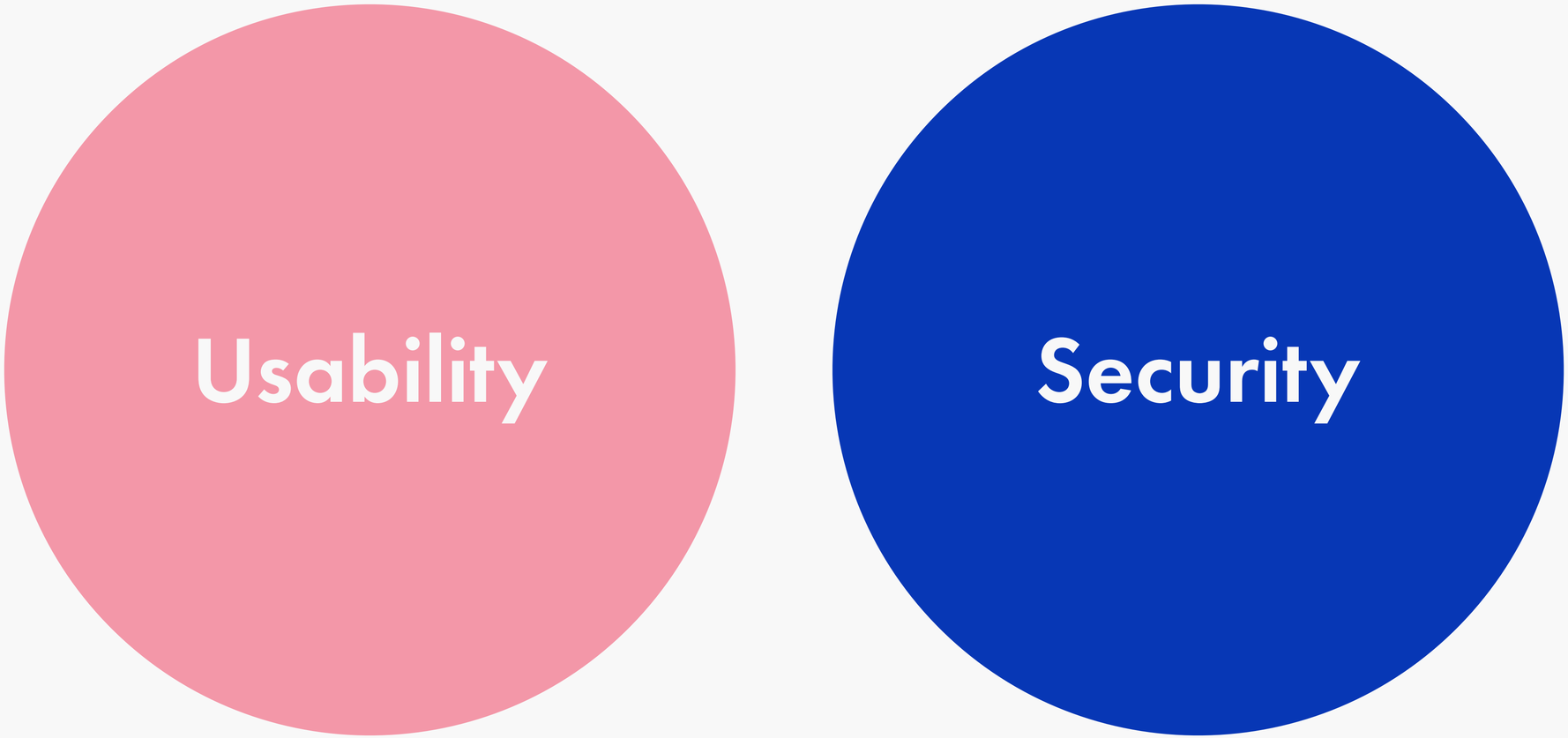
Design for Security

Serena Chen | @Sereeena | O'Reilly Velocity 2018


Usability
Security

Good user experience design and good security cannot exist without each other

Everyone deserves to be secure without being experts

We need to stop expecting people to become security experts

“I don’t care about security.”

–Everyone not watching Mr Robot right now

“Given a choice between dancing pigs and security, the user will pick dancing pigs every time.”

–MCGRAW, G., FELTEN, E., AND MACMICHAEL, R.

Securing Java: getting down to business with mobile code. Wiley Computer Pub., 1999

"Given a choice between ~~dancing pigs~~ CATS and security, the user will pick ~~dancing pigs~~ CATS every time."

–Serena Chen, not allowed pets in her apartment


Shame! Shame! Shame! Bad vampire! Shame!

Debit Card [redacted]

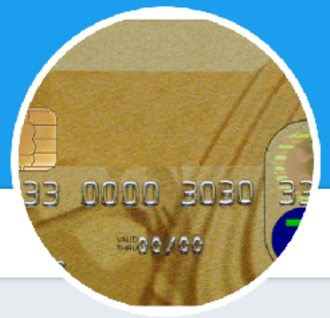
serena

Twitter, Inc. [US] | https://twitter.com/[redacted]

Home Moments

Search Twitter

Have an account? Log in



Tweets 189

Followers 18.8K

Follow

Debit Card

[redacted]

Please quit posting pictures of your debit cards, people.

Joined May 2012

Photos and videos

New to Twitter?

Sign up now to get your own personalized timeline!

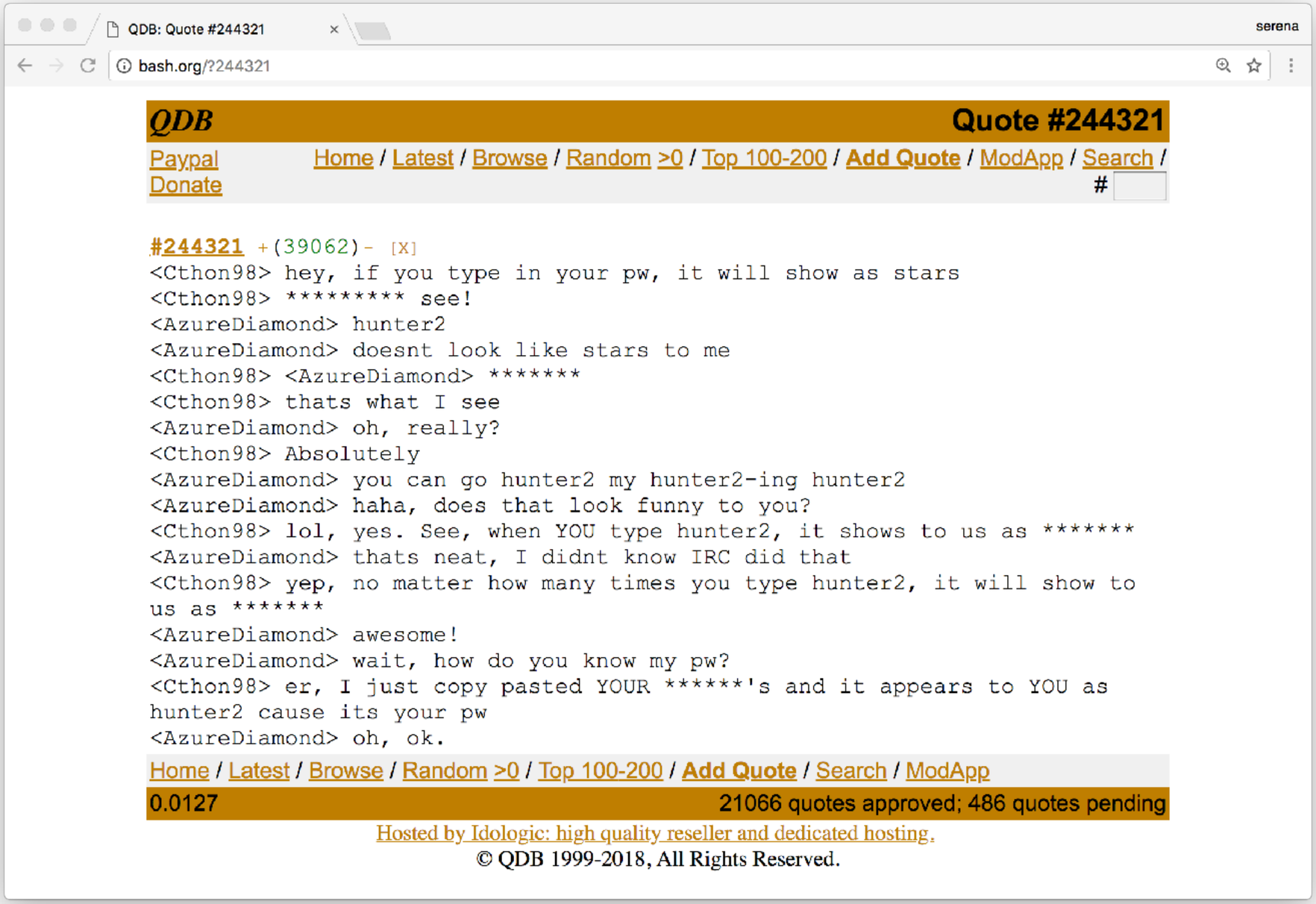
Sign up

Tweets | Tweets & replies | Media

Debit Card Retweeted

[redacted]

just got a new credit card 😍😍



QDB **Quote #244321**

Paypal Donate

Home / Latest / Browse / Random >0 / Top 100-200 / **Add Quote** / ModApp / Search / #

#244321 +(39062)- [X]

```
<Cthon98> hey, if you type in your pw, it will show as stars
<Cthon98> ********* see!
<AzureDiamond> hunter2
<AzureDiamond> doesnt look like stars to me
<Cthon98> <AzureDiamond> *******
<Cthon98> thats what I see
<AzureDiamond> oh, really?
<Cthon98> Absolutely
<AzureDiamond> you can go hunter2 my hunter2-ing hunter2
<AzureDiamond> haha, does that look funny to you?
<Cthon98> lol, yes. See, when YOU type hunter2, it shows to us as *******
<AzureDiamond> thats neat, I didnt know IRC did that
<Cthon98> yep, no matter how many times you type hunter2, it will show to
us as *******
<AzureDiamond> awesome!
<AzureDiamond> wait, how do you know my pw?
<Cthon98> er, I just copy pasted YOUR ******'s and it appears to YOU as
hunter2 cause its your pw
<AzureDiamond> oh, ok.
```

Home / Latest / Browse / Random >0 / Top 100-200 / **Add Quote** / Search / ModApp

0.0127 21066 quotes approved; 486 quotes pending

OpenPGP

serena

Secure | https://www.openpgp.org

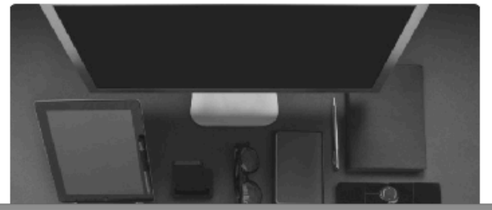
OpenPGP About OpenPGP Software Community

OpenPGP

Email encryption. For all operating systems. Standing the test of time.

Get OpenPGP Software

OpenPGP is the most widely used email encryption standard. It is defined by the OpenPGP Working Group of the Internet Engineering Task Force (IETF) as a Proposed Standard in RFC 4880. OpenPGP was originally derived from the PGP software, created by Phil Zimmermann.



LMGTFY

serena

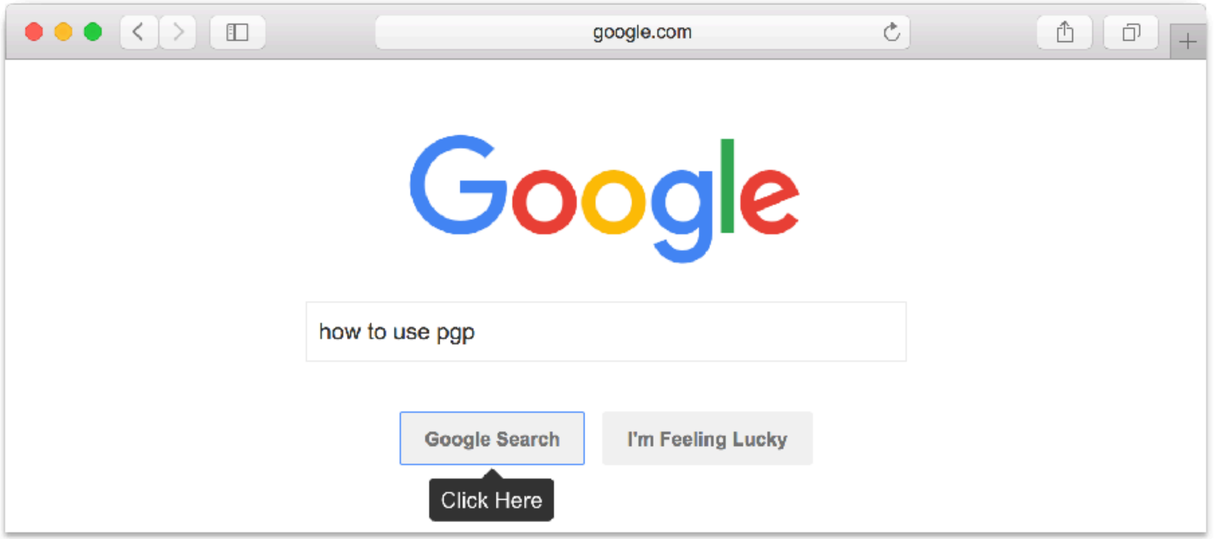
Secure | https://lmgtfy.com/?q=how+to+use+pgp

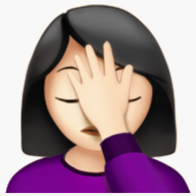
Step 1
Visit google.com

Step 2
Type your question.

