JOSHUA LONG

Joshua Long (@theJoshMeister) is the Chief Security Analyst at Intego. He is a renowned security researcher and writer, having battled spam, phishing scams, malicious sites, and malware for more than 20 years.

Josh has a master's degree in IT concentrating in Internet Security, and has taken doctorate-level coursework in Business Administration and Computer & Information Security.

Apple has publicly acknowledged Josh for discovering an Apple ID password validation vulnerability. Josh's other research has been featured by many fine publications such as CNET, CBS News, ZDNet UK, Lifehacker, CIO, Macworld, The Register, Naked Security, The Mac Security Blog, and MacTech Magazine.

Think different.

HACKING YOUR OWN THINKING

DEVELOPING A SECURITY MINDSET

*with a few notes added to the slides for clarity

DEVELOPING A SECURITY MINDSET

- Security pervades everything
- Security is everyone's problem
- How to retrain your brain
- Let's practice! (Game)
- How to train others
- Resources

SECURITY PERVADES EVERYTHING

BREACHES HAPPEN… ALL. THE. TIME.

- Target, Equifax, countless hospitals, schools, agencies, etc. …
- Organizations big and small are breached *every single day*
- Personal accounts compromised–identities stolen–*every day*
- Often it's as a result of someone *not* thinking like an attacker
- No matter who you are, security (or lack thereof) affects you
- Even if you don't care, there are reasons you should

SECURITY IS EVERYONE'S PROBLEM

> "WHY WOULD ANYONE WANT TO HACK ME? I'M NOT THAT INTERESTING."

(It doesn't matter if you're interesting.)

a typical user

*Consider credential stuffing attacks. Even a Facebook account with very few friends can be used by an attacker to defraud those friends with a "stranded overseas and need you to wire me money" scam

> “PRETEND INFERIORITY AND ENCOURAGE [YOUR ENEMY'S] ARROGANCE.”

Sun Tzu

(Don't be arrogant.)

SECURITY IS EVERYONE'S PROBLEM

*Apple told people for years that Macs are more secure than Windows PCs.
But to mistakenly assume Apple devices are "safe" is arrogance, which makes us more vulnerable.

HOW TO RETRAIN YOUR BRAIN

> “THE GENERAL WHO WINS THE BATTLE MAKES MANY CALCULATIONS…BEFORE THE BATTLE IS FOUGHT.
> “THE GENERAL WHO LOSES MAKES BUT FEW CALCULATIONS BEFOREHAND.”

(Think how your adversary thinks.)

Sun Tzu

SOCIAL ENGINEERING – BEWARE OF…

- Important-looking e-mails: “CEO fraud,” phishing, etc.
- Private messages
- Online “personality” quizzes / “Your *x* name”
- Cold calls
- Building “tailgaters”
- Visitors (even “in uniform”)
- “Can you help me?”

*e.g. your Star Trek name, or your My Little Pony name

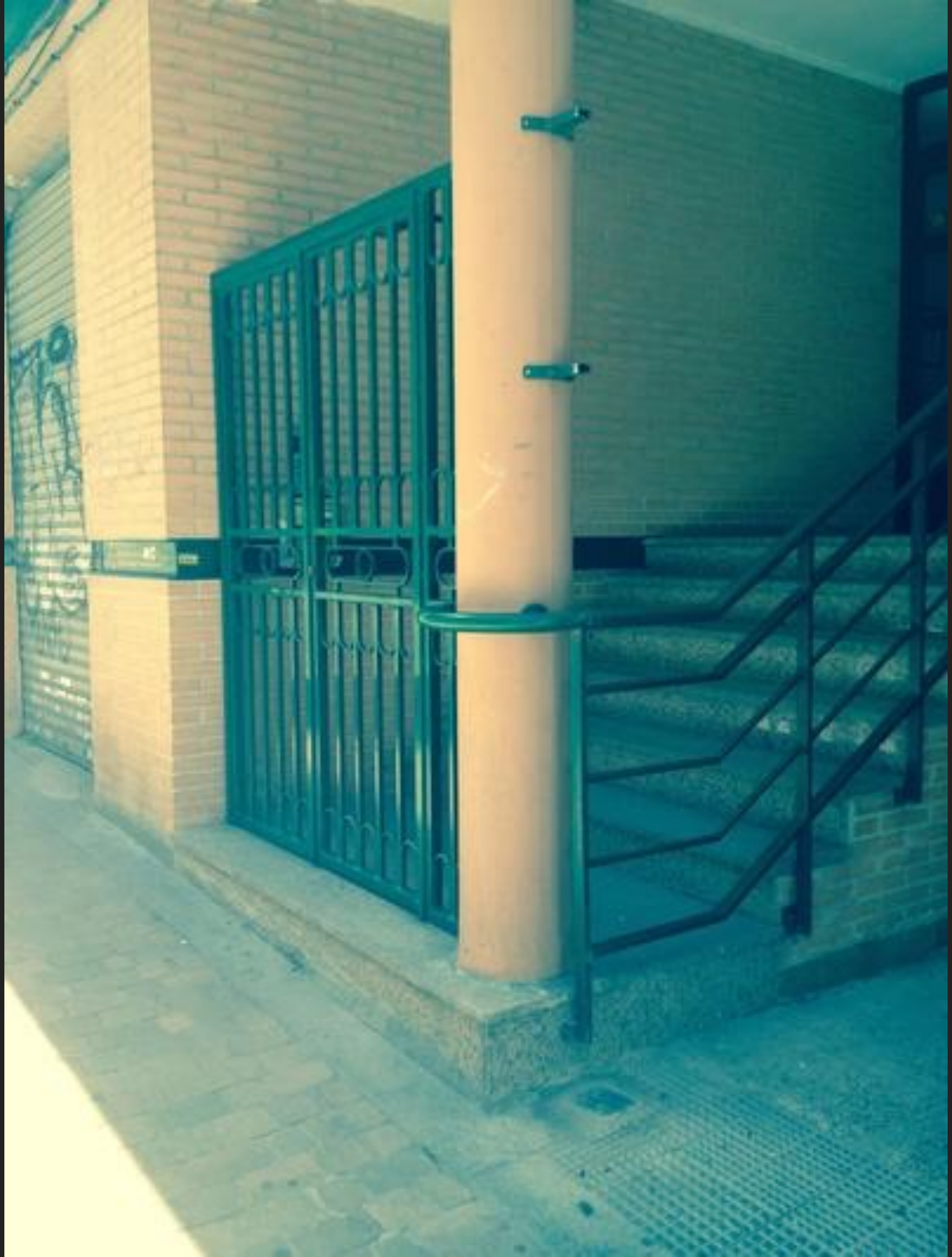
*…but there's really a lot more to it. Force yourself to look at everything from a different perspective.
In every situation and circumstance, consider your surroundings.
Then ask yourself, "If I were a bad guy, how could I use this to my advantage?"

GAME:
WHAT'S WRONG WITH THIS PICTURE?

GAME:

*AKA WHAT WOULD AN ATTACKER DO?

