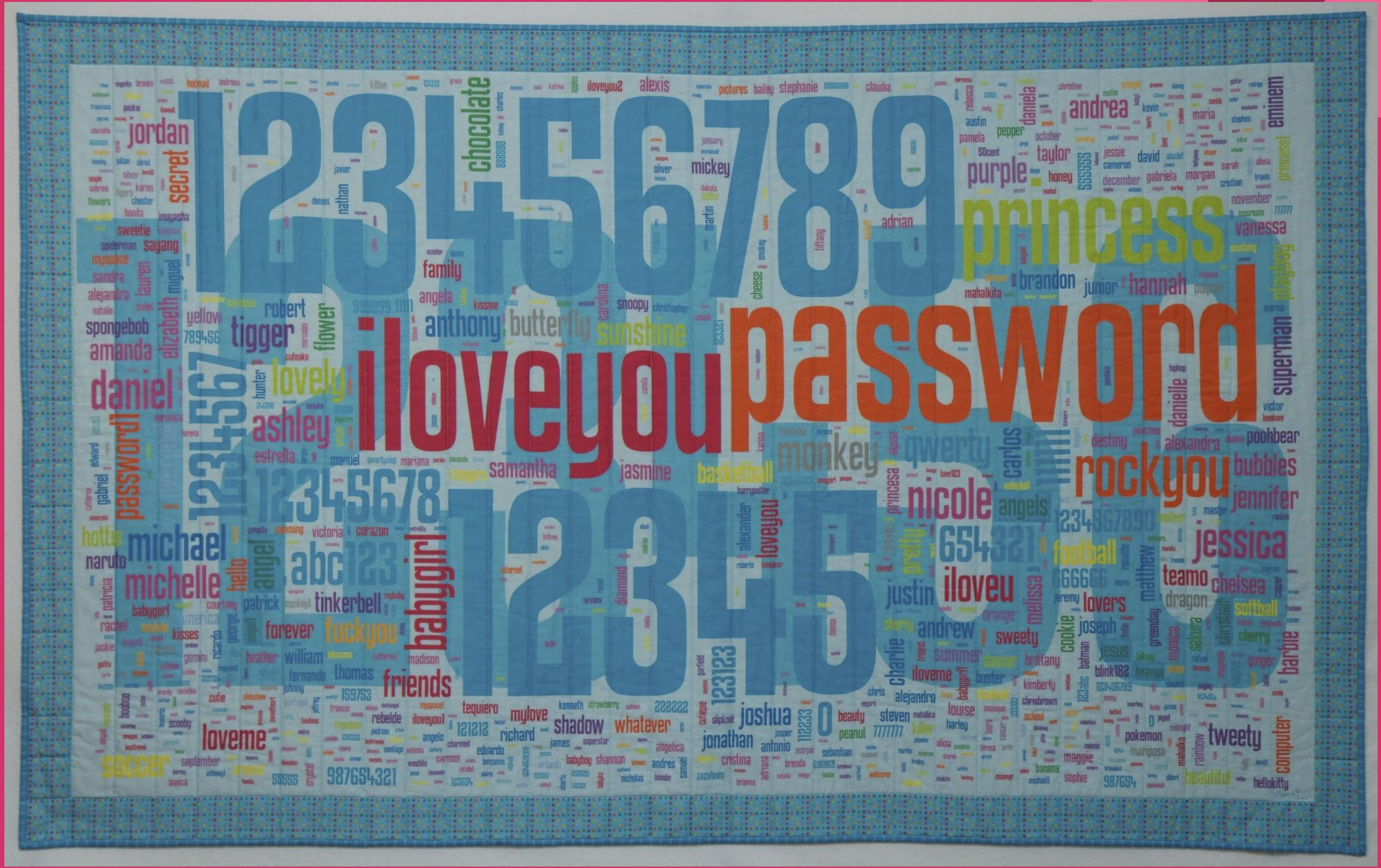
Personal Digital Security

David & Sam

https://tinyurl.com/2019gpisecurity

Goals of Security

- Confidentiality
- Integrity
- Availability


123456789
password
iloveyou
12345
princess
rockyou
1234567
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
sunshine
chocolate
password1
soccer
anthony
friends
butterfly
purple
angel
jordan
liverpool
justin
loveme
fuckyou
123123
football
secret
andrea
carlos
jennifer
joshua
bubbles
1234567890
superman
hannah
amanda
loveyou
pretty
basketball
andrew
angels
tweety
flower
playboy
hello
elizabeth
hottie
tinkerbell
charlie
samantha
barbie
chelsea
lovers
teamo
jasmine
brandon
666666
shadow
melissa
eminem
matthew
robert
danielle
forever
family
jonathan
987654321
computer
whatever
dragon
vanessa
cookie
naruto
summer
sweety
spongebob
joseph
junior
softball
taylor
yellow
daniela
lauren
mickey
princesa
alexandra
alexis
jesus
estrella
miguel
william
thomas
beautiful
mylove
angela
poohbear
patrick
iloveme
sakura
adrian
alexander
destiny
christian
121212
sayang
america
dancer
monica
richard
112233
princess1
555555
diamond
carolina
steven
rangers
louise
orange
789456
999999
shorty
11111
nathan
snoopy
gabriel
hunter
cherry
killer
sandra
alejandro
buster
george
brittany
alejandra
patricia
rachel
tequiero
7777777
cheese
159753
arsenal
dolphin
antonio
heather
david
ginger
stephanie
peanut
blink182
sweetie
222222
beauty
987654
victoria
honey
00000
fernando
pokemon
maggie
corazon
chicken
pepper
cristina
rainbow
kisses
manuel
myspace
rebelde
angel1
ricardo
babygurl
heaven
55555
baseball
martin
greenday
november
alyssa
madison
mother
123321
123abc
mahalkita
batman
september
december
morgan
mariposa
maria
gabriela
iloveyou2
bailey
jeremy
pamela
kimberly
gemini
shannon
pictures
asshole
sophie
jessie
hellokitty
claudia
babygirl1
angelica
austin
mahalko
victor
horses
tiffany
mariana
eduardo
andres
courtney
booboo
kissme
harley
ronaldo
iloveyou1
precious
october
inuyasha
peaches
veronica
chris
888888
adriana
cutie
james
banana
prince
friend
jesus1
crystal
celtic
zxcvbnm
edward
oliver
diana
samsung
freedom
angelo
kenneth
master
scooby
carmen
456789
sebastian
rebecca
jackie
spiderman
christopher
karina
johnny
hotmail
0123456789
school
barcelona
august
orlando
samuel
cameron
slipknot
cutiepie
monkey1
50cent
bonita
kevin
bitch
maganda
babyboy
casper
brenda
adidas
kitten
karen
mustang
isabel
natalie
cuteako
javier
789456123
123654
sarah
bowwow
portugal
laura
777777
marvin
denise
tigers
volleyball
jasper
rockstar
january
fuckoff
alicia
nicholas
flowers
cristian
tintin
bianca
chrisbrown
chester
101010
smokey
silver
internet
sweet
strawberry
garfield
dennis
panget
francis
cassie
benfica
love123
asdfgh
lollipop
olivia
cancer
camila
qwertyuiop
superstar
harrypotter
ihateyou
charles
monique
midnight
vincent
christine
apples
scorpio
jordan23
lorena
andreea
mercedes
katherine
charmed
abigail
rafael
icecream
mexico
brianna
nirvana
aaliyah
pookie
johncena
lovelove
fucker
abcdef
benjamin
131313
gangsta
brooke
333333
hiphop
aaaaaa
mybaby
sergio
welcome
metallica
julian
travis
myspace1
babyblue
sabrina
michael1
jeffrey
stephen
love
dakota
catherine
badboy
fernanda
westlife
blondie
sasuke
smiley
jackson
simple
melanie
steaua
dolphins
roberto
fluffy
teresa
piglet
ronald
slideshow
asdfghjkl
minnie
newyork
jason
raymond
santiago
jayson
88888888
5201314
jerome
gandako
muffin
gatita
babyko
246810
sweetheart
chivas
ladybug
kitty
popcorn
alberto
valeria
cookies
leslie
jenny
nicole1
12345678910
leonardo
jayjay
liliana
dexter
sexygirl
232323
amores
rockon
christ
babydoll
anthony1
marcus
bitch1
fatima
miamor
lover
chris1
single
eeyore
lalala
252525
scooter
natasha
skittles
brooklyn
colombia
159357
teddybear
winnie
happy
manutd
123456a
britney
katrina
christina
pasaway
cocacola
mahal
grace
linda
albert
tatiana
london
cantik
0123456
lakers
marie
teiubesc
147258369
charlotte
natalia
francisco
amorcito
smile
paola
angelito
manchester
hahaha
elephant
mommy1
shelby
147258
kelsey
genesis
amigos
snickers
xavier
turtle
marlon
linkinpark
claire
stupid
147852
marina
garcia
fuckyou1
diego
brandy
letmein
hockey
444444
sharon
bonnie
spider
iverson
andrei
justine
frankie
pimpin
disney
rabbit
54321
fashion
soccer1
red123
bestfriend
england
hermosa
456123
qazwsx
bandit
danny
allison
emily
102030
sucker
jeremiah
maryjane
mermaid
simpsons
abcd1234
jonas
lucky
lovely1
yankees
loverboy
brown

Passwords

Dr. Lorrie Cranor

How to make a good password?

How to make a good password?

“Designing Password Policies for Strength and Usability”

How to make a good password?

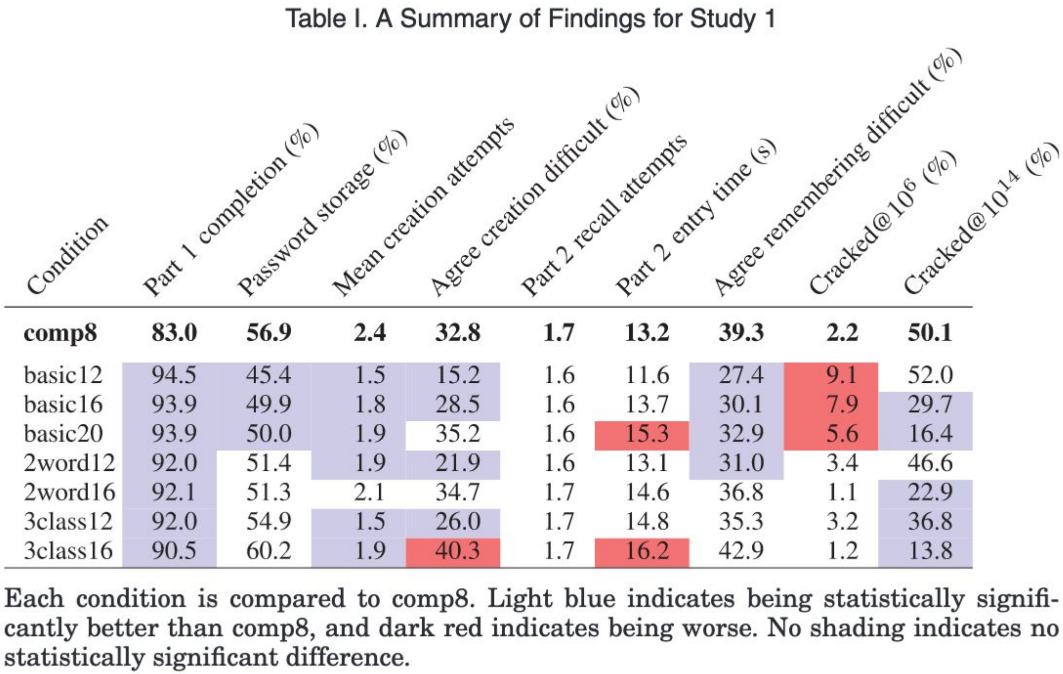


Table I. A Summary of Findings for Study 1

Condition	Part 1 completion (%)	Password storage (%)	Mean creation attempts	Agree creation difficult (%)	Part 2 recall attempts	Part 2 entry time (s)	Agree remembering difficult (%)	Cracked@10^6 (%)	Cracked@10^{14} (%)
comp8	**83.0**	**56.9**	**2.4**	**32.8**	**1.7**	**13.2**	**39.3**	**2.2**	**50.1**
basic12	94.5	45.4	1.5	15.2	1.6	11.6	27.4	9.1	52.0
basic16	93.9	49.9	1.8	28.5	1.6	13.7	30.1	7.9	29.7
basic20	93.9	50.0	1.9	35.2	1.6	15.3	32.9	5.6	16.4
2word12	92.0	51.4	1.9	21.9	1.6	13.1	31.0	3.4	46.6
2word16	92.1	51.3	2.1	34.7	1.7	14.6	36.8	1.1	22.9
3class12	92.0	54.9	1.5	26.0	1.7	14.8	35.3	3.2	36.8
3class16	90.5	60.2	1.9	40.3	1.7	16.2	42.9	1.2	13.8

Each condition is compared to comp8. Light blue indicates being statistically significantly better than comp8, and dark red indicates being worse. No shading indicates no statistically significant difference.

How to make a good password?

Table I. A Summary of Findings for Study 1

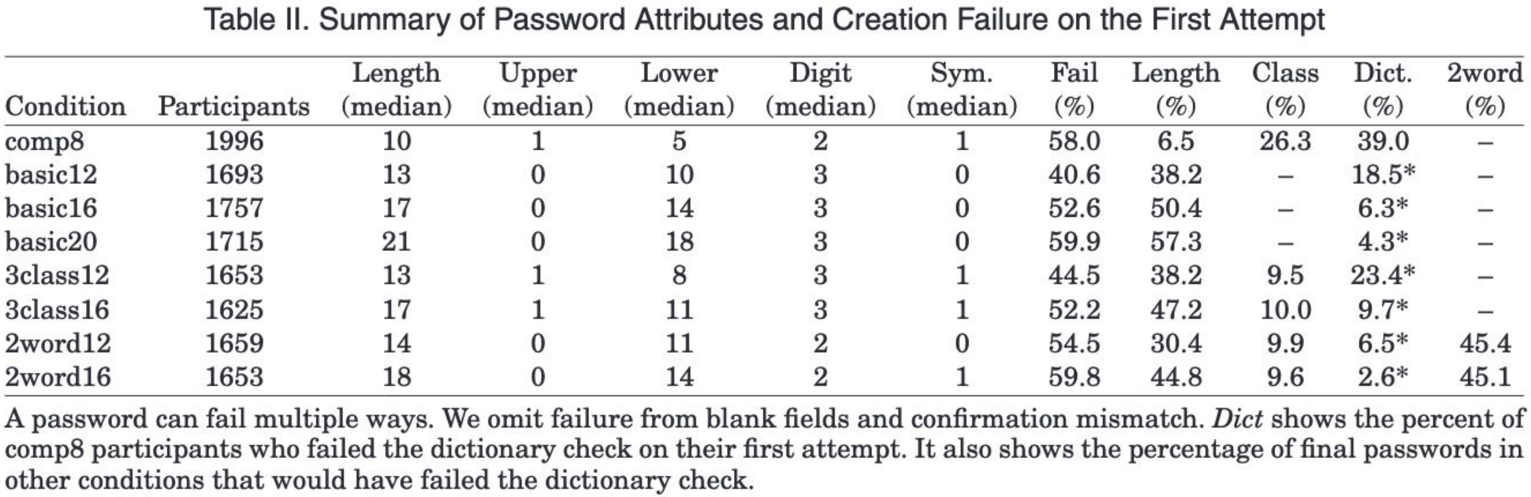
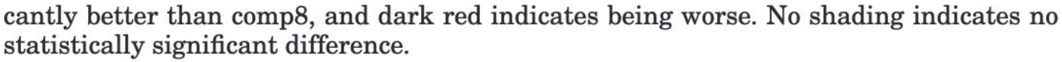


Table II. Summary of Password Attributes and Creation Failure on the First Attempt

Condition	Participants	Length (median)	Upper (median)	Lower (median)	Digit (median)	Sym. (median)	Fail (%)	Length (%)	Class (%)	Dict. (%)	2word (%)
comp8	1996	10	1	5	2	1	58.0	6.5	26.3	39.0	–
basic12	1693	13	0	10	3	0	40.6	38.2	–	18.5*	–
basic16	1757	17	0	14	3	0	52.6	50.4	–	6.3*	–
basic20	1715	21	0	18	3	0	59.9	57.3	–	4.3*	–
3class12	1653	13	1	8	3	1	44.5	38.2	9.5	23.4*	–
3class16	1625	17	1	11	3	1	52.2	47.2	10.0	9.7*	–
2word12	1659	14	0	11	2	0	54.5	30.4	9.9	6.5*	45.4
2word16	1653	18	0	14	2	1	59.8	44.8	9.6	2.6*	45.1

A password can fail multiple ways. We omit failure from blank fields and confirmation mismatch. *Dict* shows the percent of comp8 participants who failed the dictionary check on their first attempt. It also shows the percentage of final passwords in other conditions that would have failed the dictionary check.



cantly better than comp8, and dark red indicates being worse. No shading indicates no statistically significant difference.

