

Security Training For Everyone

FEBRUARY 2018



Rich Adams
Security & Incident Response





Gain insight into the threats we face,
and learn how to protect us from them.



“Best training I’ve ever been to. Rich is awesome! I should give him a promotion, a raise, and \$100 from my own pocket right this instant!”

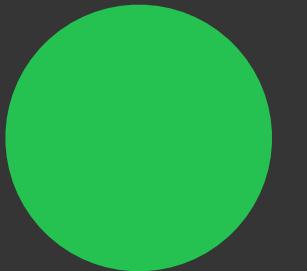


But seriously, all joking aside, this stuff is important. Please pay attention.



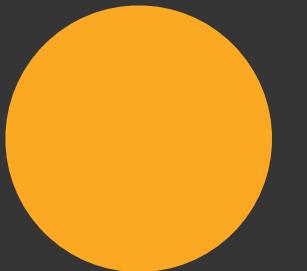
Arup Chakrabarti
Security Enthusiast

Also Rich’s boss. Assuming Rich still has a job after this.



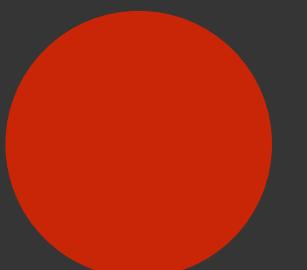
PUBLIC

*Slide **can be shared publicly** with family/friends, Twitter, etc.*



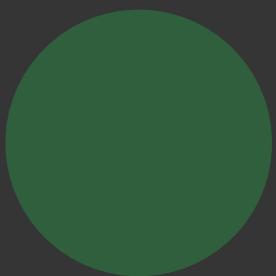
RESTRICTED

*Slide can only be shared with **customers under an NDA**.*



INTERNAL ONLY

*Slide is **not to be shared** with anyone outside of PagerDuty.*



PUBLIC

Slide can be shared

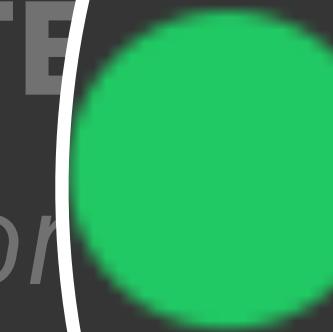
RESTRICTED

Slide can only be shared with family/friends, Twitter, etc.



INTERNAL ONLY

Slide is not to be shared outside of PagerDuty.



PUBLIC

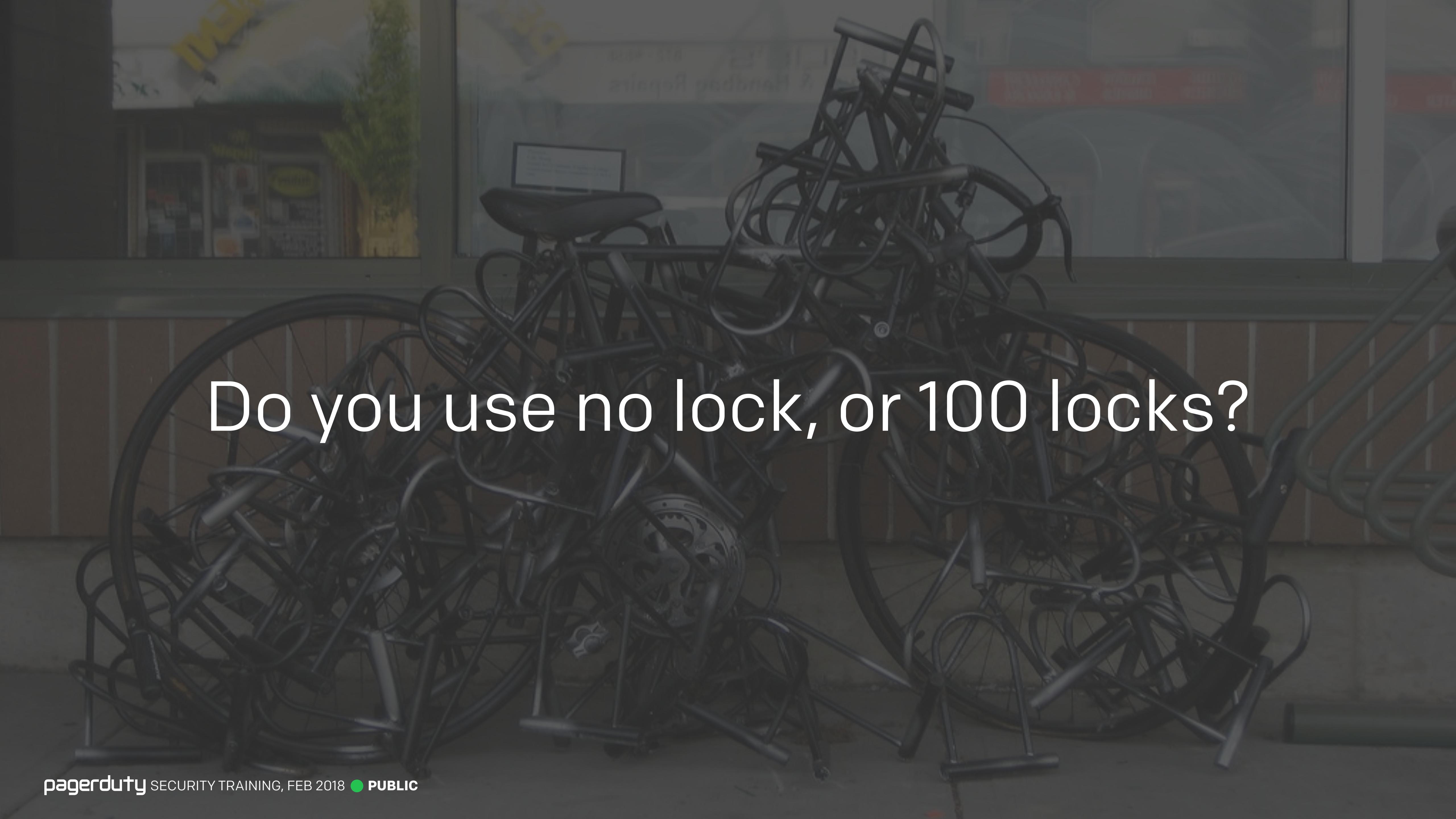


[REDACTED]

A dark, moody photograph of a person sitting on a large, textured rock. The person is in profile, facing right, with their head bowed and hands clasped together in their lap. The scene is dimly lit, with the person's silhouette and the texture of the rock being the primary light sources.

Our job is to make it easy for you
to do the right thing.

BLUE

A dark, cluttered bike rack filled with many bicycles, symbolizing security risks.

Do you use no lock, or 100 locks?

“Given the choice between security and convenience, people complain about security, but opt for convenience.”



Be Secure, But Usable

A row of colorful wooden nutcracker figurines standing in a row. They are dressed in traditional red and white uniforms with tall hats. Some have black belts and buttons, while others have green or blue trim. The figures are slightly blurred, creating a sense of depth.

No Lies, No Pretending

“Faking security is the path to the dark side. Faking leads to false hope. False hope leads to false security. False security leads to suffering.”

Totally real quote from Star Wars.



“Security theater is the practice of investing in countermeasures intended to provide the feeling of improved security while doing little or nothing to actually achieve it.”



The Washington Post

About 14 million checked bags passed through TSA hands during the Thanksgiving holiday weekend.



The Washington Post

Security officers have master keys for TSA-approved baggage locks.

[This repository](#)[Search](#)[Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)

Xyl2k / TSA-Travel-Sentry-master-keys

[Watch](#) [172](#)[Star](#) [2,127](#)[Fork](#) [603](#)[Code](#)[Issues 7](#)[Pull requests 0](#)[Projects 0](#)[Wiki](#)[Insights](#)

Branch: master

[TSA-Travel-Sentry-master-keys / README.md](#)[Find file](#) [Copy path](#)

johnnyxmas Added Safe Skies Master Key

5635ddb on Jul 24, 2016

4 contributors



65 lines (36 sloc) | 4.67 KB

[Raw](#)[Blame](#)[History](#)

Social Engineering





*“Psychological manipulation of people
into performing actions or divulging
confidential information.”*



catch me if you can

Building Trust

- Little bits of info can snowball.
- Attackers will claim to be a new employee to get info.
- Human nature is to want to help others.
- Confirm via another channel.

[REDACTED]

~~Fishing~~ Phishing



Lots of money for you!

Dear friend,

I am a Nigerian prince. I want to give you lots of money: \$2,400,000

Just send me your bank account details, social security number, a photocopy of your passport, your birth certificate, and your first born child.



Free! Check if your credit card has been stolen!

If you fear your credit card info has been stolen, enter it here and you can find out for free. Avoiding fraud has never been easier!

[About](#)

Credit card number

Name on credit card

Expiration Date

01 / 2017





Debit Card

@NeedADebitCard

TWEETS

206

FOLLOWERS

18K



Debit Card Retweeted



® @_rafael1_j · 15 Apr 2015

Found my Debit card. Thought I lost it 😊



ⓘ <https://twitter.com/needadebitcard>

pagerduty SECURITY TRAINING, FEB 2018 ● PUBLIC

Reel or Fish?

~~Reel or Fish?~~
Real or Phish?



Your account has a debt and is past due

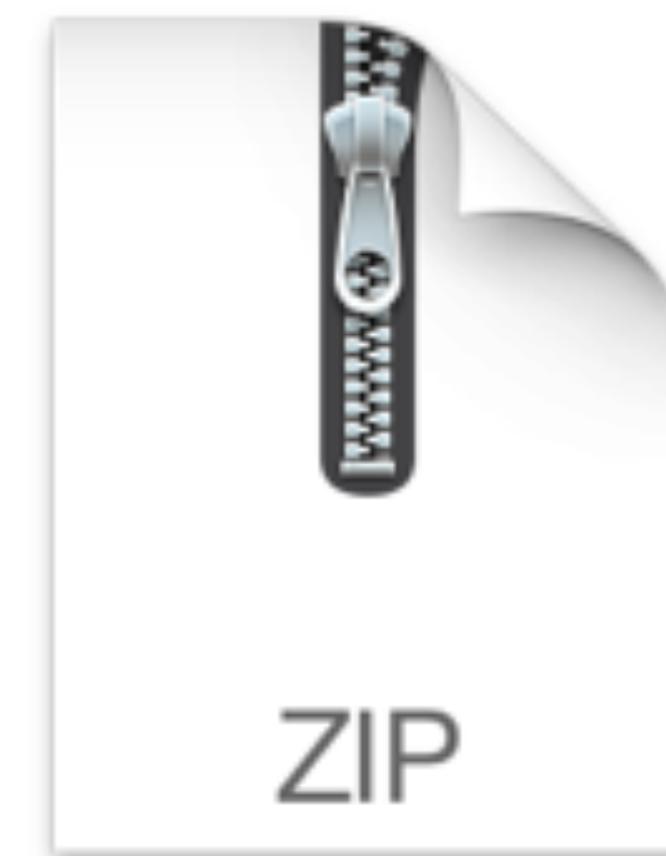
☆ Letitia Madden To: jriley ▾

⌚ 12/16/15, 12:49 PM

Dear Customer,

Our records show that your account has a debt of \$436.{rand(10,99)}. Previous attempts of collecting this sum have failed.

Down below you can find an attached file with the information on your case.



ZIP

SCAN_INVOICE_33566292.zip



Your account has a debt and is past due

★ Letitia Madden T

12/16/15, 12:49 PM

Dear Customer,

Our records show that your account has a debt of \$436.{rand(10,99)} Previous attempts of collecting this sum have failed.

Down below you can find an attached file with the information on your case.



Sites will usually use your real name.
Rarely will it just be "Customer".



Attacker has left in some code.
Choosing random digit from 10-99.



Beware of ZIP attachments.
Invoices would usually be PDF.



SCAN_INVOICE_33566292.zip



Not to scale.



From: "Cameron Smith via DocuSign" <dse@docusgn.com>
Subject: Completed: [pagerduty.com](#) - Wire Transfer Instructions for
Date: May 9, 2017 at 7:35:49 AM PDT
To: < @pagerduty.com>
Reply-To: "Cameron Smith via DocuSign" <dse@docusgn.com>

Document Ready for Signature



Your document has been completed

REVIEW DOCUMENT



From: "Cameron Smith via DocuSign" <dse@docusgn.com>
Subject: Completed: [pagerduty.com](#) - Wire Transfer Instructions for
Date: May 9, 2017 at 7:35:49 AM PDT
To: <@pagerduty.com>
Reply To: "Cameron Smith via DocuSign" <dse@docusgn.com>

Document Ready for Signature



Hover over and see link goes to
<http://.../file.php?email=...>

REVIEW DOCUMENT



Not the real docusign.com domain!

[REDACTED]

A photograph of a person spearfishing in the ocean. The person is wearing a wetsuit and fins, and is holding a spear gun. The water is dark and reflects the light from above.

Spear Phishing

For illustrative purposes only.
Real attacks may not contain spears, or fishes.

[REDACTED]

Protecting Yourself!

- Watch out for suspicious emails.
- “From:” addresses can be spoofed!
- To verify if from employee, ask them via IM or in person.
- If suspicious, forward the original email to us!



Security training is great!



Inbox x



Rich Adams <rich@pagerduty.com>

to me ▼

3:11 PM (0 minutes ago) ☆



Hi PagerDuty Employee,

Security training is really awesome. If you agree, you should click this link,

<http://totally-legit.ru/get-password.php?id=aab4625d7ac6472>

Regards,
Rich



Click here to [Reply](#) or [Forward](#)



Security training is great!



Inbox x



Rich Adams <rich@pagerduty.com>

to me ▾

Hi PagerDuty Employee,

Security training is really awesome. If you agree, you should click this link,

<http://totally-legit.ru/get-password.php?id=aab4625d7ac6472>

Regards,
Rich



Click here to [Reply](#) or [Forward](#)

3:11 PM (1 minute ago) star



- ◀ Reply
- ▶ Forward
- Filter messages like this
- Print
- Delete this message
- Report spam
- Report phishing
- Show original**
- Translate message
- Mark as unread



We need to get the original message
with all headers.



Original Message

Message ID	< Dw@mail.gmail.com >
Created at:	Sun, Jan 7, 2018 at 3:11 PM (Delivered after 0 seconds)
From:	Rich Adams < rich@pagerduty.com >
To:	Rich Adams < rich@pagerduty.com >
Subject:	Security training is great!



Click this to get all the info we need
in your clipboard.

[Download Original](#)

[Copy to clipboard](#)

Is this phishing?