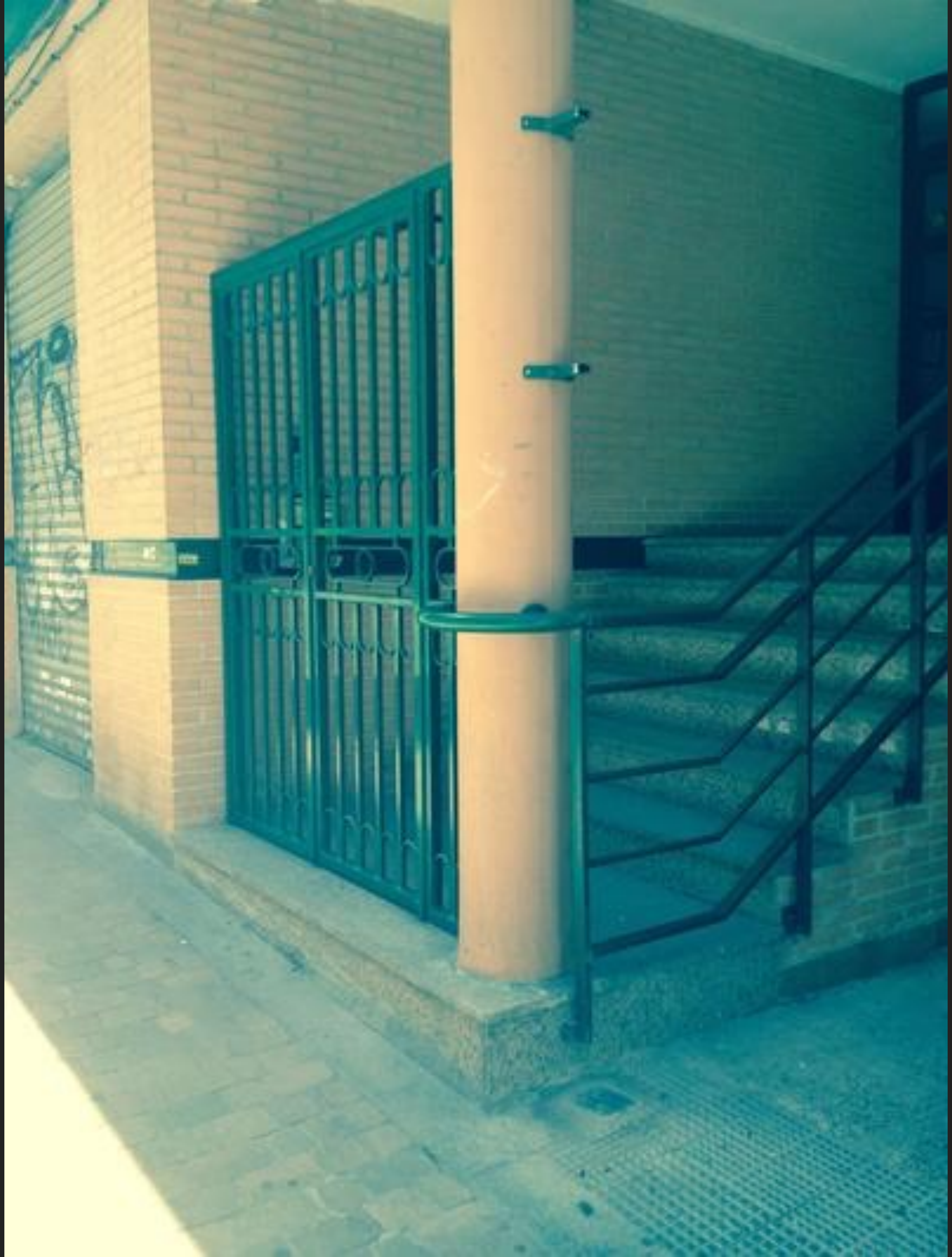
WHAT'S WRONG WITH THIS PICTURE?



intego

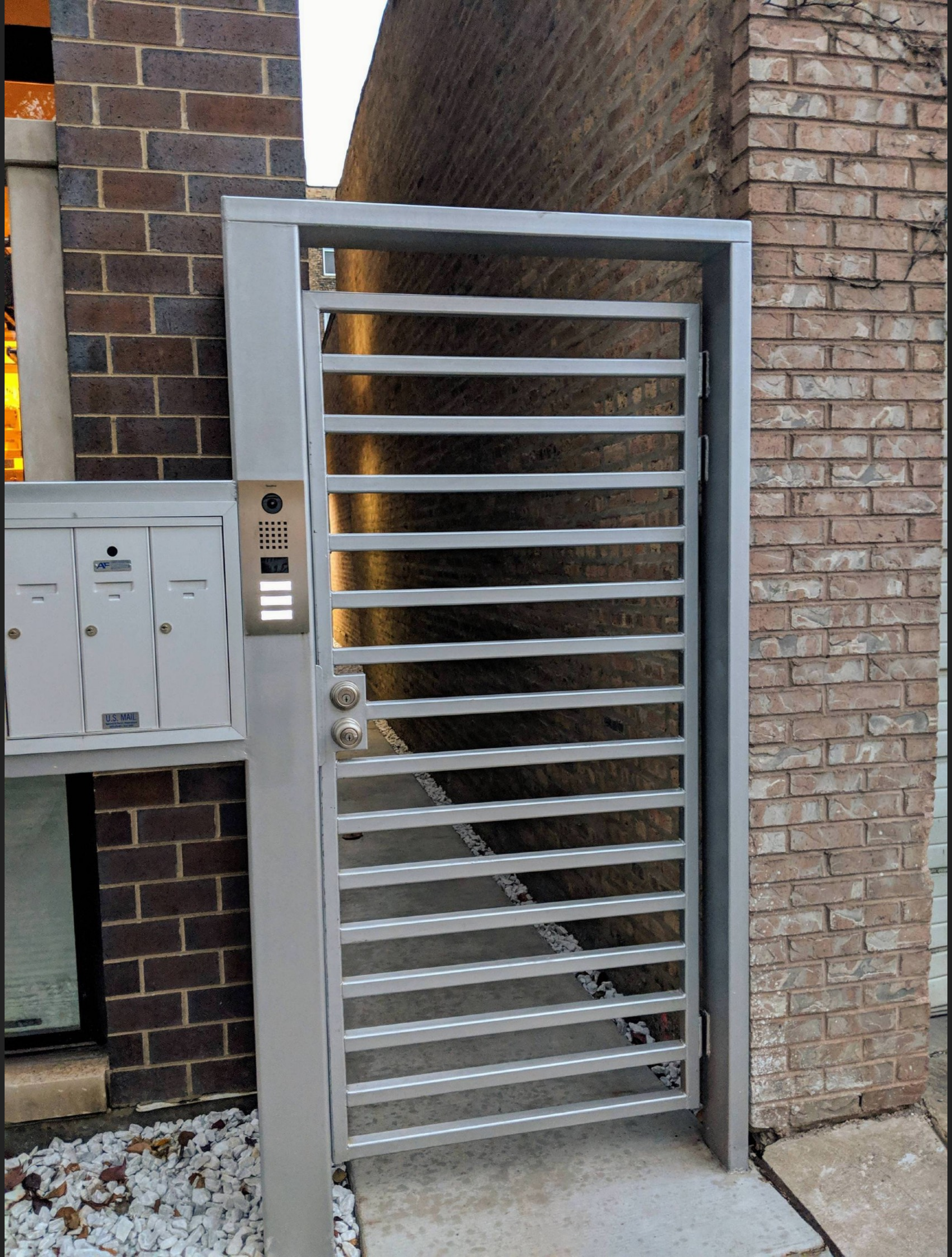
MACTECH CONFERENCE 2019

WHAT'S WRONG WITH THIS PICTURE?