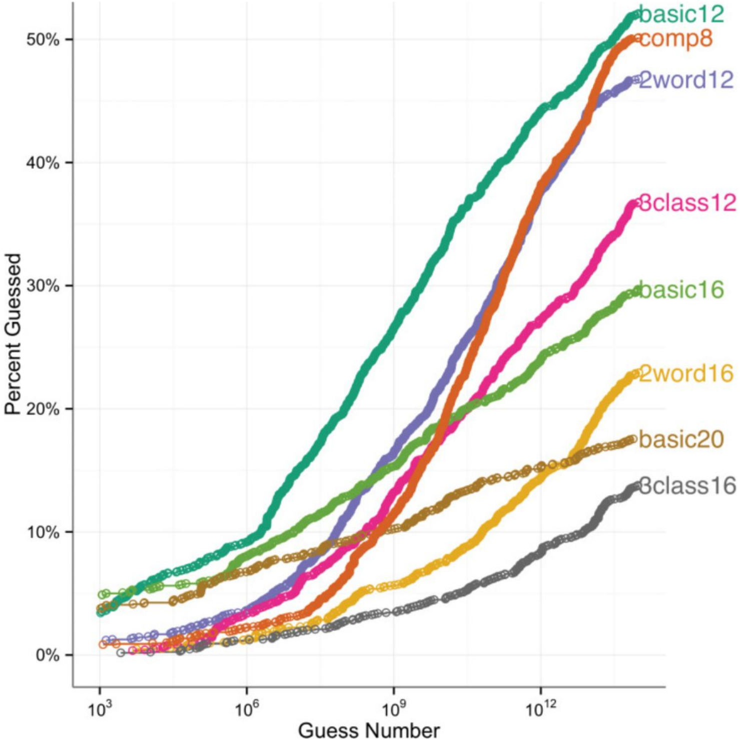
How to make a good password?

Table II. Su rst Attempt

Condition	Participants	(	gth ɓ)	Class (%)	Dict. (%)	2word (%)
comp8	1996		5	26.3	39.0	–
basic12	1693		.2	–	18.5*	–
basic16	1757		.4	–	6.3*	–
basic20	1715		.3	–	4.3*	–
3class12	1653		.2	9.5	23.4*	–
3class16	1625		.2	10.0	9.7*	–
2word12	1659		.4	9.9	6.5*	45.4
2word16	1653		.8	9.6	2.6*	45.1

A password can fail multipl h. *Dict* shows the percent of
comp8 participants who fail entage of final passwords in
other conditions that would

cantly be icates no
statistica



How to make a good password?

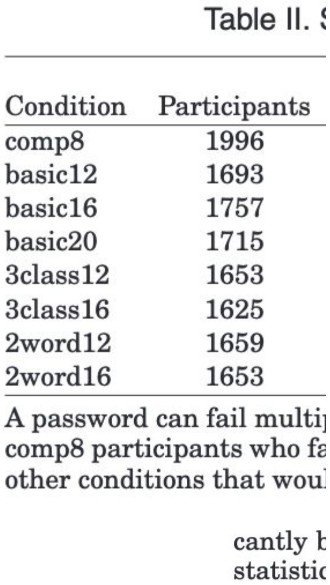


Table II. S

Condition	Participants
comp8	1996
basic12	1693
basic16	1757
basic20	1715
3class12	1653
3class16	1625
2word12	1659
2word16	1653

A password can fail multi
comp8 participants who fa
other conditions that woul

cantly b
statistic

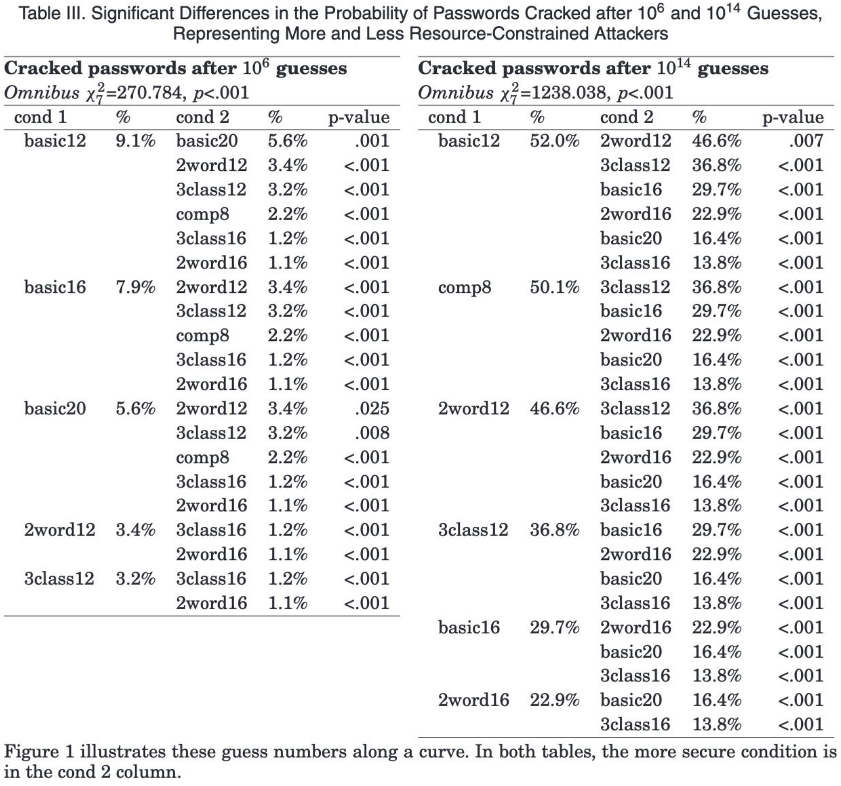


Table III. Significant Differences in the Probability of Passwords Cracked after 10^6 and 10^{14} Guesses, Representing More and Less Resource-Constrained Attackers

Cracked passwords after 10^6 guesses

Omnibus χ^2_7=270.784, p<.001

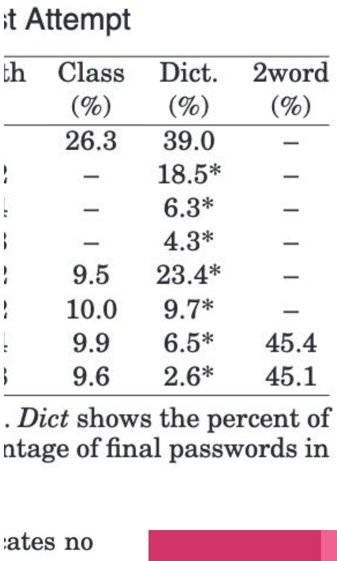
cond 1	%	cond 2	%	p-value
basic12	9.1%	basic20	5.6%	.001
		2word12	3.4%	<.001
		3class12	3.2%	<.001
		comp8	2.2%	<.001
		3class16	1.2%	<.001
		2word16	1.1%	<.001
basic16	7.9%	2word12	3.4%	<.001
		3class12	3.2%	<.001
		comp8	2.2%	<.001
		3class16	1.2%	<.001
		2word16	1.1%	<.001
basic20	5.6%	2word12	3.4%	.025
		3class12	3.2%	.008
		comp8	2.2%	<.001
		3class16	1.2%	<.001
		2word16	1.1%	<.001
2word12	3.4%	3class16	1.2%	<.001
		2word16	1.1%	<.001
3class12	3.2%	3class16	1.2%	<.001
		2word16	1.1%	<.001

Cracked passwords after 10^{14} guesses

Omnibus χ^2_7=1238.038, p<.001

cond 1	%	cond 2	%	p-value
basic12	52.0%	2word12	46.6%	.007
		3class12	36.8%	<.001
		basic16	29.7%	<.001
		2word16	22.9%	<.001
		basic20	16.4%	<.001
		3class16	13.8%	<.001
comp8	50.1%	3class12	36.8%	<.001
		basic16	29.7%	<.001
		2word16	22.9%	<.001
		basic20	16.4%	<.001
		3class16	13.8%	<.001
2word12	46.6%	3class12	36.8%	<.001
		basic16	29.7%	<.001
		2word16	22.9%	<.001
		basic20	16.4%	<.001
		3class16	13.8%	<.001
3class12	36.8%	basic16	29.7%	<.001
		2word16	22.9%	<.001
		basic20	16.4%	<.001
		3class16	13.8%	<.001
basic16	29.7%	2word16	22.9%	<.001
		basic20	16.4%	<.001
		3class16	13.8%	<.001
2word16	22.9%	basic20	16.4%	<.001
		3class16	13.8%	<.001

Figure 1 illustrates these guess numbers along a curve. In both tables, the more secure condition is in the cond 2 column.



t Attempt

th	Class (%)	Dict. (%)	2word (%)
	26.3	39.0	–
	–	18.5*	–
	–	6.3*	–
	–	4.3*	–
	9.5	23.4*	–
	10.0	9.7*	–
	9.9	6.5*	45.4
	9.6	2.6*	45.1

. *Dict* shows the percent of
ntage of final passwords in

ates no

How to make a good password?

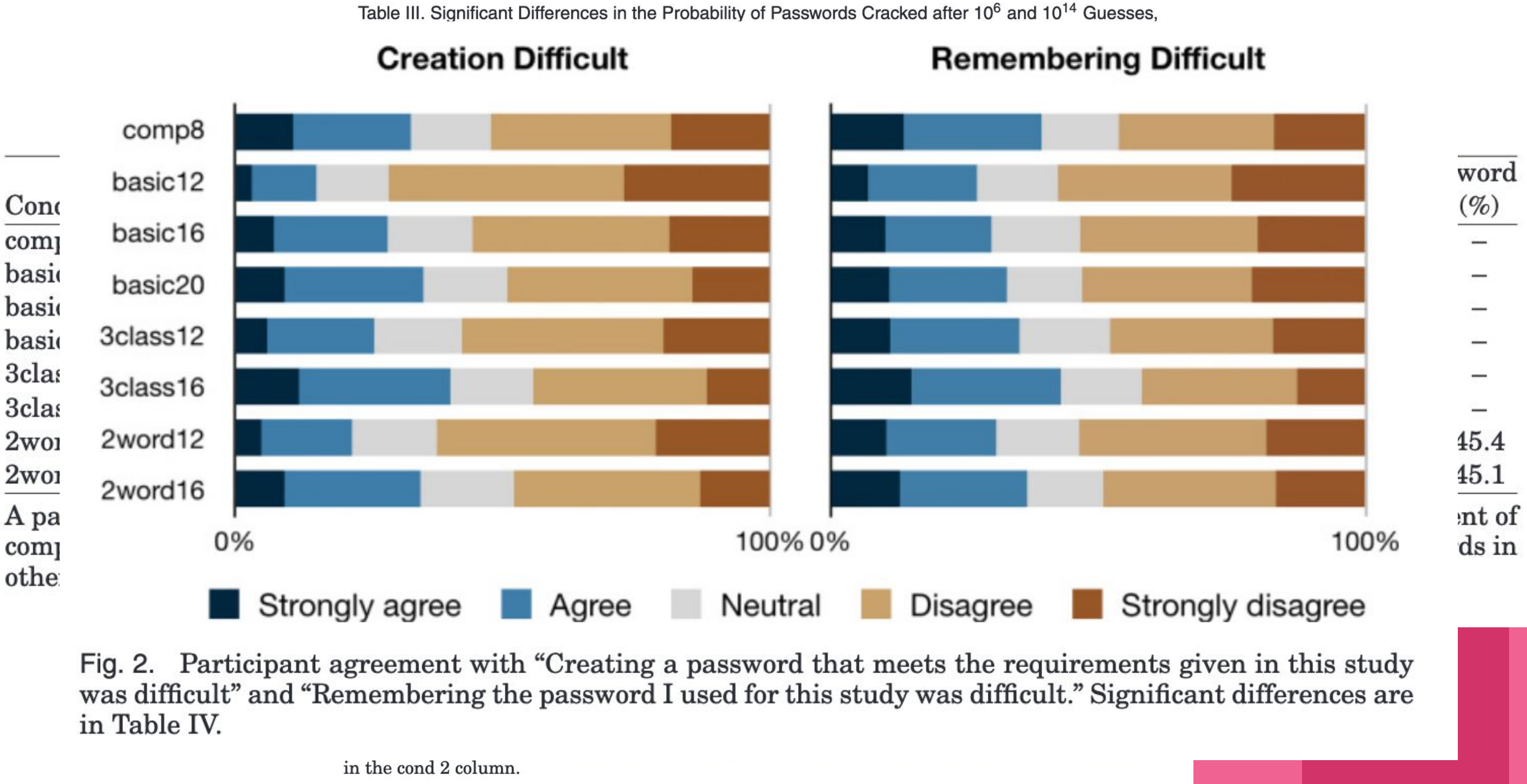


Table III. Significant Differences in the Probability of Passwords Cracked after 10^6 and 10^{14} Guesses,

Cond
comp
basi
basi
basi
3clas
3clas
2wor
2wor

A pa
comp
othe

word
(%)
–
–
–
–
–
–
45.4
45.1

nt of
ds in

Fig. 2. Participant agreement with “Creating a password that meets the requirements given in this study was difficult” and “Remembering the password I used for this study was difficult.” Significant differences are in Table IV.

in the cond 2 column.

How to make a good password?

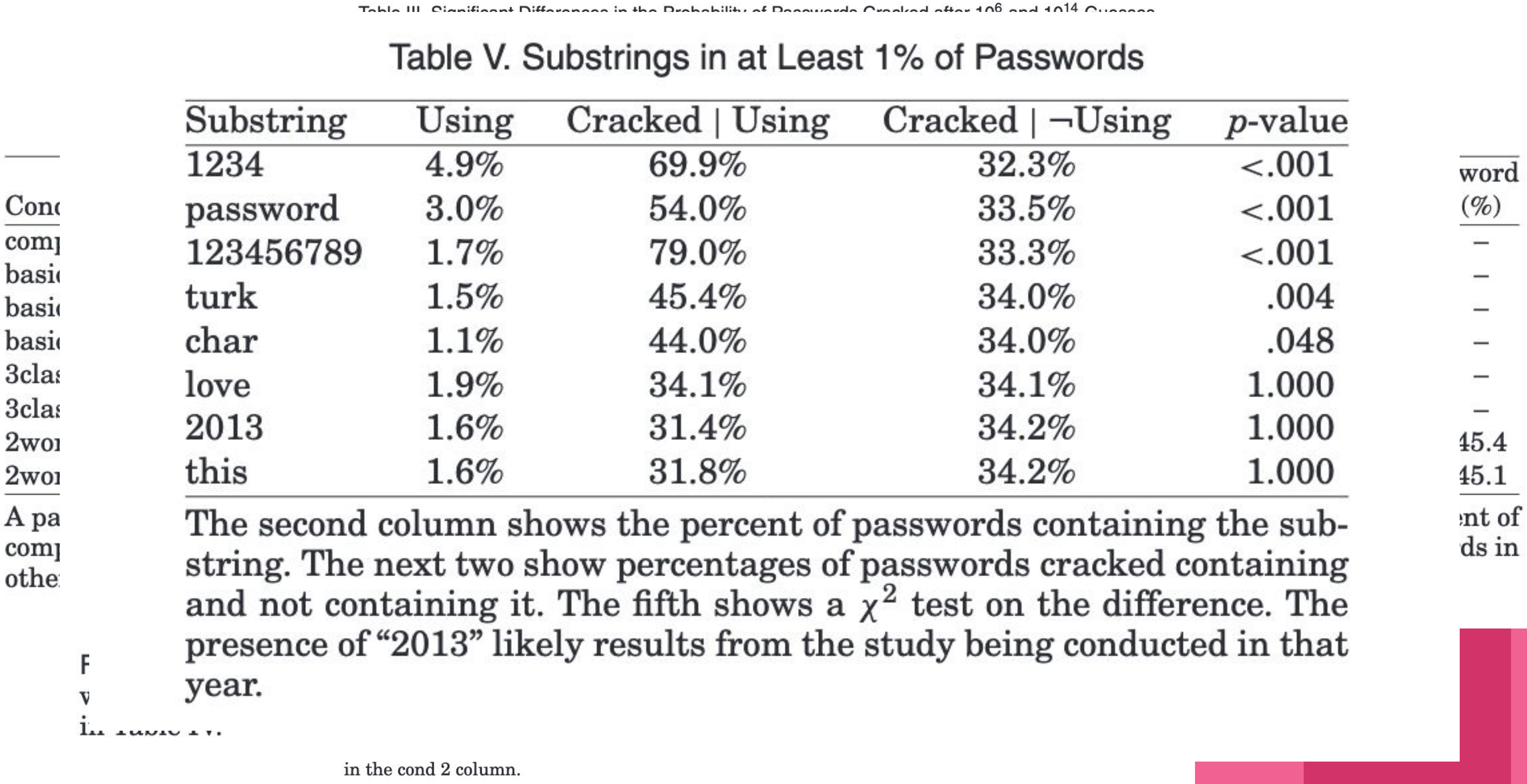


Table III. Significant Differences in the Probability of Passwords Cracked after 10^6 and 10^{14} Guesses

Table V. Substrings in at Least 1% of Passwords

Substring	Using	Cracked | Using	Cracked | ¬Using	*p*-value
1234	4.9%	69.9%	32.3%	<.001
password	3.0%	54.0%	33.5%	<.001
123456789	1.7%	79.0%	33.3%	<.001
turk	1.5%	45.4%	34.0%	.004
char	1.1%	44.0%	34.0%	.048
love	1.9%	34.1%	34.1%	1.000
2013	1.6%	31.4%	34.2%	1.000
this	1.6%	31.8%	34.2%	1.000

The second column shows the percent of passwords containing the substring. The next two show percentages of passwords cracked containing and not containing it. The fifth shows a χ^2 test on the difference. The presence of "2013" likely results from the study being conducted in that year.