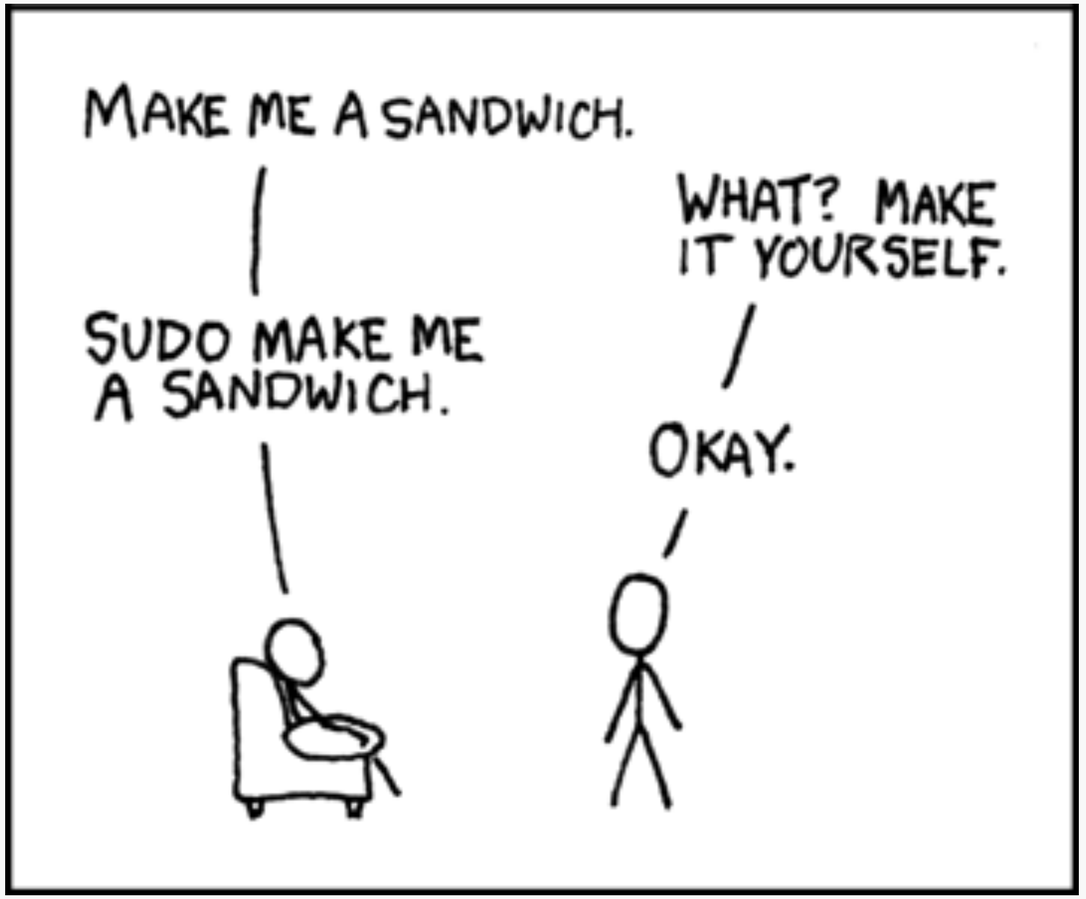
Step 3
Click the button.

That's it!





Shaming people is lazy



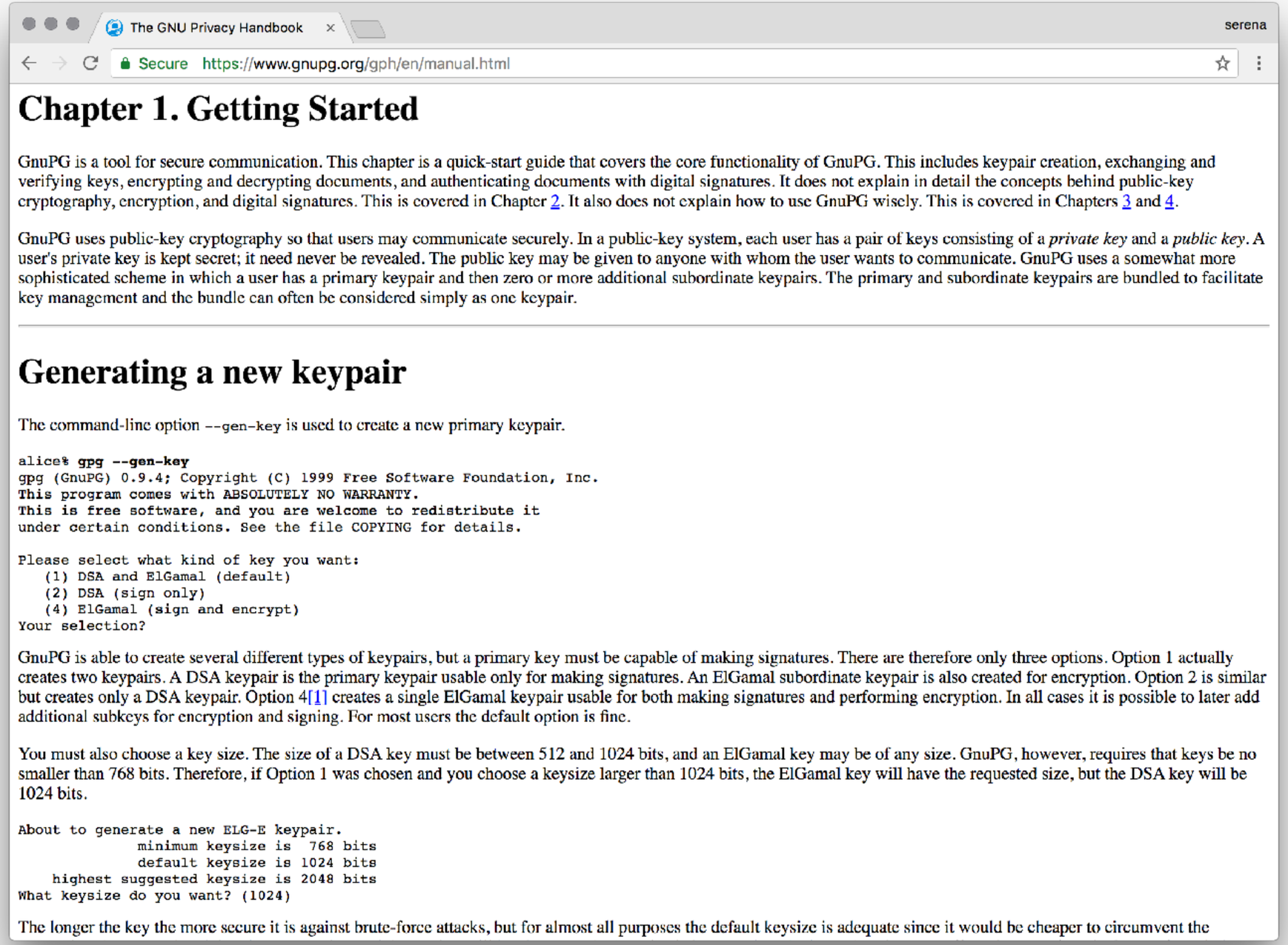
Obligatory xkcd: https://xkcd.com/149/

“I don’t care about security.”

–Everyone not watching Mr Robot right now

“I care!!!”

–Serena Chen, lone nerd screaming into the void



Chapter 1. Getting Started

GnuPG is a tool for secure communication. This chapter is a quick-start guide that covers the core functionality of GnuPG. This includes keypair creation, exchanging and verifying keys, encrypting and decrypting documents, and authenticating documents with digital signatures. It does not explain in detail the concepts behind public-key cryptography, encryption, and digital signatures. This is covered in Chapter 2. It also does not explain how to use GnuPG wisely. This is covered in Chapters 3 and 4.

GnuPG uses public-key cryptography so that users may communicate securely. In a public-key system, each user has a pair of keys consisting of a *private key* and a *public key*. A user's private key is kept secret; it need never be revealed. The public key may be given to anyone with whom the user wants to communicate. GnuPG uses a somewhat more sophisticated scheme in which a user has a primary keypair and then zero or more additional subordinate keypairs. The primary and subordinate keypairs are bundled to facilitate key management and the bundle can often be considered simply as one keypair.

Generating a new keypair

The command-line option `--gen-key` is used to create a new primary keypair.

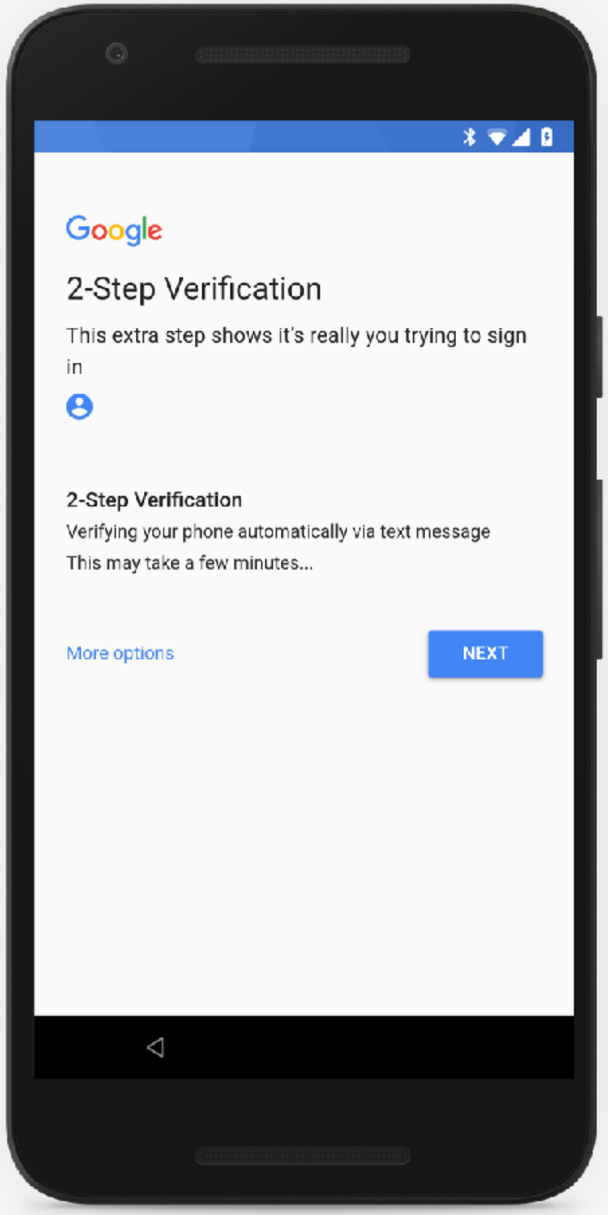
```
alice% gpg --gen-key
gpg (GnuPG) 0.9.4; Copyright (C) 1999 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Please select what kind of key you want:
   (1) DSA and ElGamal (default)
   (2) DSA (sign only)
   (4) ElGamal (sign and encrypt)
Your selection?
```

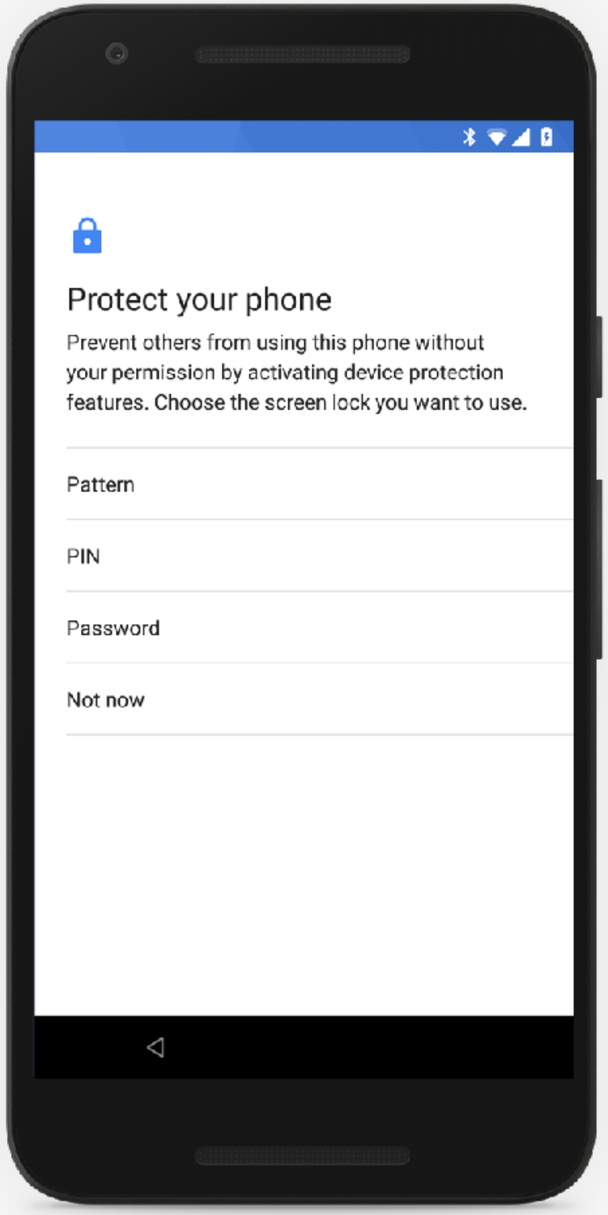
GnuPG is able to create several different types of keypairs, but a primary key must be capable of making signatures. There are therefore only three options. Option 1 actually creates two keypairs. A DSA keypair is the primary keypair usable only for making signatures. An ElGamal subordinate keypair is also created for encryption. Option 2 is similar but creates only a DSA keypair. Option 4[1] creates a single ElGamal keypair usable for both making signatures and performing encryption. In all cases it is possible to later add additional subkeys for encryption and signing. For most users the default option is fine.

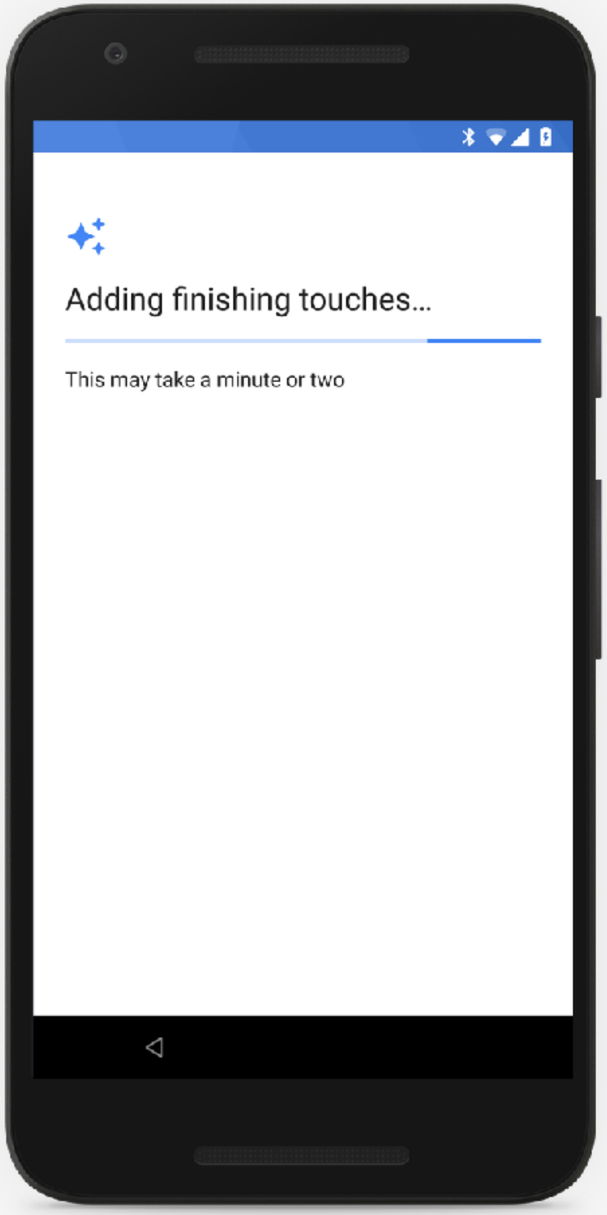
You must also choose a key size. The size of a DSA key must be between 512 and 1024 bits, and an ElGamal key may be of any size. GnuPG, however, requires that keys be no smaller than 768 bits. Therefore, if Option 1 was chosen and you choose a keysize larger than 1024 bits, the ElGamal key will have the requested size, but the DSA key will be 1024 bits.

```
About to generate a new ELG-E keypair.
              minimum keysize is  768 bits
              default keysize is 1024 bits
    highest suggested keysize is 2048 bits
What keysize do you want? (1024)
```

The longer the key the more secure it is against brute-force attacks, but for almost all purposes the default keysize is adequate since it would be cheaper to circumvent the


Google
2-Step Verification
This extra step shows it's really you trying to sign in
2-Step Verification
Verifying your phone automatically via text message
This may take a few minutes...
More options
NEXT


Protect your phone
Prevent others from using this phone without your permission by activating device protection features. Choose the screen lock you want to use.
Pattern
PIN
Password
Not now


Adding finishing touches...
This may take a minute or two

Signal >> Home

serena

Secure | https://signal.org

Signal

SUPPORT BLOG DEVELOPERS JOBS

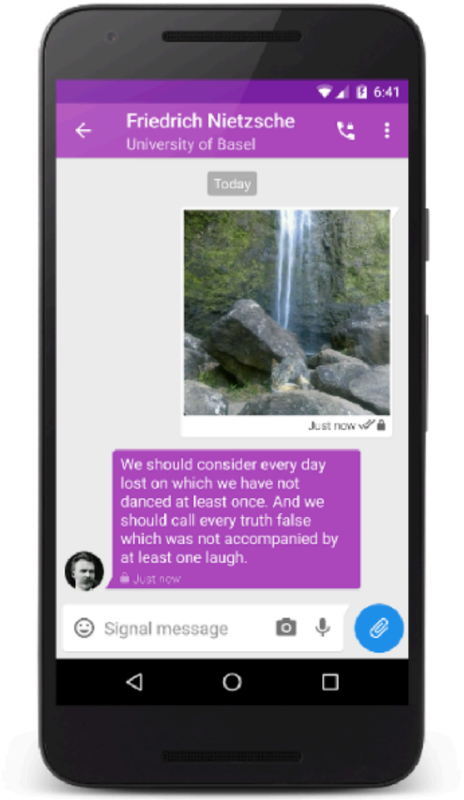
Fast, simple, secure.