To PagerDuty Security <security@pagerduty.com>

From Rich Adams <rich@pagerduty.com>

- ✎ ✕

Cc Bcc

Is this phishing?



Send it to the security team. We'll take care of the rest!

MIME-Version: 1.0

Received: by with HTTP; Sun, 7 Jan 2018 15:11:13 -0800 (PST)

Date: Sun, 7 Jan 2018 15:11:13 -0800

Delivered-To: rich@pagerduty.com

Dw@mail.gmail.com

Message-ID: <

Subject: Security training is great!

From: Rich Adams <rich@pagerduty.com>

To: Rich Adams <rich@pagerduty.com>

Content-Type: multipart/alternative; boundary="f4f5e80336d04d02e2056237cc72"

--f4f5e80336d04d02e2056237cc72

Content-Type: text/plain; charset="UTF-8"

Hi PagerDuty Employee,

Fixed Wi...

T

B

I

U

A

≡

≡

≡

≡

≡

,

X

should click this

Send

A

U

△

\$

○

🔗

😊

trash

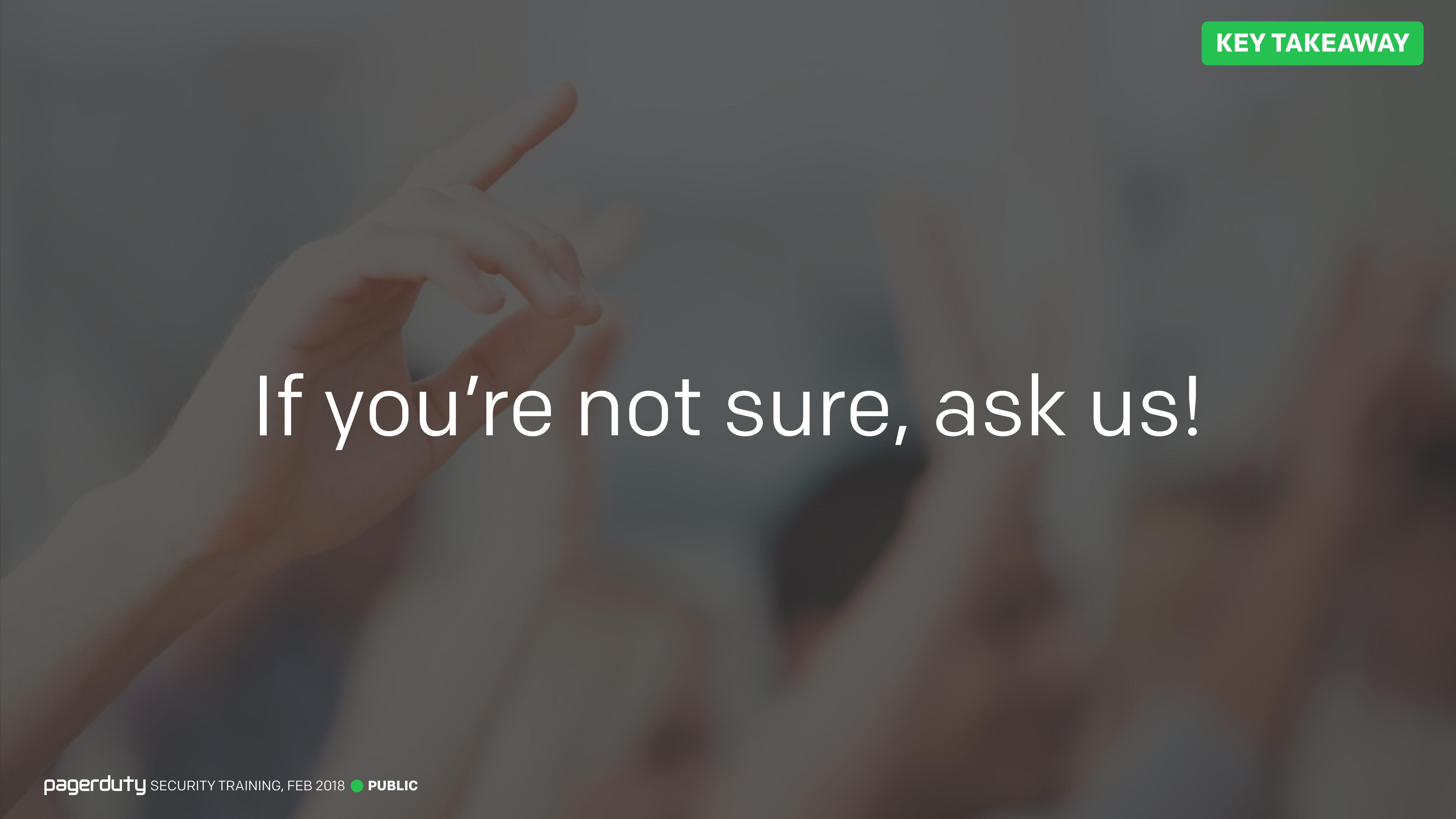


YOU are our greatest asset in the
fight against phishing!

Seriously! We've preemptively blocked several phishing attacks thanks to employee reports.

Not Just Phishing

- Pretexting.
- Baiting.
- Quid Pro Quo.

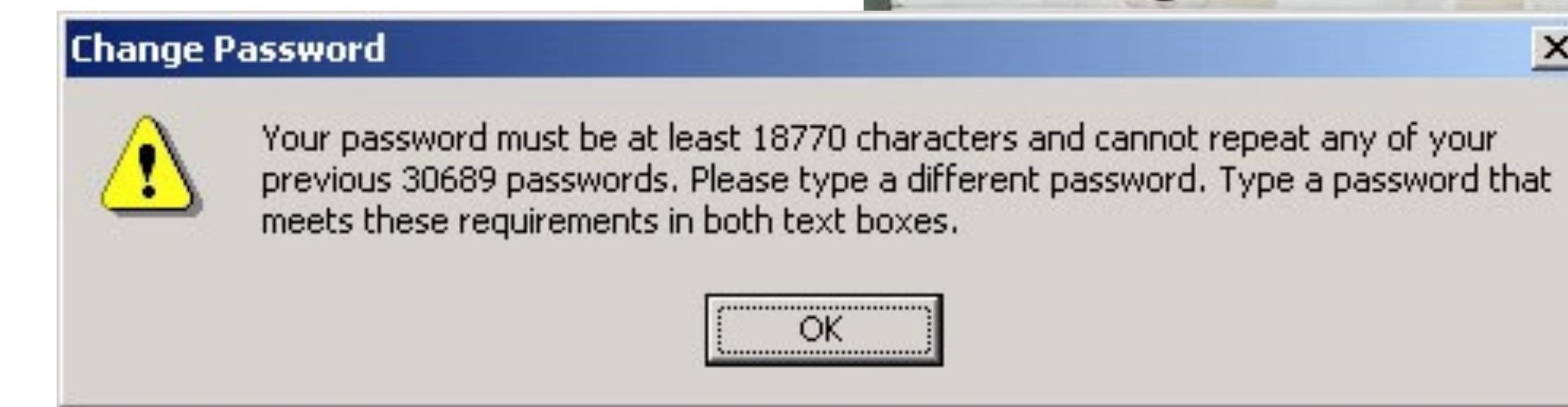
A blurred background image of a person's hand pointing their index finger upwards towards the top right corner of the slide.

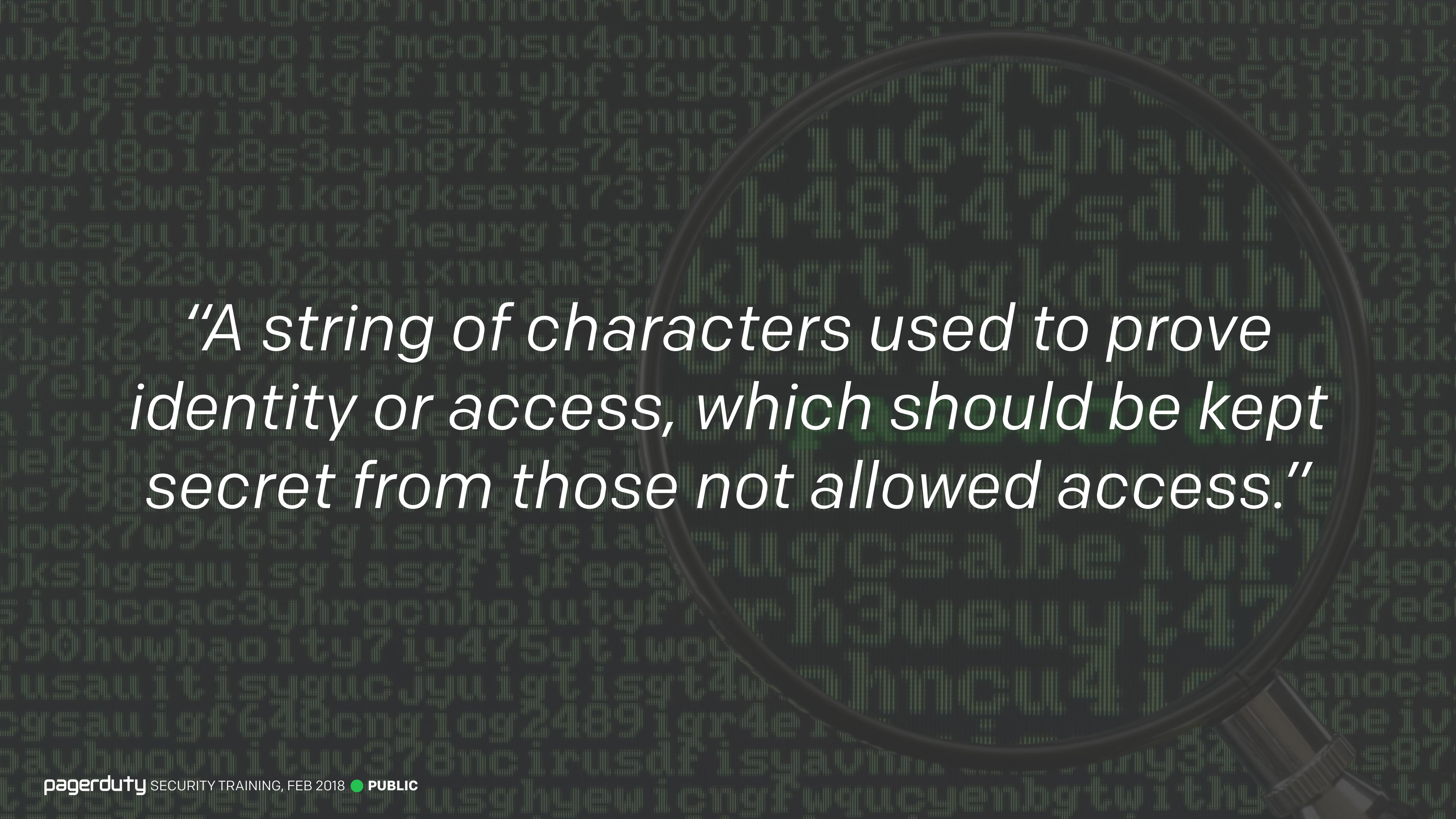
If you're not sure, ask us!

Sorry but your password must contain
an uppercase letter, a
number, a haiku, a gang
sign, a hieroglyph, and
the blood of a virgin.

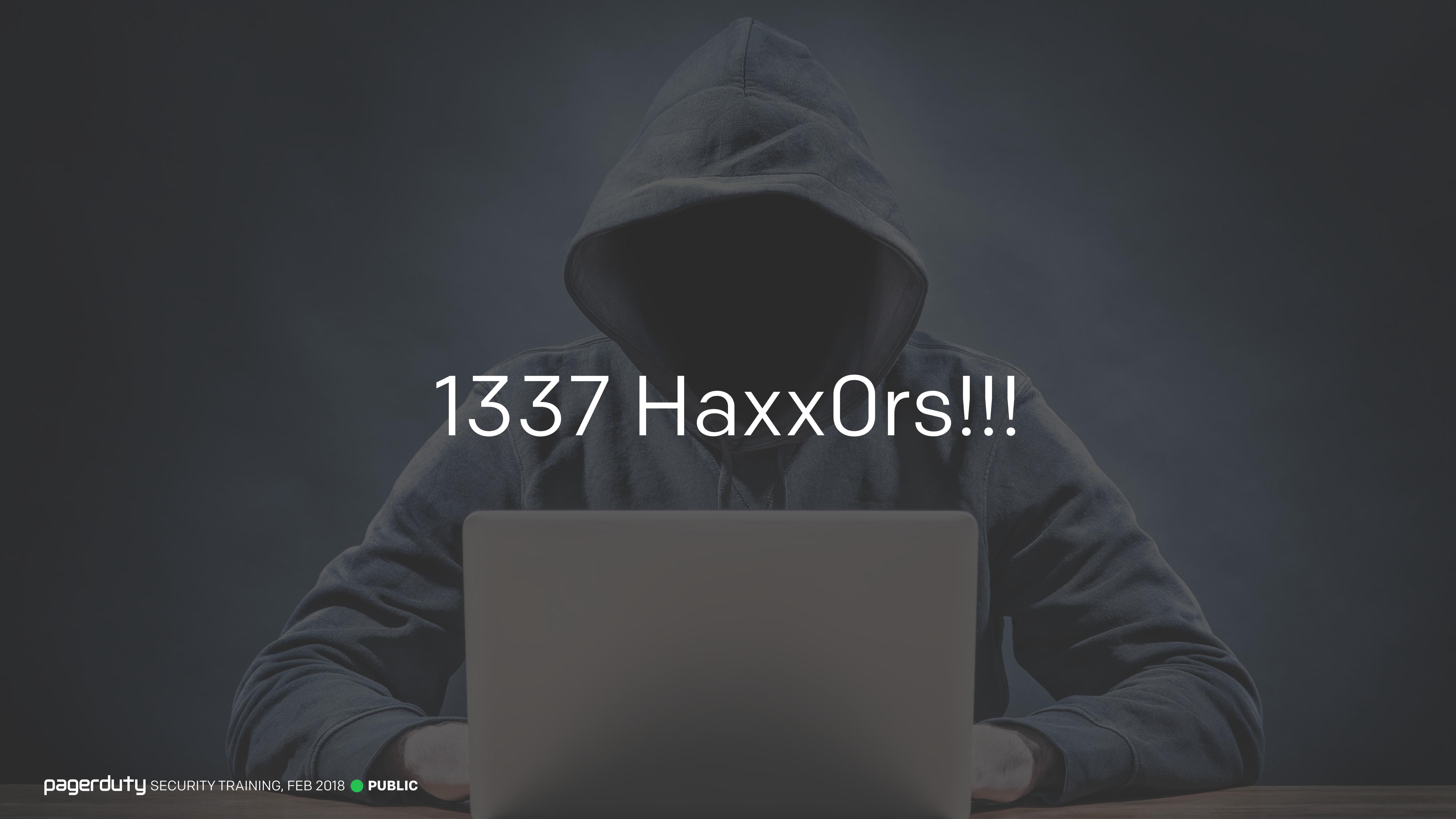


Passwords





“A string of characters used to prove identity or access, which should be kept secret from those not allowed access.”