Conc
comp
basic
basic
basic
3clas
3clas
2wor
2wor
A pa
comp
othe

word
(%)
–
–
–
–
–
–
45.4
45.1
nt of
ds in

in the cond 2 column.

How to make a good password?

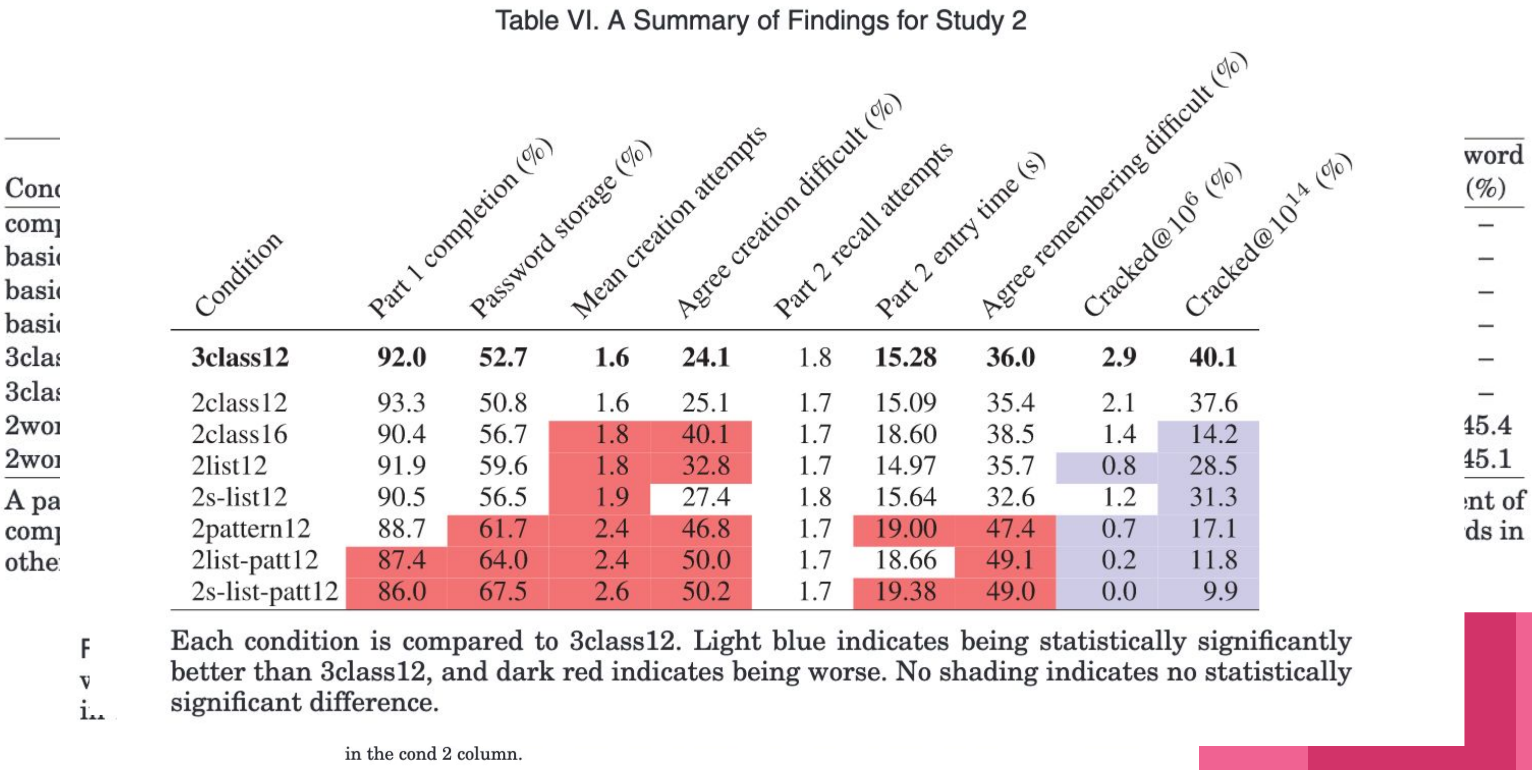


Table VI. A Summary of Findings for Study 2

Condition	Part 1 completion (%)	Password storage (%)	Mean creation attempts	Agree creation difficult (%)	Part 2 recall attempts	Part 2 entry time (s)	Agree remembering difficult (%)	Cracked@10^6 (%)	Cracked@10^{14} (%)
3class12	**92.0**	**52.7**	**1.6**	**24.1**	1.8	**15.28**	**36.0**	**2.9**	**40.1**
2class12	93.3	50.8	1.6	25.1	1.7	15.09	35.4	2.1	37.6
2class16	90.4	56.7	1.8	40.1	1.7	18.60	38.5	1.4	14.2
2list12	91.9	59.6	1.8	32.8	1.7	14.97	35.7	0.8	28.5
2s-list12	90.5	56.5	1.9	27.4	1.8	15.64	32.6	1.2	31.3
2pattern12	88.7	61.7	2.4	46.8	1.7	19.00	47.4	0.7	17.1
2list-patt12	87.4	64.0	2.4	50.0	1.7	18.66	49.1	0.2	11.8
2s-list-patt12	86.0	67.5	2.6	50.2	1.7	19.38	49.0	0.0	9.9

Each condition is compared to 3class12. Light blue indicates being statistically significantly better than 3class12, and dark red indicates being worse. No shading indicates no statistically significant difference.

Conc
comp
basic
basic
basic
3clas
3clas
2wor
2wor
A pa
comp
othe

word
(%)
–
–
–
–
–
–
45.4
45.1
ent of
ds in

F
v
i..

in the cond 2 column.

How to make a good password?

Table VI. A Summary of Findings for Study 2

Cond	word (%)
comp	–
basi	–
basi	–
basi	–
3cla	–
3cla	–
2wo	45.4
2wo	45.1

A pa nt of
comp ds in
othe

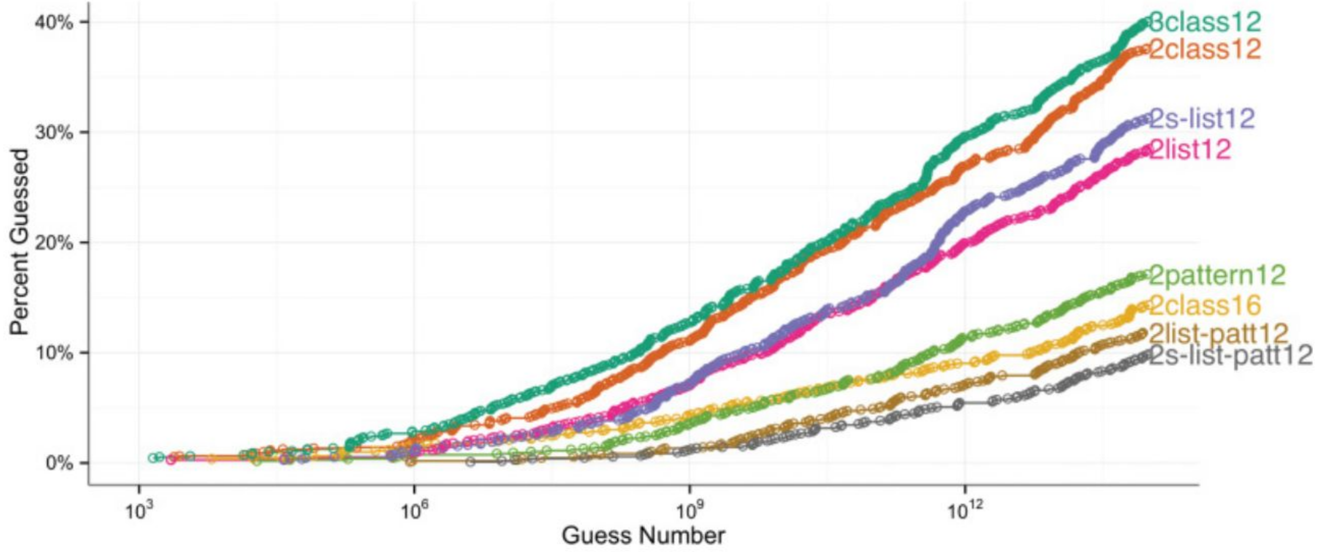
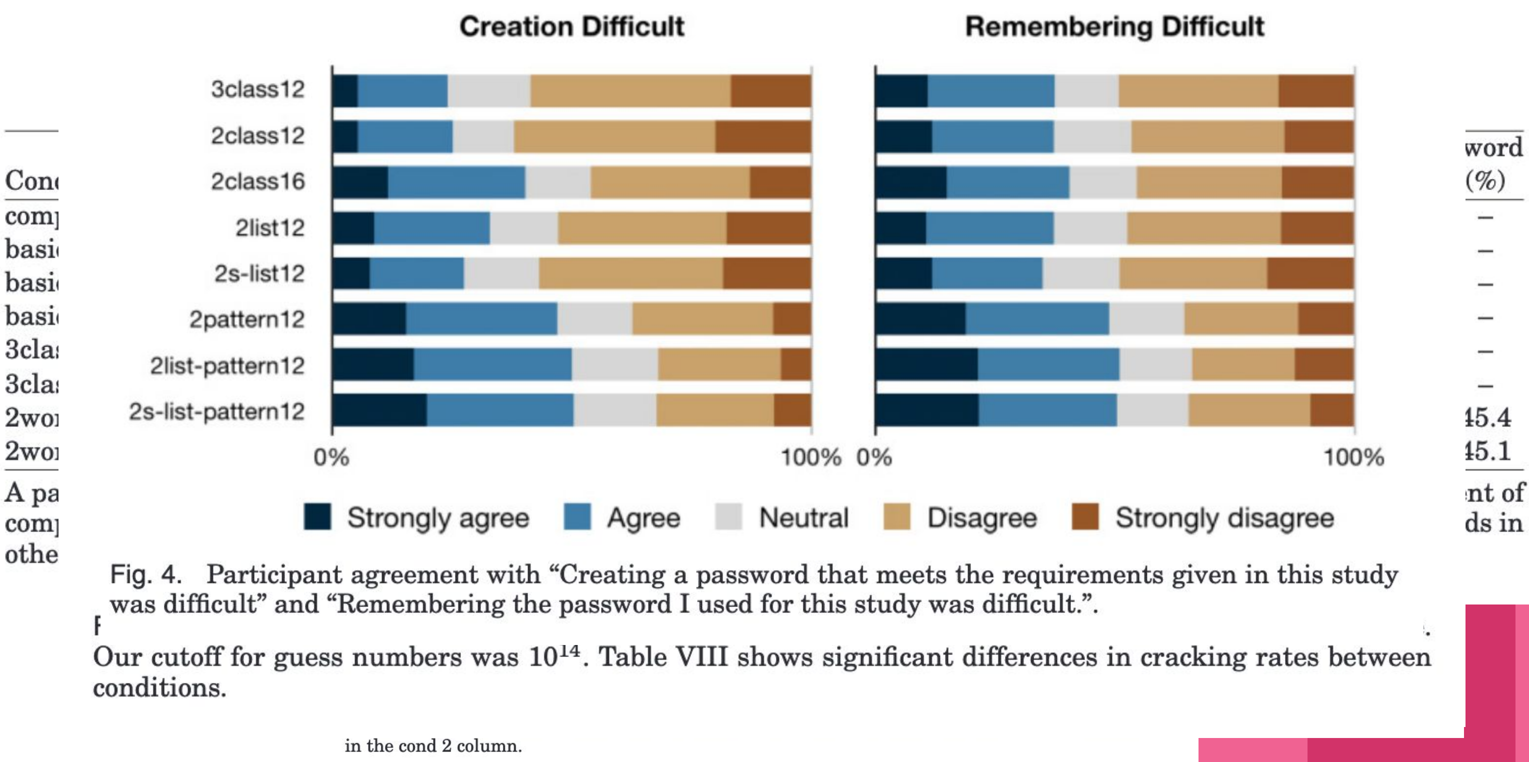


Fig. 3. The percentage of passwords cracked in each condition by the number of guesses made in log scale. Our cutoff for guess numbers was 10^{14}. Table VIII shows significant differences in cracking rates between conditions.

in the cond 2 column.

How to make a good password?



Con
comp
basi
basi
basi
3cla
3cla
2wo
2wo

A pa
comp
othe

word
(%)
–
–
–
–
–
–
45.4
45.1

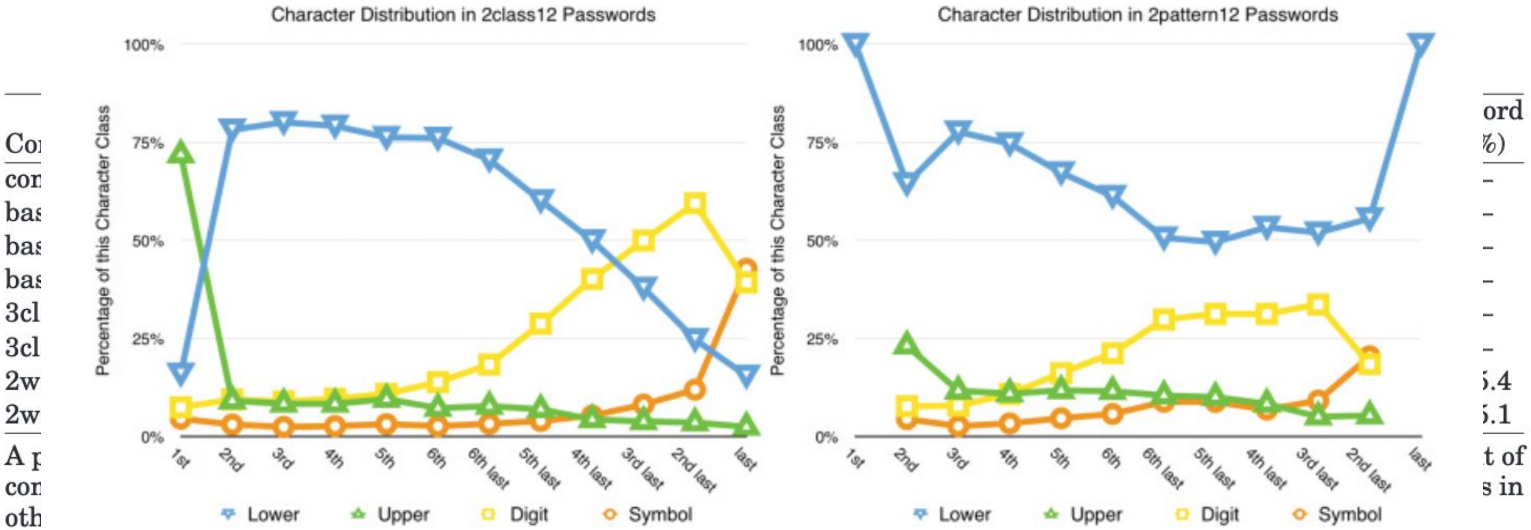
nt of
ds in

Fig. 4. Participant agreement with “Creating a password that meets the requirements given in this study was difficult” and “Remembering the password I used for this study was difficult.”.