Privacy that fits in your pocket.

Android

iPhone

Desktop



Design thinking is another tool in the problem solving tool belt

For your consideration:

1.

2.

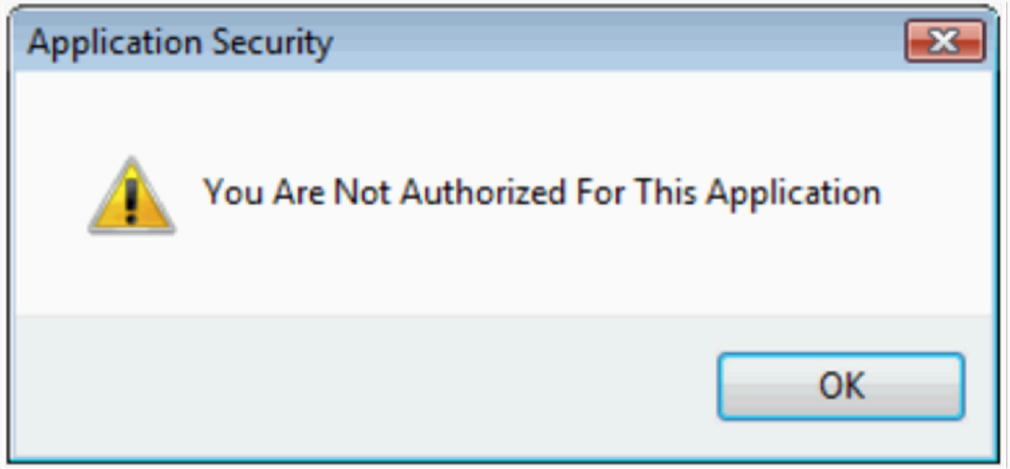
3.

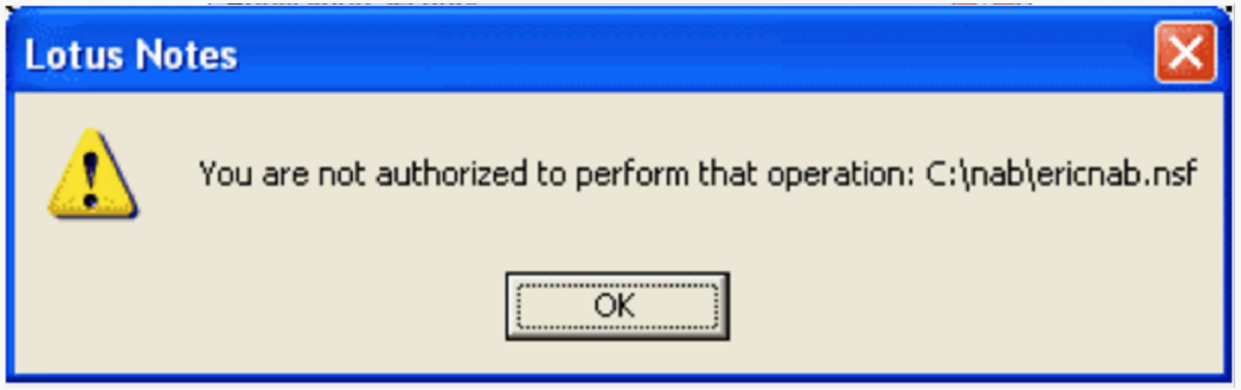
4.

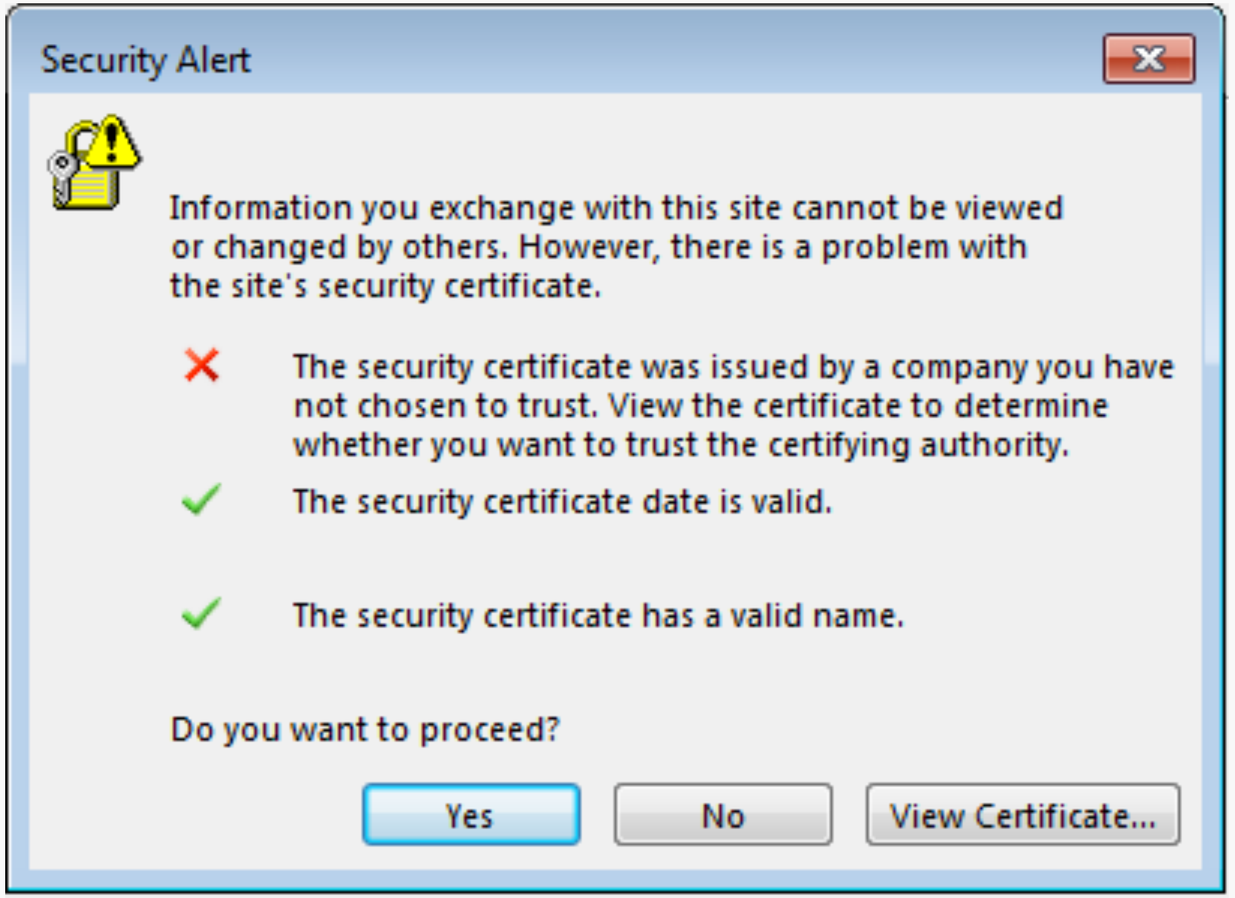
For your consideration:

1. Paths of Least Resistance
2.
3.
4.

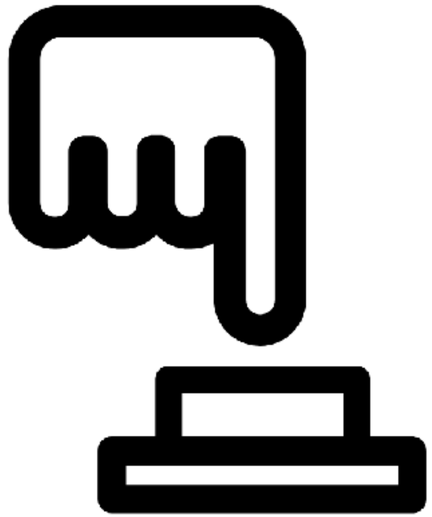
Paths of Least Resistance


Application Security
You Are Not Authorized For This Application
OK

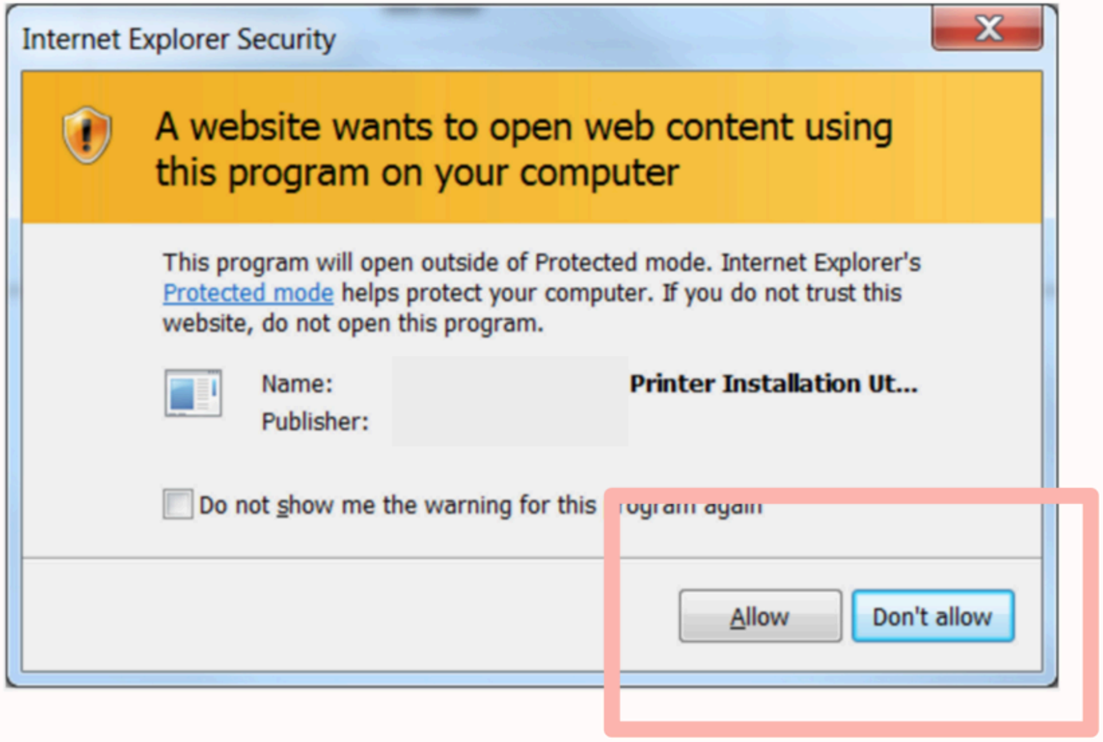

Lotus Notes
You are not authorized to perform that operation: C:\nab\ericnab.nsf
OK


Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name.
Do you want to proceed?
Yes
No
View Certificate...

To stop internet, press firmly



Consider the “secure by default” principle


Internet Explorer Security
A website wants to open web content using this program on your computer
This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program.
Name:
Printer Installation Ut...
Publisher:
Do not show me the warning for this
Allow
Don't allow

Normalise security

Welcome to Simple

serena

Secure | https://arrow.simple.com/personal/phone

SIMPLE

Account info | Personal info | Identity | Review & submit

Enter your phone number

Getting your phone number allows us to verify you are the only one who can log into your account.