A dark, moody photograph of a person wearing a hooded sweatshirt, seen from behind. They are sitting at a desk with a laptop open in front of them. The background is dark and out of focus.

1337 Haxx0rs!!!

Hashing

“password” → **SHA-1** → “5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8”

Hashing

“password” →  → “5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8”

Magic

“password” → **MAGIC** → “5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8”

Repeatable

“password” → **MAGIC** → “5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8”

“password” → **MAGIC** → “5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8”

Irreversible

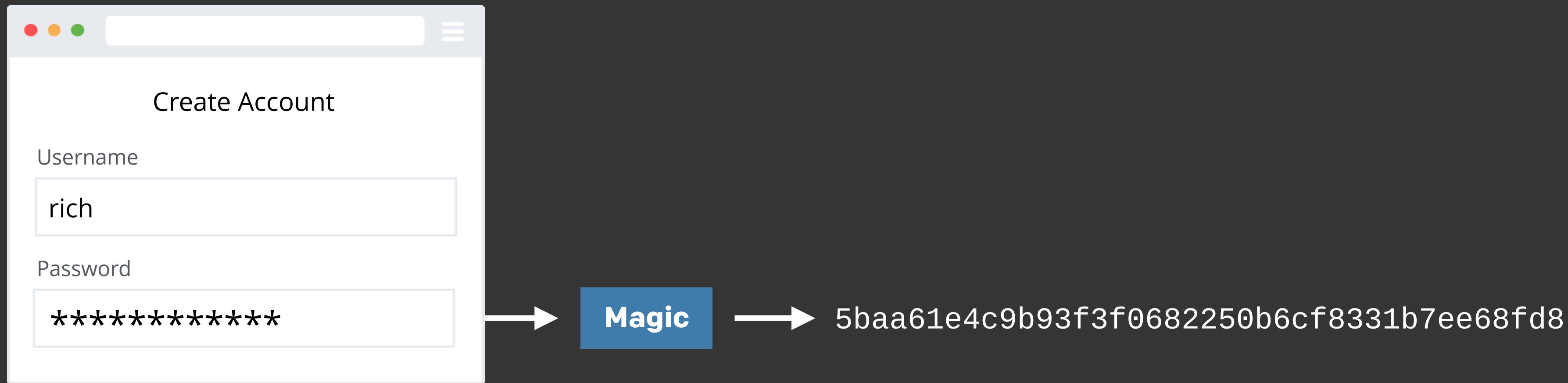
“password”

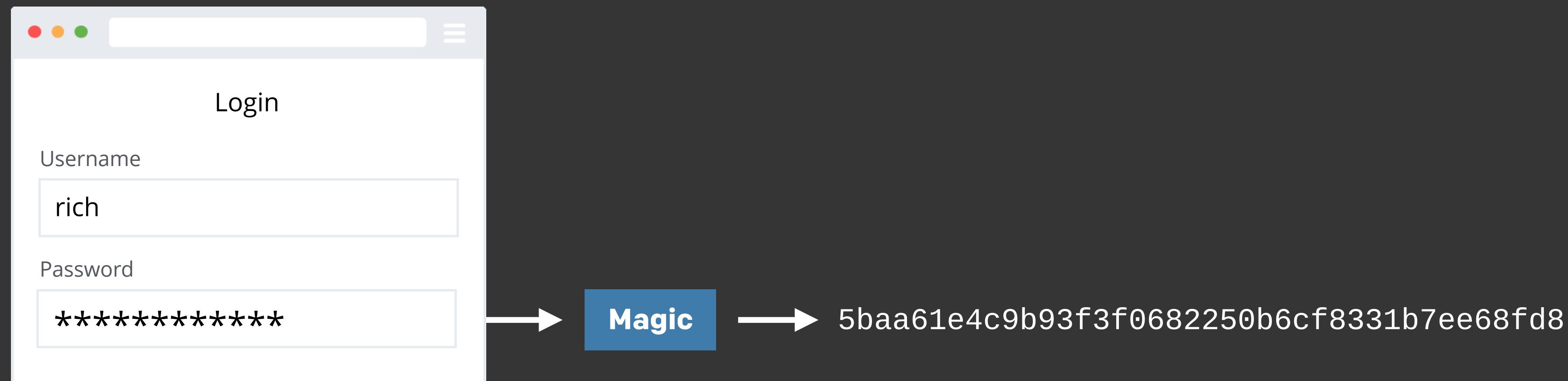
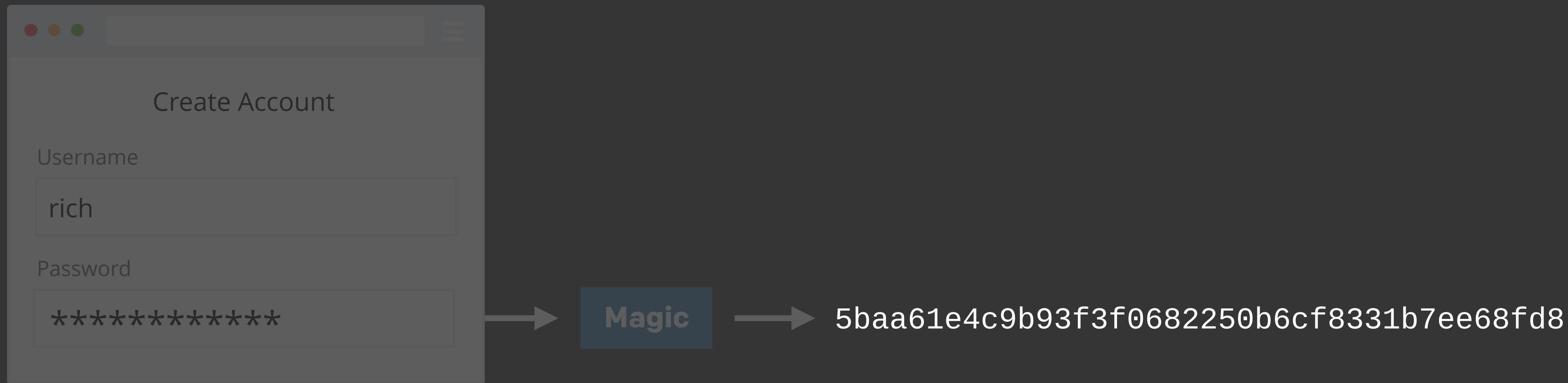


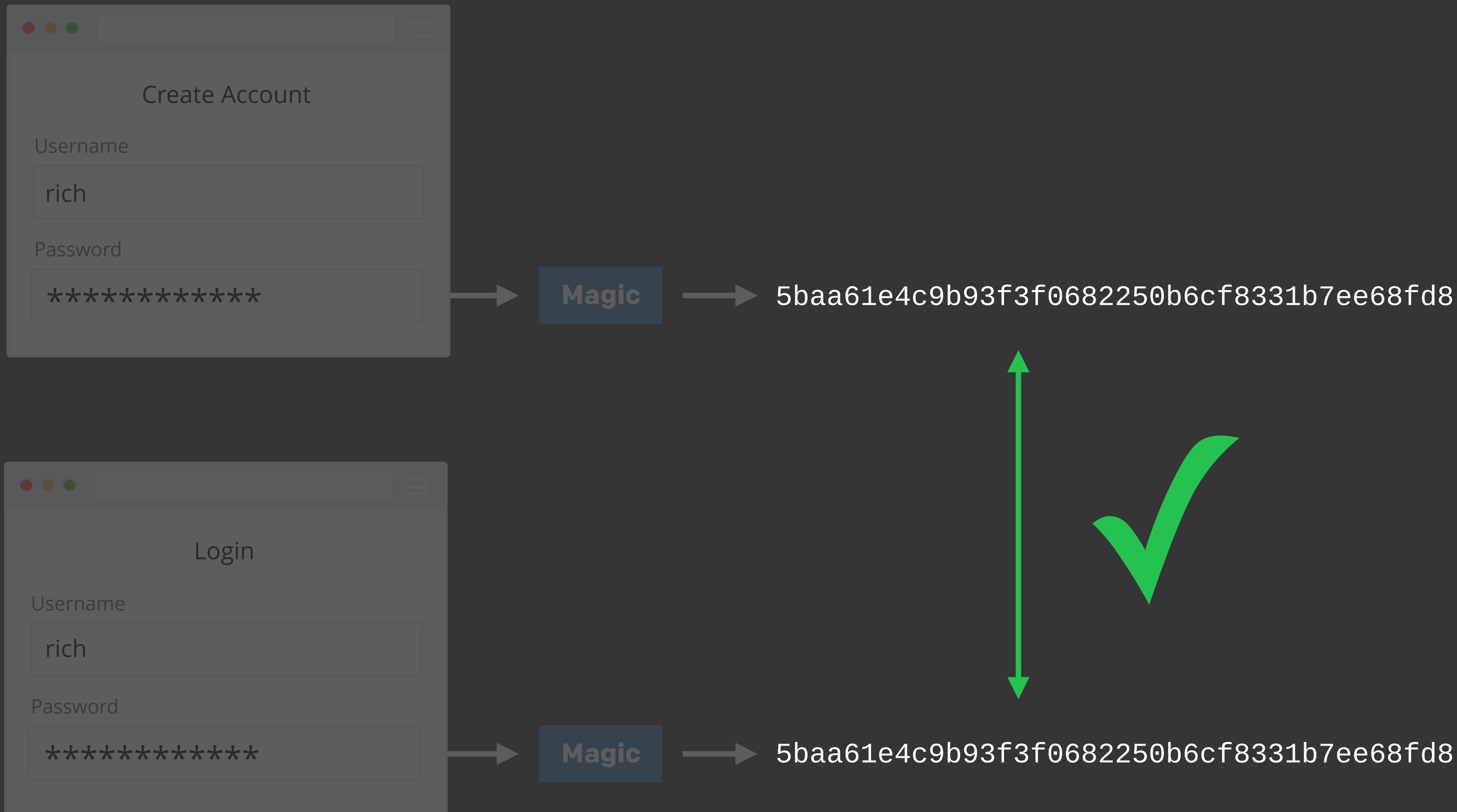
???



“5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8”







E Evil Corp™ Customer Database

id	username	password_hash	password_hint
1	admin	77ba9cd915c8e359d9733edcfe9c61e5aca92afb	NULL
2	rich	410114109270c8ffe4af1706adcad6e29c421f4d	fav person
3	sarah	34ea99829a8df97f54dddc3c747c13c6b34c2a93	NULL
4	james	410114109270c8ffe4af1706adcad6e29c421f4d	Freddie Mercury's band
5	arup	d9bc17fe6fdf4909187612e5374b74a7d593975e	scary movie
6	allison	7c4a8d09ca3762af61e59520943dc26494f8941b	NULL
7	pumpkin22	d9bc17fe6fdf4909187612e5374b74a7d593975e	fav holiday

E Evil Corp™ Customer Database

id	username	password_hash	password_hint
1	admin	77ba9cd915c8e359d9733edcfe9c61e5aca92afb	NULL
2	rich	410114109270c8ffe4af1706adcad6e29c421f4d	fav person
3	sarah	34ea99829a8df97f54dddc3c747c13c6b34c2a93	NULL
4	james	410114109270c8ffe4af1706adcad6e29c421f4d	Freddie Mercury's band
5	arup	d9bc17fe6fdf4909187612e5374b74a7d593975e	scary movie
6	allison	7c4a8d09ca3762af61e59520943dc26494f8941b	NULL
7	pumpkin22	d9bc17fe6fdf4909187612e5374b74a7d593975e	fav holiday

E Evil Corp™ Customer Database

id	username	password_hash	password_hint
1	admin	77ba9cd915c8e359d9733edcfe9c61e5aca92afb	NULL
2	rich	410114109270c8ffe4af1706adcad6e29c421f4d	fav person
3	sarah	34ea99829a8df97f54dddc3c747c13c6b34c2a93	NULL
4	james	410114109270c8ffe4af1706adcad6e29c421f4d	Freddie Mercury's band
5	arup	d9bc17fe6fdf4909187612e5374b74a7d593975e	scary movie
6	allison	7c4a8d09ca3762af61e59520943dc26494f8941b	NULL
7	pumpkin22	d9bc17fe6fdf4909187612e5374b74a7d593975e	fav holiday

邪恶公司™ 客户数据库

id	username	password_hash	password_hint
1	admin	77ba9cd915c8e359d9733edcfe9c61e5aca92afb	NULL
2	rich	410114109270c8ffe4af1706adcad6e29c421f4d	fav person
3	sarah	34ea99829a8df97f54dddc3c747c13c6b34c2a93	NULL
4	james	410114109270c8ffe4af1706adcad6e29c421f4d	Freddie Mercury's band
5	arup	halloween	scary movie
6	allison	7c4a8d09ca3762af61e59520943dc26494f8941b	NULL
7	pumpkin22	halloween	fav holiday

E Evil Corp™ Customer Database

id	username	password_hash	password_hint
1	admin	77ba9cd915c8e359d9733edcfe9c61e5aca92afb	NULL
2	rich	410114109270c8ffe4af1706adcad6e29c421f4d	fav person
3	sarah	34ea99829a8df97f54dddc3c747c13c6b34c2a93	NULL
4	james	410114109270c8ffe4af1706adcad6e29c421f4d	Freddie Mercury's band
5	arup	halloween	scary movie
6	allison	7c4a8d09ca3762af61e59520943dc26494f8941b	NULL
7	pumpkin22	halloween	fav holiday

E Evil Corp™ Customer Database

id	username	password_hash	password_hint
1	admin	77ba9cd915c8e359d9733edcfe9c61e5aca92afb	NULL
2	rich	410114109270c8ffe4af1706adcad6e29c421f4d	fav person
3	sarah	34ea99829a8df97f54dddc3c747c13c6b34c2a93	NULL
4	james	410114109270c8ffe4af1706adcad6e29c421f4d	Freddie Mercury's band
5	arup	halloween	scary movie
6	allison	7c4a8d09ca3762af61e59520943dc26494f8941b	NULL
7	pumpkin22	halloween	fav holiday

E Evil Corp™ Customer Database

id	username	password_hash	password_hint
1	admin	77ba9cd915c8e359d9733edcfe9c61e5aca92afb	NULL
2	rich	queen	fav person
3	sarah	34ea99829a8df97f54dddc3c747c13c6b34c2a93	NULL
4	james	queen	Freddie Mercury's band
5	arup	halloween	scary movie
6	allison	7c4a8d09ca3762af61e59520943dc26494f8941b	NULL
7	pumpkin22	halloween	fav holiday

E Evil Corp™ Customer Database

id	username	password_hash	password_hint
1	admin	77ba9cd915c8e359d9733edcfe9c61e5aca92afb	NULL
2	rich	queen	fav person
3	sarah	34ea99829a8df97f54dddc3c747c13c6b34c2a93	NULL
4	james	queen	Freddie Mercury's band
5	arup	halloween	scary movie
6	allison	7c4a8d09ca3762af61e59520943dc26494f8941b	NULL
7	pumpkin22	halloween	fav holiday

“1” → **MAGIC** → “356a192b7913b04c54574d18c28d46e6395428ab”

“2” → **MAGIC** → “da4b9237baccdf19c0760cab7aec4a8359010b0”

“3” → **MAGIC** → “77de68daecd823babbb58edb1c8e14d7106e83bb”

“4” → **MAGIC** → “1b6453892473a467d07372d45eb05abc2031647a”

“5” → **MAGIC** → “ac3478d69a3c81fa62e60f5c3696165a4e5e6ac4”

```
require 'digest/sha1'
```

RUBY

```
(1..1000000).each do |n|
  sha1 = Digest::SHA1.hexdigest n.to_s
  puts "#{sha1} = #{n}"
end
```



Nerd alert.