Our cutoff for guess numbers was 10^{14}. Table VIII shows significant differences in cracking rates between conditions.

in the cond 2 column.

How to make a good password?



Co
co
ba
ba
ba
3cl
3cl
2w
2w
A p
co
oth

ord
%)
–
–
–
–
–
–
.4
.1
t of
s in

Fig. 5. For the first and last six characters, these graphs show the percentage of each character class in 2class12 and 2pattern12.

conditions.

in the cond 2 column.

How to make a good password?

“Designing Password Policies for Strength and Usability”

3class12

e.g. w2bgePWNy8Zz

2word16 (“passphrase”)

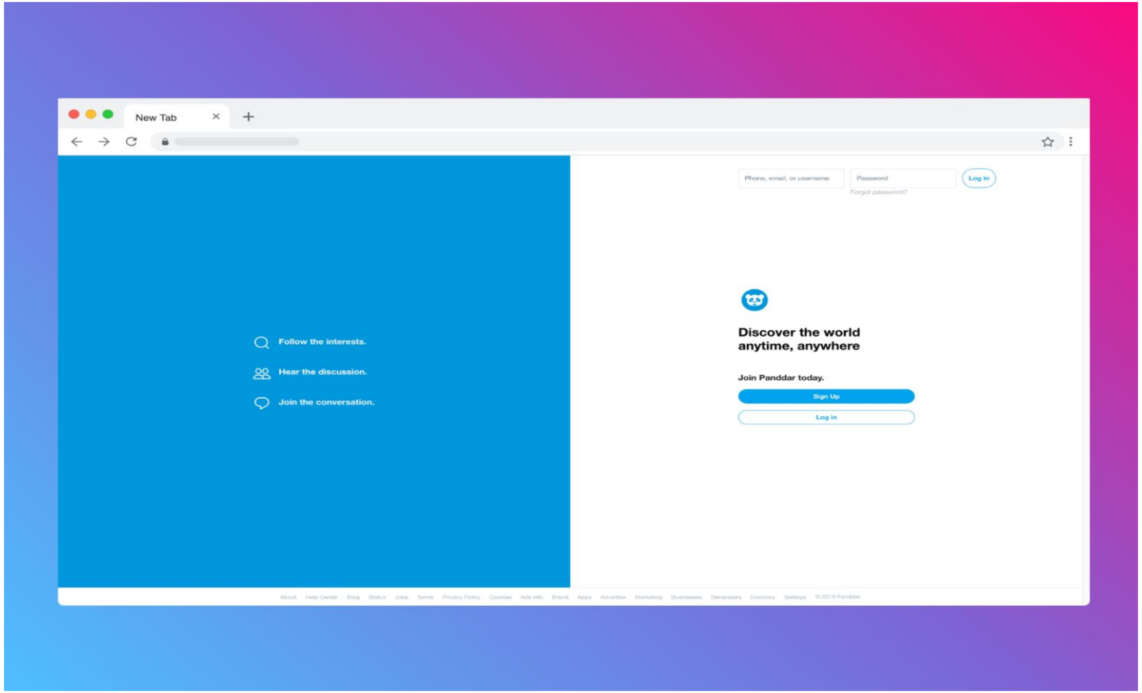
“letter sequences separated by a non-letter sequence”
e.g. secure42password

How to make a good password?

“Studying Passwords to Create Domain-Specific Blacklists”

How to make a good password?

“Studying Passwords to Create Domain-Specific Blacklists”



Follow the interests.

Hear the discussion.

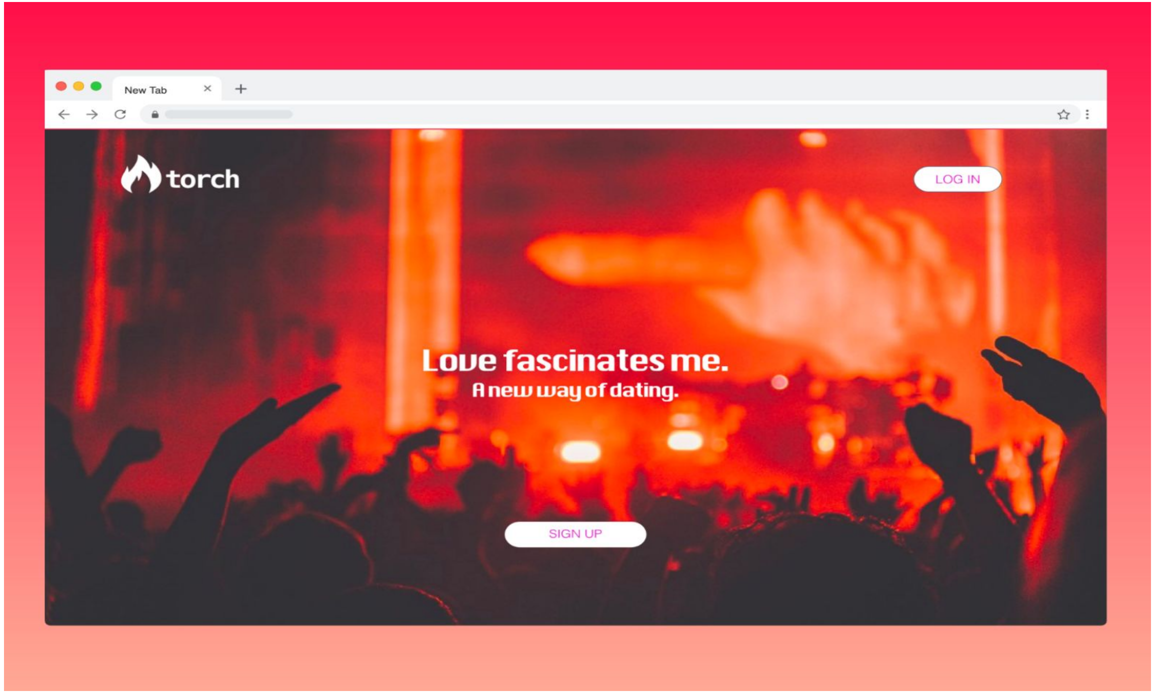
Join the conversation.

Discover the world anytime, anywhere

Join Panddar today.

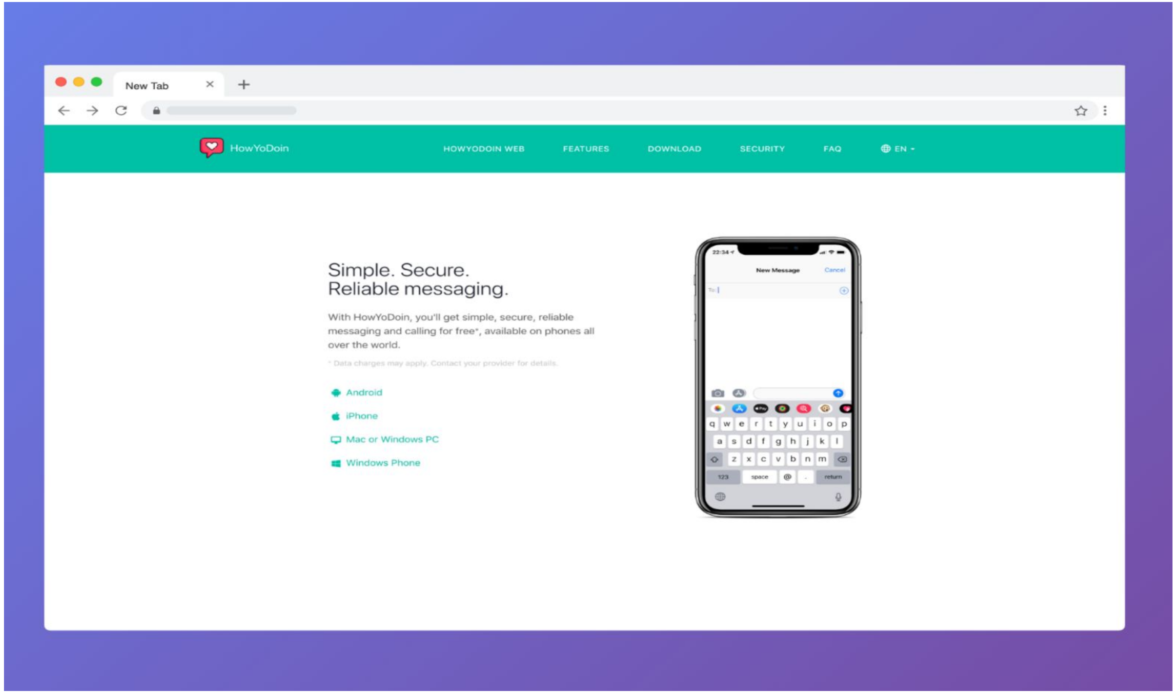
How to make a good password?

“Studying Passwords to Create Domain-Specific Blacklists”



How to make a good password?

“Studying Passwords to Create Domain-Specific Blacklists”



Simple. Secure.
Reliable messaging.

With HowYoDoin, you'll get simple, secure, reliable messaging and calling for free*, available on phones all over the world.

* Data charges may apply. Contact your provider for details.

- Android
- iPhone
- Mac or Windows PC
- Windows Phone

How to make a good password?

“Studying Passwords to Create Domain-Specific Blacklists”

Associated words:

Related topics:

Pictures or Logos:

How to make a good password?

“Studying Passwords to Create Domain-Specific Blacklists”

Associated words: Panddar1$, T0rched1!

Related topics:

Pictures or Logos:

How to make a good password?

“Studying Passwords to Create Domain-Specific Blacklists”

Associated words: Panddar1$, T0rched1!

Related topics: LoveBugs56$, Sexy!1337

Pictures or Logos:

How to make a good password?

“Studying Passwords to Create Domain-Specific Blacklists”

Associated words: Panddar1$, TOrched1!

Related topics: LoveBugs56$, Sexy!1337

Pictures or Logos: Fire-2019, 9Hands%%

have i been pwned
https://haveibeenpwned.com

Use 3class12 or 2word16.

Use 3class12 or 2word16.
Do not use domain related language.

Use 3class12 or 2word16.
Do not use domain related language.
Use unique passwords.

How many accounts do you have?

How to make a good password? 2.0

Do not make passwords

How to make a good password? 2.0

Do not make passwords yourself.

How to make a good password? 2.0

Do not make passwords yourself.

Password Managers

How to make a good password? 2.0

Do not make passwords yourself.

Password Managers

And of course, make 1 good password for the password manager.

Do not email passwords to yourself.

Do not write it down and carry it around.

Do not use SMS for account recovery. ever.

Multi-factor Authentication

Multi-factor Auth

what you know

what you have

what you are

Multi-factor Auth

what you know	ATM card pin
what you have	
what you are	

Multi-factor Auth

what you know	ATM card pin
what you have	physical card
what you are	

Multi-factor Auth

what you know	ATM card pin
what you have	physical card
	driver’s license
what you are	

Multi-factor Auth

what you know	ATM card pin
what you have	physical card
	driver’s license
what you are	your face

SMS

~~SMS~~

Security Questions

~~Security Questions~~

Hardware Tokens

Hardware Tokens

Software Tokens

Software Tokens

Software Tokens

Software Tokens
TOTP

Always set up 2FA.

Always set up 2FA.
Do not use SMS for 2FA.

Always set up 2FA.
Do not use SMS for 2FA.
Do not use email for 2FA.

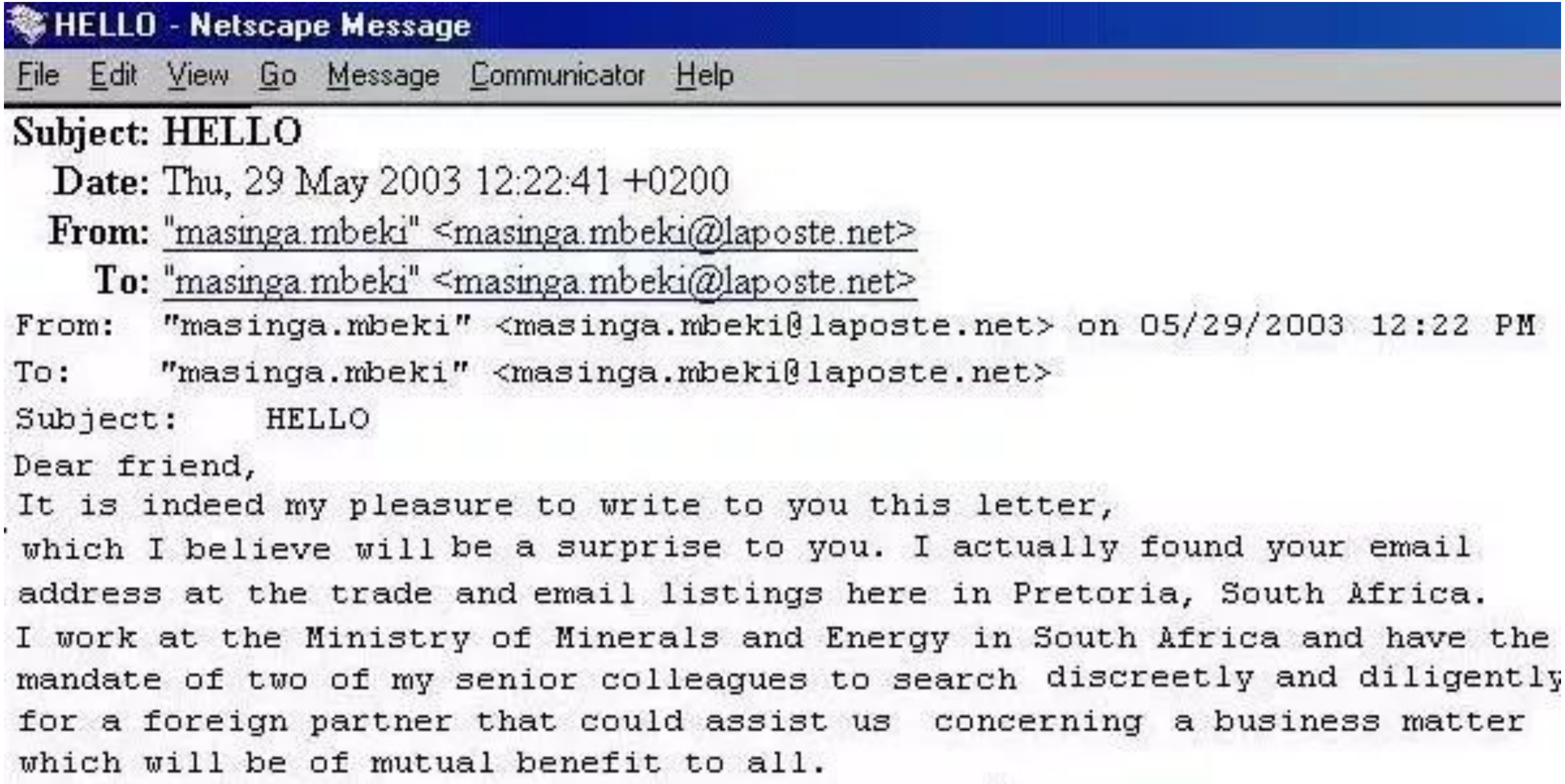
Always set up 2FA.
Do not use SMS for 2FA.
Do not use email for 2FA.
Do not trust security questions.

Phishing, Hijacking, and Theft

Phishing

“the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.”

https://www.lexico.com/en/definition/phishing



Subject: HELLO
Date: Thu, 29 May 2003 12:22:41 +0200
From: "masinga.mbeki" <masinga.mbeki@laposte.net>
To: "masinga.mbeki" <masinga.mbeki@laposte.net>

```
From:   "masinga.mbeki" <masinga.mbeki@laposte.net> on 05/29/2003 12:22 PM
To:     "masinga.mbeki" <masinga.mbeki@laposte.net>
Subject:     HELLO
```

Dear friend,
It is indeed my pleasure to write to you this letter,
which I believe will be a surprise to you. I actually found your email
address at the trade and email listings here in Pretoria, South Africa.
I work at the Ministry of Minerals and Energy in South Africa and have the
mandate of two of my senior colleagues to search discreetly and diligently
for a foreign partner that could assist us concerning a business matter
which will be of mutual benefit to all.