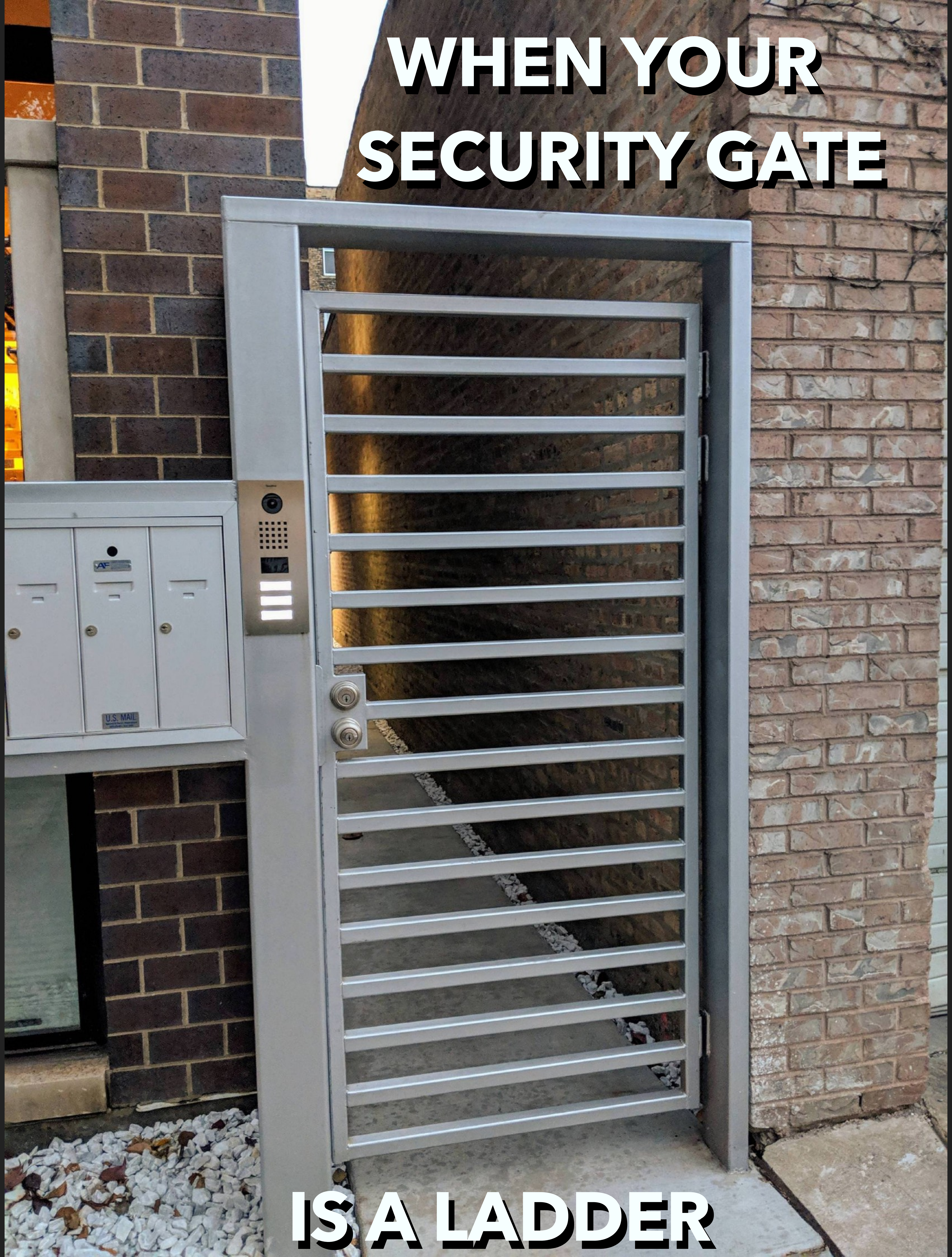


*How effective is a big, locked gate if you can just step over the railing right next to it?

WHAT'S WRONG WITH THIS PICTURE?



WHAT'S WRONG WITH THIS PICTURE?