邪恶公司™ 客户数据库

id	username	password_hash	password_hint
1	admin	1337	NULL
2	rich	queen	fav person
3	sarah	34ea99829a8df97f54dddc3c747c13c6b34c2a93	NULL
4	james	queen	Freddie Mercury's band
5	arup	halloween	scary movie
6	allison	123456	NULL
7	pumpkin22	halloween	fav holiday

E Evil Corp™ Customer Database

id	username	password_hash	password_hint
1	admin	1337	NULL
2	rich	queen	fav person
3	sarah	34ea99829a8df97f54dddc3c747c13c6b34c2a93	NULL
4	james	queen	Freddie Mercury's band
5	arup	halloween	scary movie
6	allison	123456	NULL
7	pumpkin22	halloween	fav holiday

“a” → MAGIC → “86f7e437faa5a7fce15d1ddcb9eaeaea377667b8”

“aal” → MAGIC → “e61e506ca0fd8251f850bc313f709cc07cbcecf2”

“aalil” → MAGIC → “f60f98341248eca0d2270cb0145d4d17f818366c”

“aardvark” → MAGIC → “ff49abca9701606b01b6245d587d26c31b63a433”

“aardwolf” → MAGIC → “661e46b960572398e02f82878e2dfadb4518899”

E Evil Corp™ Customer Database

id	username	password_hash	password_hint
1	admin	1337	NULL
2	rich	queen	fav person
3	sarah	34ea99829a8df97f54dddc3c747c13c6b34c2a93	NULL
4	james	queen	Freddie Mercury's band
5	arup	halloween	scary movie
6	allison	123456	NULL
7	pumpkin22	halloween	fav holiday

A hand is holding a smartphone in a dark environment. The screen of the phone is visible, showing a dark-themed mobile application with a navigation bar at the top and several icons or cards below it. The background is mostly black, with some ambient light reflecting off the phone's screen and the person's hand.

Trying everything will take too long.

Rainbow Tables Magic Lists

SHA1 Magic Lists

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
sha1_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495	99.9 %	52 GB 64 GB	Perfect Non-perfect	Perfect Non-perfect
sha1_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120	96.8 %	460 GB 576 GB	Perfect Non-perfect	Perfect Non-perfect
sha1_mixalpha-numeric#1-8	mixalpha-numeric	1 to 8	221,919,451,578,090	99.9 %	127 GB 160 GB	Perfect Non-perfect	Perfect Non-perfect
sha1_mixalpha-numeric#1-9	mixalpha-numeric	1 to 9	13,759,005,997,841,642	96.8 %	690 GB 864 GB	Perfect Non-perfect	Perfect Non-perfect
sha1_loweralpha-numeric#1-9	loweralpha-numeric	1 to 9	104,461,669,716,084	99.9 %	65 GB 80 GB	Perfect Non-perfect	Perfect Non-perfect
sha1_loweralpha-numeric#1-10	loweralpha-numeric	1 to 10	3,760,620,109,779,060	96.8 %	316 GB 396 GB	Perfect Non-perfect	Perfect Non-perfect

E Evil Corp™ Customer Database

id	username	password_hash	password_hint
1	admin	1337	NULL
2	rich	queen	fav person
3	sarah	gLCbYt9MX	NULL
4	james	queen	Freddie Mercury's band
5	arup	halloween	scary movie
6	allison	123456	NULL
7	pumpkin22	halloween	fav holiday

gLcByt9MX



Lowercase letters.



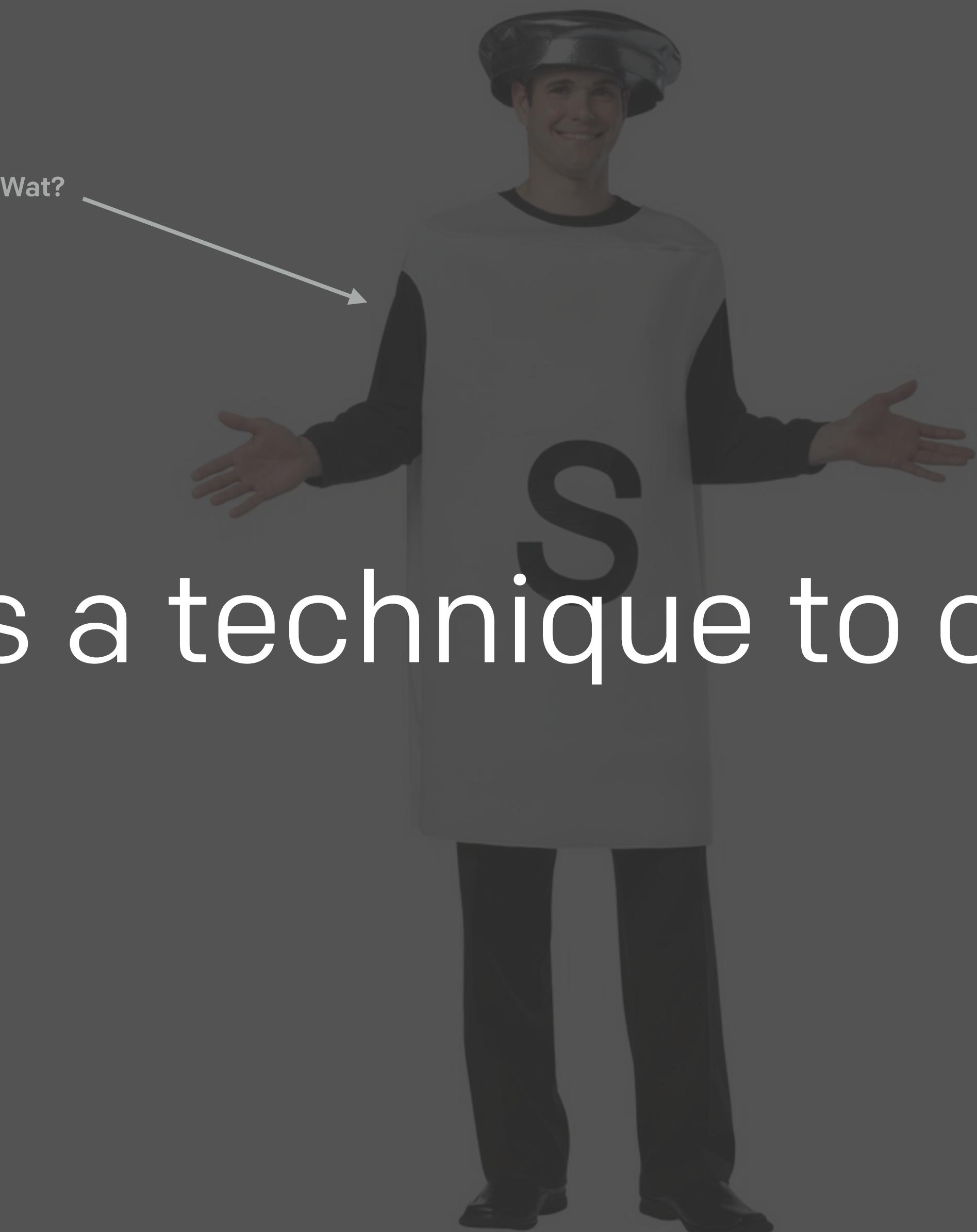
Uppercase letters.



Numbers.



Special characters.



Wat?

Salting is a technique to combat this.

Password Leaks

- LinkedIn (2012) - **Unsalted SHA-1**  **This is exactly how I just showed you passwords being stored!**
- Evernote (2013) - **Unsalted MD5**
- Last.fm (2012) - **Unsalted MD5**
- eHarmony (2012) - **Unsalted MD5**
- Yahoo (2013) - **MD5**  **WTF?! (Not joking, they have it in their FAQ!)**



1.	.com:muRRay000
2.	tmail.com:swordfish91
3.	com:j7dokmg1
4.	ett@gmail.com:lew0rthy
5.	o.com:123890vh
6.	@yahoo.com:spot123
7.	.com:Kitty12
8.	ol.com:appleyapps19308
9.	gmail.com:poopoo1
10.	d12@live.com:kylie2380
11.	n@gmail.com:stark1701
12.	ow@yahoo.com:m0nkey123
13.	l.com:youdontno1
14.	b.de:teddy2003
15.	ail.com:mrTree9
16.	ahoo.com:skellah1
17.	l.com:orangeto2
18.	tmail.com:omg777999
19.	88@gmail.com:hacker2233
20.	ail.com:ibmx41trock

Best Practices

- Long (15+ chars).
- Random.
- Unique.
- Private.



Long

- Longer = Harder to break (mostly).
- Break 8 characters in less than a day*.
- DoD Standards say 15+ chars.
- You should use 50+ if you can.

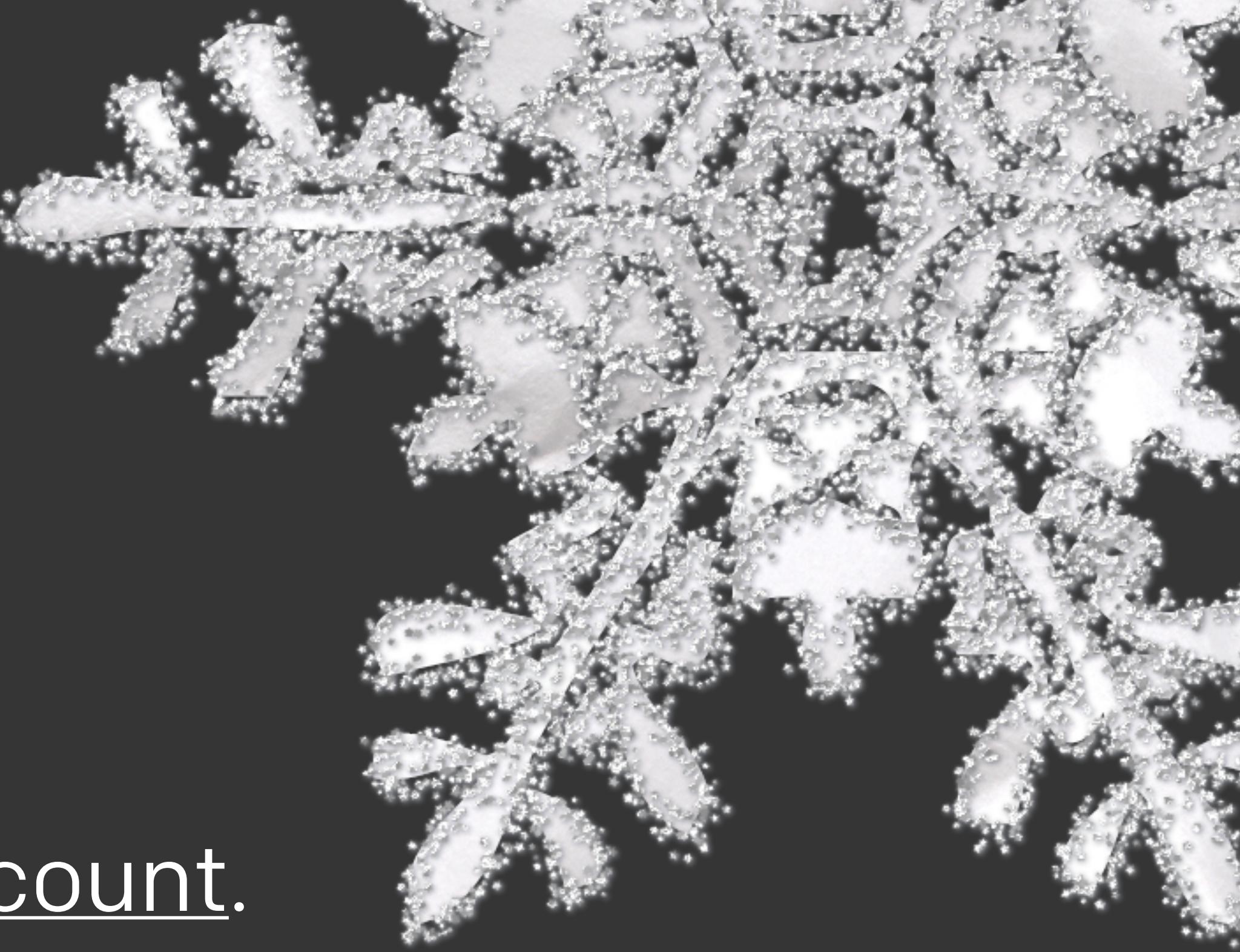


Random

- Don't use "dictionary" words.
- Completely random. Humans are bad at random.
- Most complex you can make it given rules of website.