He Tried to Bilk Google and Facebook Out of $100 Million With Fake Invoices

https://www.nytimes.com/2019/03/25/business/facebook-google-wire-fraud.html

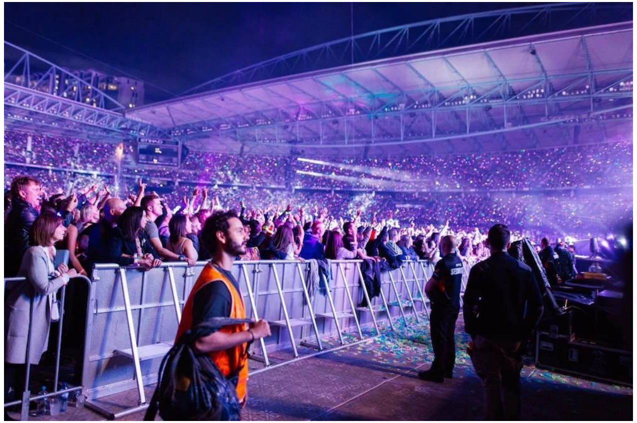
The New York Times

Social Engineering

- Generalization of phishing
    - Emails
    - Phone calls
    - Act like you belong / physical intrusion

Entertainment

Turns Out Wearing a Hi-Vis Vest Gets You into Everything for Free



https://www.vice.com/en_us/article/mgv4gn/chalecos-reflectantes-entrar-gratis

https://www.youtube.com/watch?v=yhE372sqURU

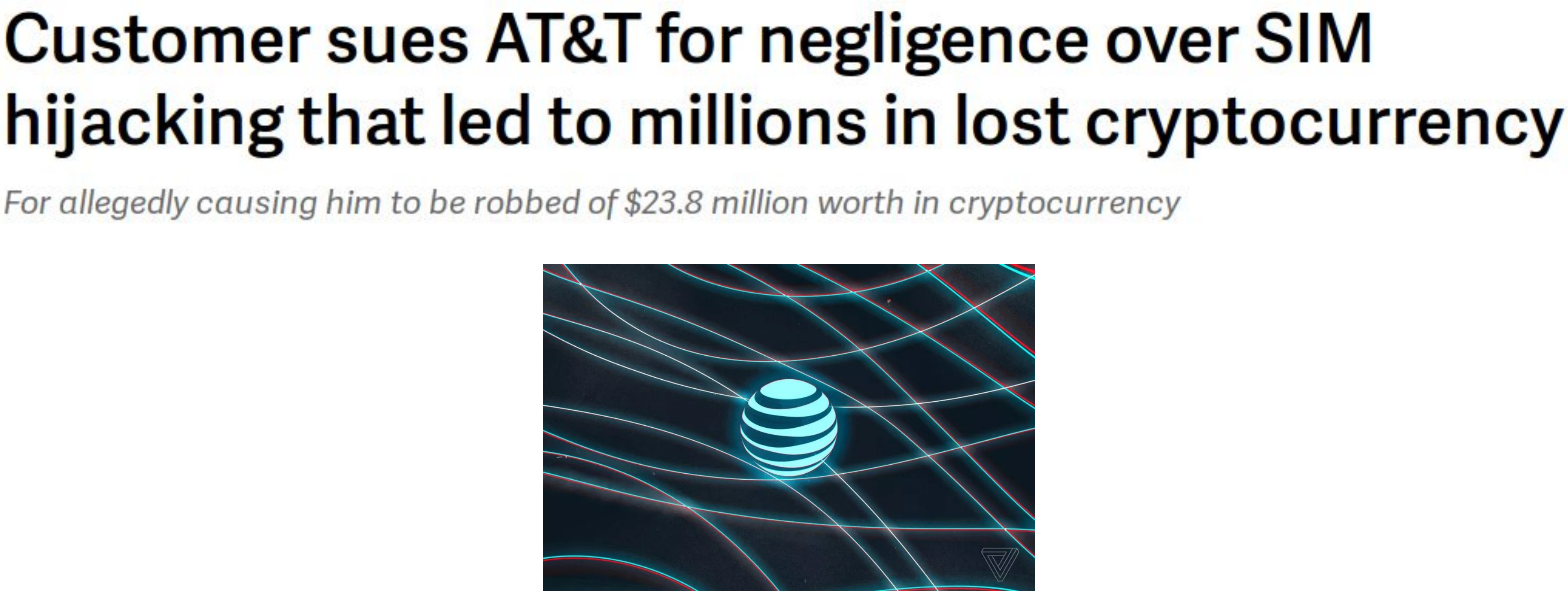
Common targets of social engineering

- Banks
- Phone providers
- Corporations
- The elderly

Social Engineering enables SIM Hijacking

SIM Hijacking

1. Attacker collects enough information to convincingly pretend to be you.
2. Attacker calls phone company support and convinces them to port your phone number to a different SIM card that they control.
3. Attacker now controls SMS-based 2FA and account recovery.

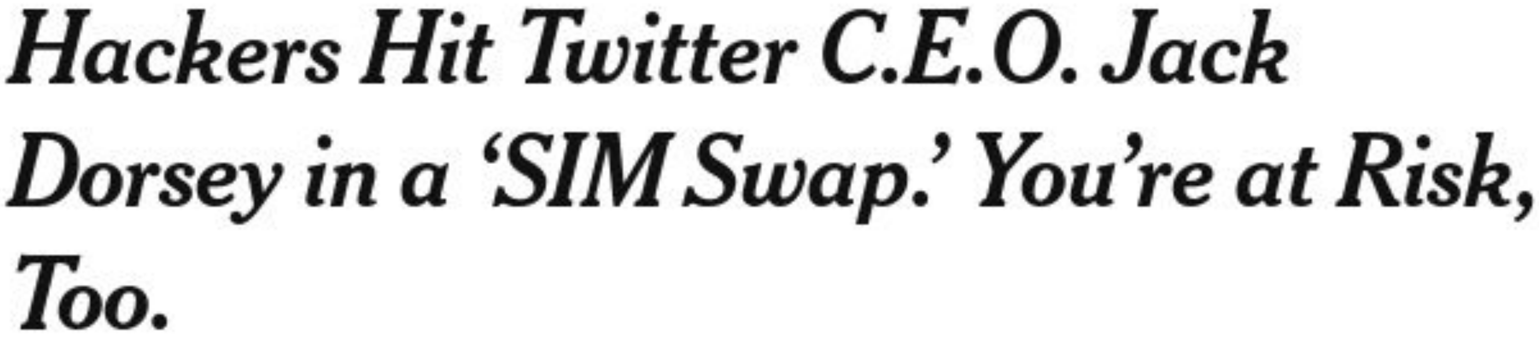


Customer sues AT&T for negligence over SIM hijacking that led to millions in lost cryptocurrency

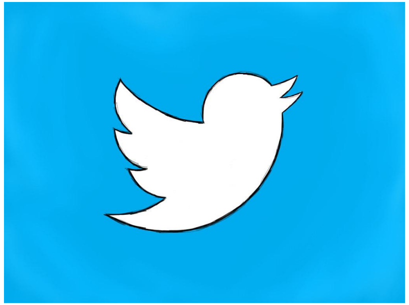
For allegedly causing him to be robbed of $23.8 million worth in cryptocurrency

https://www.theverge.com/2018/8/15/17695132/att-sued-over-lost-cryptocurrency-sim-swap-theft

THE VERGE



Hackers Hit Twitter C.E.O. Jack Dorsey in a 'SIM Swap.' You're at Risk, Too.



https://www.nytimes.com/2019/09/05/technology/sim-swap-jack-dorsey-hack.html

The New York Times

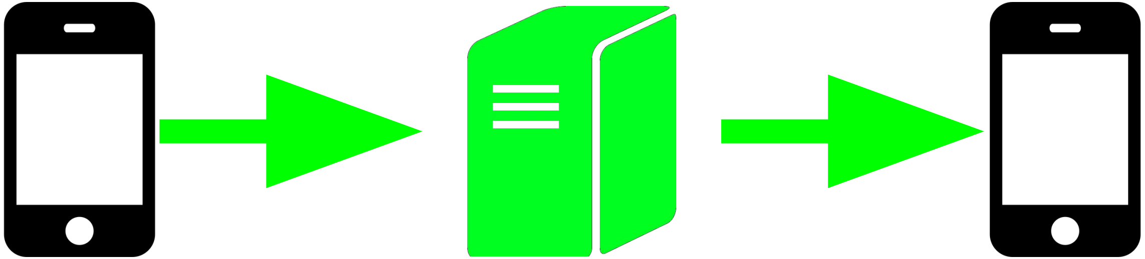
SIM Hijacking is why SMS 2FA is insecure

If a site only provides SMS 2FA, then register a Google Voice number and use it only for SMS 2FA

Web Security

End-to-end encryption (E2EE)

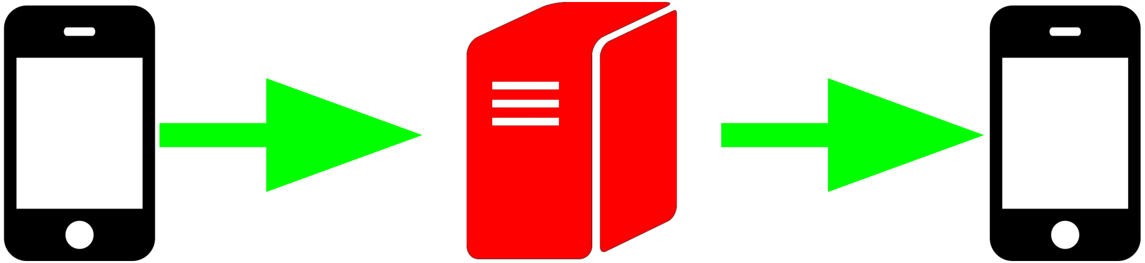
- Data is encrypted by the sender and decrypted by the receiver



phone icon from scott desmond, server icon from aLf, both from Noun Project

Typical TLS / HTTPS encryption

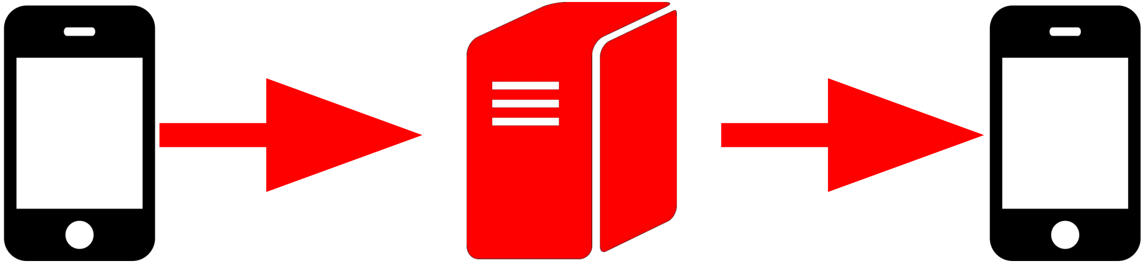
- Data is also decrypted / re-encrypted by the server



phone icon from scott desmond, server icon from aLf, both from Noun Project

No encryption (HTTP)

- Nothing is encrypted, ISP / router sees all traffic



phone icon from scott desmond, server icon from aLf, both from Noun Project

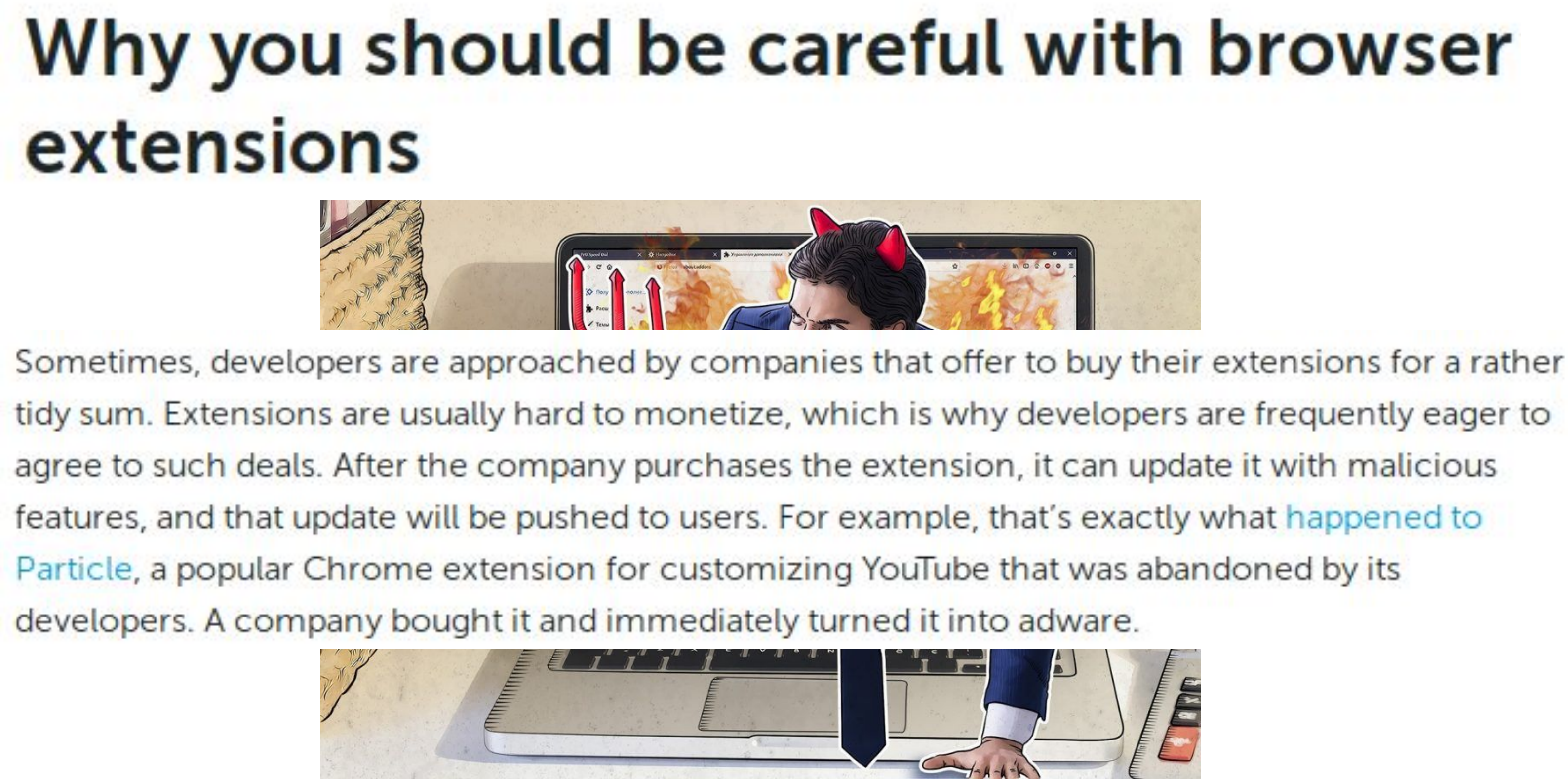
Web browser extensions

- Typically have privileged access to browser
- Can read and rewrite page content
- Limit the number of extensions installed

Why you should be careful with browser extensions

https://www.kaspersky.com/blog/browser-extensions-security/20886/

kaspersky daily



Why you should be careful with browser extensions

Sometimes, developers are approached by companies that offer to buy their extensions for a rather tidy sum. Extensions are usually hard to monetize, which is why developers are frequently eager to agree to such deals. After the company purchases the extension, it can update it with malicious features, and that update will be pushed to users. For example, that's exactly what happened to Particle, a popular Chrome extension for customizing YouTube that was abandoned by its developers. A company bought it and immediately turned it into adware.