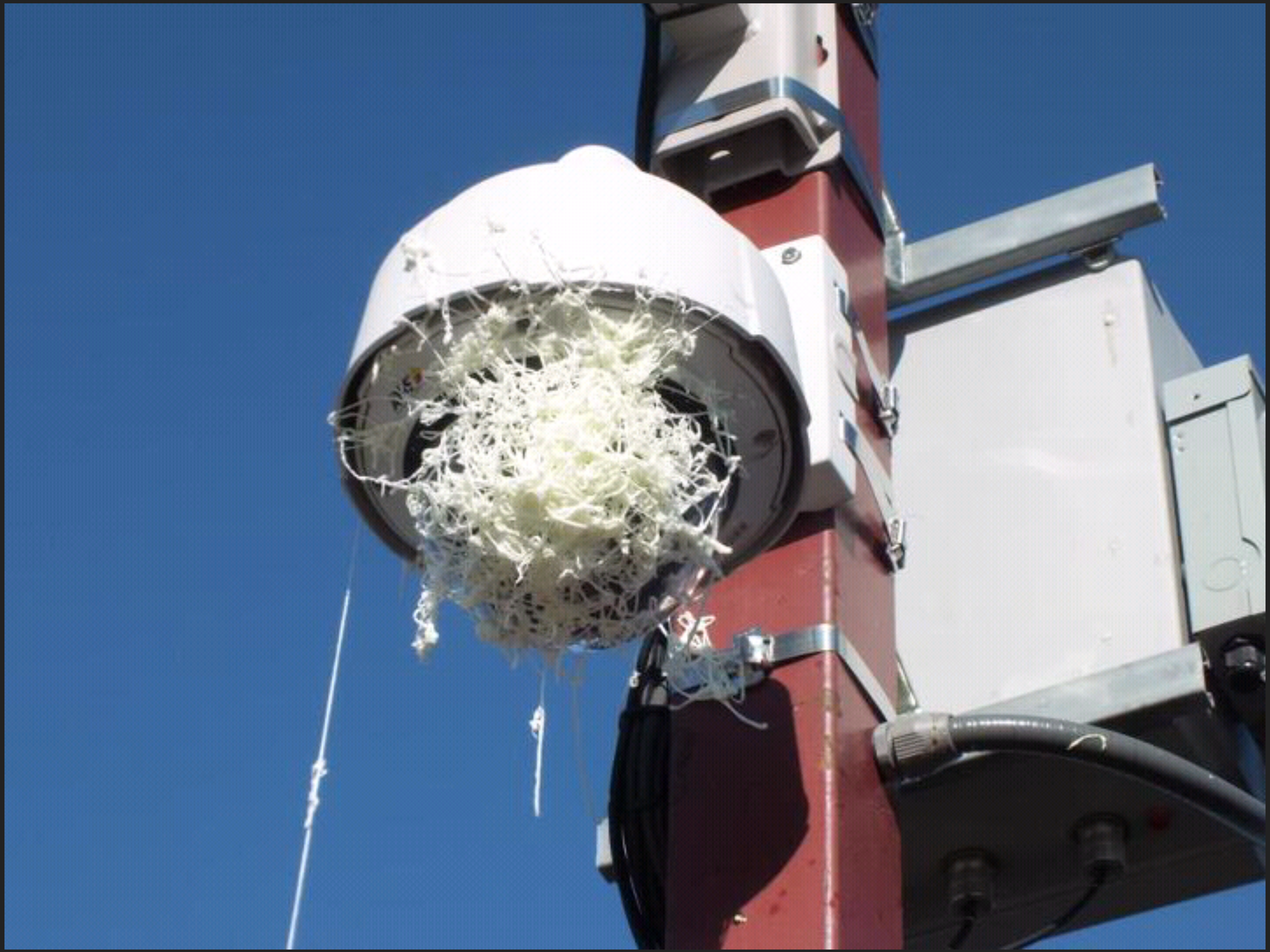


intego

WHAT'S WRONG WITH THIS PICTURE?

*This is advertised as a "vandal-proof" camera. They mean, "not easily breakable with blunt force." If you were a bad guy, what else could you do about a security camera?

WHAT'S WRONG WITH THIS PICTURE?



WHAT'S WRONG WITH THIS PICTURE?

SURVEILLANCE CAMERA... $900
CAN OF SILLY STRING... $2
DEFEATING THE SYSTEM... PRICELESS.

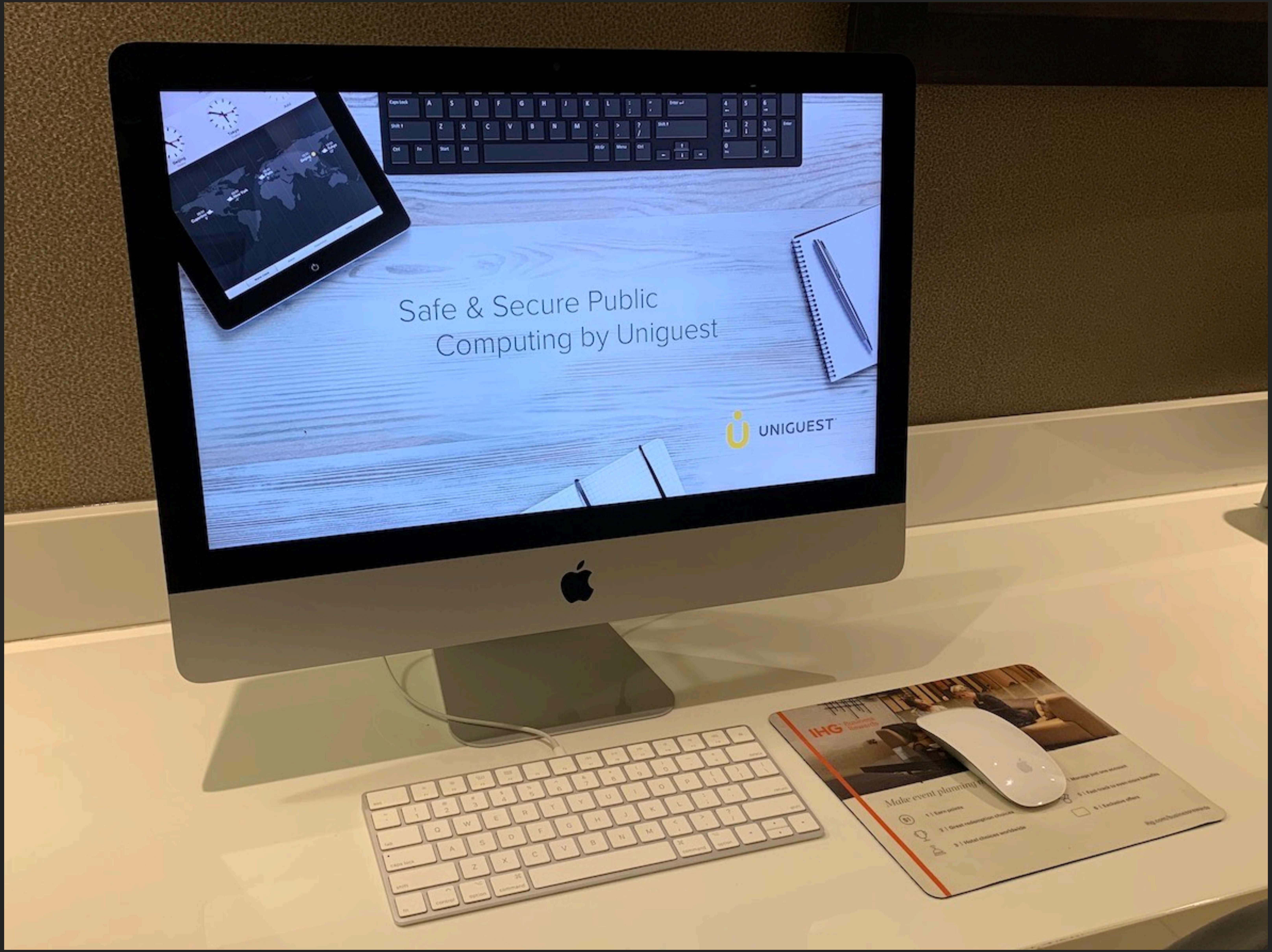
WHAT'S WRONG WITH THIS PICTURE?

*Google Home, Apple HomePod, Amazon Echo devices

WHAT'S WRONG WITH THIS PICTURE?