Phone number

(000) 000-0000

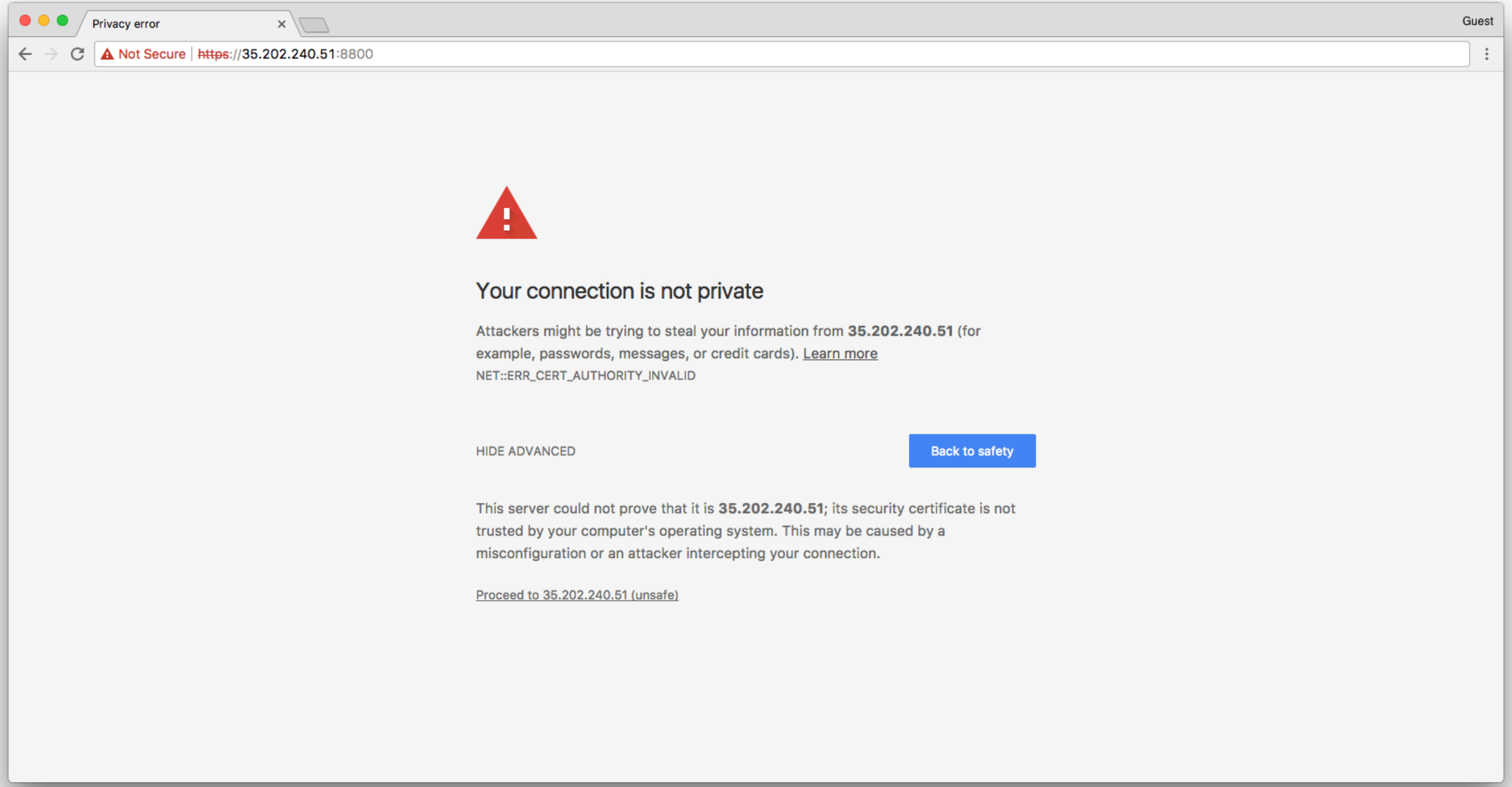
Back

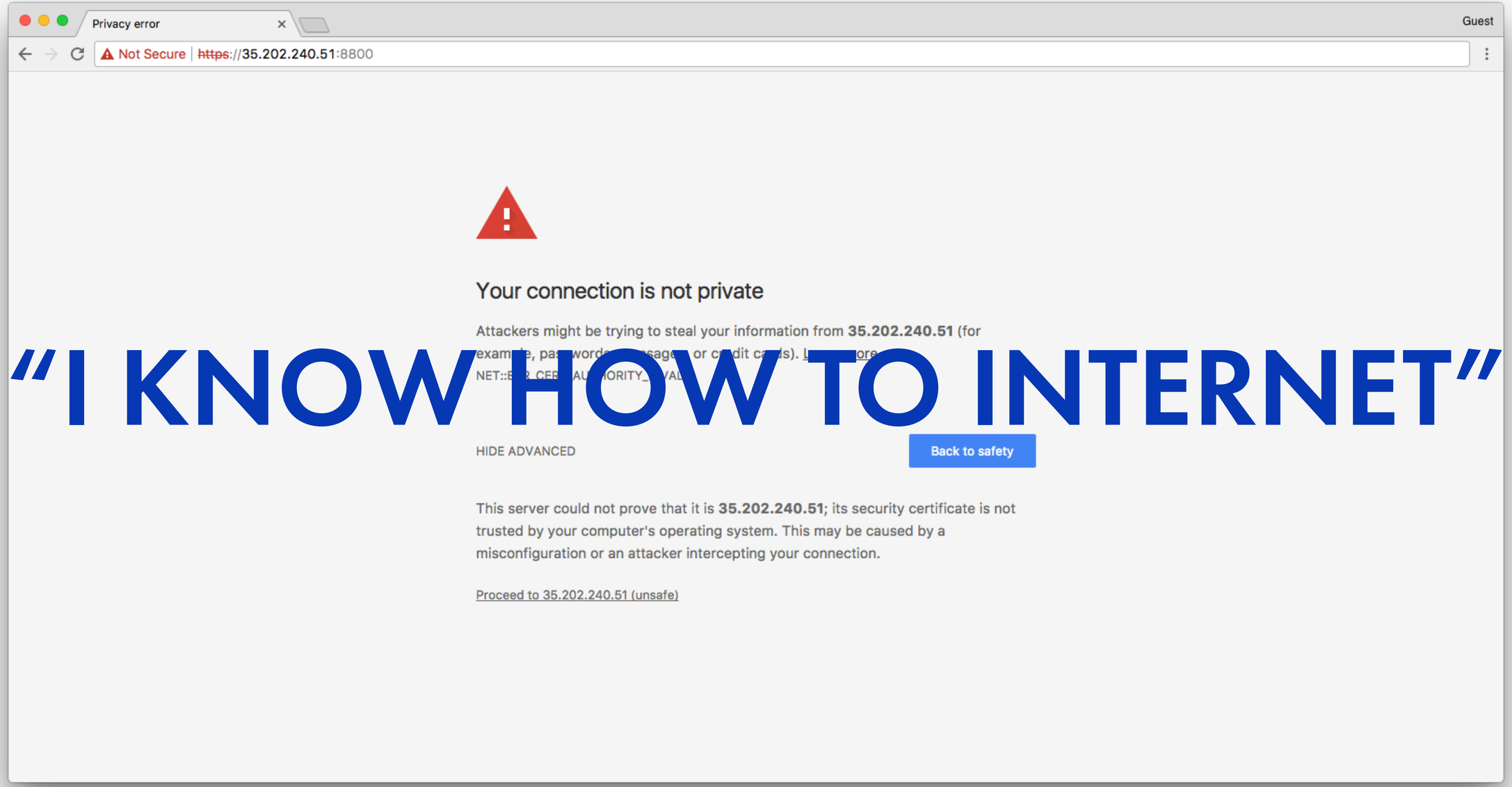
Next

Group similar tasks

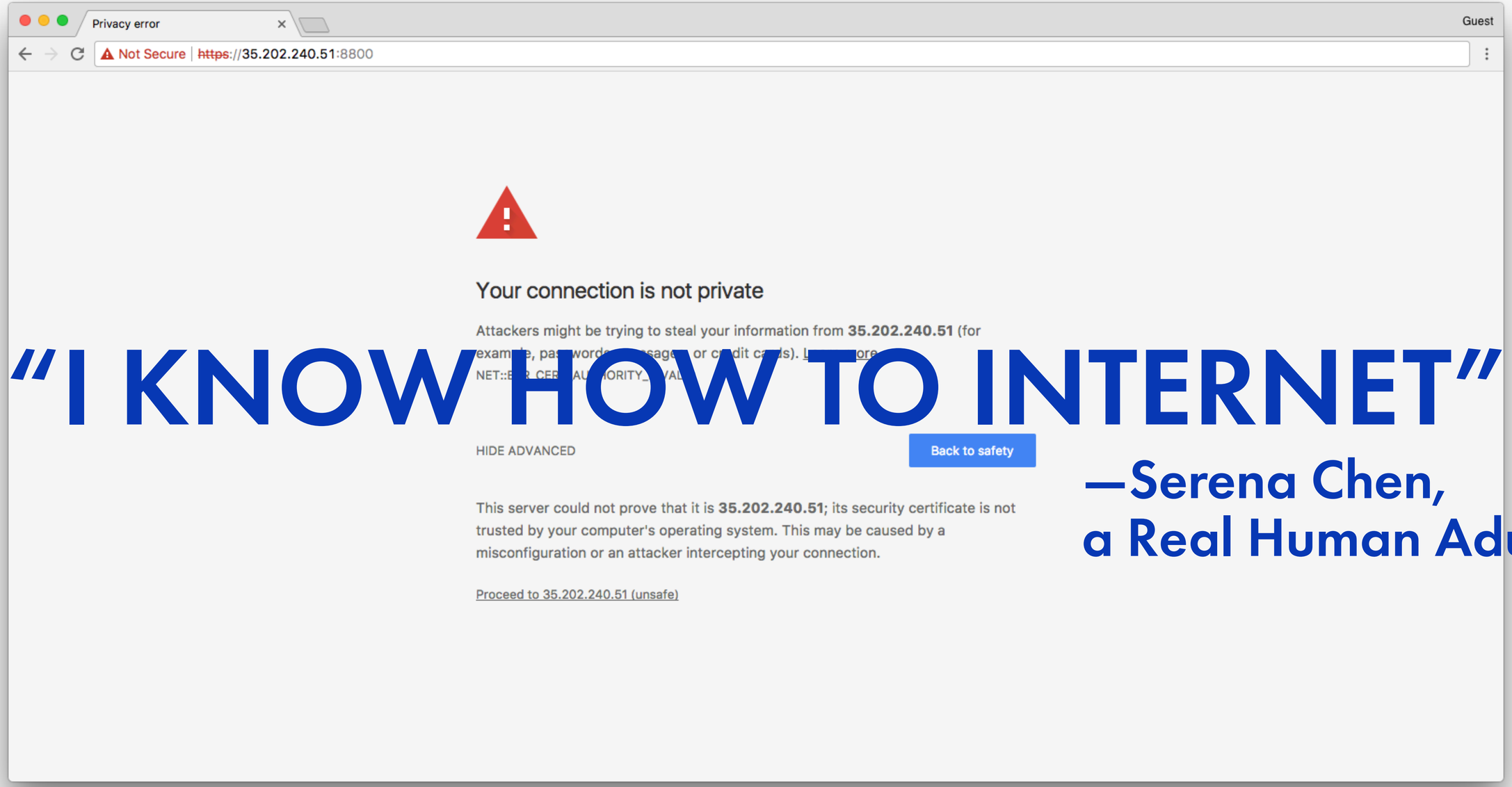
People are ~~lazy~~ efficient

Align your goals with the end user’s goals


Privacy error
Guest
Not Secure | https://35.202.240.51:8800
Your connection is not private
Attackers might be trying to steal your information from 35.202.240.51 (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
HIDE ADVANCED
Back to safety
This server could not prove that it is 35.202.240.51; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to 35.202.240.51 (unsafe)

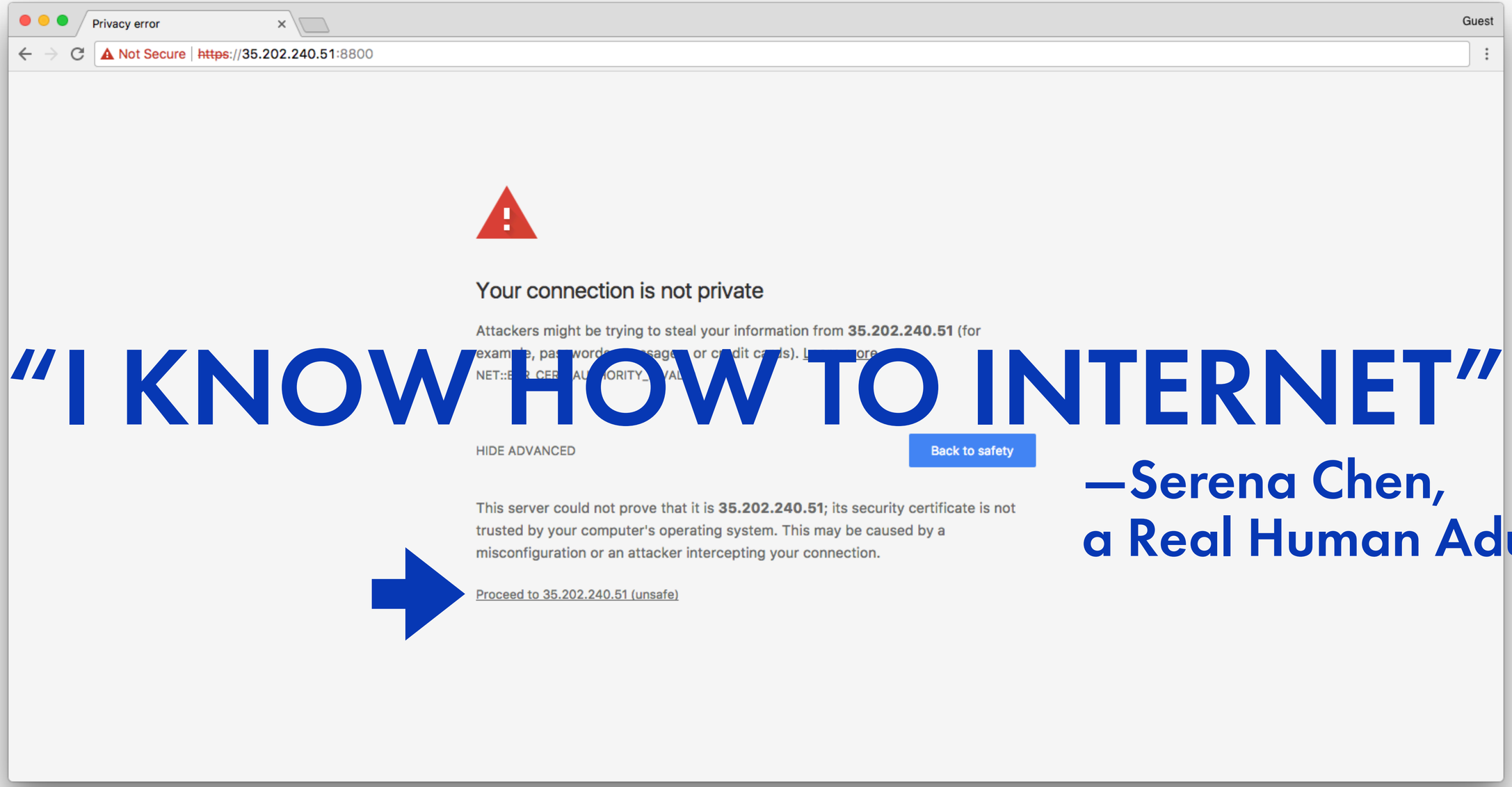


"I KNOW HOW TO INTERNET"



"I KNOW HOW TO INTERNET"