https://www.kaspersky.com/blog/browser-extensions-security/20886/

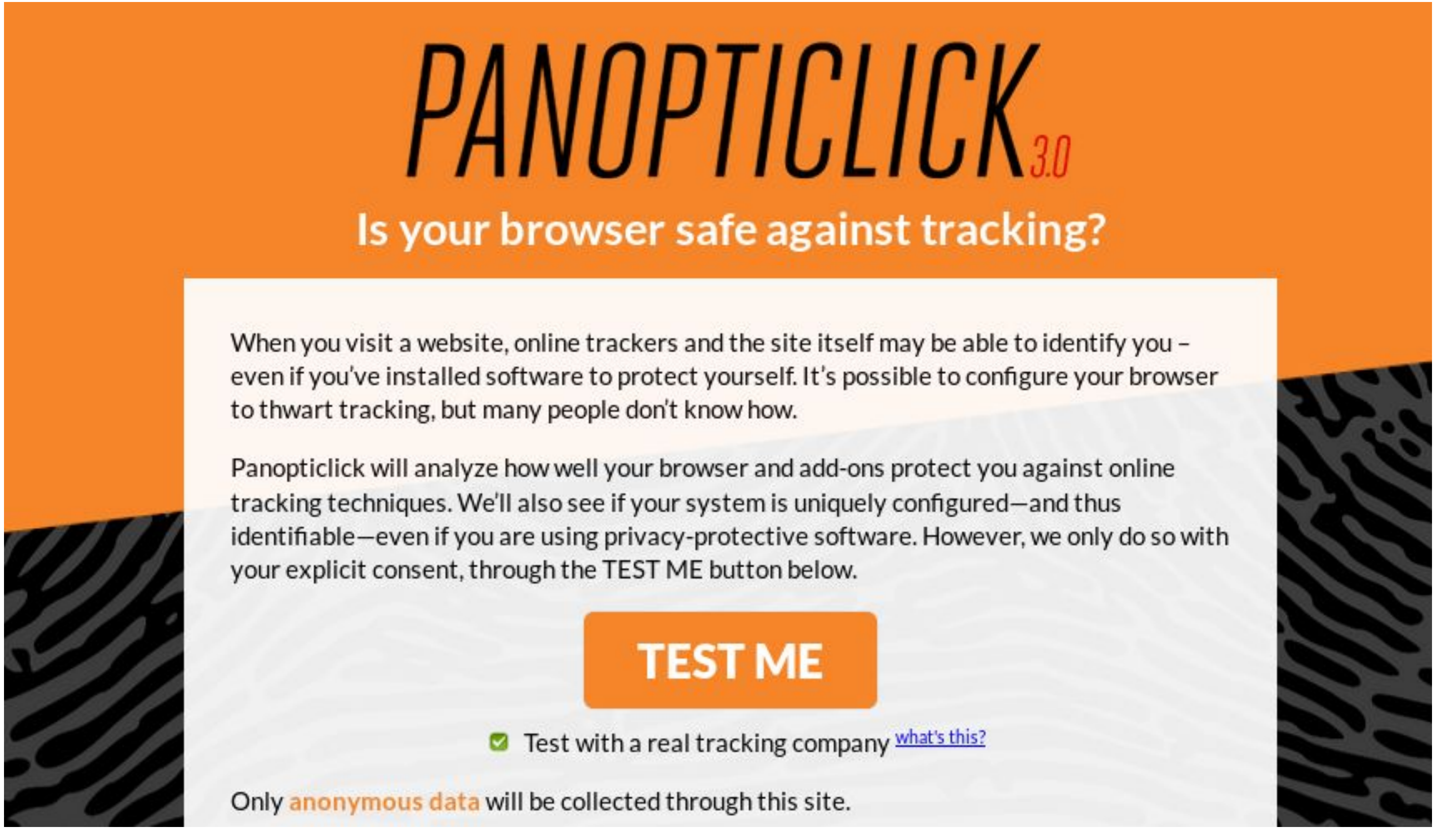
kaspersky daily

Ad blockers

- Ads are typically not malicious, but they do pose a threat to privacy on the web
- If you’re concerned about the impact on revenue for creators / companies, you can whitelist certain websites
- Some ad blockers also have settings to allow “acceptable ads”
    - https://adblockplus.org/acceptable-ads

Browser fingerprinting

- Web Browsers reveal a lot of information about the underlying system through User-Agent, extensions, plugins, system fonts, etc.
- This is often enough to uniquely identify users even without client-side cookies



PANOPTICLICK 3.0

Is your browser safe against tracking?

When you visit a website, online trackers and the site itself may be able to identify you – even if you've installed software to protect yourself. It's possible to configure your browser to thwart tracking, but many people don't know how.

Panopticlick will analyze how well your browser and add-ons protect you against online tracking techniques. We'll also see if your system is uniquely configured—and thus identifiable—even if you are using privacy-protective software. However, we only do so with your explicit consent, through the TEST ME button below.

☑ Test with a real tracking company what's this?

Only anonymous data will be collected through this site.

https://panopticlick.eff.org/

ELECTRONIC FRONTIER FOUNDATION

Email Security

Email (in)security

“Talk about email and attachments. This part is almost like sex education: you preach abstinence, but you know the moment you leave the room, they'll be double-clicking on whatever Excel spreadsheet…

“Try to push the campaign towards shared Google Docs and Signal instead of email.”

https://idlewords.com/2019/05/what_i_learned_trying_to_secure_congressional_campaigns.htm

Email (in)security

Do not trust attachments in email.

Email (in)security

Do not trust attachments in email.

Do not trust python script your friend emailed you.

Email (in)security

Do not trust attachments in email.

Do not trust python script your friend emailed you.

Do not email python script to your friend.

Email (in)security

Do not trust attachments in email.

Do not trust python script your friend emailed you.

Do not email python script to your friend.

Do not trust attachments in email.

Email (in)security

Emails are NOT encrypted via transit.

Email (in)security

Emails are NOT encrypted via transit.

Emails stored on your devices are NOT encrypted.

Email (in)security

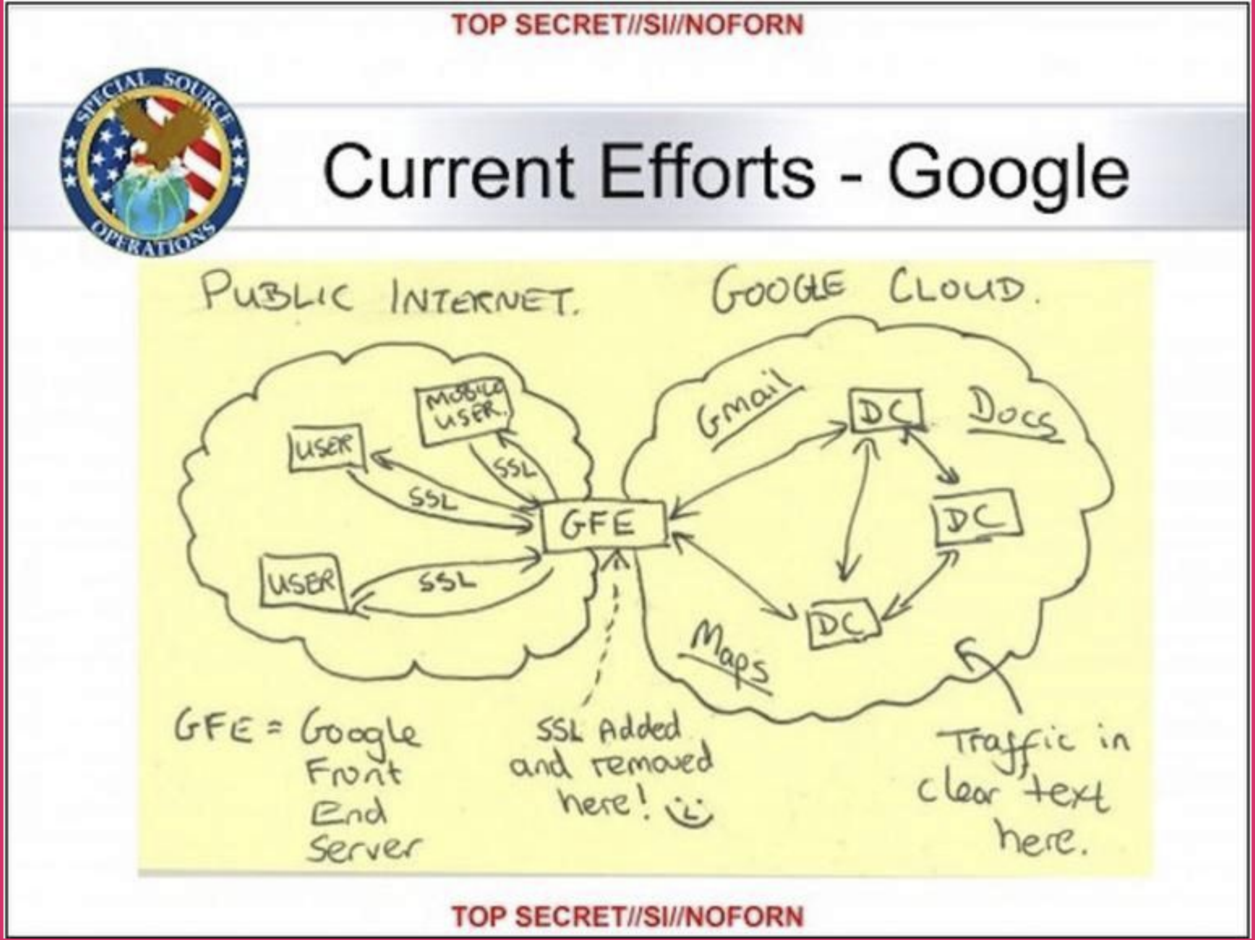
Emails are NOT encrypted via transit.

Emails stored on your devices are NOT encrypted.

Emails stored on the server are NOT encrypted.

NSA “Muscular”

An NSA presentation slide, titled "Google Cloud Exploitation," shows a hand-drawn note intersecting the two noting that encryption is "added and removed here."



TOP SECRET//SI//NOFORN

Current Efforts - Google

GFE = Google Front End Server

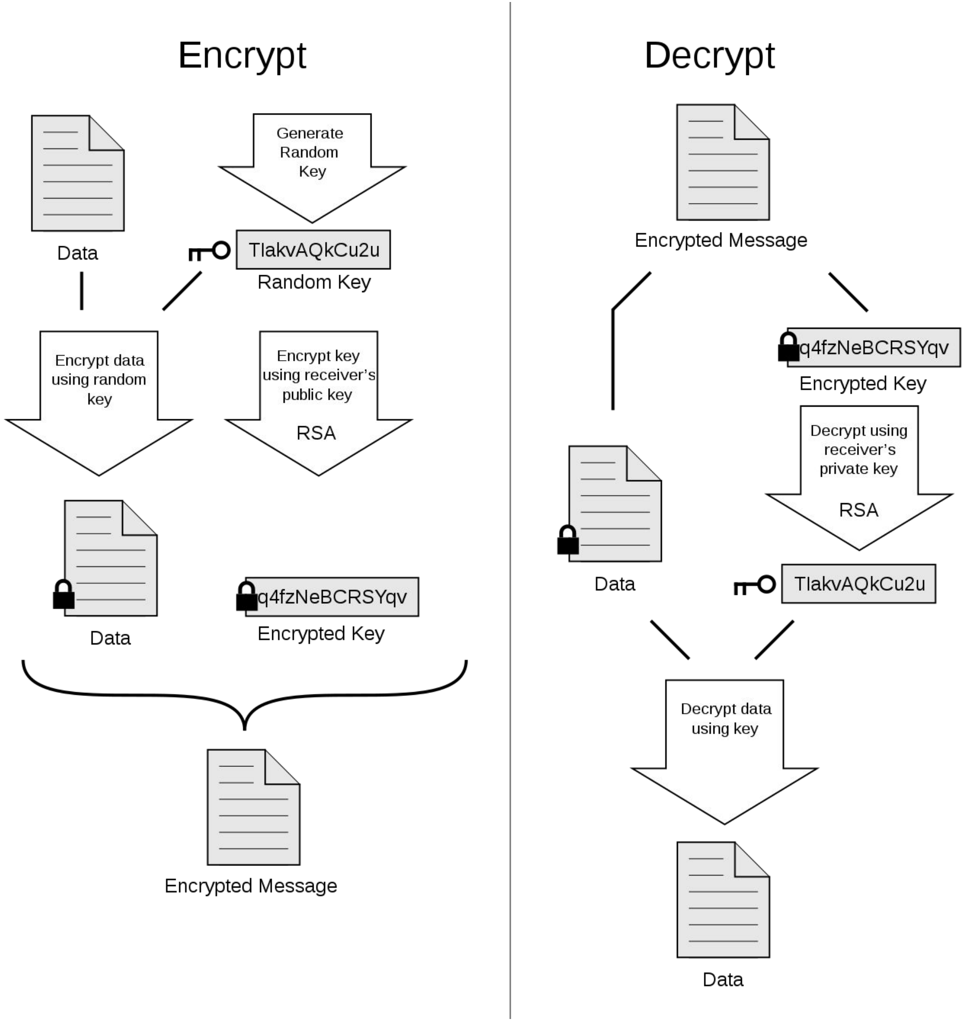
SSL Added and removed here! ☺

Traffic in clear text here.

TOP SECRET//SI//NOFORN

Pretty Good Privacy

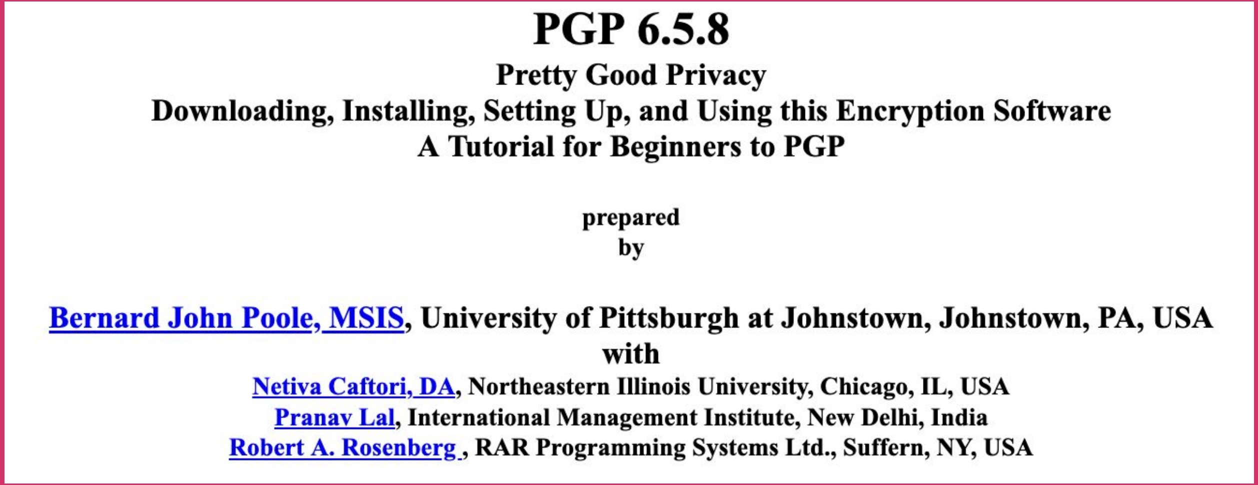
OpenPGP



“Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0”

“Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0”

“We conclude that PGP 5.0 is not usable enough to provide effective security for most computer users”