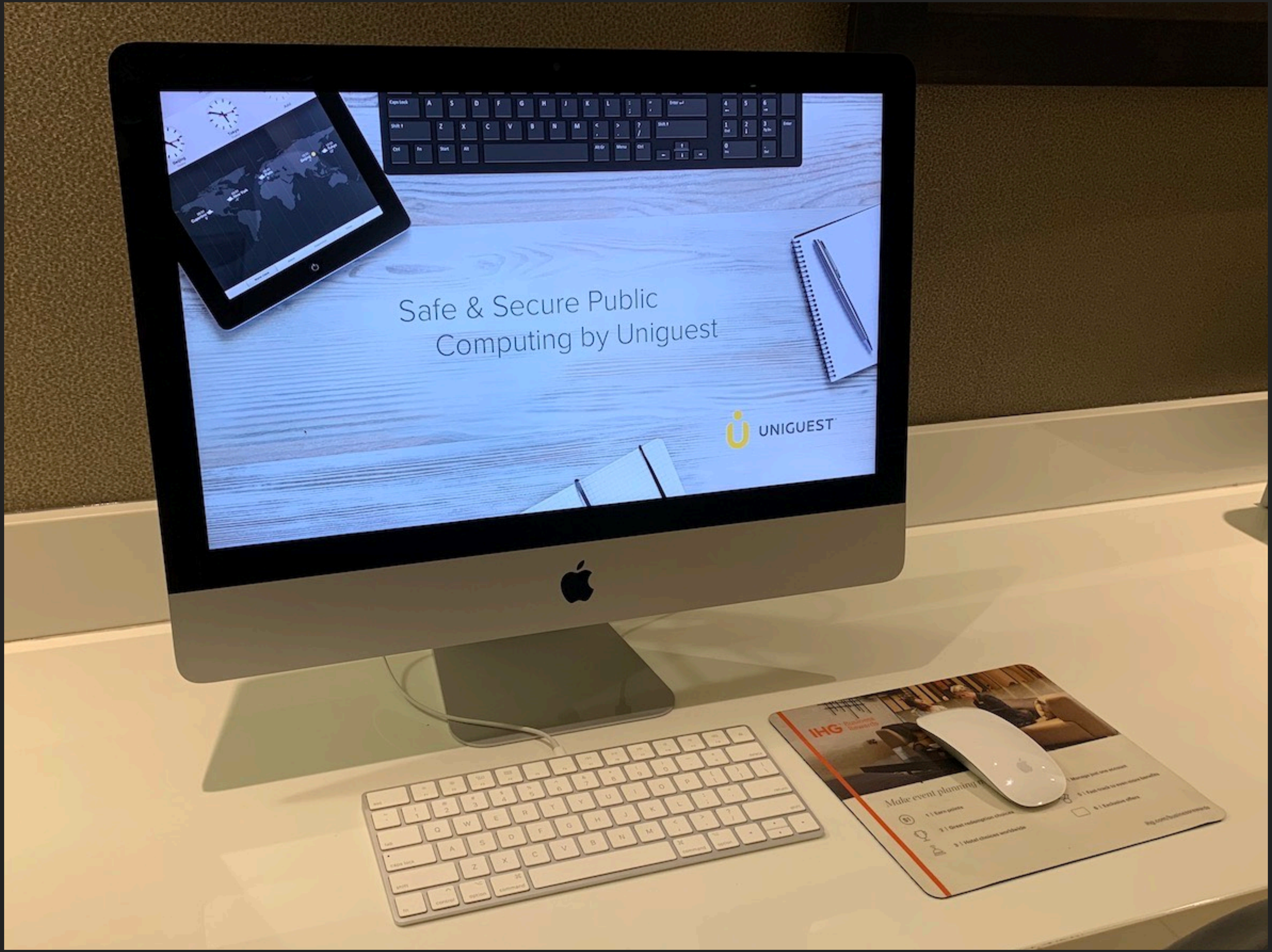
*Some ideas: DolphinAttack to turn off someone's lights or start playing creepy music unexpectedly

WHAT'S WRONG WITH THIS PICTURE?



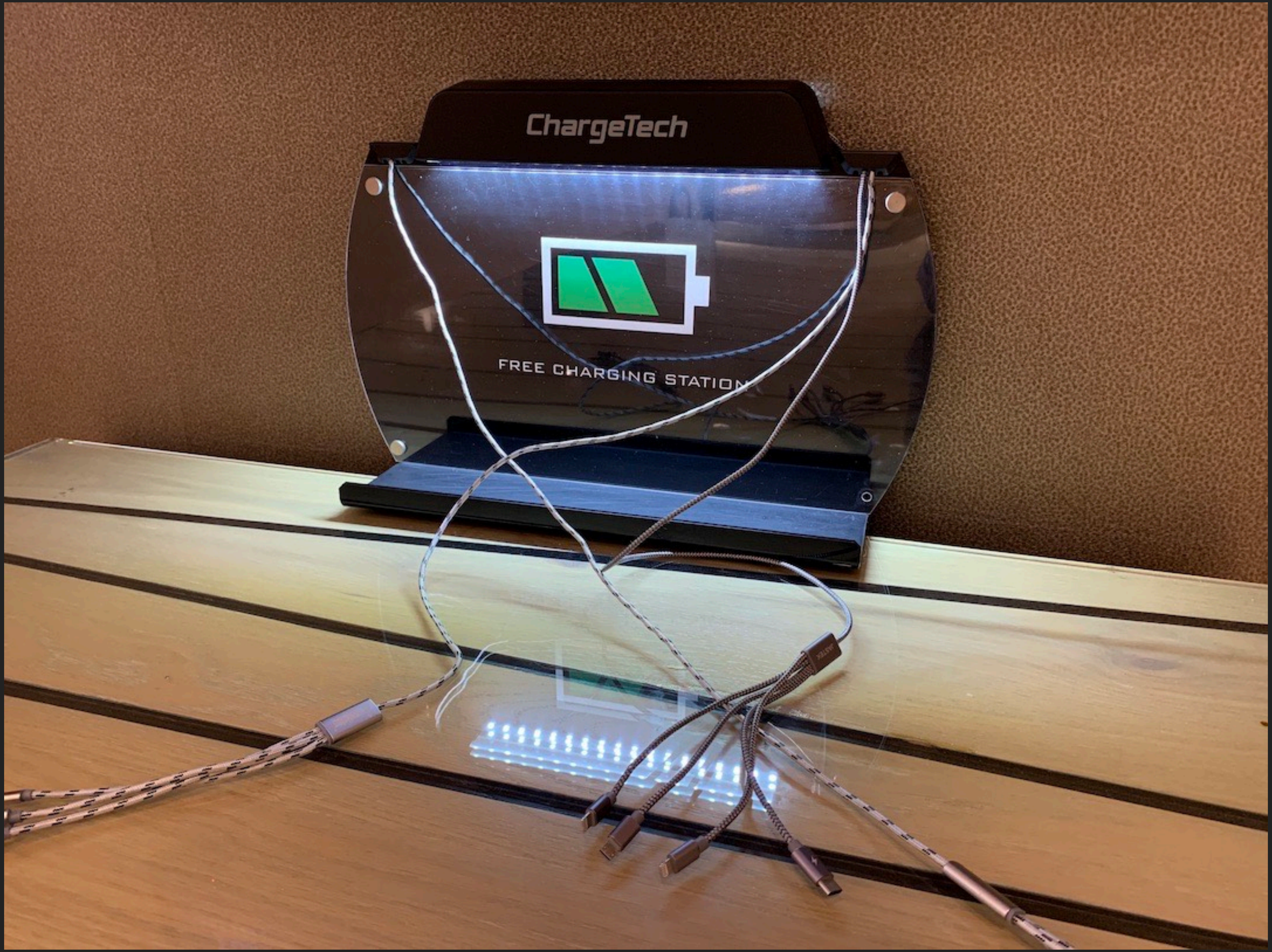
*A public computer kiosk here at the MacTech Conference hotel

WHAT'S WRONG WITH THIS PICTURE?