—Serena Chen,
a Real Human Adult™



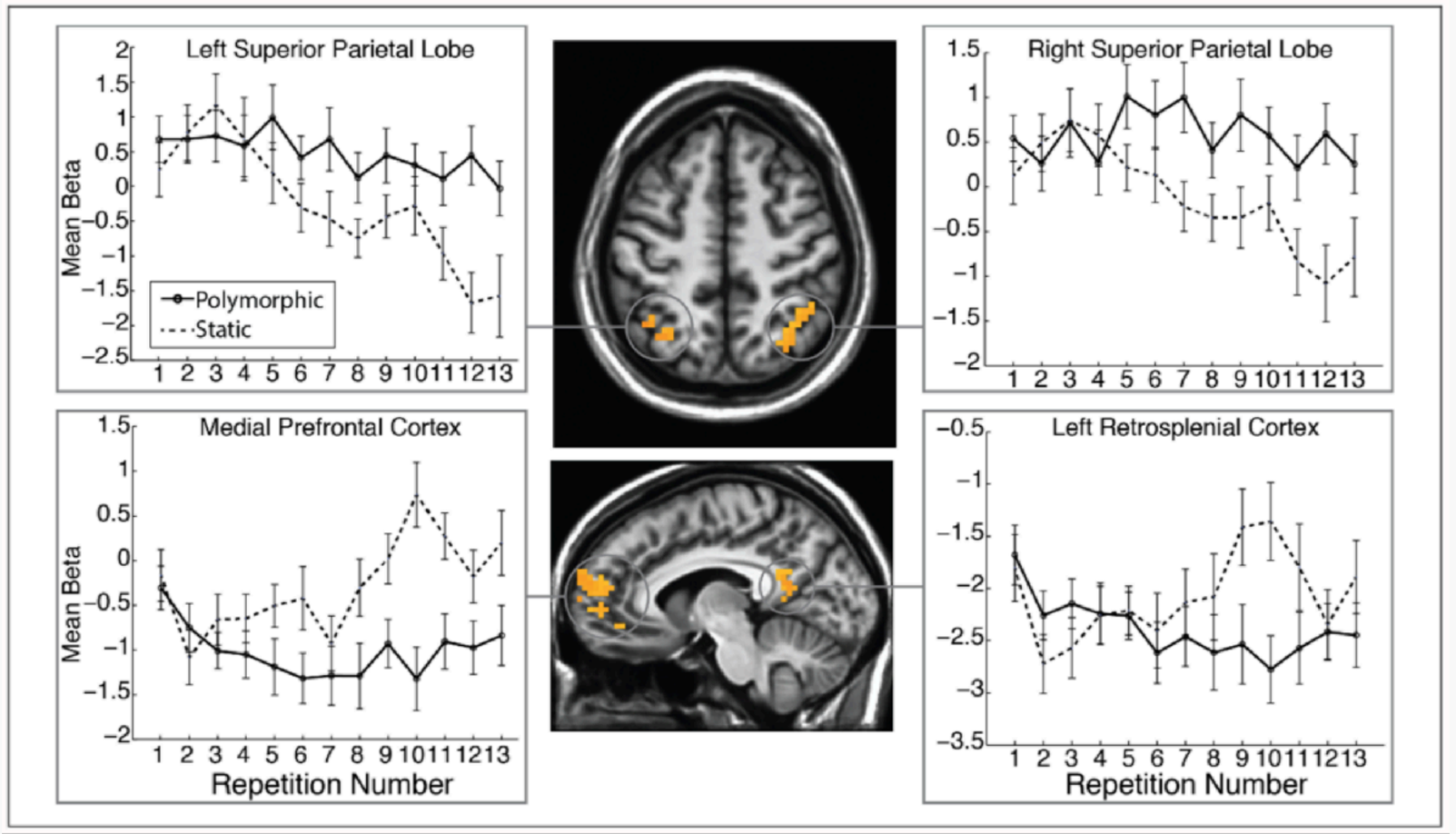
"I KNOW HOW TO INTERNET"

—Serena Chen,
a Real Human Adult™

Path of (Perceived) Least Resistance

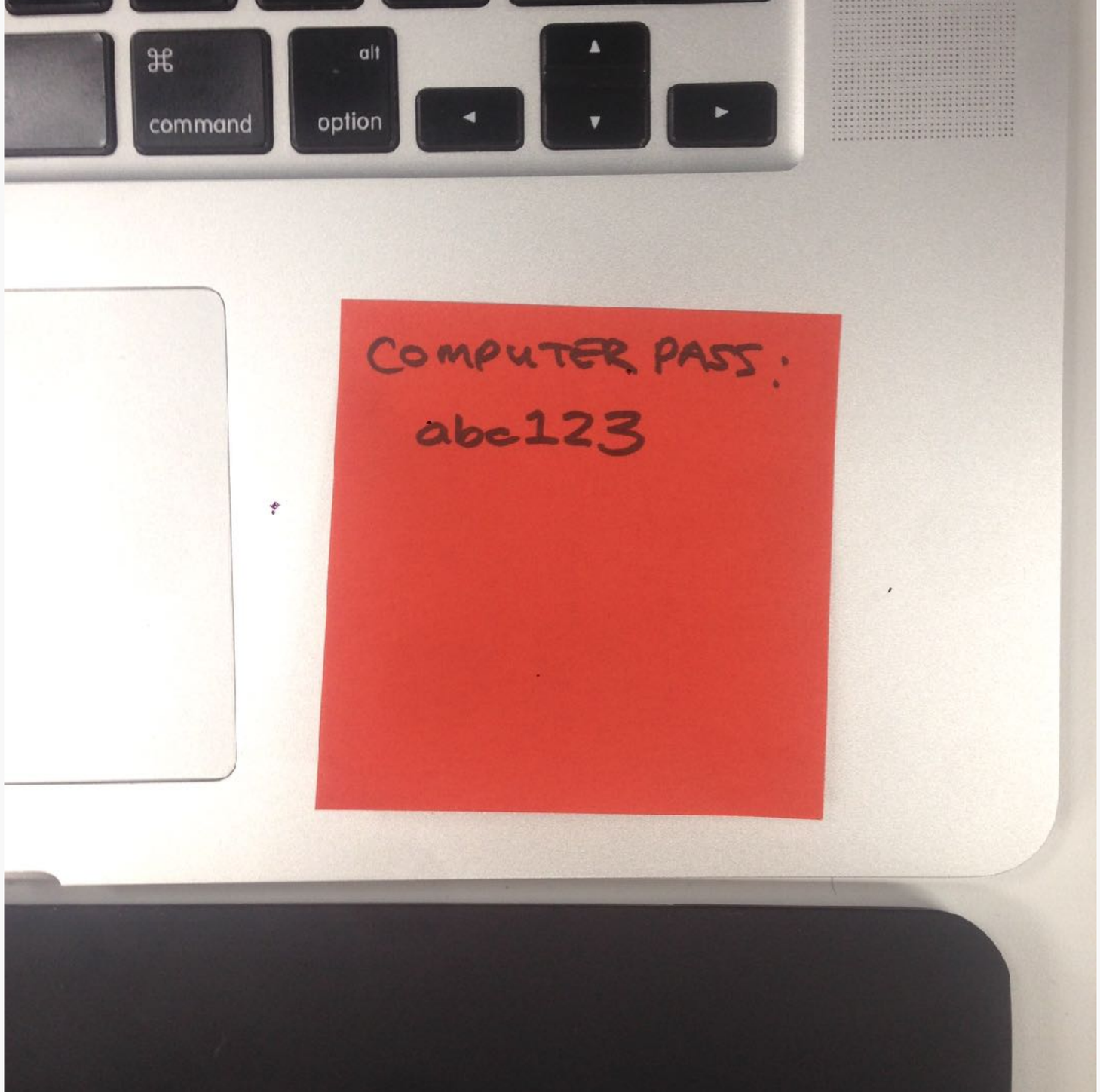
“Each false alarm reduces the credibility of a warning system.”

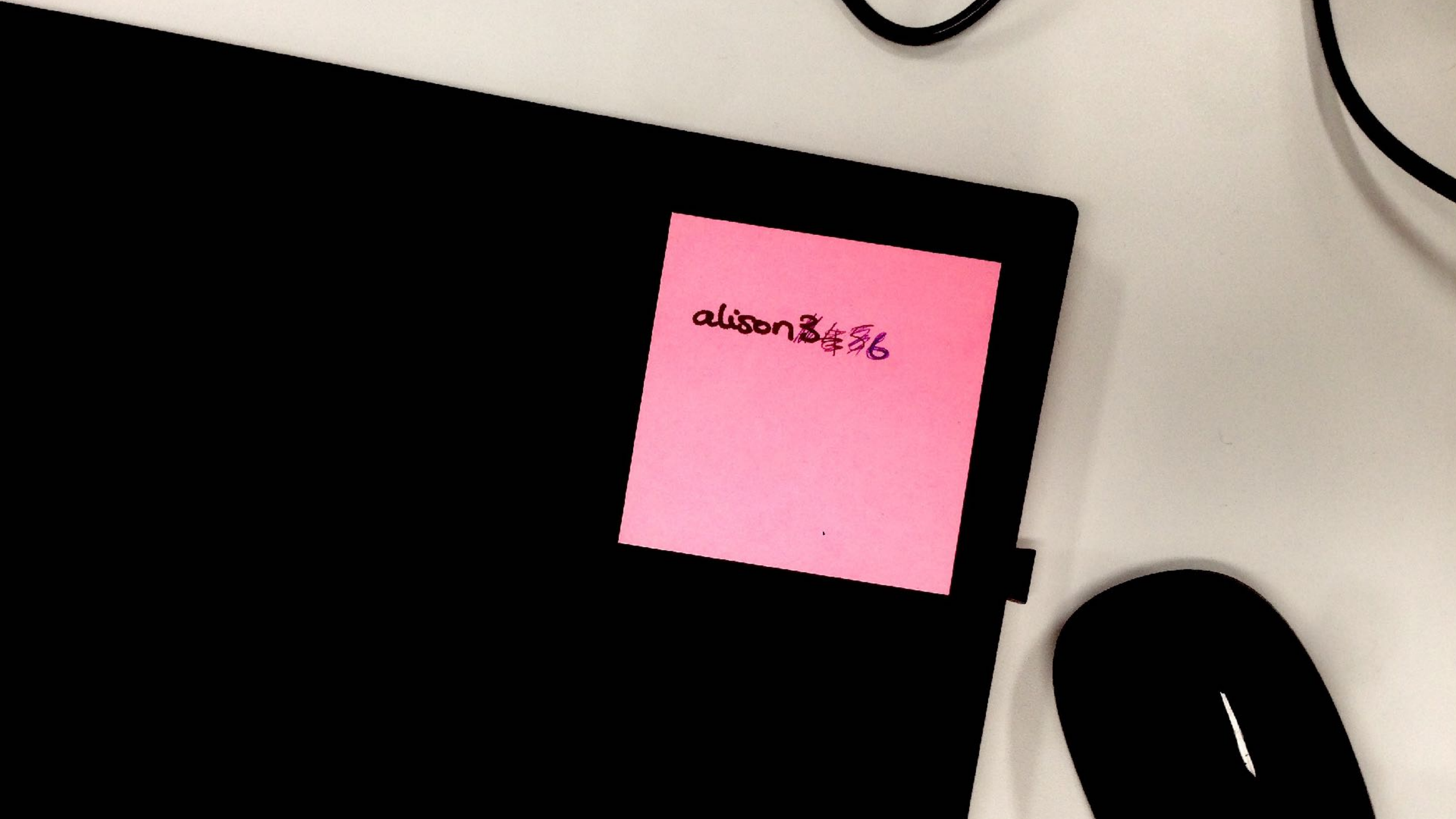
–S. Breznitz and C. Wolf. The psychology of false alarms.
Lawrence Erbaum Associates, NJ, 1984



Anderson et al. How polymorphic warnings reduce habituation in the brain: Insights from an fMRI study. *In Proceedings of CHI*, 2015

Shadow IT is a massive vulnerability


command
option
alt
COMPUTER PASS:
abc123


alison3隼596

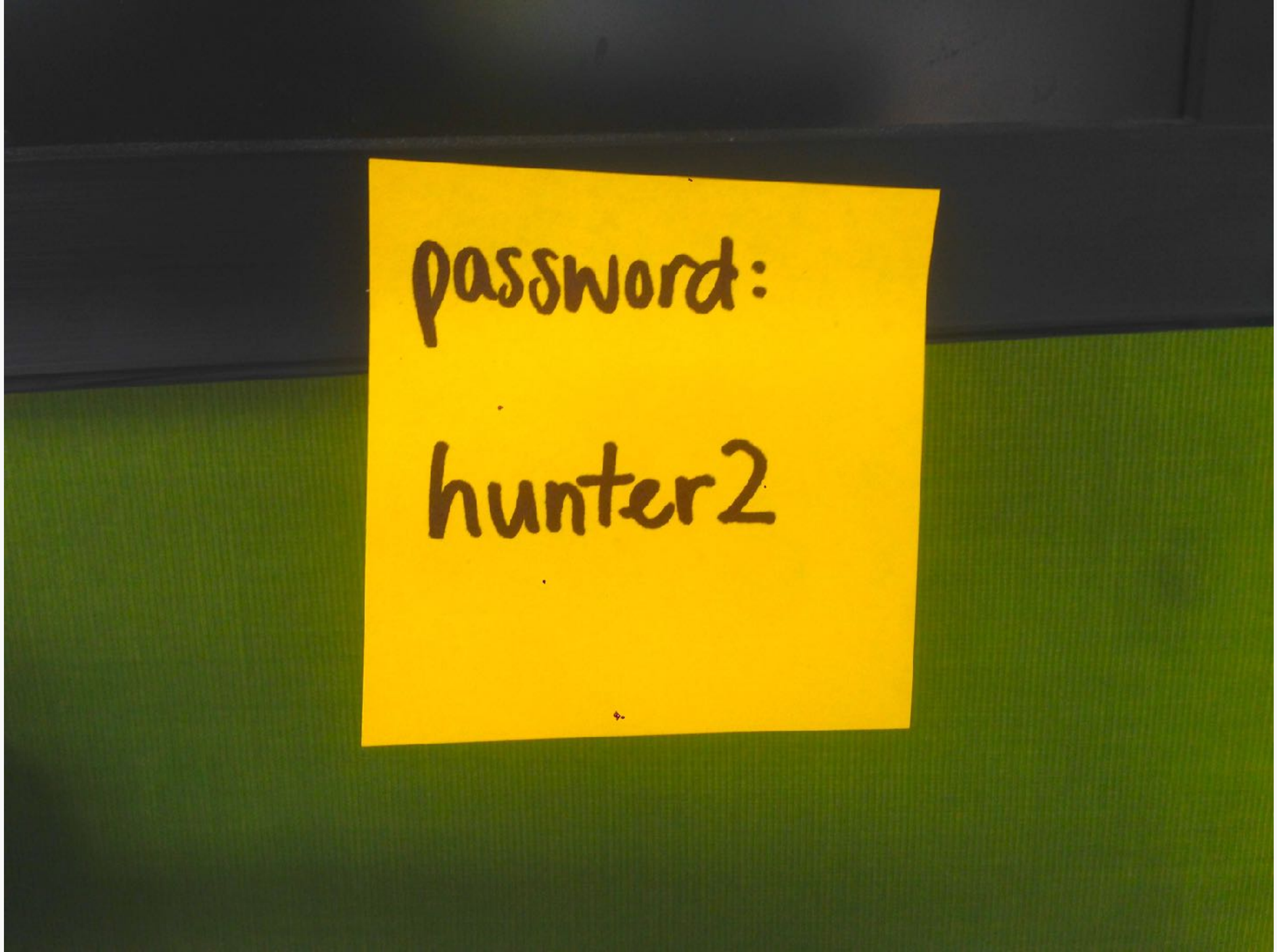

password:
hunter2

Illustration by Megan Pendergrass

Fixing bad paths

- Use security tools for ***security concerns***, not management concerns
  - If you block enough non-threats, people will get really good at subverting your security

Building good paths

- Don’t make me think!
  - Make the secure path the easiest path
  - e.g. BeyondCorp model at Google

"We designed our tools so that the user-facing components are **clear and easy** to use. [...] For the vast majority of users, BeyondCorp is **completely invisible.**

–V. M. Escobedo, F. Zyzniewski, B. (A. E.) Beyer, M. Saltonstall,
"BeyondCorp: The User Experience", Login, 2017

Align your goals with the end user’s goals

For your consideration:

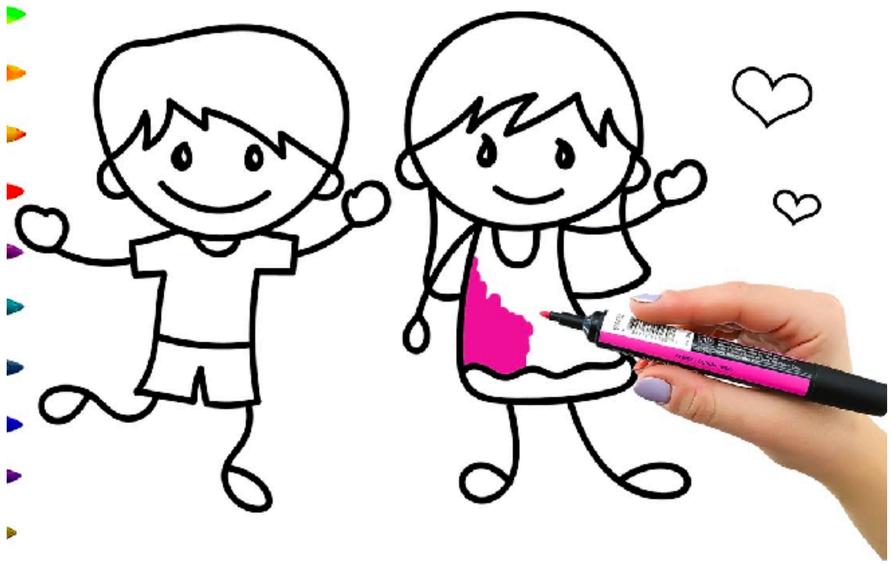
1. Paths of Least Resistance
2.
3.
4.

