61) as a function of variables measured or controlled in the simulation system

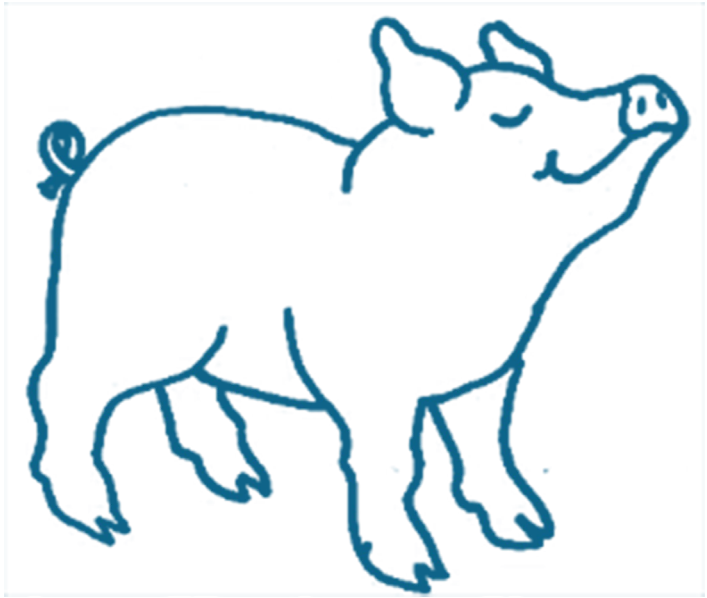


Differences in *ability* (differences in *cost*) alter behavior

Differences in *account valuation* alter behavior

Behavioral security allows us to understand what initially looks irrational and unfixable.

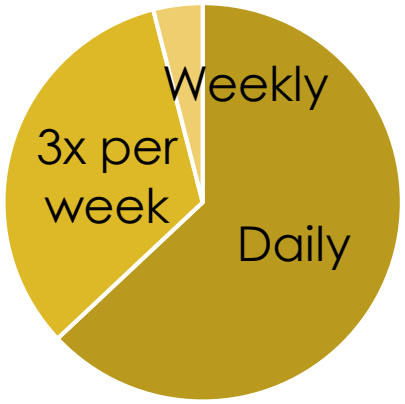




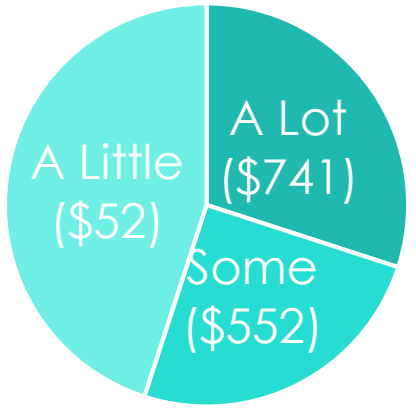
RSAConference2019

Easier idea: just require 2FA!

Requiring security can be costly: 2FA code fees + engagement losses



Login frequencies



Value of accounts to users

Approach	User Costs	2FA Benefit	Loss/Gain	Market Impact 500K MTurk Users
2FA Required	$275 per 1000 MTurkers	$148 per 1000 MTurkers	(-) $126 per 1000 MTurkers	(-) $63,606
Perfect Rationality	$32 per 1000 MTurkers	$128 per 1000 MTurkers	(+) $96 per 1000 MTurkers	(+) $47,865
No 2FA Offered	$266 per 1000 MTurkers	$0 per 1000 MTurkers	(-) $266 per 1000 MTurkers	(-) $133,000

Apply What You Have Learned Today

Instead of prompting on sign-up
prompt after account use or value has increased

Consider nudging by communicating risk or using social influence calculated based on similar profiles

Consider providing resources that reduce security costs to low skill / high risk users

Users are boundedly rational: they make burden-risk tradeoffs affected by human biases

What We Learned About Security Behavior

Boundedly Rational: users take into account burden & risk

Anchoring Effects: tendency to stick with first decision

Account Value Effects: more protective of existing assets

Driving Toward "Security Rationality"

We're starting beta tests for a system to optimize company cost & risk using dynamic automated security requirement setting. Email me!

Elissa Redmiles eredmiles@cs.umd.edu