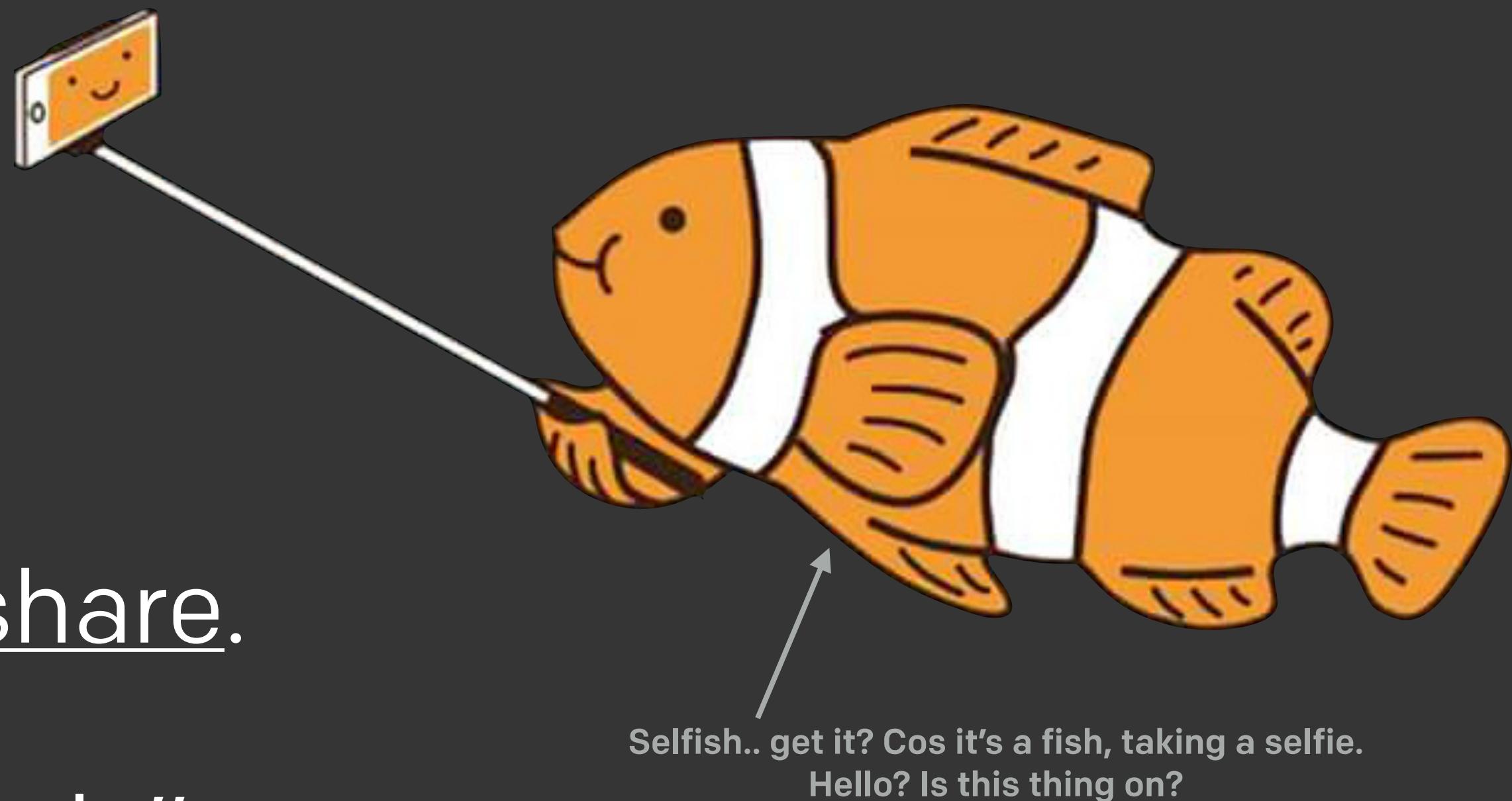
Unique

- Don't follow patterns.
- Different password for every single account.
- Can't assume websites store your password properly.
- If you use same one everywhere, everywhere is vulnerable.

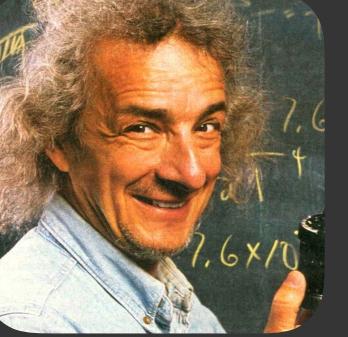


Private

- They're yours. Be selfish. Never share.
- Don't send over "insecure channels":
 - i.e. Email, IM, Facebook, Slack, etc.
- We'll never ask you for your password.



“Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months.”



Clifford Stoll



Please get a new toothbrush more frequently than this.



Bad Passwords

password ← σ_σ

P4SSW0rd

P&SSW0~d

I Like Rainbows!

CorrectHorseBatteryStaple

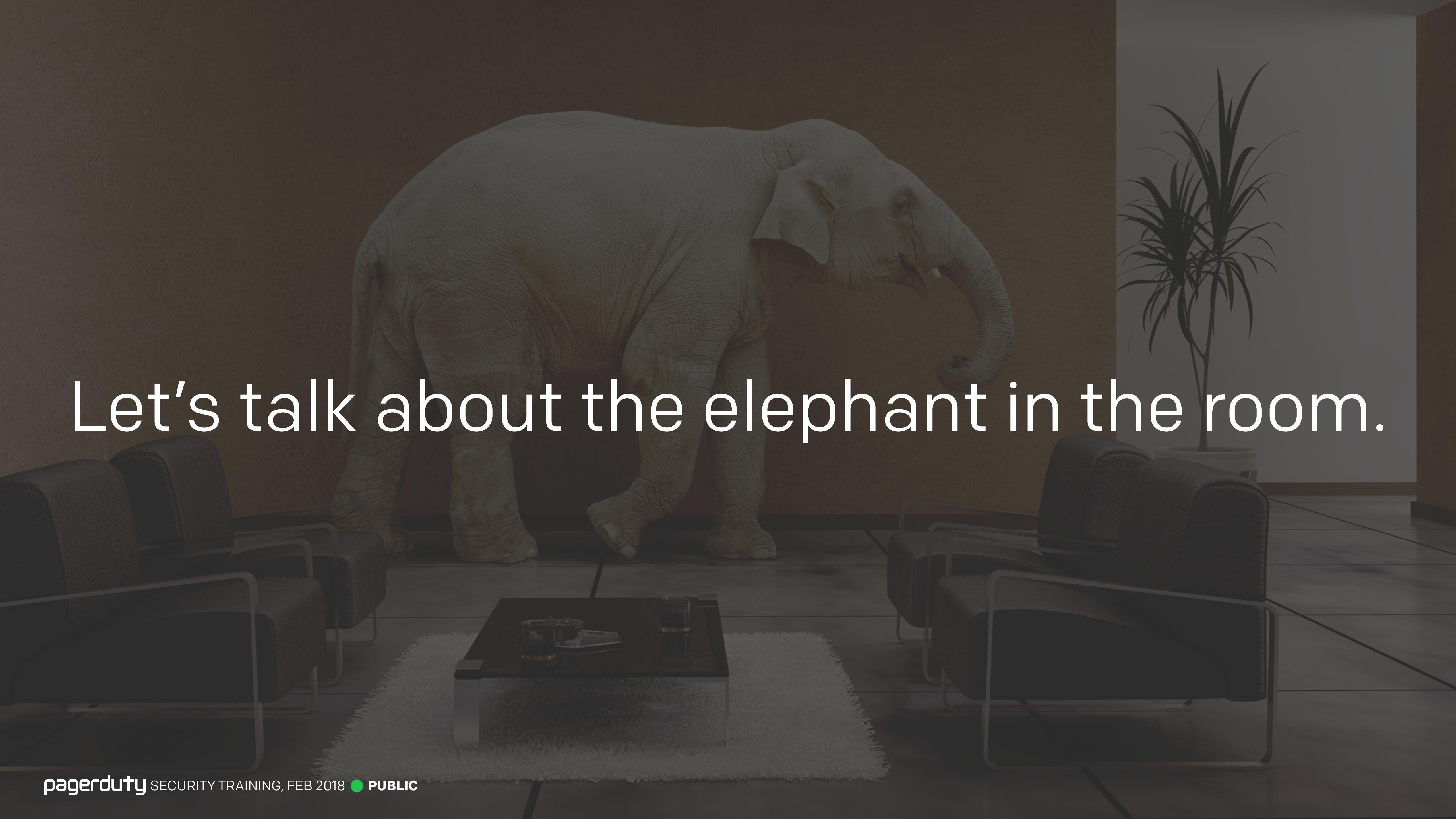


Good Passwords

lakuSj>qP&^`H;Bk^jo]3%}&'iT\U*7iw">k:w0ZC:t/3A?
-#!frWr[:pGYur=R5E:,gpr%h;]t#}#FjZpwesims(dvRw<!c
Q2D" g(l^C34sNqFv^huED{n*1jmqZ;,3`ROQ\$,y2(2dt7|+1z
+}J*%hH! ;F&?-f\$yUKv.-f&8ZT!y[L]`0\SVV,H}#^[\\"nk1e
.urydi3;!NPcy9T*wjXFYK<UCJT}]bL(:)ob0`("V;jF<A14p



Except these are now public, and are no longer good passwords.

A large, light-colored elephant stands in a conference room. It is positioned behind a long, rectangular conference table. On the table, there are two glasses filled with a dark liquid, possibly beer or whisky. The room contains several dark-colored office chairs arranged around the table. In the background, a large window looks out onto a bright, overexposed outdoor area. A tall, green potted plant stands near the window. The overall atmosphere is surreal and humorous, as the elephant is a clear metaphor for a large, often overlooked issue.

Let's talk about the elephant in the room.



“I can’t remember that!”

Use a Password Manager

Password Managers

- Generate secure passwords based on any criteria.
- Remember all your passwords for you.
- Allow you to easily use different passwords for everything.

Password Managers

- Not going to lie, they are annoying at first.
- Much better in the long run!
- Not just for work! Use for personal stuff!



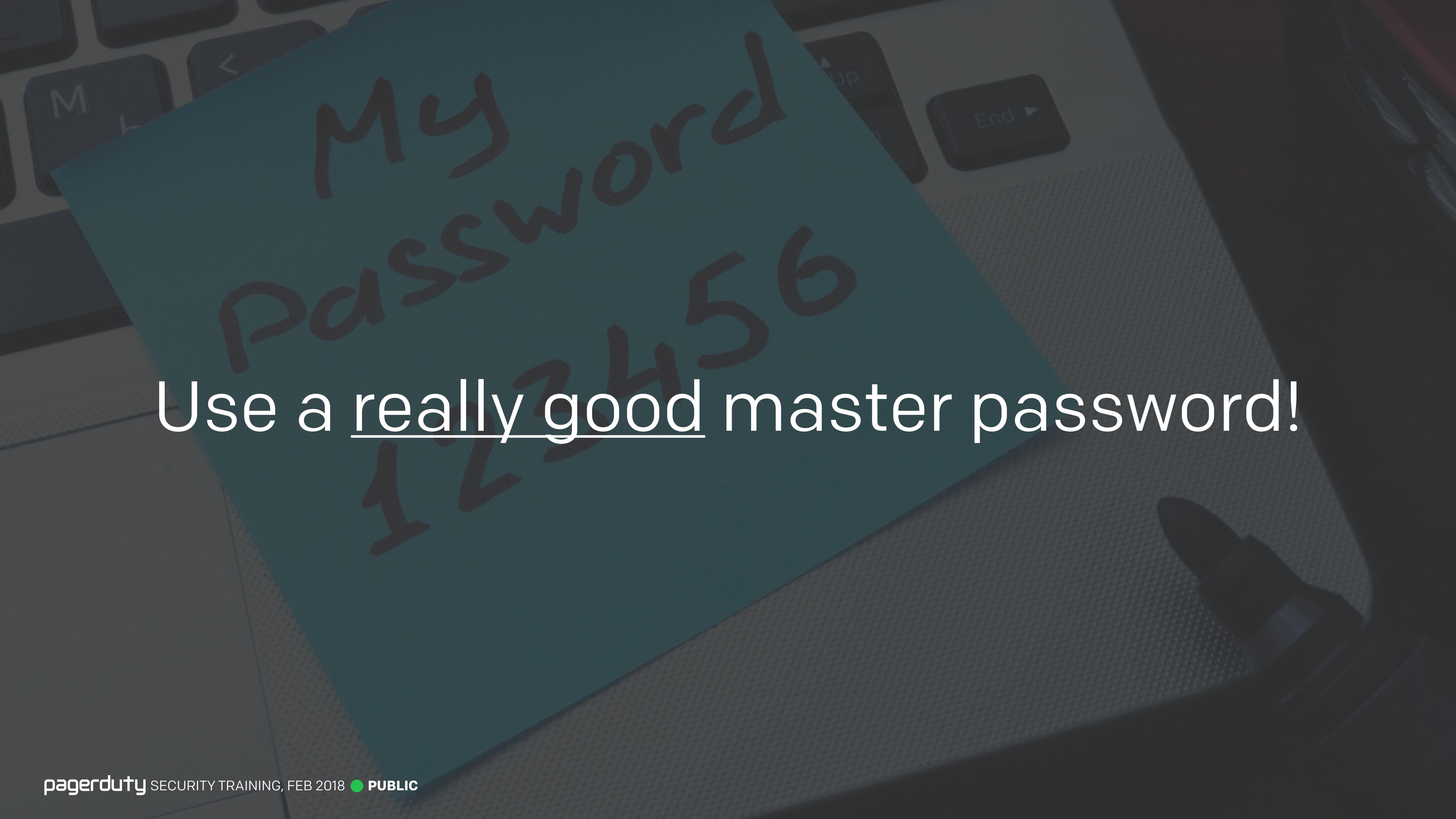
Putting all our eggs in one basket?

“Password managers don’t have to be perfect, they just have to be better than not having one.”



Troy Hunt

Creator of haveibeenpwned.com



Use a really good master password!

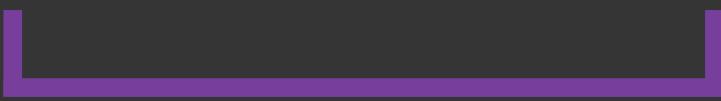
a7hD

%^Ht

#0Fd

{ - 1G

A8Th



- Generate the password the same way as any other.
- Split into chunks of 4 or 5 characters.
- Sit down and memorize it (much easier than you think!)
- Type it out lots of times to get it into muscle memory.

But Wait, There's More!



Billy Mays, not Drew from HelpDesk.

Password Equivalency

- Security question answers.
- Personal information.
- Two-factor authentication secrets (sort of).