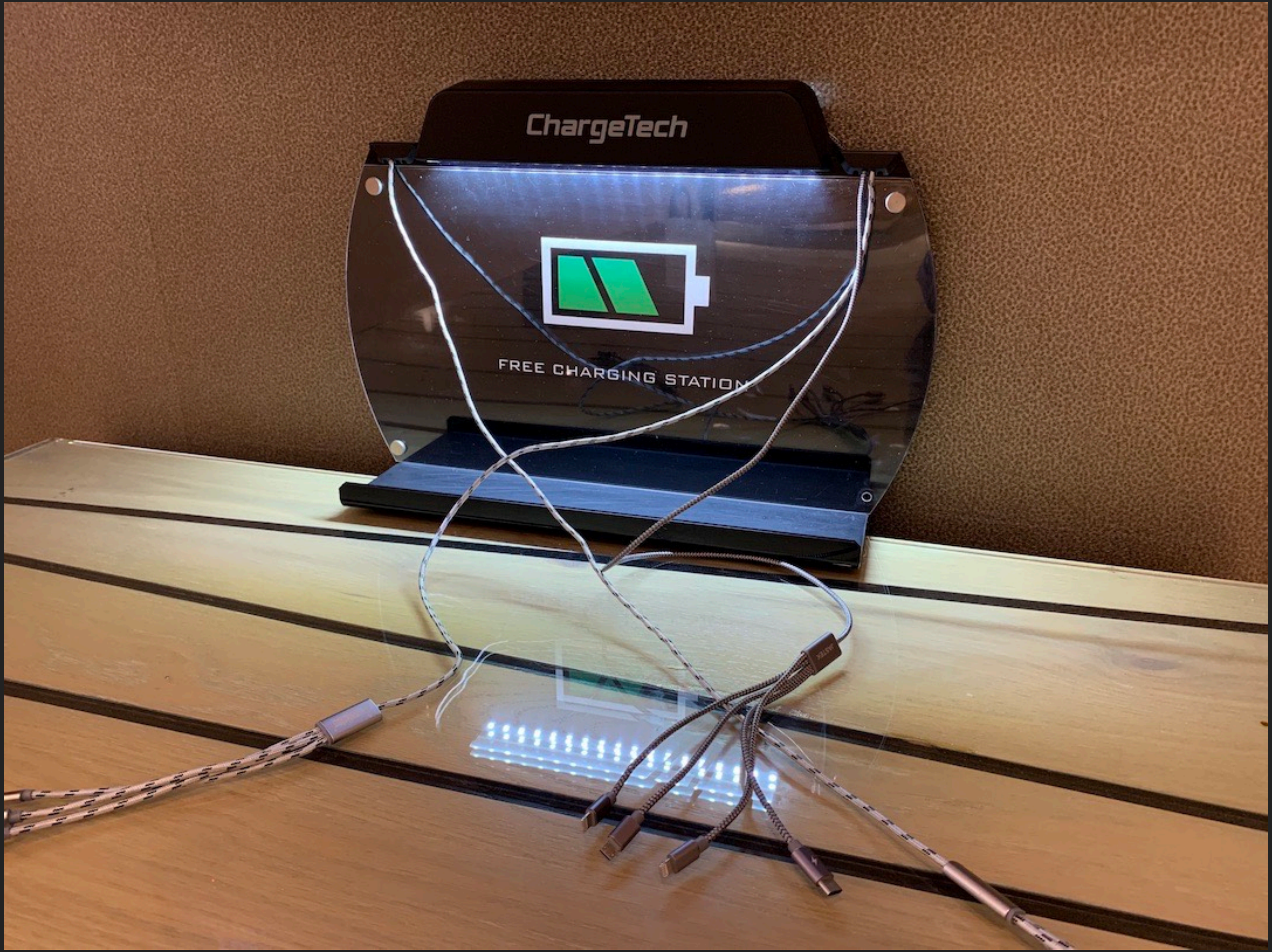
*A guest could have installed a software/hardware keylogger; avoid logging into accounts

WHAT'S WRONG WITH THIS PICTURE?



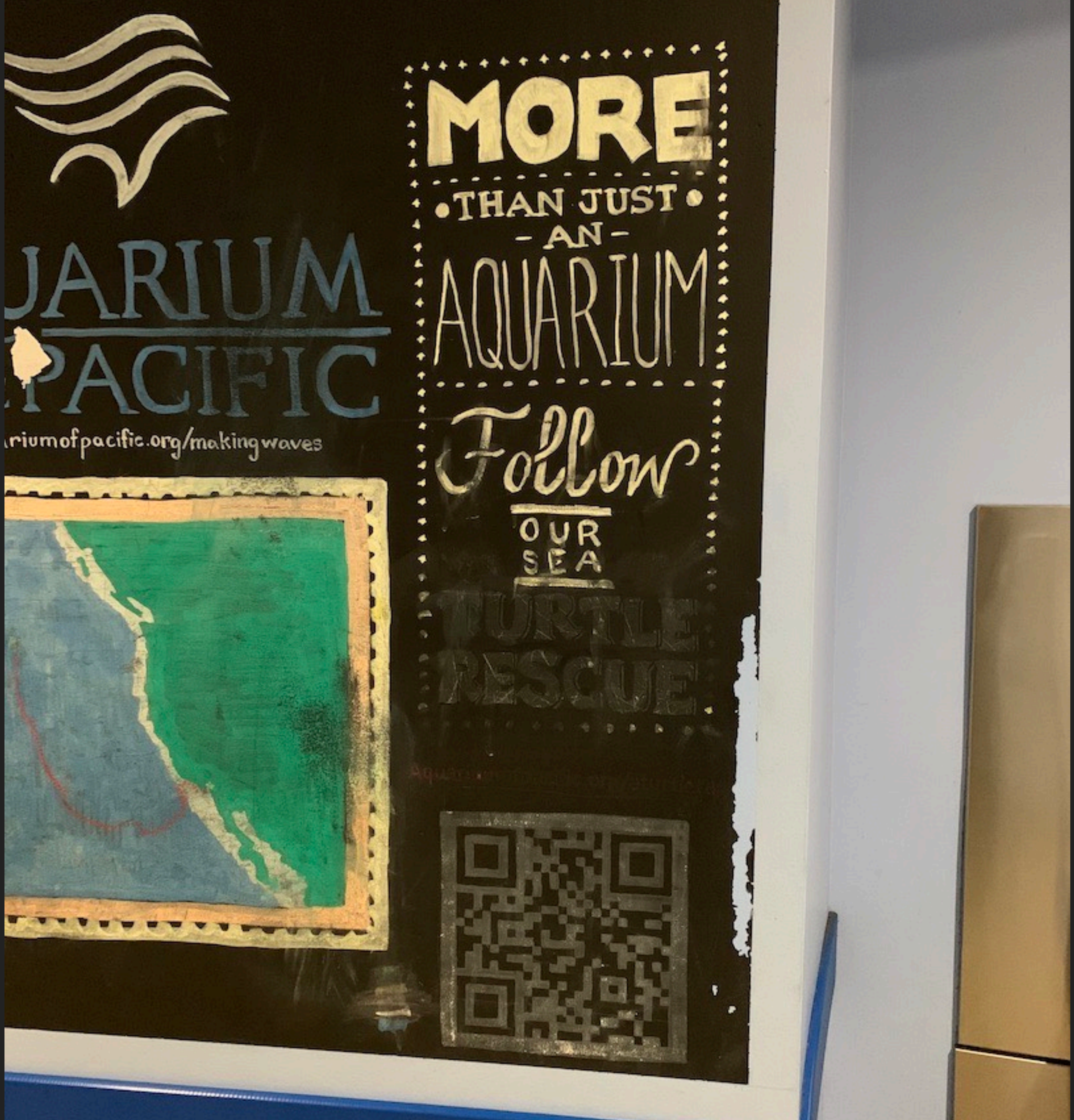
*A charging station here at the MacTech Conference hotel