For your consideration:

1. Paths of Least Resistance
2. Intent
3.
4.

Intent

Tension between usability and security happens when we cannot accurately determine intent.



“make it easy”

“lock it down”

It is not our job to make everything easy

It is not our job to make everything locked down

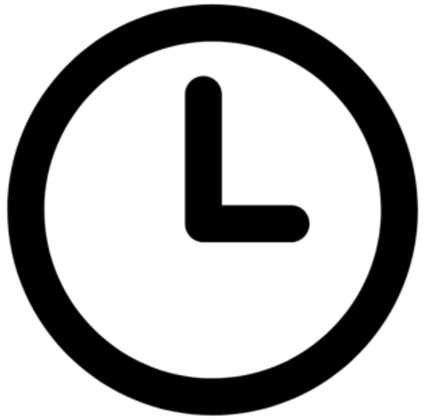
Our job is to make a specific **action**

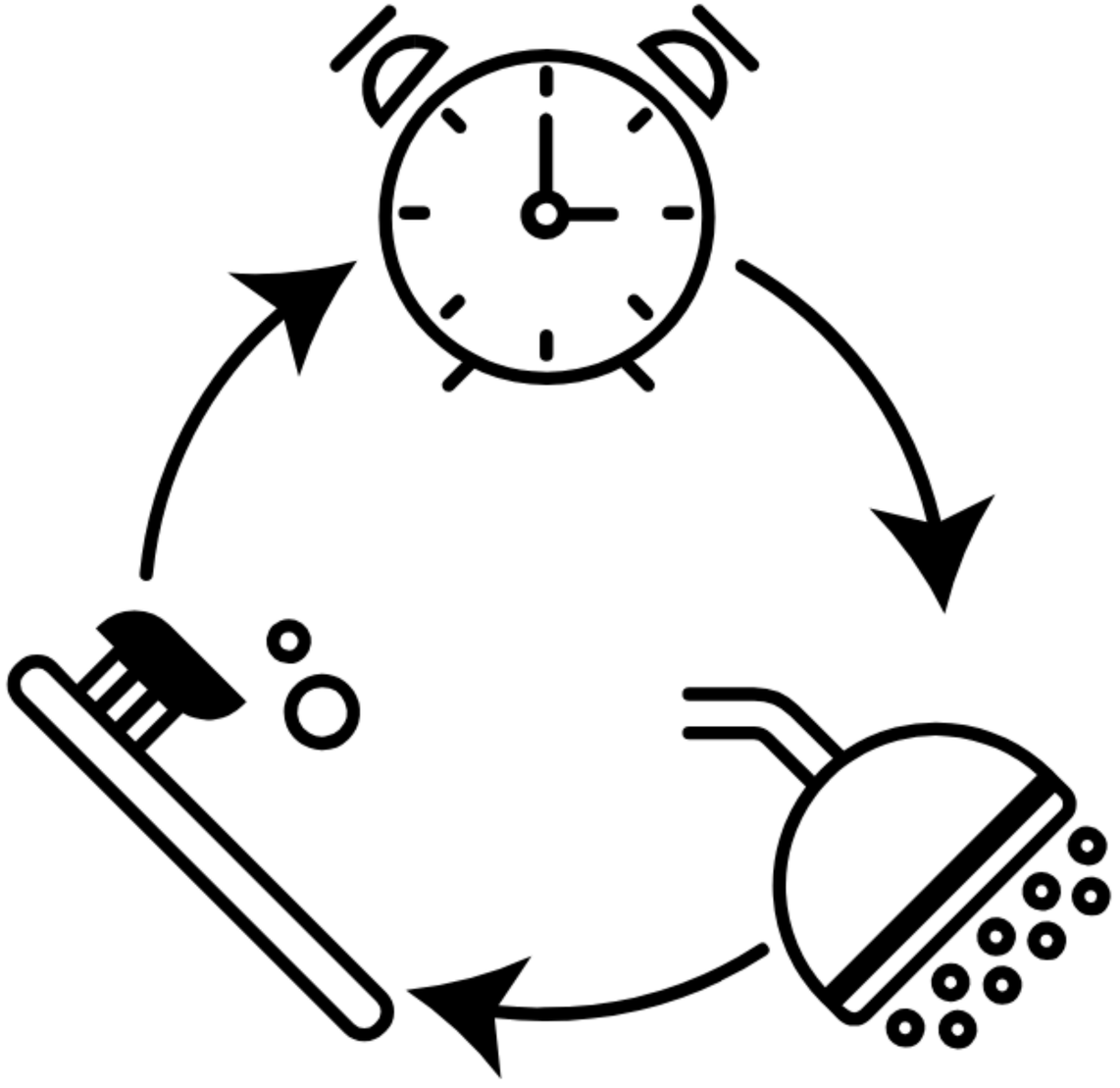
- that a specific **user** wants to take
- at that specific **time**
- in that specific **place**

...easy

Everything else we can lock down.

Knowing intent = usability and security without compromise





For your consideration:

1. Paths of Least Resistance
2. Intent
3.
4.

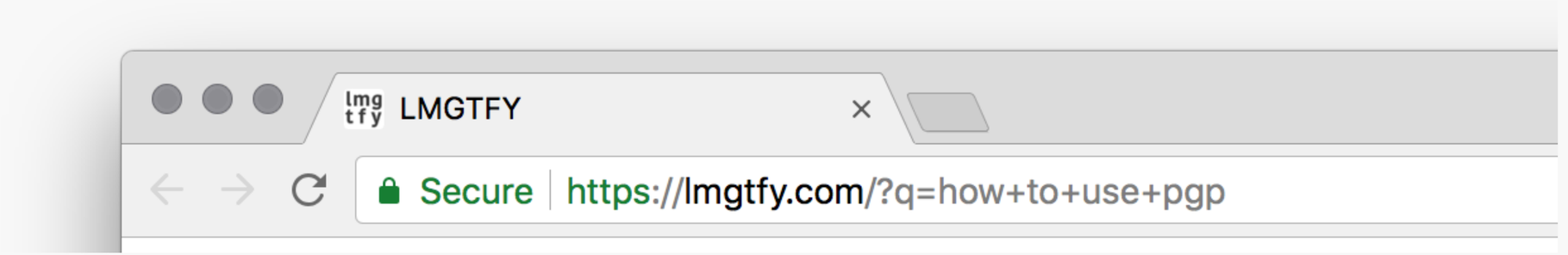
For your consideration:

1. Paths of Least Resistance
2. Intent
3. (Mis)communication
4.

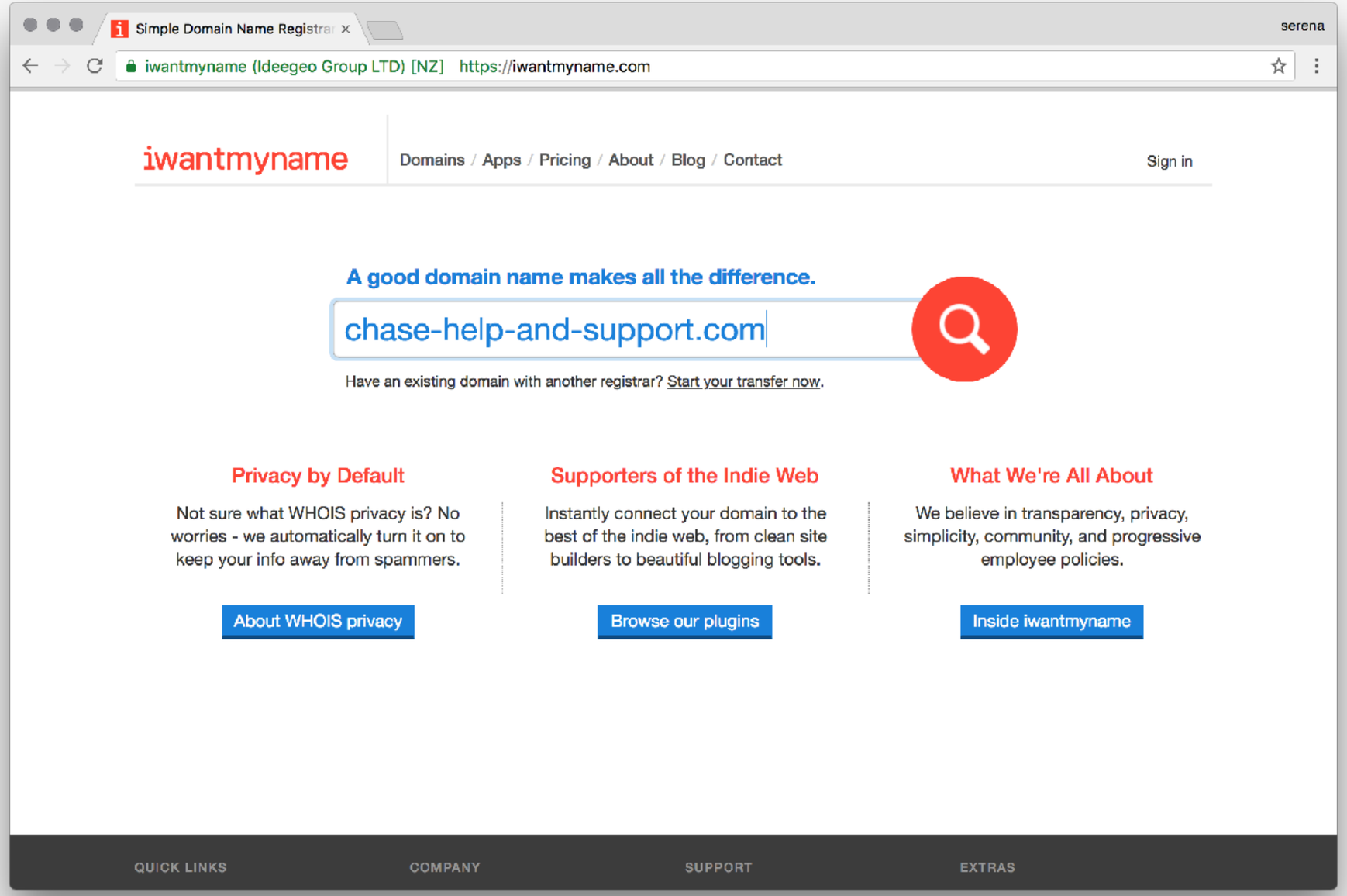
(Mis)communication

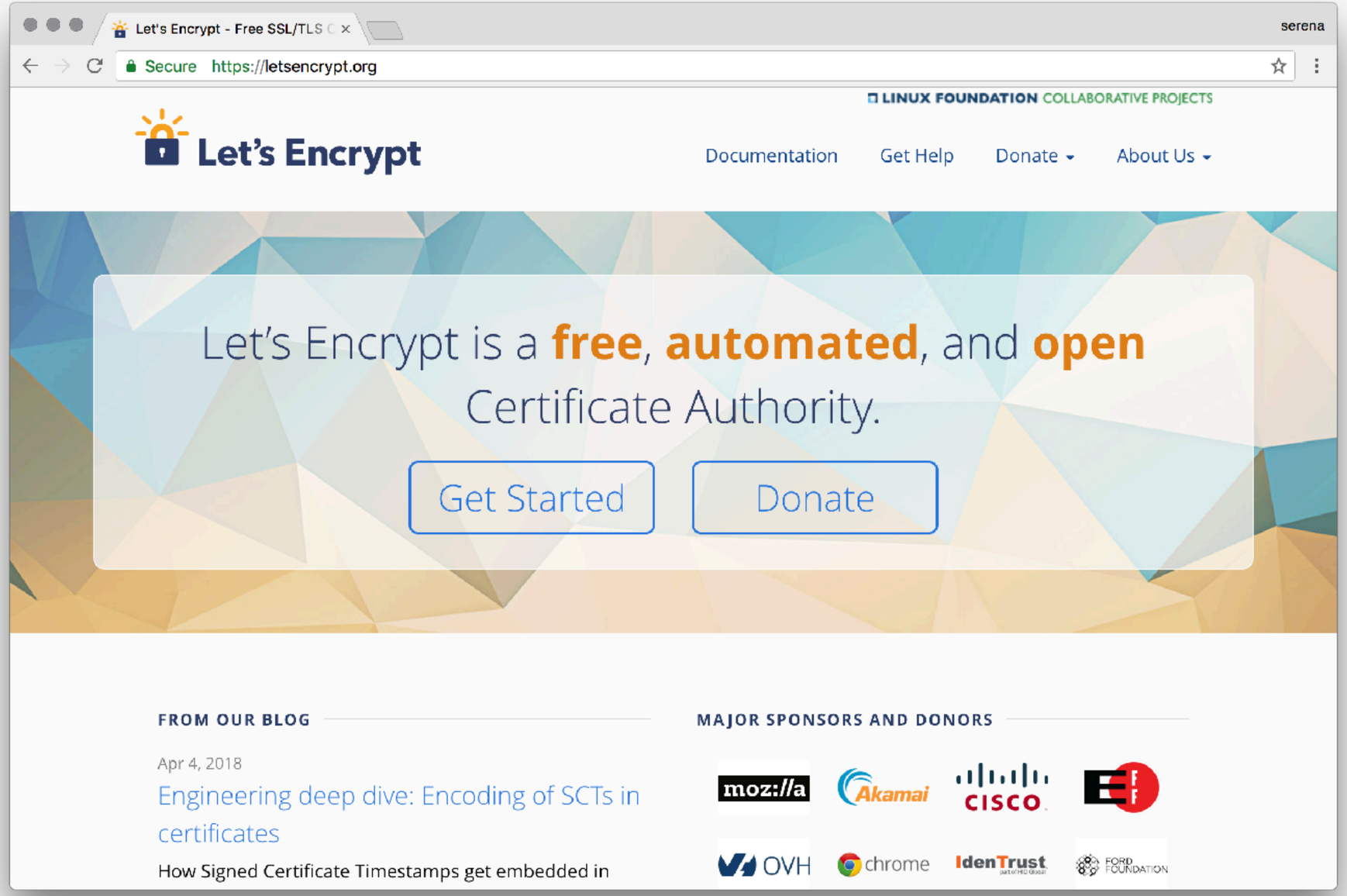
Wherever there is a miscommunication, there exists a human security vulnerability.