Answer your security questions

Hello PizzaCatLover, just one more step. Please answer these security questions:

What is your favorite food?

answer

What is your favorite animal

answer

[Cancel](#)

[Continue](#)

Security Questions

- Never use real information.
- Answers should follow same rules as passwords.
- Most websites store these in the clear. Beware!



- 1 Email
- 2 Security
- 3 Password

MileagePlus account security enhancements

In order to enhance the security of your MileagePlus account, we need you to make a few account updates. You will no longer be able to use a PIN to access your account online, although your PIN will still be required for certain phone transactions.

Please select security questions and answers from the dropdown menus.

Question 1 of 5

What is your favorite flavor of ice crea... ▾

Select your answer* ▾

- Banana
- Birthday cake
- Black cherry
- Black sesame
- Brownie
- Butter brickle
- Butter pecan
- Butter rum
- Cajeta/caramel
- Chocolate
- Chocolate almond
- Chocolate chip

Question 2 of 5

Select question* ▾

Question 3 of 5

Select question* ▾



Multi-Factor?

- Knowledge.
- Possession.
- Inherence.

Multi-Factor?

- ~~Knowledge~~. Something you know.
- ~~Possession~~. Something you have.
- ~~Inherence~~. Something you are.

Multi-Factor?

- ~~Knowledge~~. Something you know. Password.
- ~~Possession~~. Something you have. Device.
- ~~Inherence~~. Something you are. Fingerprint.

Two-Factor

This is a Yubikey. They're awesome!



- Pick two of the factors. e.g. Password + Phone.
- Don't store two-factor secret with passwords!
- Keep backup codes separate too.

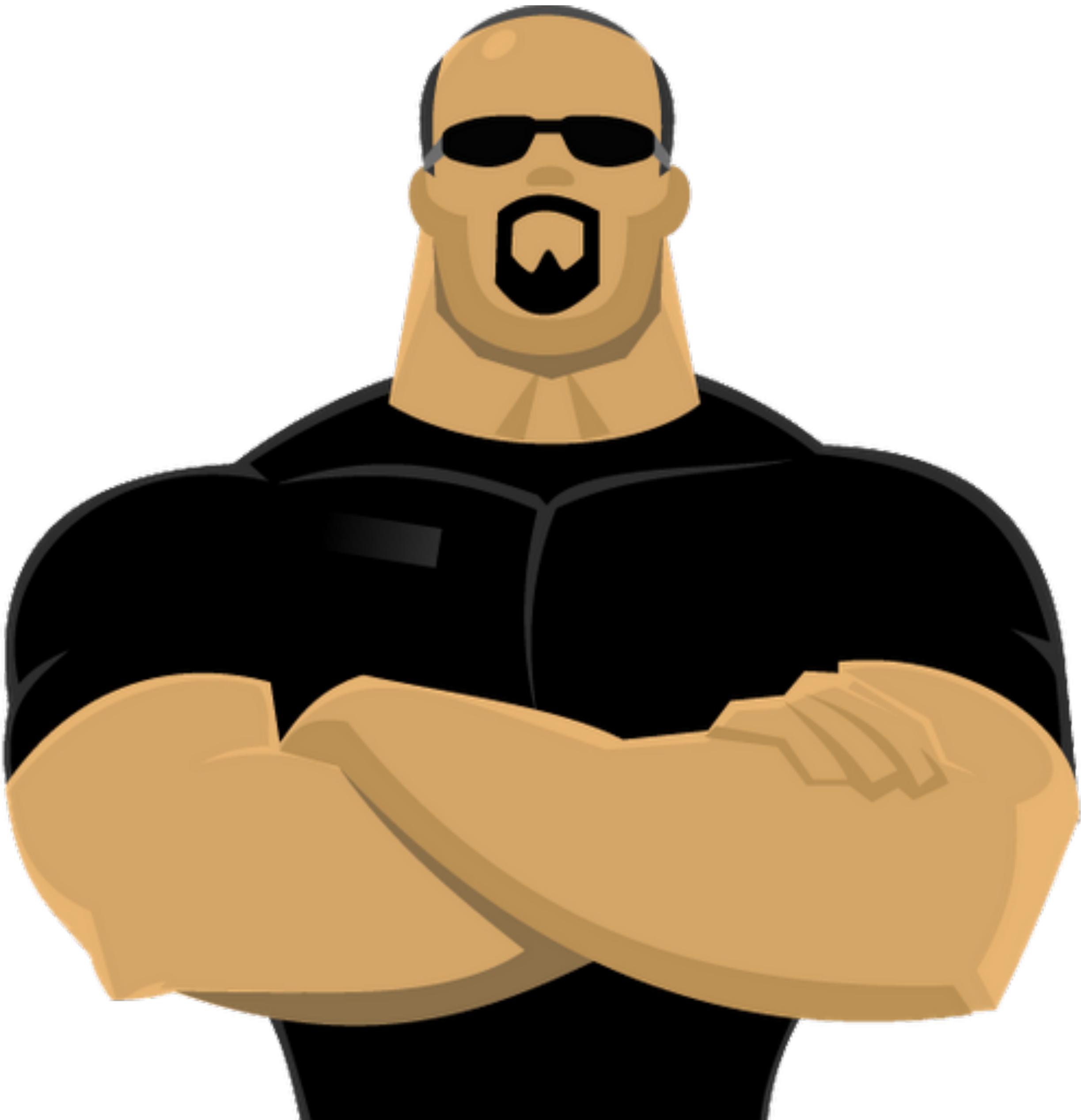


We use Yubikeys!

Use Two-Factor Authentication



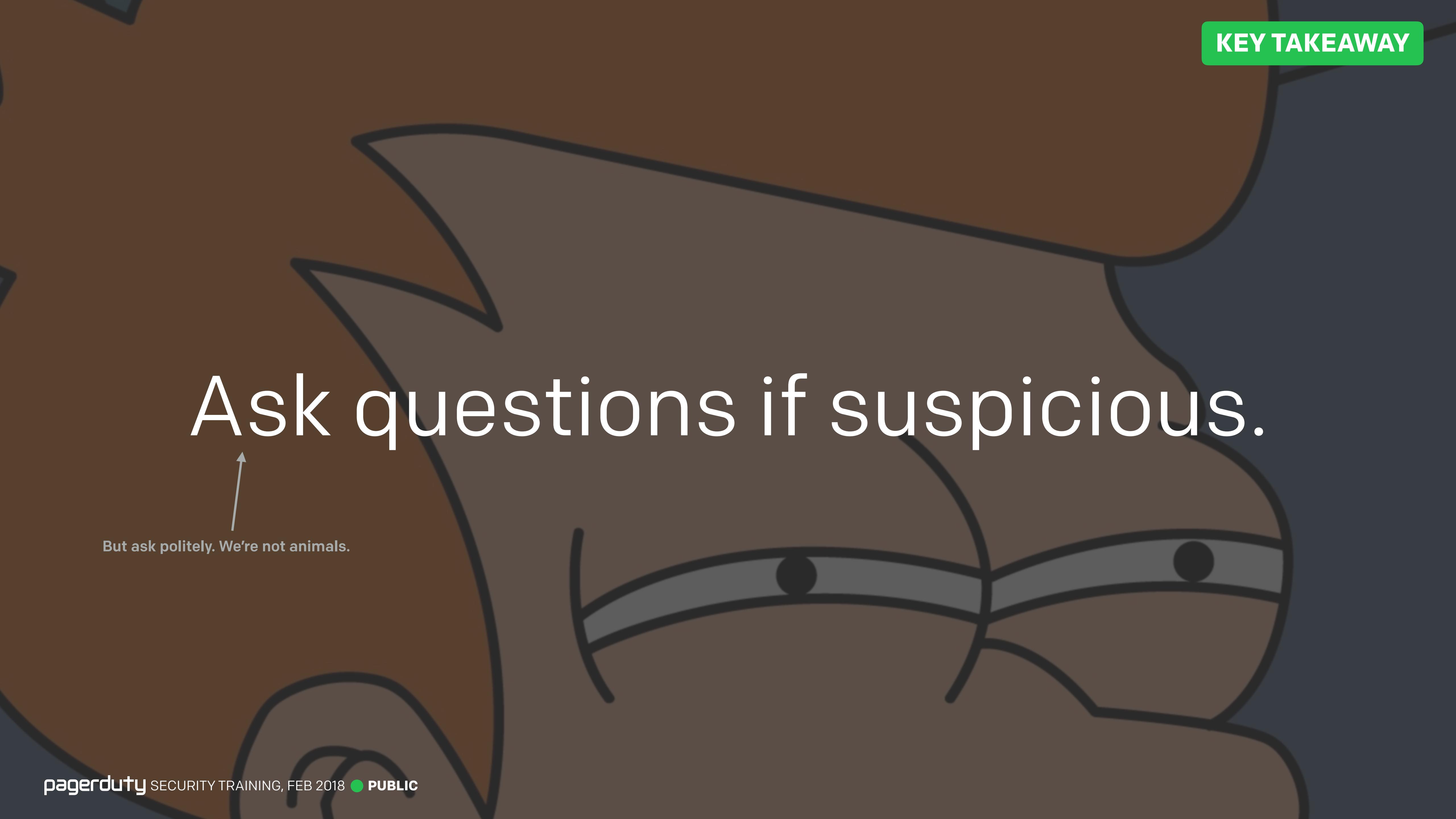
Physical Security



“Security measures that are designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm.”

Basic Guidelines

- Question unknown people (politely).
- Verify if unsure.
- Alert Security Team to suspicious activities!

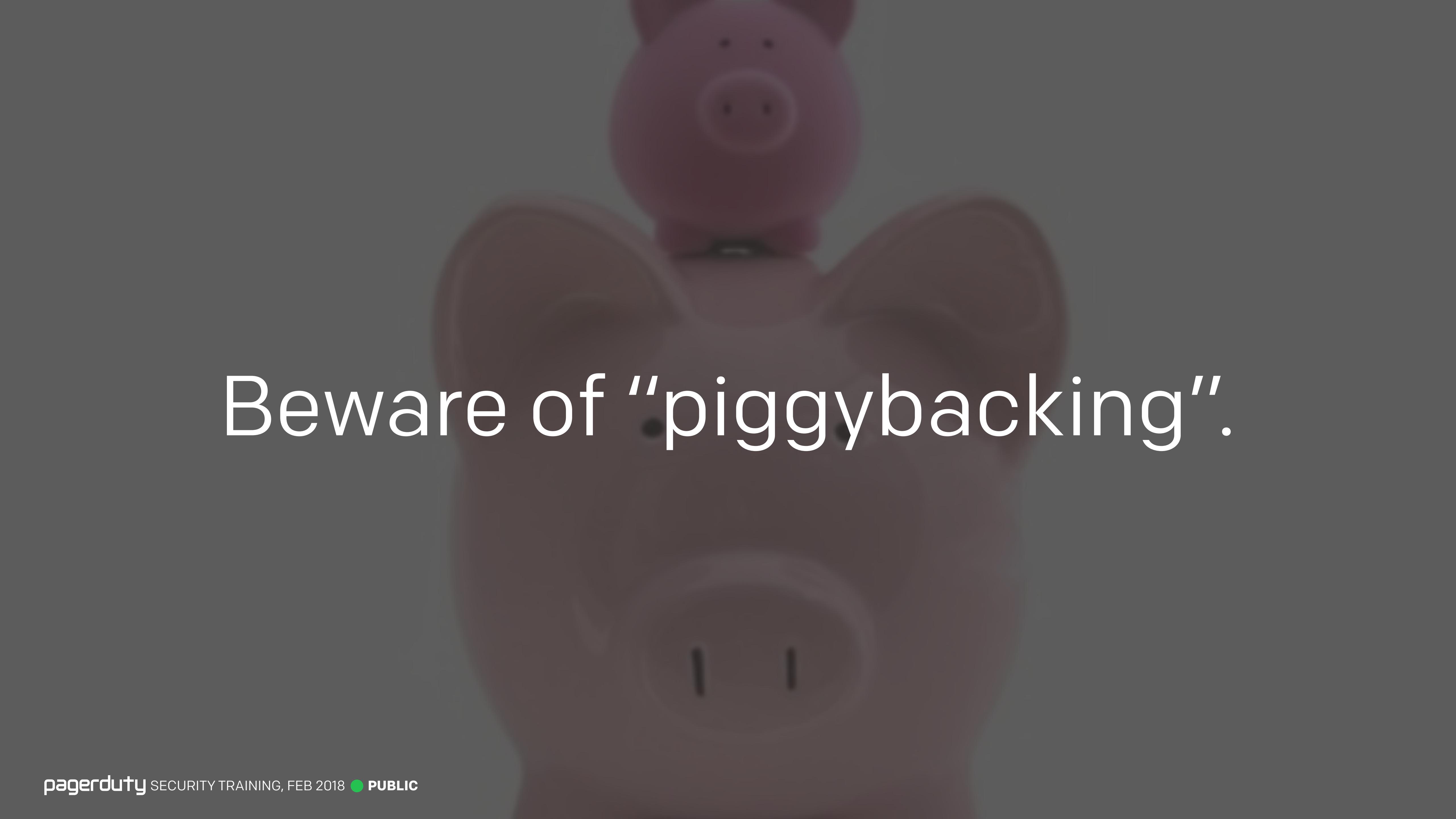


Ask questions if suspicious.

But ask politely. We're not animals.