WHAT'S WRONG WITH THIS PICTURE?



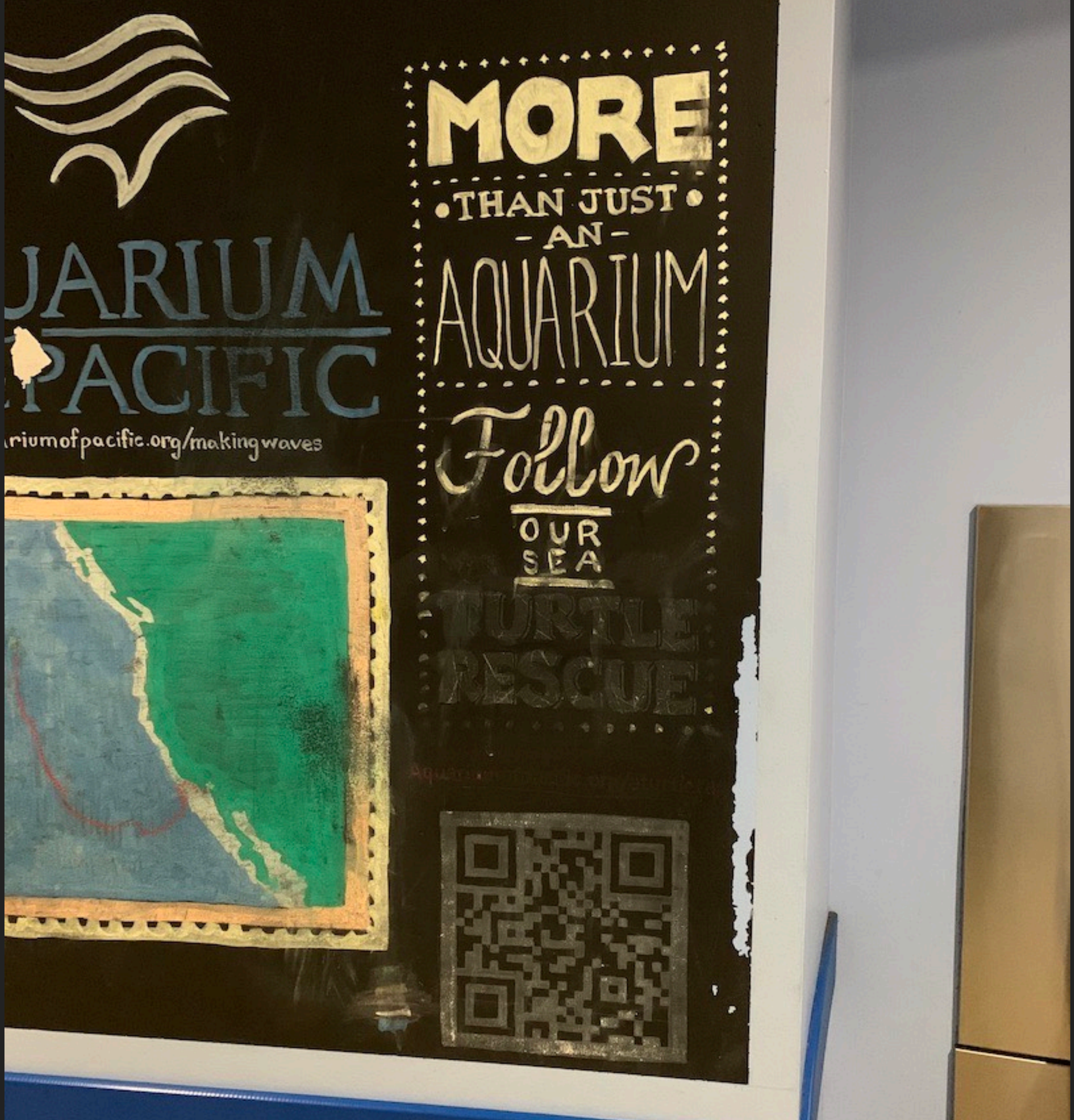
*There could be a hidden computer on the other end; look up "trustjacking"

WHAT'S WRONG WITH THIS PICTURE?



*A public QR code seen last night at Aquarium of the Pacific

WHAT'S WRONG WITH THIS PICTURE?