What are you unintentionally miscommunicating?


lmg tfy
LMGTFY
Secure
https://lmgtfy.com/?q=how+to+use+pgp

Wherever there is a miscommunication, there exists a human security vulnerability.


Simple Domain Name Registrar
serena
iwantmyname (Ideegeo Group LTD) [NZ] https://iwantmyname.com
iwantmyname
Domains / Apps / Pricing / About / Blog / Contact
Sign in
A good domain name makes all the difference.
chase-help-and-support.com
Have an existing domain with another registrar? Start your transfer now.
Privacy by Default
Not sure what WHOIS privacy is? No worries - we automatically turn it on to keep your info away from spammers.
About WHOIS privacy
Supporters of the Indie Web
Instantly connect your domain to the best of the indie web, from clean site builders to beautiful blogging tools.
Browse our plugins
What We're All About
We believe in transparency, privacy, simplicity, community, and progressive employee policies.
Inside iwantmyname
QUICK LINKS
COMPANY
SUPPORT
EXTRAS


Let's Encrypt - Free SSL/TLS
serena
Secure https://letsencrypt.org
LINUX FOUNDATION COLLABORATIVE PROJECTS
Let's Encrypt
Documentation
Get Help
Donate
About Us
Let's Encrypt is a free, automated, and open Certificate Authority.
Get Started
Donate
FROM OUR BLOG
Apr 4, 2018
Engineering deep dive: Encoding of SCTs in certificates
How Signed Certificate Timestamps get embedded in
MAJOR SPONSORS AND DONORS
moz://a
Akamai
CISCO
OVH
chrome
IdenTrust
FORD FOUNDATION

Credit Card, Mortgage, Bankin ×

serena

Secure | https://chase-help-and-support.com

CHASE

CONGRATS ON ANOTHER ONE!

#StrengthInNumbers

Welcome

Username

Password

Remember me Use token >

Sign in

Forgot username/password? >

Not enrolled? Sign up now. >

Open an account

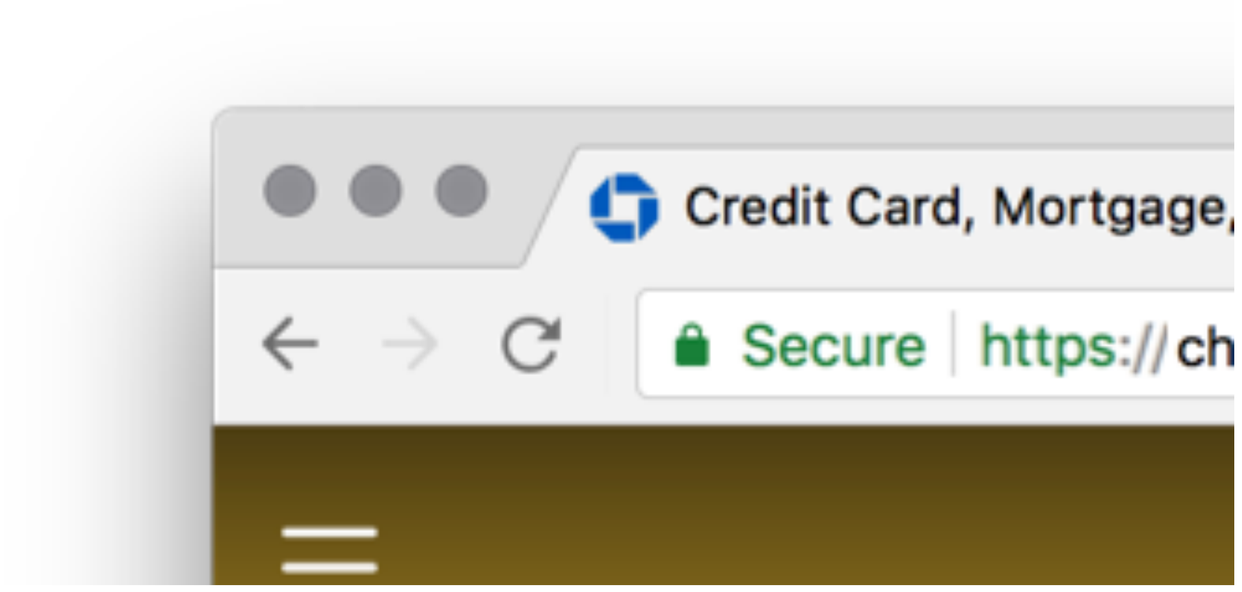
Savings Accounts & CDs

Checking Accounts

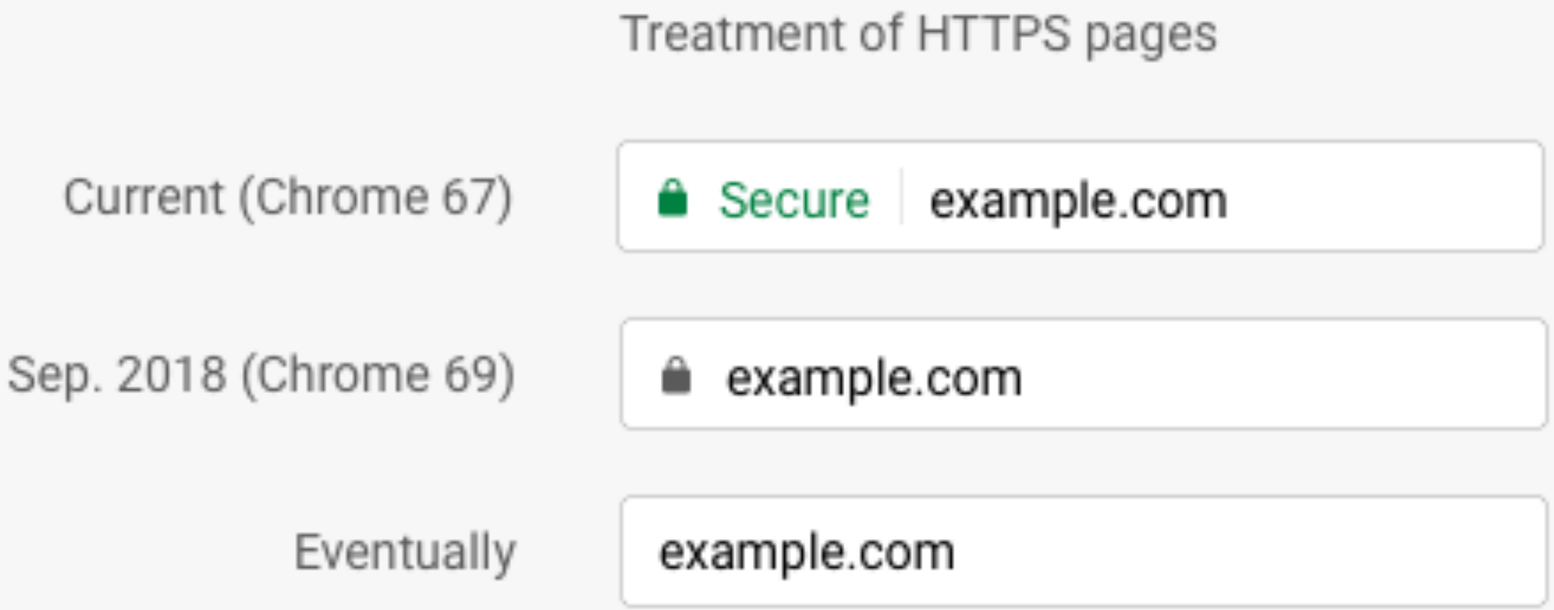
Find a credit card

Home Lending

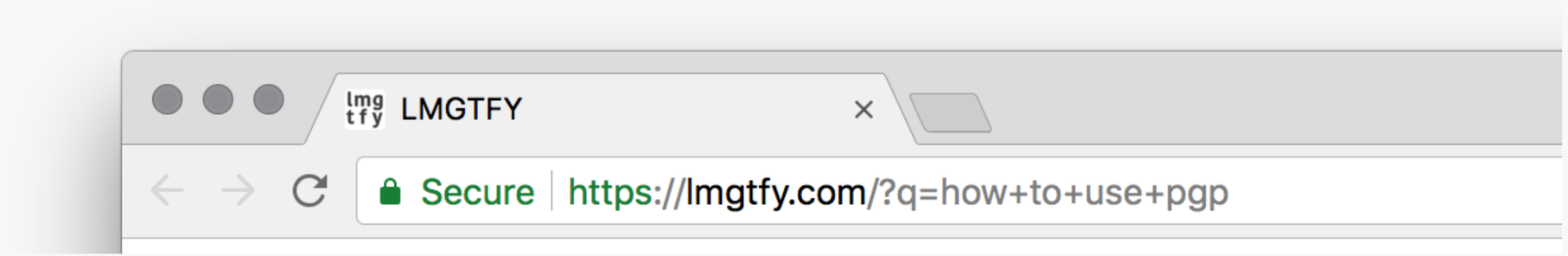
Car Buying & Loans


Credit Card, Mortgage,
Secure
https://ch

(I didn’t actually do this)



https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html



Do your end users know what you're trying to communicate?

What is their mental model of what's happening, compared to yours?

For your consideration:

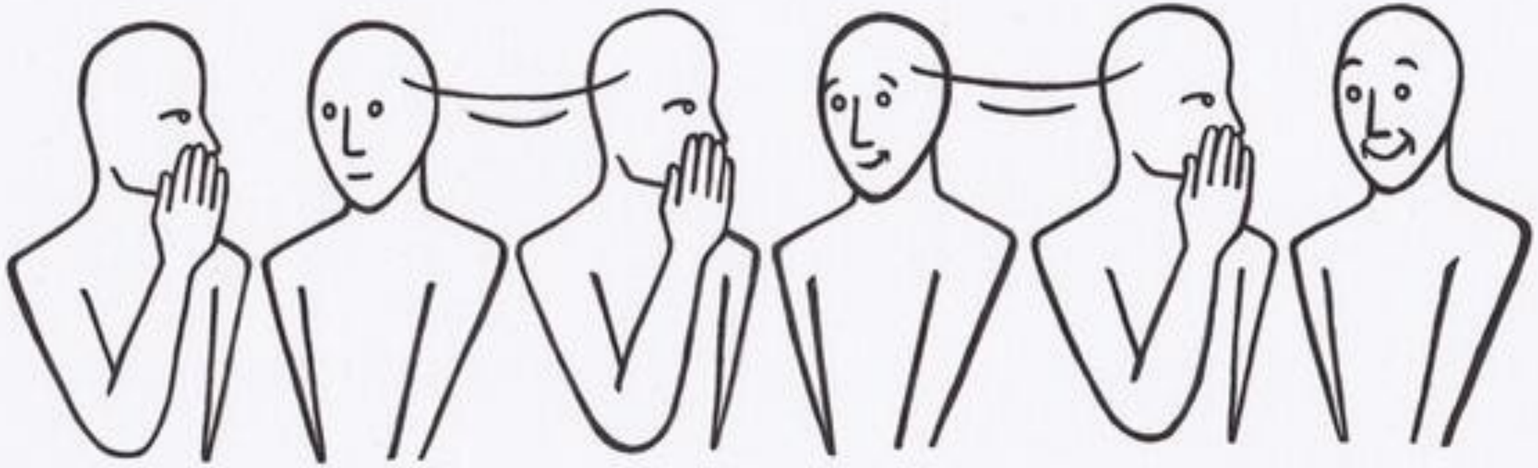
1. Intent
2. Path of Least Resistance
3. (Mis)communication
4.

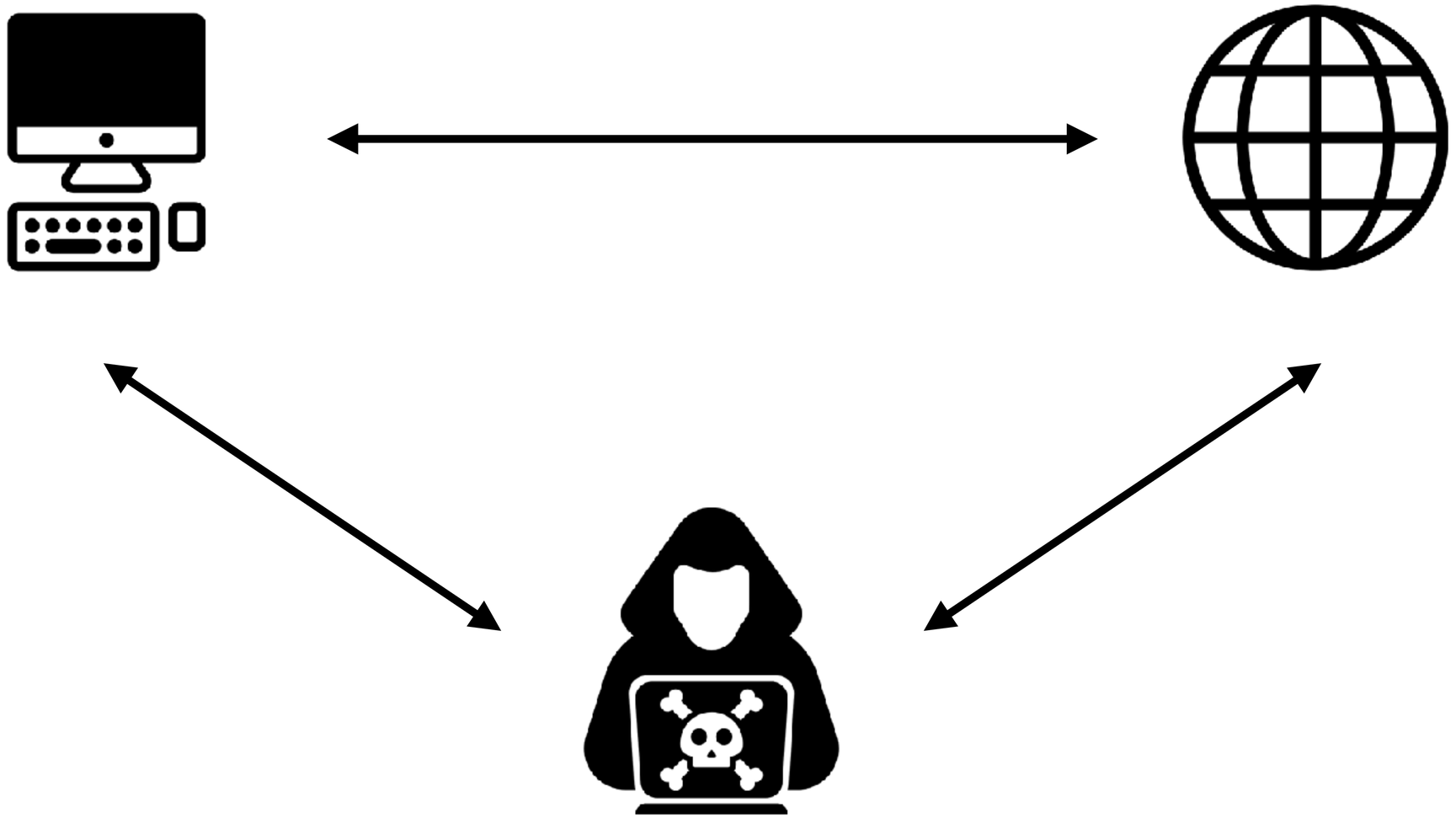
For your consideration:

1. Intent
2. Path of Least Resistance
3. (Mis)communication
4. Mental model matching

Mental models

It’s the user’s expectations that define whether a system is secure or not.