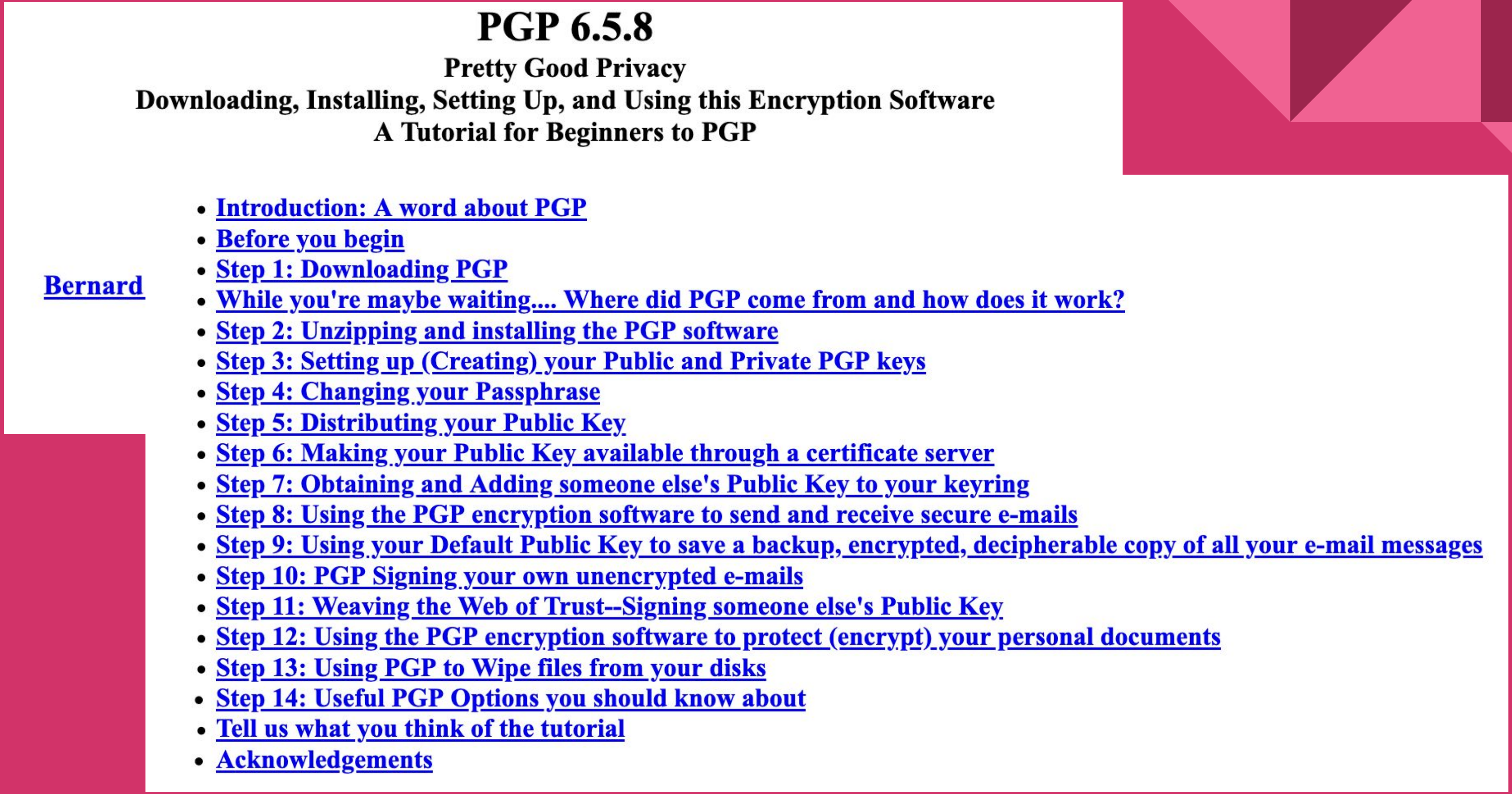


PGP 6.5.8

Pretty Good Privacy
Downloading, Installing, Setting Up, and Using this Encryption Software
A Tutorial for Beginners to PGP

**prepared
by**

Bernard John Poole, MSIS, University of Pittsburgh at Johnstown, Johnstown, PA, USA
with
Netiva Caftori, DA, Northeastern Illinois University, Chicago, IL, USA
Pranav Lal, International Management Institute, New Delhi, India
Robert A. Rosenberg , RAR Programming Systems Ltd., Suffern, NY, USA

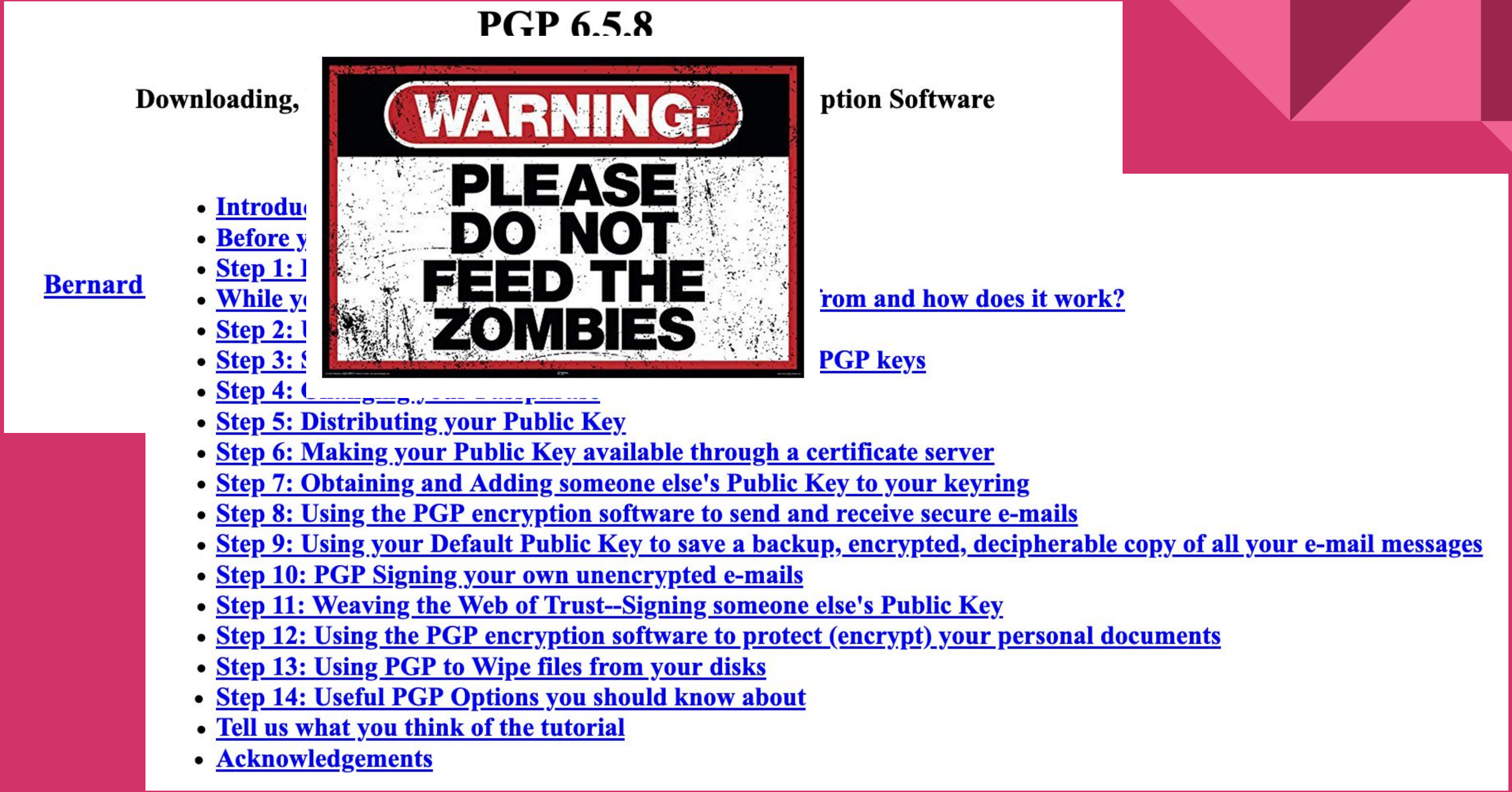


PGP 6.5.8

Pretty Good Privacy
Downloading, Installing, Setting Up, and Using this Encryption Software
A Tutorial for Beginners to PGP

Bernard

- Introduction: A word about PGP
- Before you begin
- Step 1: Downloading PGP
- While you're maybe waiting.... Where did PGP come from and how does it work?
- Step 2: Unzipping and installing the PGP software
- Step 3: Setting up (Creating) your Public and Private PGP keys
- Step 4: Changing your Passphrase
- Step 5: Distributing your Public Key
- Step 6: Making your Public Key available through a certificate server
- Step 7: Obtaining and Adding someone else's Public Key to your keyring
- Step 8: Using the PGP encryption software to send and receive secure e-mails
- Step 9: Using your Default Public Key to save a backup, encrypted, decipherable copy of all your e-mail messages
- Step 10: PGP Signing your own unencrypted e-mails
- Step 11: Weaving the Web of Trust--Signing someone else's Public Key
- Step 12: Using the PGP encryption software to protect (encrypt) your personal documents
- Step 13: Using PGP to Wipe files from your disks
- Step 14: Useful PGP Options you should know about
- Tell us what you think of the tutorial
- Acknowledgements

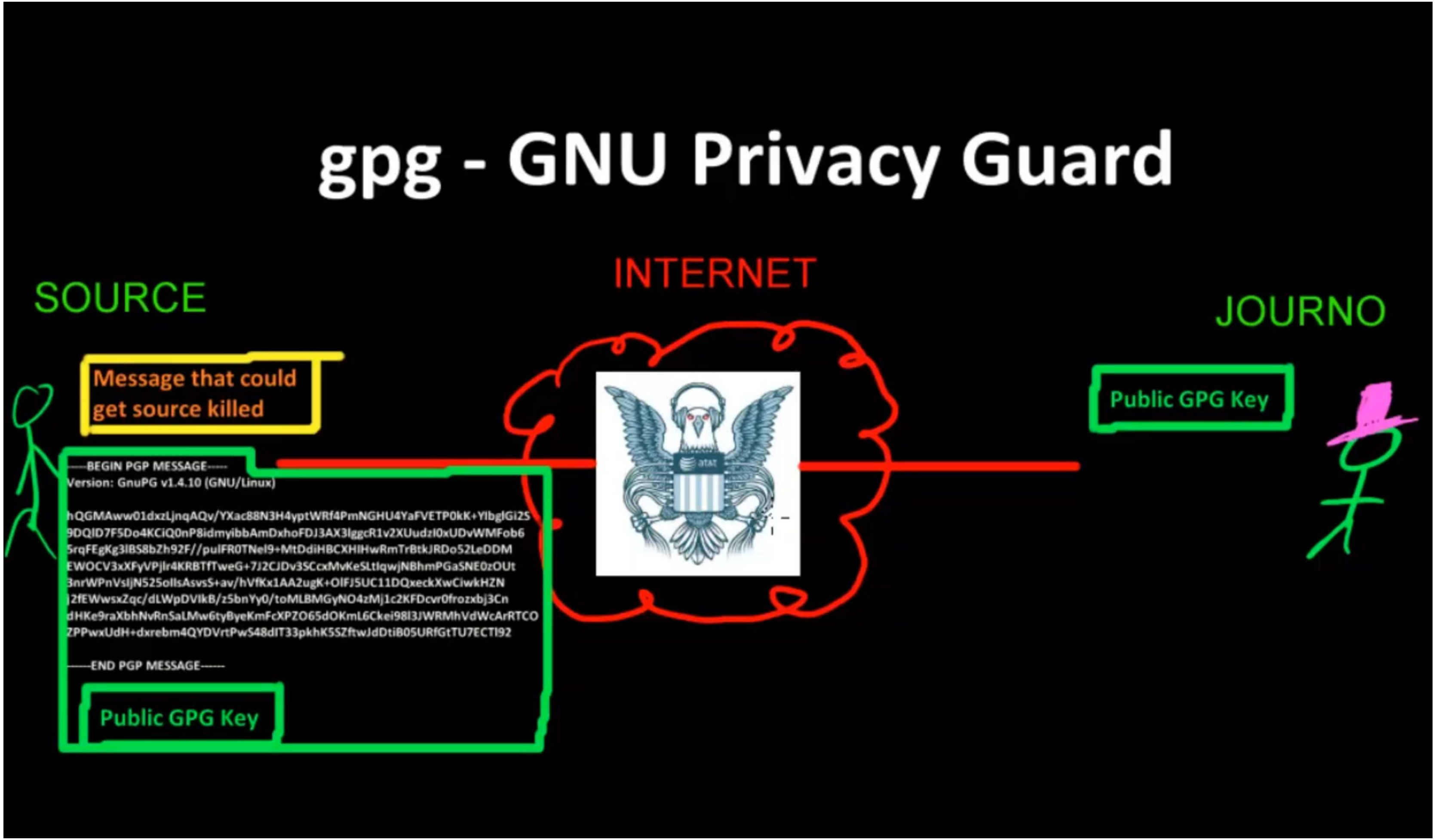


PGP 6.5.8

Downloading, ption Software

Bernard

- Introdu
- Before y
- Step 1: I
- While yo rom and how does it work?
- Step 2: U
- Step 3: S PGP keys
- Step 4: C
- Step 5: Distributing your Public Key
- Step 6: Making your Public Key available through a certificate server
- Step 7: Obtaining and Adding someone else's Public Key to your keyring
- Step 8: Using the PGP encryption software to send and receive secure e-mails
- Step 9: Using your Default Public Key to save a backup, encrypted, decipherable copy of all your e-mail messages
- Step 10: PGP Signing your own unencrypted e-mails
- Step 11: Weaving the Web of Trust--Signing someone else's Public Key
- Step 12: Using the PGP encryption software to protect (encrypt) your personal documents
- Step 13: Using PGP to Wipe files from your disks
- Step 14: Useful PGP Options you should know about
- Tell us what you think of the tutorial
- Acknowledgements

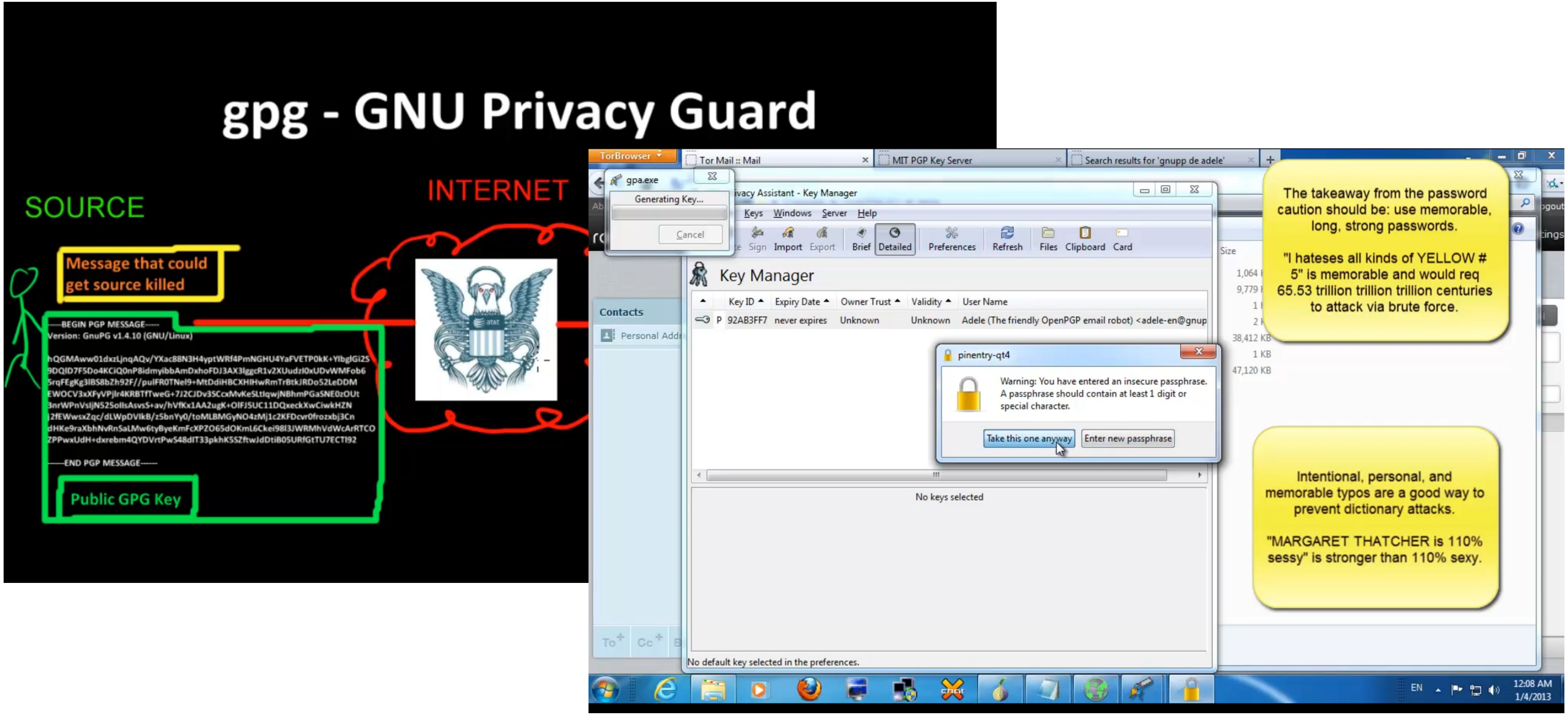


gpg - GNU Privacy Guard

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.10 (GNU/Linux)

hQGMAww01dxzLjnqAQv/YXac88N3H4yptWRf4PmNGHU4YaFVETP0kK+YlbglGi2S
9DQID7F5Do4KCiQ0nP8idmyibbAmDxhoFDJ3AX3lggcR1v2XUudzl0xUDvWMFob6
5rqFEgKg3lBS8bZh92F//pulFR0TNel9+MtDdiHBCXHIHwRmTrBtkJRDo52LeDDM
EWOCV3xXFyVPjlr4KRBTfTweG+7J2CJDv35CcxMvKeSLtlqwjNBhmPGaSNE0zOUt
3nrWPnVsIjN525ollsAsvsS+av/hVfKx1AA2ugK+OlFJ5UC11DQxeckXwCiwkHZN
j2fEWwsxZqc/dLWpDVlkB/z5bnYy0/toMLBMGyNO4zMj1c2KFDcvr0frozxbj3Cn
dHKe9raXbhNvRnSaLMw6tyByeKmFcXPZO65dOKmL6Ckei98l3JWRMhVdWcArRTCO
ZPPwxUdH+dxrebm4QYDVrtPwS48dIT33pkhK5SZftwJdDtiB05URfGtTU7ECTl92