KEY TAKEAWAY

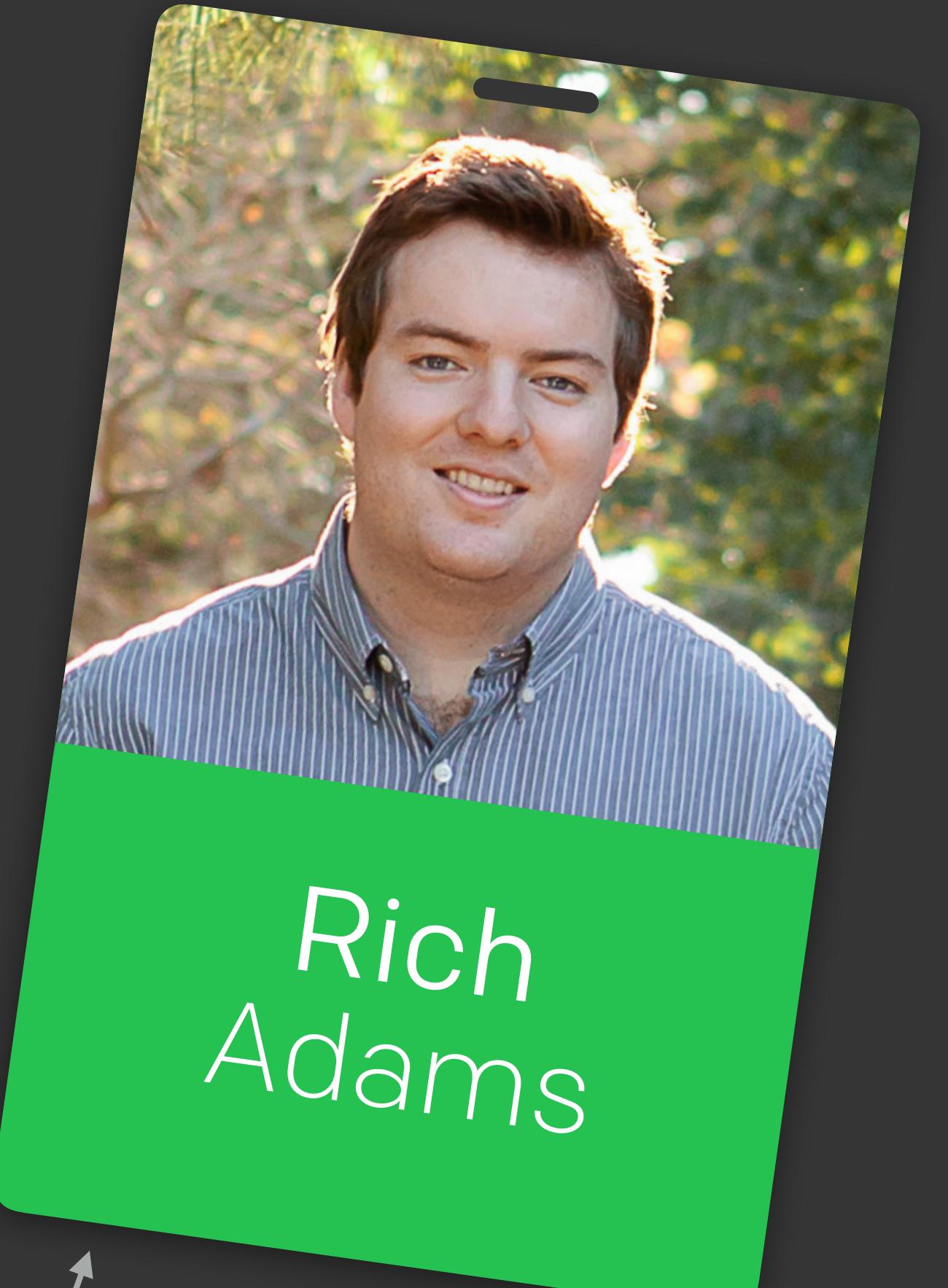
Lock your computers!



Beware of “piggybacking”.

Building Keycards

- Always carry your keycard with you.
- Keycards required on all doors.
- Photos will likely be required soon.
- Don't leave your keycard at your desk!



Yet another Hackday project I never finished.

Building Security

- Do not prop open doors.
- Make sure all visitors sign in.



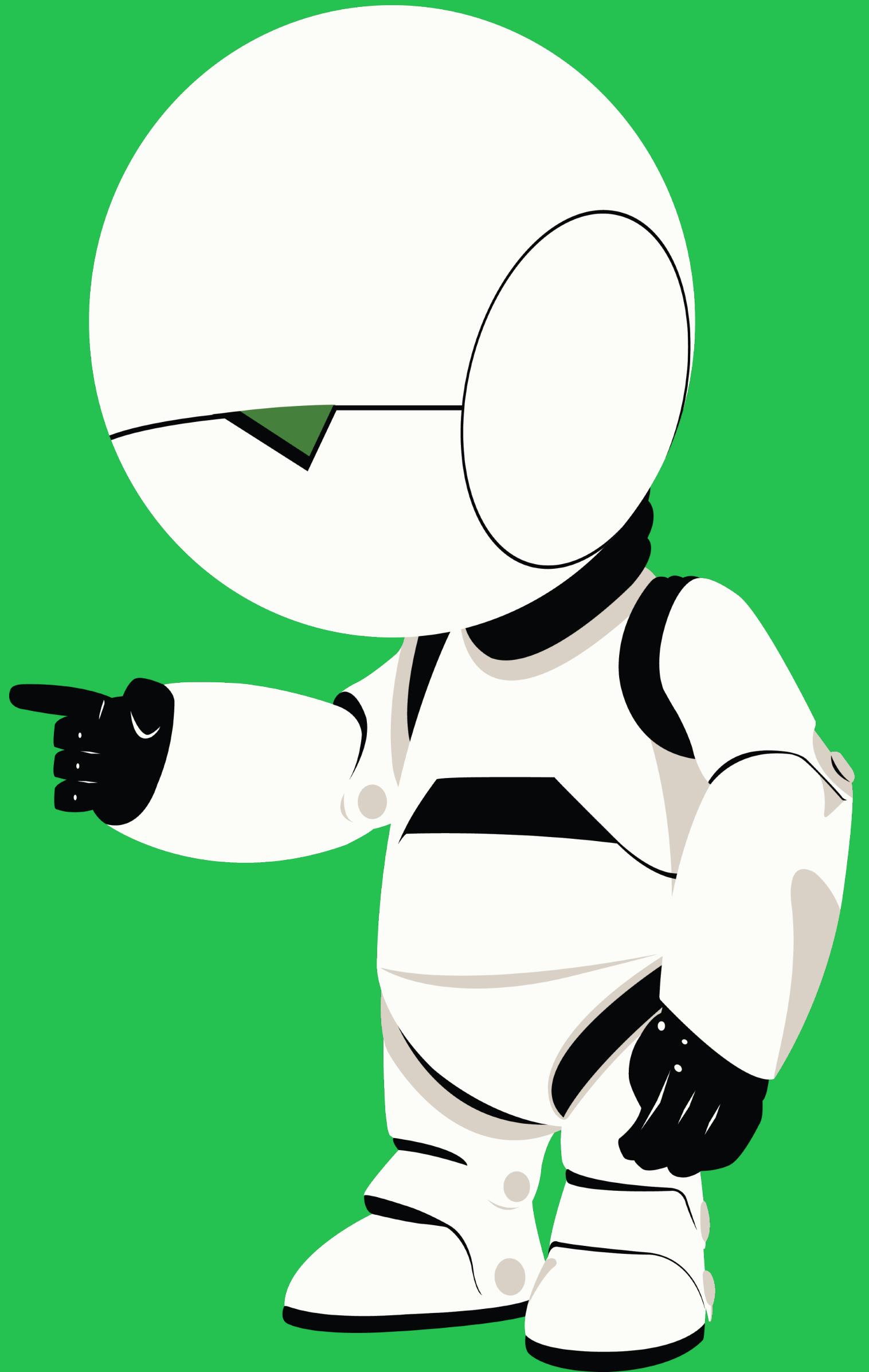
Laptop Stolen?!



New MacBook Pro. Coming soon!



DON'T PANIC





Page HelpDesk or Security at any time for lost/stolen devices.

You will not get into trouble!

Personally Identifiable Information

Also known as "PII".



“Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.”

Basic Guidelines

- Don't discuss company info in public.
- Don't look at info you shouldn't.
- Don't disable encryption!
- Be careful with company data...

A man in a flight suit is looking at a handheld device with a screen. He is in a dark, futuristic environment with glowing panels in the background.

Company Data?

No, not this kind of data.

Wonder if this comes with an unlimited data plan. 🤔

Data Classification

General Data

Anything intentionally available to the public.

Business Data

Anything used to operate the business.

Customer Data

Anything provided by the customer.

Data Handling

	Authentication	Access Control	Storage	Auditing	Encryption	Distribution	Destruction
General	✓	✓	✓		✓		
Business	✓	✓	✓	✓	✓		✓
Customer	✓	✓	✓	✓	✓		✓

Wiki Page Classifications

PUBLIC

Can be shared with anyone, even outside PagerDuty.

RESTRICTED

Can only be shared with customers under an NDA.

Default

INTERNAL ONLY

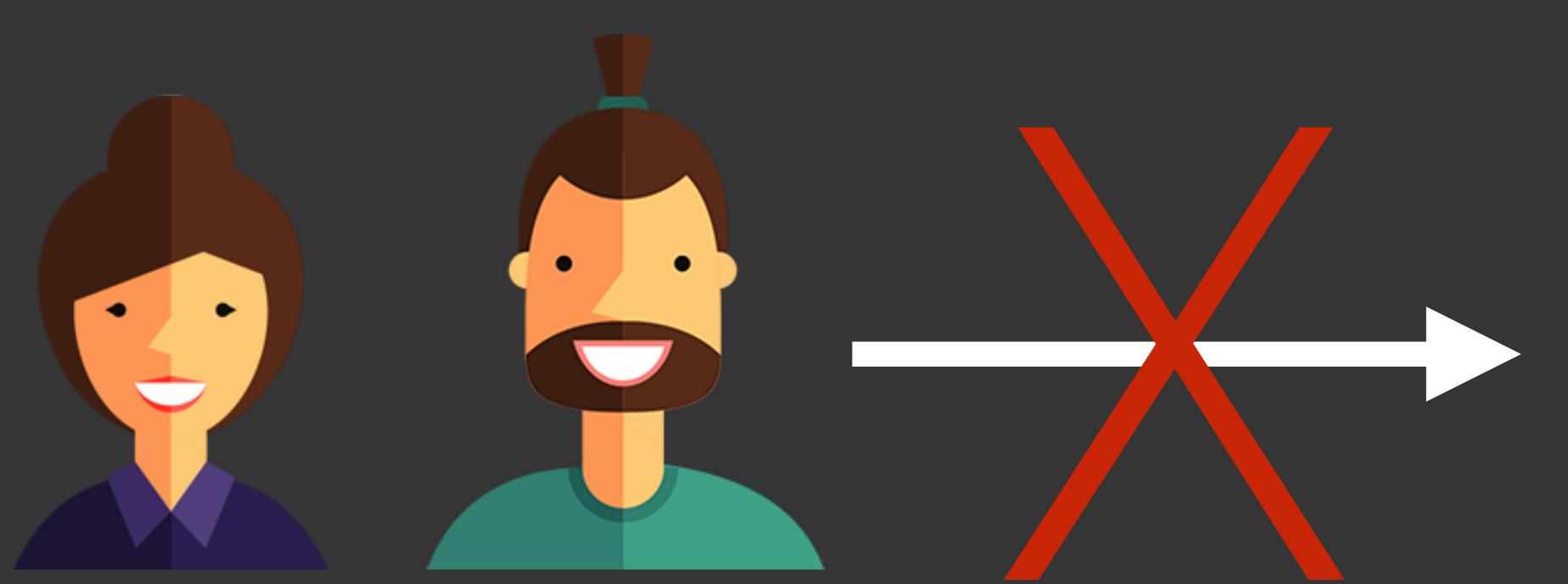
Not to be shared with anyone outside of PagerDuty.

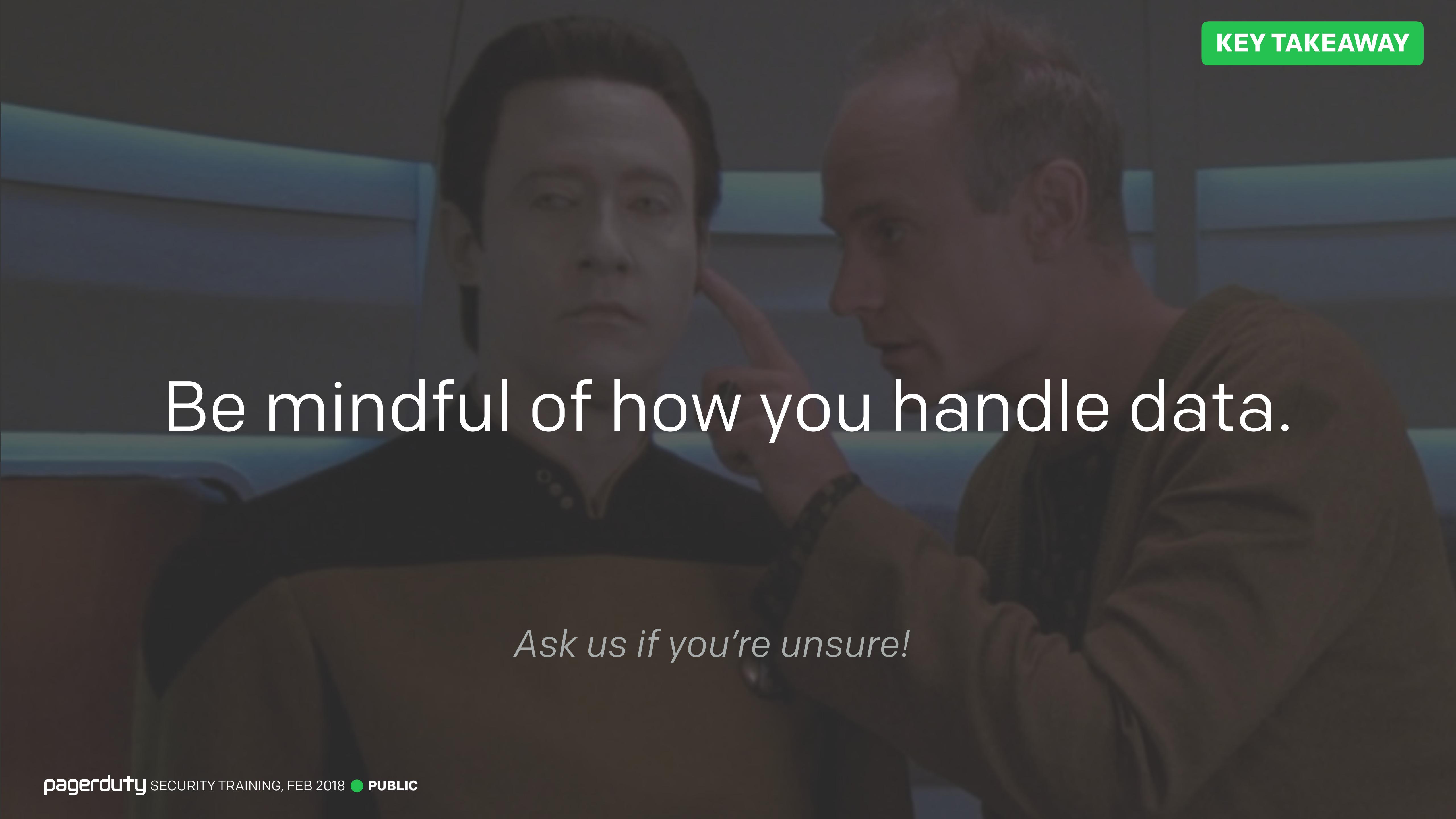
Hey look, I used the same system for these slides!