“A system is secure from a given user’s perspective if the set of actions that each actor can do are bounded by what the user believes it can do.”

–Ka-Ping Yee, “User Interaction Design for Secure Systems”,
Proc. 4th Int’l Conf. Information and Communications Security, Springer-Verlag, 2002

Find their model,
match to that

+

Influence their model,
match to system

Find their model

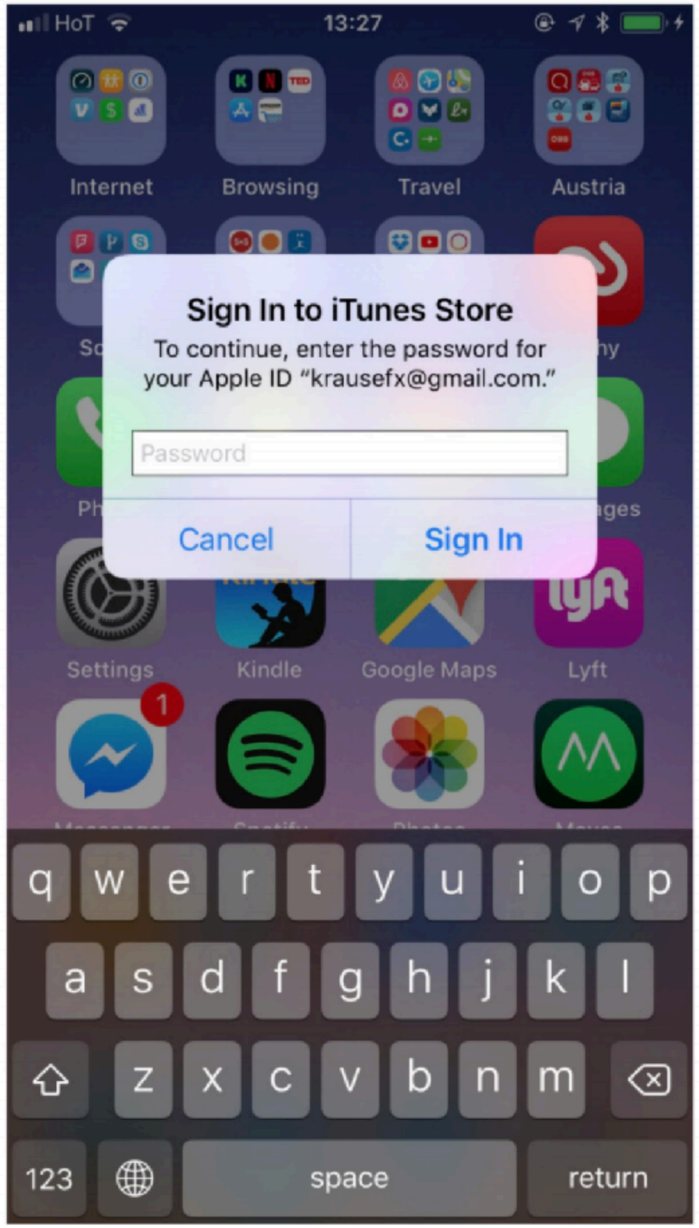
- Go to customer sessions!
- Observe end users
- Infer intent through context

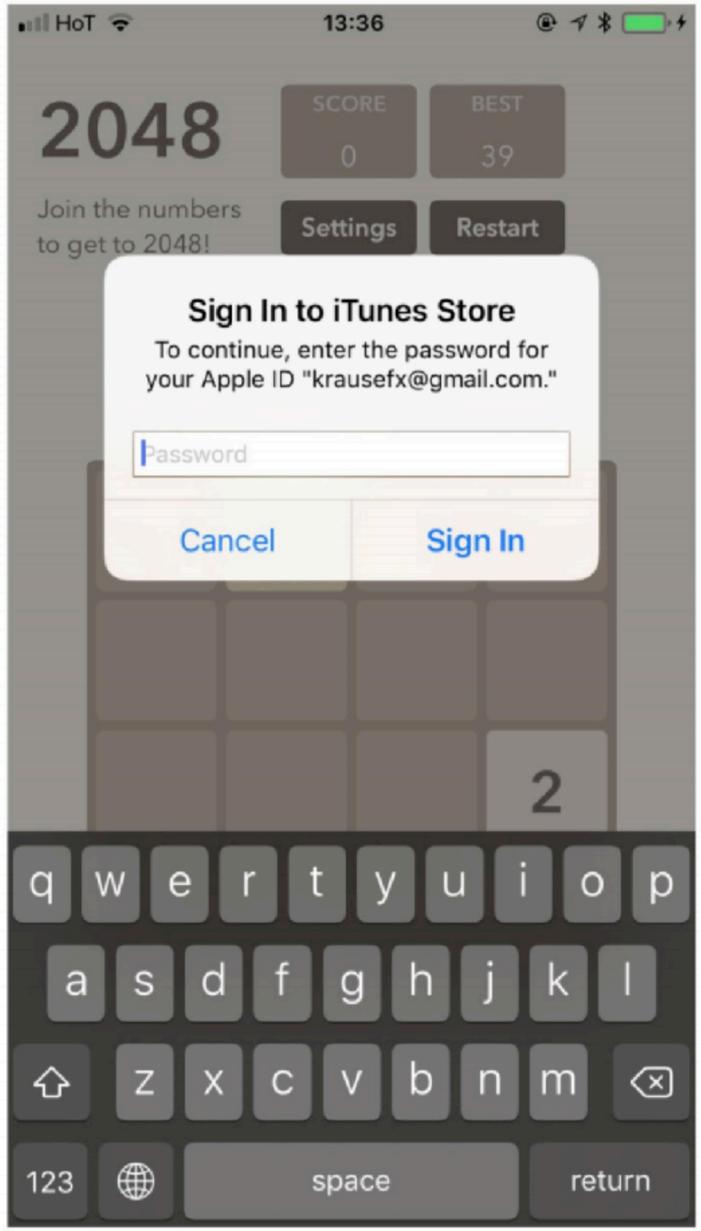
Influence their model

- When we make, we teach
- Whenever someone interacts with us / a thing we made, they learn.
- Path of least resistance becomes the default “way to do things”.

How are we already influencing users' models?

iOS

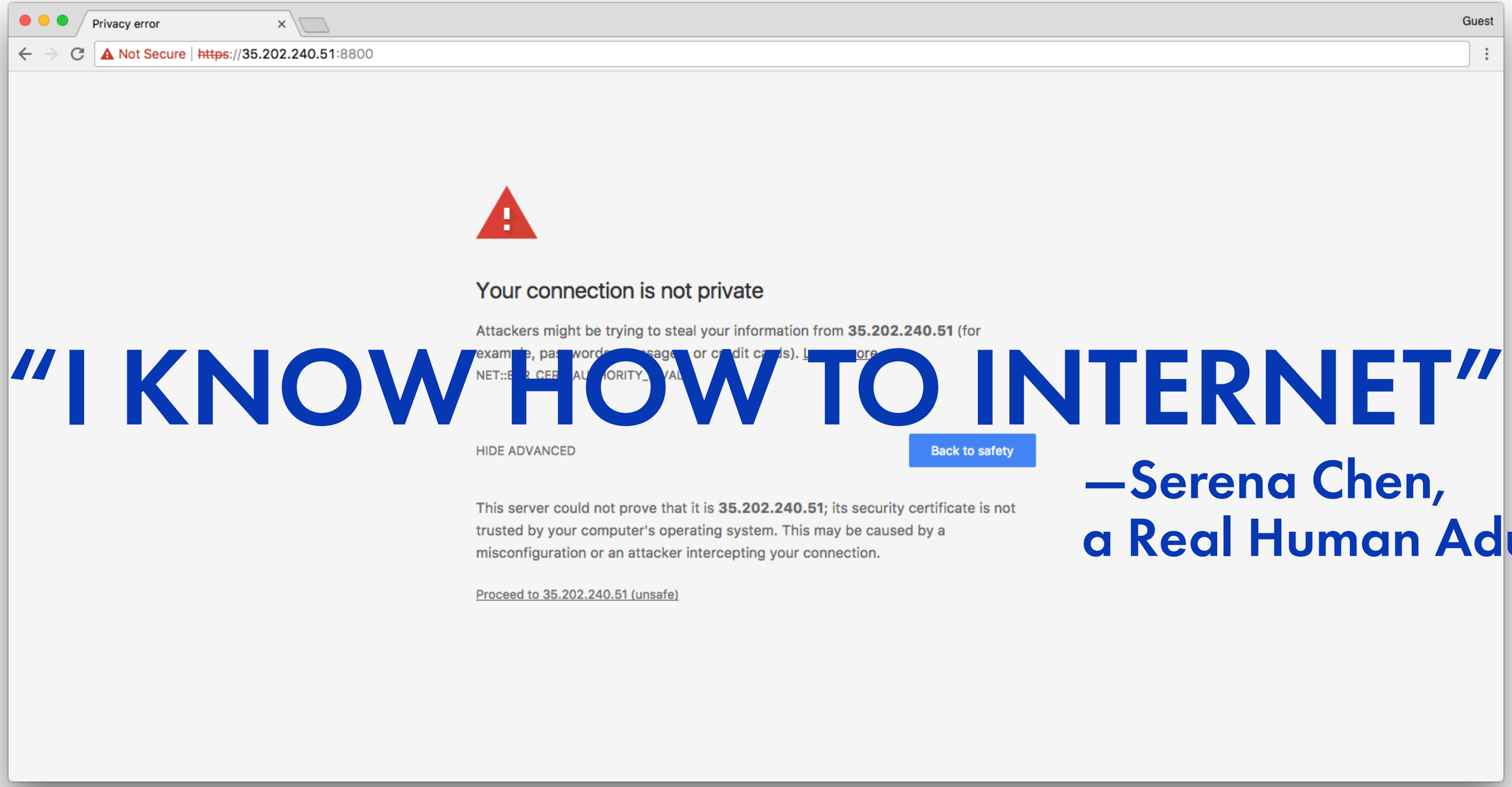




Phish

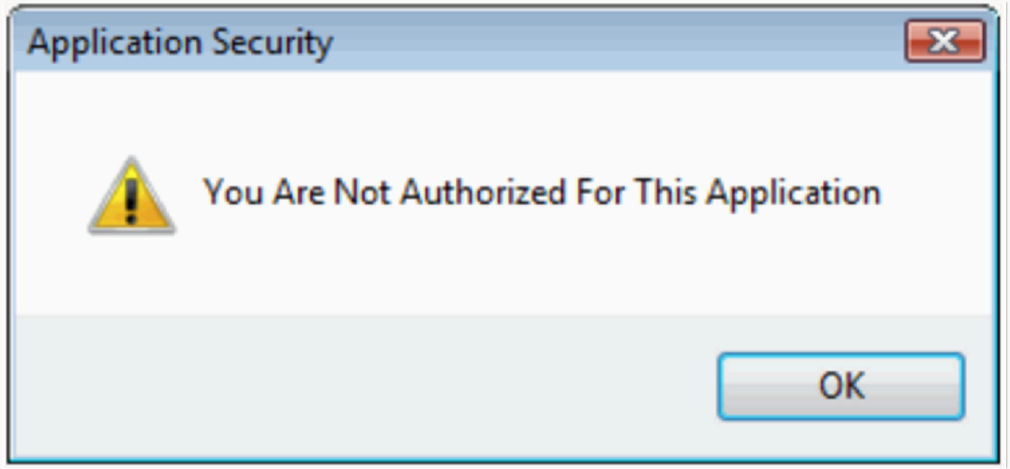
https://krausefx.com/blog/ios-privacy-stealpassword-easily-get-the-users-apple-id-password-just-by-asking

What are we teaching?

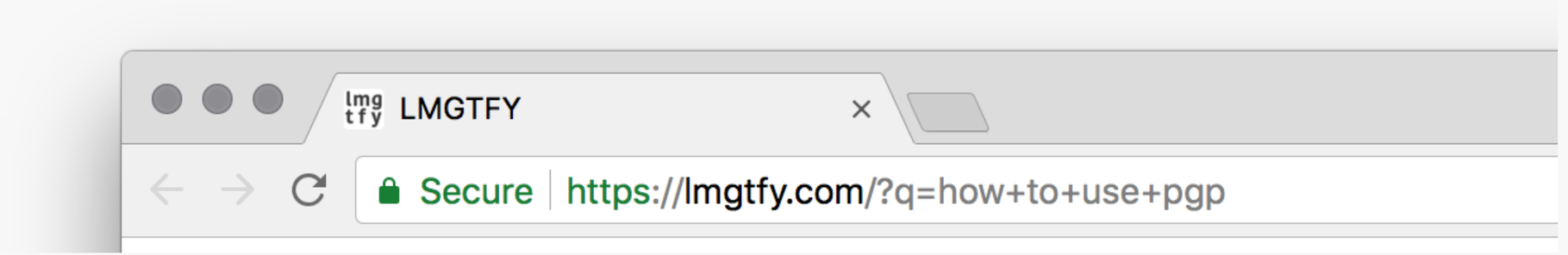


"I KNOW HOW TO INTERNET"

—Serena Chen,
a Real Human Adult™


Application Security
You Are Not Authorized For This Application
OK

Understand end user mental models


lmg tfy
LMGTFY
Secure
https://lmgtfy.com/?q=how+to+use+pgp

What are your users' mental models?

Review

Takeaways

- Cross pollination is rare. This is a missed opportunity!
- Our jobs are about *outcomes* based on our specific goals
- Align the user's goals to your security goals

Takeaways

- Aim to know their intent
- Collaborate with design to craft secure paths of least resistance
- Understand their mental model vs yours
- Communicate to that model

One final anecdote…


No!

Thanks!

Fight me @Sereeena