-----END PGP MESSAGE-----
```



gpg - GNU Privacy Guard

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.10 (GNU/Linux)

hQGMAww01dxzLjnqAQv/YXac88N3H4yptWRf4PmNGHU4YaFVETP0kK+YlbglGi2S
9DQID7F5Do4KCiQ0nP8idmyibbAmDxhoFDJ3AX3lggcR1v2XUudzI0xUDvWMFob6
5rqFEgKg3lBS8bZh92F//pulFR0TNel9+MtDdiHBCXHlHwRmTrBtkJRDo52LeDDM
EWOCV3xXFyVPjlr4KRBTfTweG+7J2CJDv3SCcxMvKeSLtlqwjNBhmPGaSNE0zOUt
3nrWPnVsIjN525ollsAsvsS+av/hVfKx1AA2ugK+OlFJ5UC11DQxeckXwCiwkHZN
j2fEWwsxZqc/dLWpDVIkB/z5bnYy0/toMLBMGyNO4zMj1c2KFDcvr0frozxbj3Cn
dHKe9raXbhNvRnSaLMw6tyByeKmFcXPZO65dOKmL6Ckei98l3JWRMhVdWcArRTCO
ZPPwxUdH+dxrebm4QYDVrtPwS48dIT33pkhK5SZftwJdDtiB05URfGtTU7ECTI92

-----END PGP MESSAGE-----
```

	Key ID	Expiry Date	Owner Trust	Validity	User Name
P	92AB3FF7	never expires	Unknown	Unknown	Adele (The friendly OpenPGP email robot) <adele-en@gnup

No keys selected

No default key selected in the preferences.

pinentry-qt4

Warning: You have entered an insecure passphrase. A passphrase should contain at least 1 digit or special character.

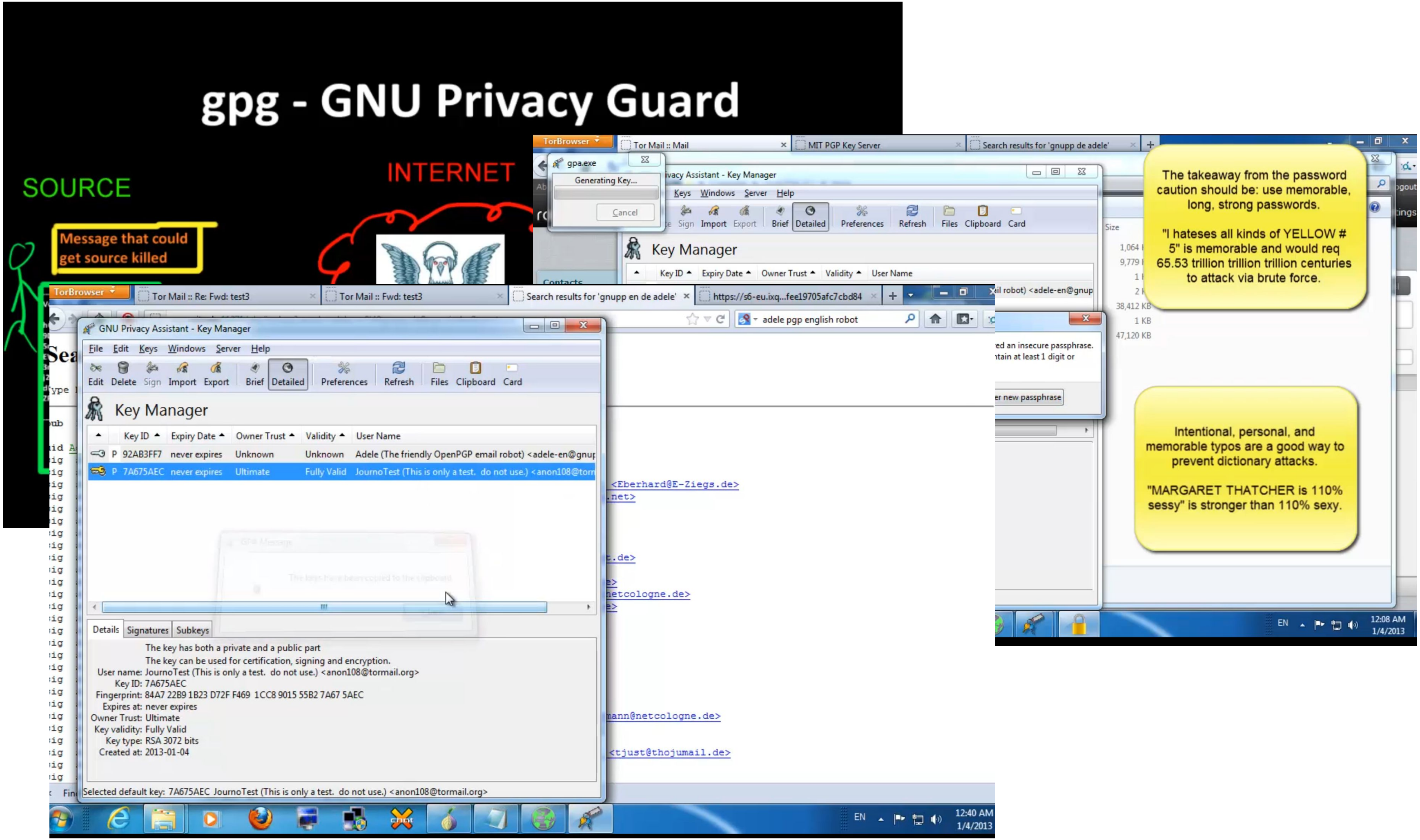
The takeaway from the password caution should be: use memorable, long, strong passwords.

"I hateses all kinds of YELLOW # 5" is memorable and would req 65.53 trillion trillion trillion centuries to attack via brute force.

Intentional, personal, and memorable typos are a good way to prevent dictionary attacks.

"MARGARET THATCHER is 110% sessy" is stronger than 110% sexy.

gpg - GNU Privacy Guard



Key ID	Expiry Date	Owner Trust	Validity	User Name
P 92AB3FF7	never expires	Unknown	Unknown	Adele (The friendly OpenPGP email robot) <adele-en@gnup
P 7A675AEC	never expires	Ultimate	Fully Valid	JournoTest (This is only a test. do not use.) <anon108@torm

The key has both a private and a public part
The key can be used for certification, signing and encryption.
User name: JournoTest (This is only a test. do not use.) <anon108@tormail.org>
Key ID: 7A675AEC
Fingerprint: 84A7 22B9 1B23 D72F F469 1CC8 9015 55B2 7A67 5AEC
Expires at: never expires
Owner Trust: Ultimate
Key validity: Fully Valid
Key type: RSA 3072 bits
Created at: 2013-01-04

Selected default key: 7A675AEC JournoTest (This is only a test. do not use.) <anon108@tormail.org>

The takeaway from the password caution should be: use memorable, long, strong passwords.

"I hateses all kinds of YELLOW # 5" is memorable and would req 65.53 trillion trillion trillion centuries to attack via brute force.

Intentional, personal, and memorable typos are a good way to prevent dictionary attacks.

"MARGARET THATCHER is 110% sessy" is stronger than 110% sexy.

Snowden teach Glenn PGP

Virtual Private Network

Private Browsing

VPN

“VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.”

https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html

VPN

“it will not encrypt and hide the traffic that goes from VPNs server to target destination and vice versa”

https://hackernoon.com/vpns-for-beginners-what-a-vpn-can-and-cannot-do-26rz3wrd

VPN

“it will not encrypt and hide the traffic that goes from VPNs server to target destination and vice versa”

“IP masking does not equal anonymity”

https://hackernoon.com/vpns-for-beginners-what-a-vpn-can-and-cannot-do-26rz3wrd

VPN

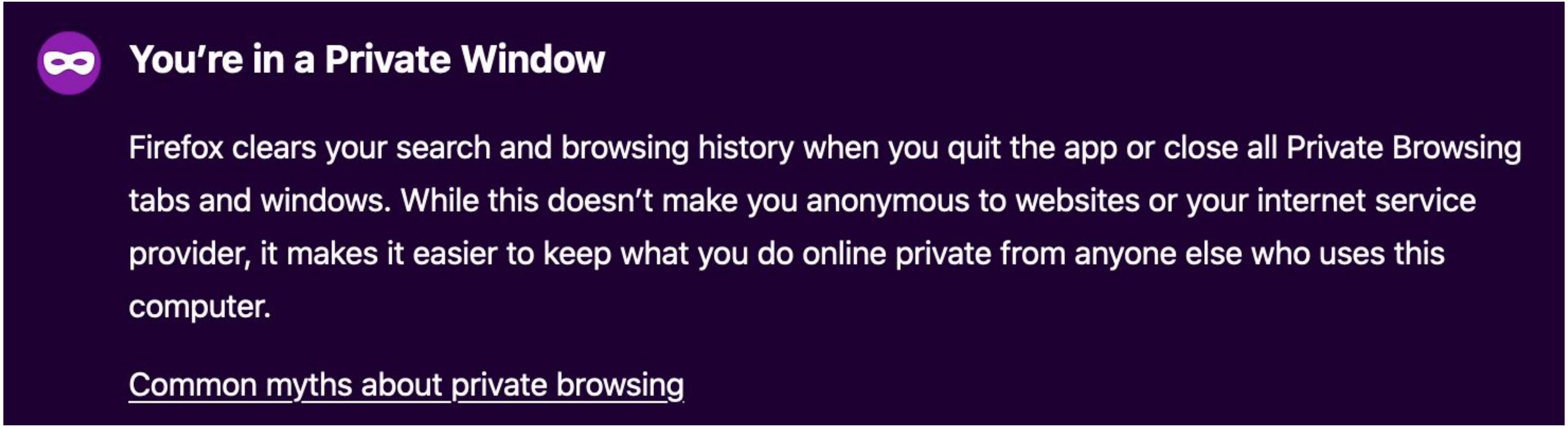
“it will not encrypt and hide the traffic that goes from VPNs server to target destination and vice versa”

“IP masking does not equal anonymity”

“your VPN provider can monitor everything you do online”

https://hackernoon.com/vpns-for-beginners-what-a-vpn-can-and-cannot-do-26rz3wrd

Private Browsing



You’re in a Private Window

Firefox clears your search and browsing history when you quit the app or close all Private Browsing tabs and windows. While this doesn’t make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private from anyone else who uses this computer.

Common myths about private browsing

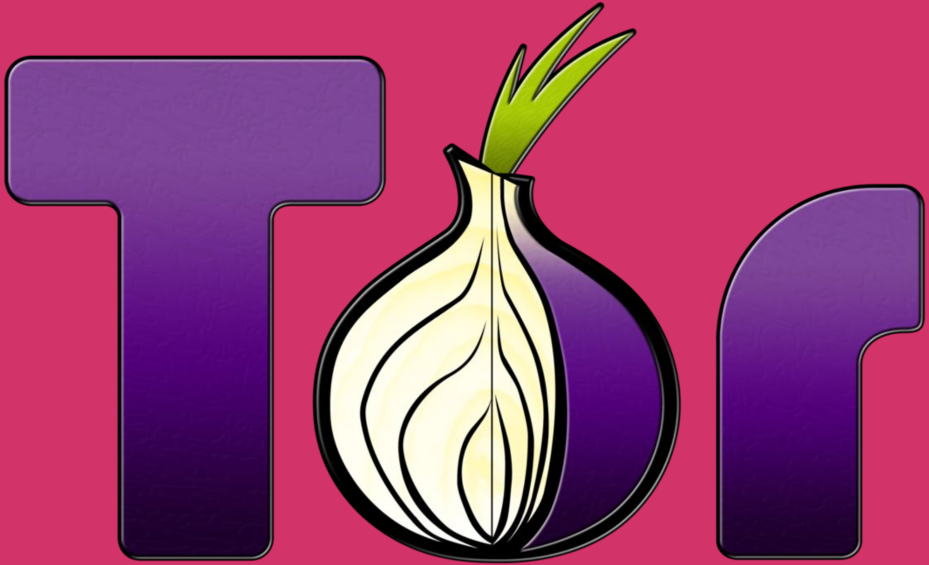
Private Browsing

Private Browsing makes you anonymous on the internet.

Private Browsing

~~Private Browsing makes you anonymous on the internet.~~

Browser fingerprints!

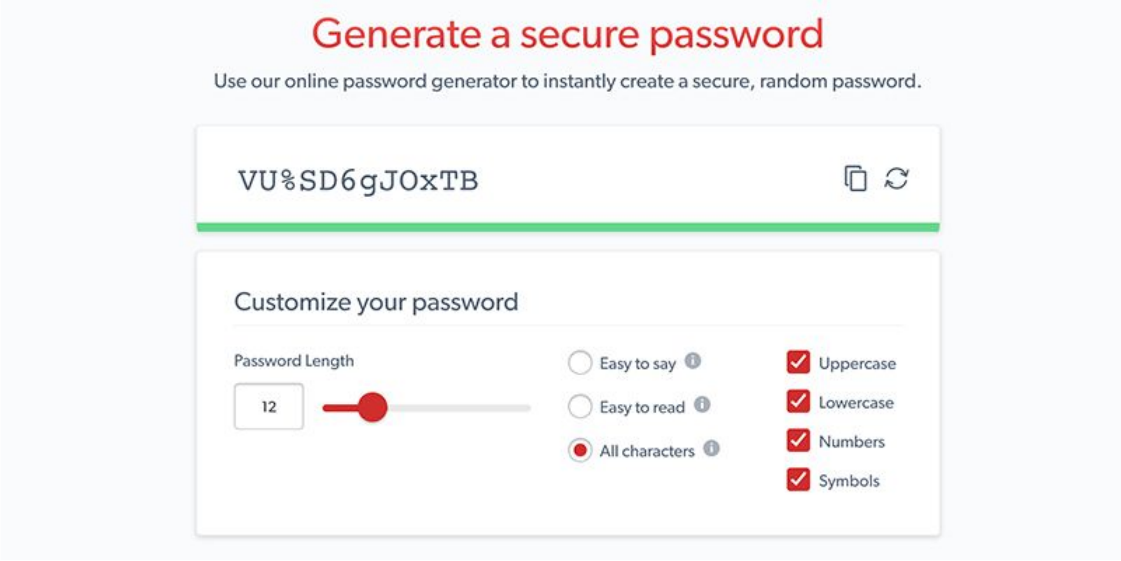

Tor

Concrete Recommendations

Security is a process,
it isn’t all or nothing
and any improvement
helps

LastPass for Password Manager

3class12 or 2word16 for master password, randomly-generated unique passwords for everything stored in vault



Generate a secure password

Use our online password generator to instantly create a secure, random password.

VU%SD6gJOxTB

Customize your password

Password Length

12

○ Easy to say

○ Easy to read

● All characters

☑ Uppercase

☑ Lowercase

☑ Numbers

☑ Symbols

Duo for TOTP 2FA

iMessage or WhatsApp for secure chat

uBlock Origin (no ads) or Adblock Plus (acceptable ads) for Ad blocker

Whatever you do, make sure that you have a path to recover access your accounts without access to your phone / computer

MyCrypto's Security Guide For Dummies And Smart People Too

An in-depth guide on how to be safe in the crypto world and the online world in general.

Taylor Monahan

Jul 15, 2018 · 16 min read

https://medium.com/mycrypto/mycryptos-security-guide-for-dummies-and-smart-people-too-ab178299c82e