No PagerDuty data on personal devices!



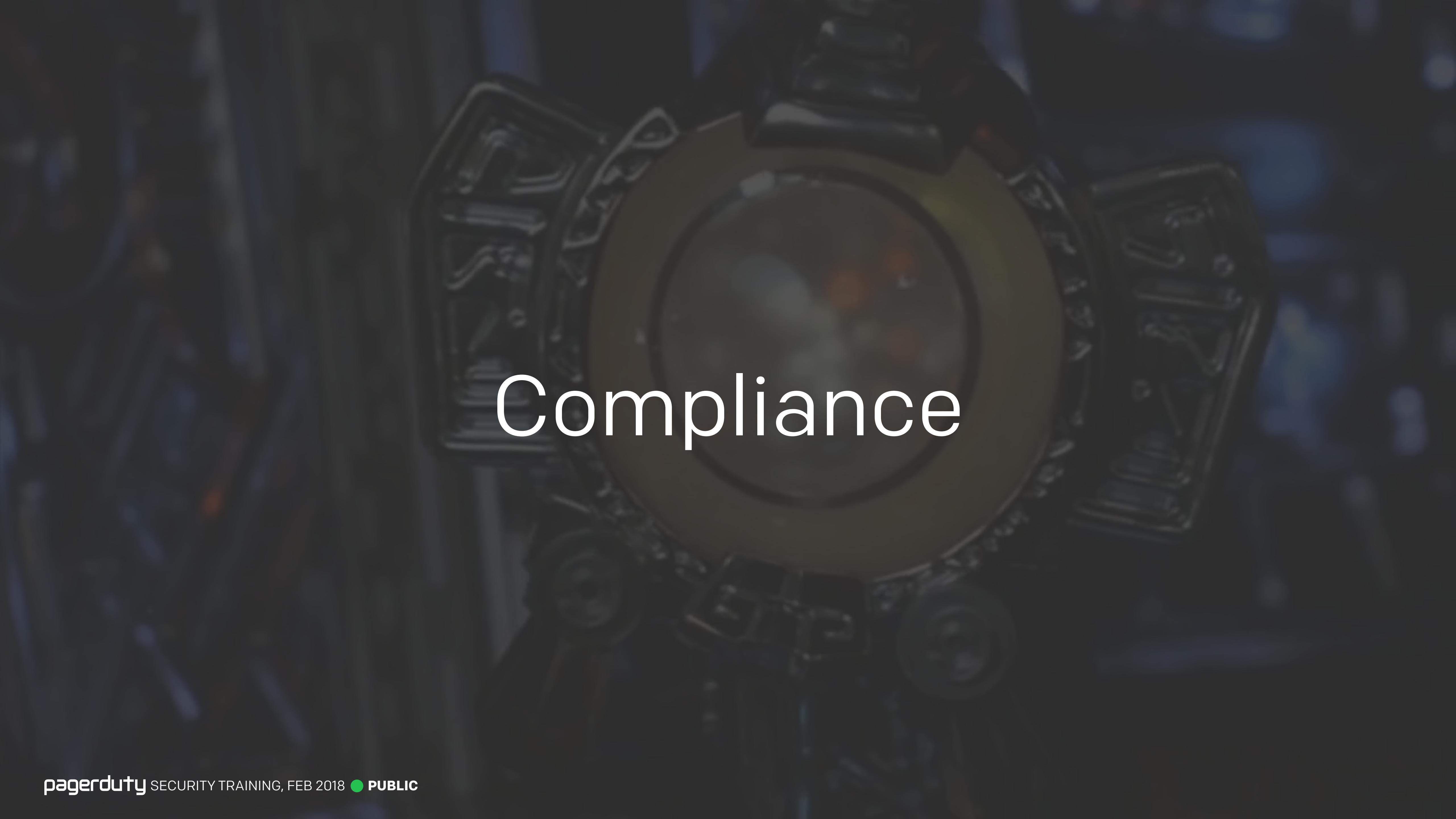
No customer data on PagerDuty devices!



A dark, slightly blurred photograph of two people, a man and a woman, sitting at a desk and looking at a computer screen together. They appear to be in a professional or educational setting.

Be mindful of how you handle data.

Ask us if you're unsure!



Compliance



European General Data Protection
Regulation (GDPR) is a thing.

GDPR

- Data Controller vs Data Processor.
- Privacy by design.
- Data portability.
- Right to be forgotten.
- Intended purpose.
- Big penalties!



Pwn All The Things

@pwnallthethings

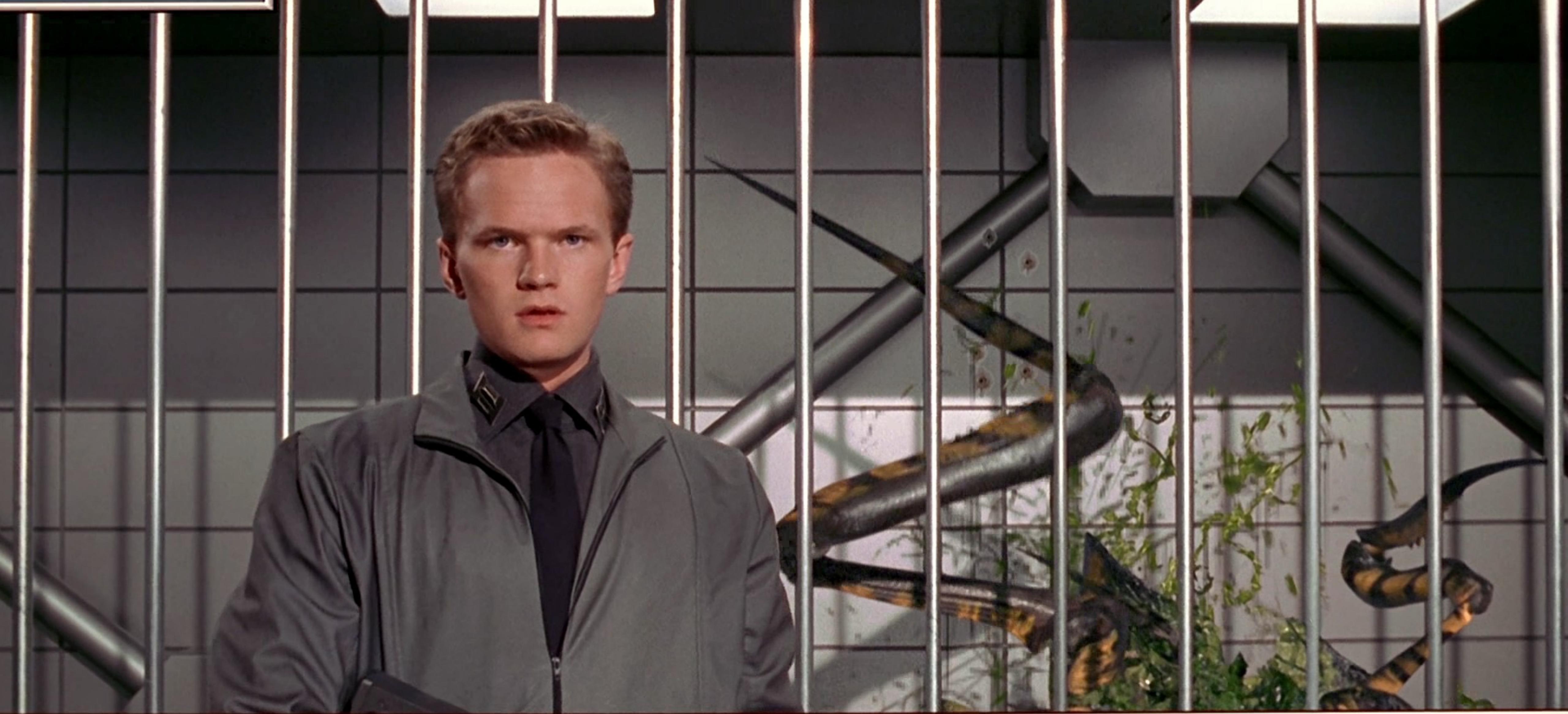
Dear Santa,

I am writing to invoke my right to be removed from the naughty list, as per Article 17(1) of the EU GDPR and hereby withdraw my consent for my information to be ever held there as per Article 7(3).

Yours faithfully,
Timmy (age 5)

PS I would like a red bike for xmas

[REDACTED]



† WOULD YOU LIKE TO KNOW MORE ?

[REDACTED]

LLAMA



Morbo DEMANDS Your Questions!



Gain Insight: <http://o.aolcdn.com/hss/storage/midas/3feea042a6aabe431c0ce19a83d9281e/204753737/594644139.jpg>

Our Job: <https://media-exp1.licdn.com/mpr/mpr/AEAAQAAAAAAAmaAAAAJDdiY2Q1NjM5LWRjNzMtNGM5NS05YjQ1LTU1NWQwODJIMDziMA.jpg>

Bike Lock: <https://www.flickr.com/photos/dusting/501791705>

Chains: <https://wallup.net/chains-padlock-computer-notebooks-laptop/>

Lying: <https://steemit-production-imageproxy-upload.s3.amazonaws.com/DQmeL84DqBvLi5jYUg3gaWsR7DnUoLWVGyMwgTsexVhTQvX>

TSA Keys: <http://1.bp.blogspot.com/-hu8Kr6-3nrs/VdtMPbThXhI/AAAAAAADjIA/3Mw-5akcpq8/s1600/tsa-master-keys-blurred.jpg>

Social Engineering: http://1.bp.blogspot.com/-jlfzV5Jp6fU/U90R09_puql/AAAAAAAAC1E/r-xBTskaNRM/s1600/telephone_scam.jpg

Social Engineering (2): <http://arsicha.info/wp-content/uploads/2017/11/social-engeener-1000x600.jpg>

Phishing: <https://web-ster.com/img/other/password-thief-trans.png>

Spear Phishing: <https://www.deeperblue.com/wp-content/uploads/2016/03/Evren-Wide-Kick-3.jpg>

We Want You: <https://cdn.shakewellmagazine.com/wp-content/uploads/2016/01/16140712/we-want-you.png>

Ask Question: https://www.goldenmeadowsretrievers.com/wp-content/uploads/2014/08/iStock_000021006935_Medium1.jpg

Passwords: <https://cdn.someecards.com/someecards/usercards/MjAxMy1mYzEzN2U0NzhIZWZmNDU3.png>

Passwords (2): <https://twitter.com/desmondholden/status/965747299468136448>

Passwords (3): https://www.secplivity.org/wp-content/uploads/2012/06/password-magnifying-glass-cyber-crime-dreamstime_xl_1809270.jpg

Hooded Hacker: <https://i.warosu.org/data/g/img/0587/92/1486223405498.jpg>

Sad: <http://coolwidewallpapers.com/uploads/389/208582-sad.jpg>

Salting: https://images-na.ssl-images-amazon.com/images/I/71VNlbjBHAL._UL1500_.jpg

Borat: http://yourbrandlive.com/assets//images/blog/great_success_brandlive.png

Giraffe: <http://www.guibingzhuche.com/data/out/273/1736834.png>

Selfish: <https://i.pinimg.com/originals/ce/54/f8/ce54f88dbdb69ed5be679e738adc1bb.jpg>

Elephant: <http://www.elephantsintherivingroom.org/backgrounds/elephant-in-room.jpg>

Dory: <https://i.ytimg.com/vi/ixVaAQVEiSM/maxresdefault.jpg>

Password Manager: https://cdn.vox-cdn.com/uploads/chorus_image/image/55851763/password_manager_stock.0.jpg

Eggs: <http://moziru.com/images/drawn-egg-faces-wallpaper-9.jpg>

Password: http://byteshunt.com/wp-content/uploads/2017/12/1513652650558-shutterstock_414545476.jpeg

Billy Mays: <http://i0.kym-cdn.com/entries/icons/original/000/000/233/billymays1.png>

Two Factor: <https://www.revesecure.com/wp-content/uploads/2017/02/Two-Factor-Authentication-Makes-Your-Password-Unusable-for-Hackers-6.jpg>

Physical Security: <https://yt3.ggpht.com/-IBn3WjnwfBY/AAAAAAAAAAAI/AAAAAAAAAAA/C1xM-oTt7os/s900-c-k-no/photo.jpg>

Padlock: https://passwd.org/sites/default/files/styles/passwd_fullnode/public/chain-padlock-security-fail.jpg?itok=IM2DDncW

Suspicious: <http://i0.kym-cdn.com/entries/icons/original/000/006/026/NOTSUREIF.jpg>

Lock Computer: <http://i.imgur.com/RIN87.jpg>

Piggybacking: http://cdn2.itpro.co.uk/sites/itpro/files/styles/article_main_wide_image/public/images/dir_142/it_photo_71118.jpg?itok=ImjU-RuU

Propped Door: http://www.barkinganddagenhampost.co.uk/polopoly_fs/1.4529708!/image/image.jpg_gen/derivatives/landscape_630/image.jpg

Laptop Stolen?: <https://motherboard-images.vice.com/content-images/contentimage/no-id/1423588697646224.jpg>

Fry Panic: <https://alice961994.files.wordpress.com/2014/11/futurama-fry-stress.png>

Hack the Planet: <https://i.imgur.com/xjtVvON.jpg>

PII: <https://i.pinimg.com/originals/9f/36/da/9f36da538d12b2387825b0b3a3ac617f.jpg>

Personal Information: http://mrsc.org/getmedia/a0ba5128-d6fb-4008-bf30-893a43abf131/personal_info_618x353.jpg.aspx?width=618&height=353&ext=.jpg

Company Data: https://vignette.wikia.nocookie.net/memoryalpha/images/b/bd/Data_phone.jpg/revision/latest?cb=20141214221139&path-prefix=en

Handling Data: <http://www.trekologic.com/wp-content/uploads/2015/09/02-touching-data.jpg>

Compliance: <https://assets1.ignimgs.com/vid-thumbnails/user/2012/11/28/naviTNT280w.jpg>

GDPR: <https://zdnet4.cbsistatic.com/hub/i/r/2017/11/15/be5d1ea8-0ad7-45e6-8588-e2c7eafecd79/resize/770xauto/1f9ea28914a62218eb8a5d8c5c92a3a7/istock-gdpr-concept-image.jpg>

Would You Like To Know More?: <https://static1.squarespace.com/static/574f0b9a37013b939ab0b866/t/5936b0e717bffc7a44df2ca0/1496756488470/>

Morbo: https://orig00.deviantart.net/baf4/f/2009/364/2/f/morbo_by_kornykattos.png