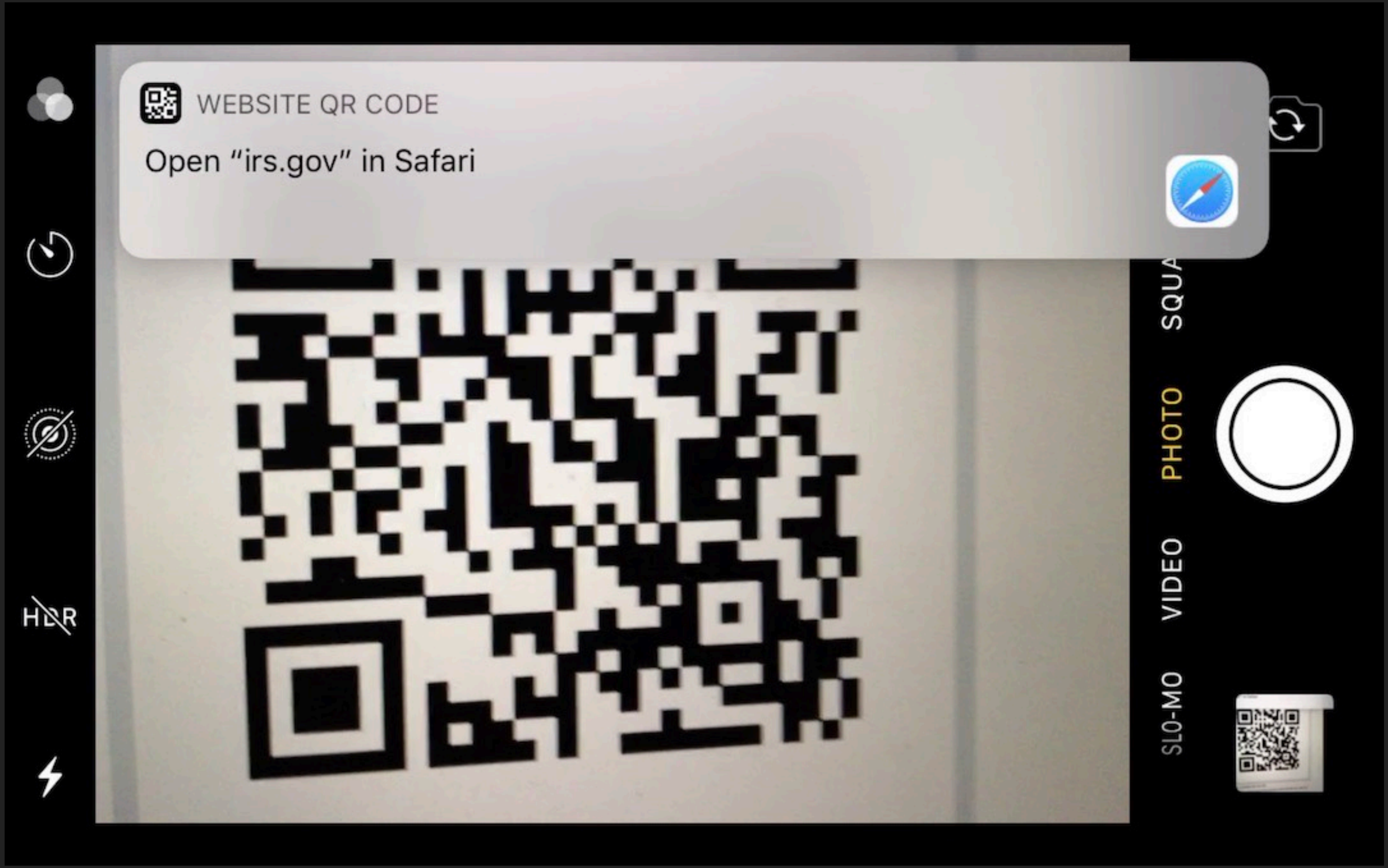
*Nothing particularly wrong here (it would be difficult for someone to paint a malicious QR code over this large, hand-painted one), but don't become desensitized to scanning QR codes in public.

There have been "pay with Bitcoin" sign scams in China and elsewhere.

WHAT'S WRONG WITH THIS PICTURE?

*Sometimes someone with malicious intent may put a QR code sticker over the top of legitimate QR codes in public places.

WHAT'S WRONG WITH THIS PICTURE?



WEBSITE QR CODE

Open "irs.gov" in Safari

*There was a flaw in the built-in QR code reader in iOS 11's Camera app that enabled URL spoofing…

WHAT'S WRONG WITH THIS PICTURE?

*…scan this to see my tweet with a fun video about that (trust me)

WHAT'S WRONG WITH THIS PICTURE?

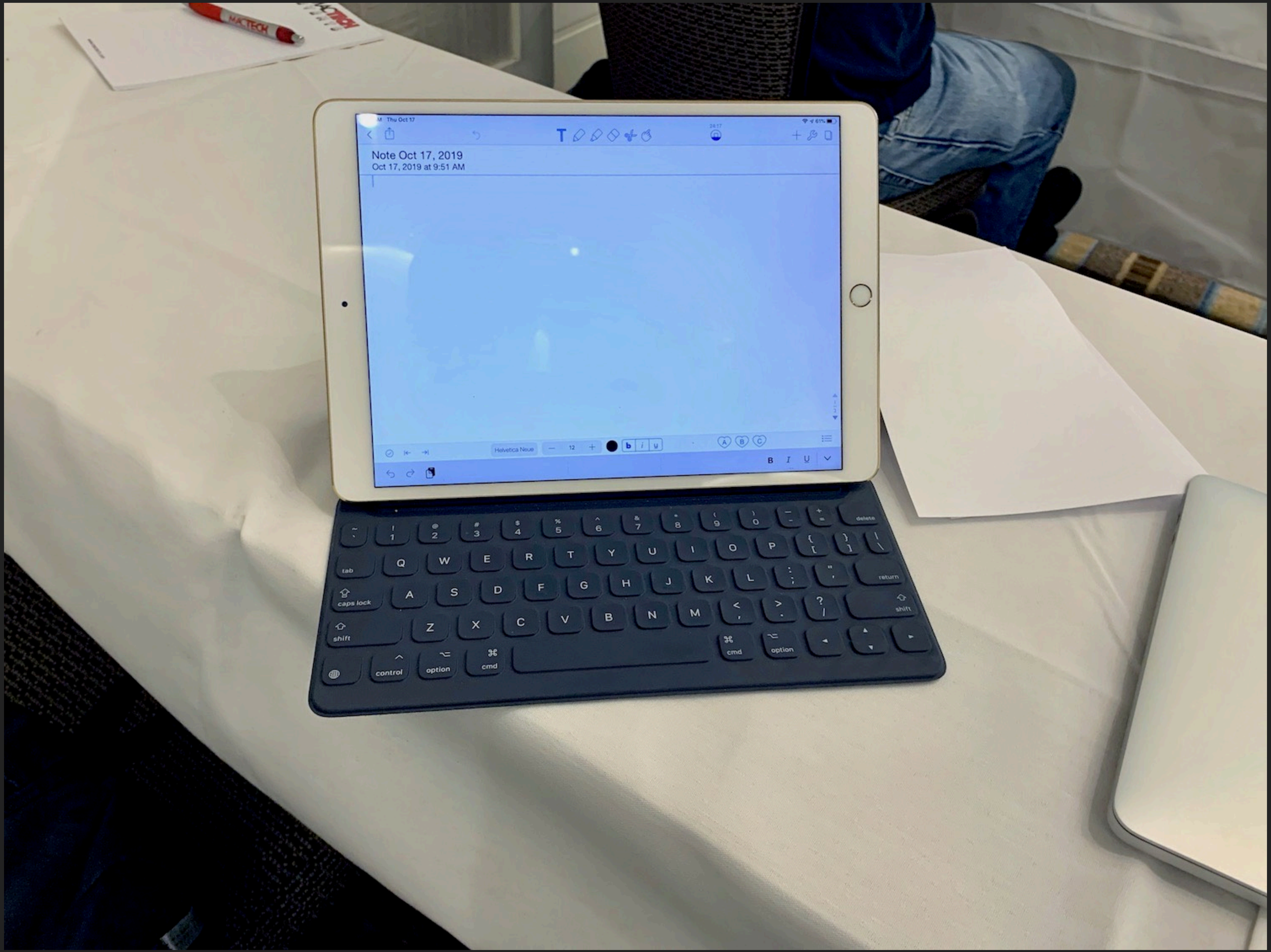
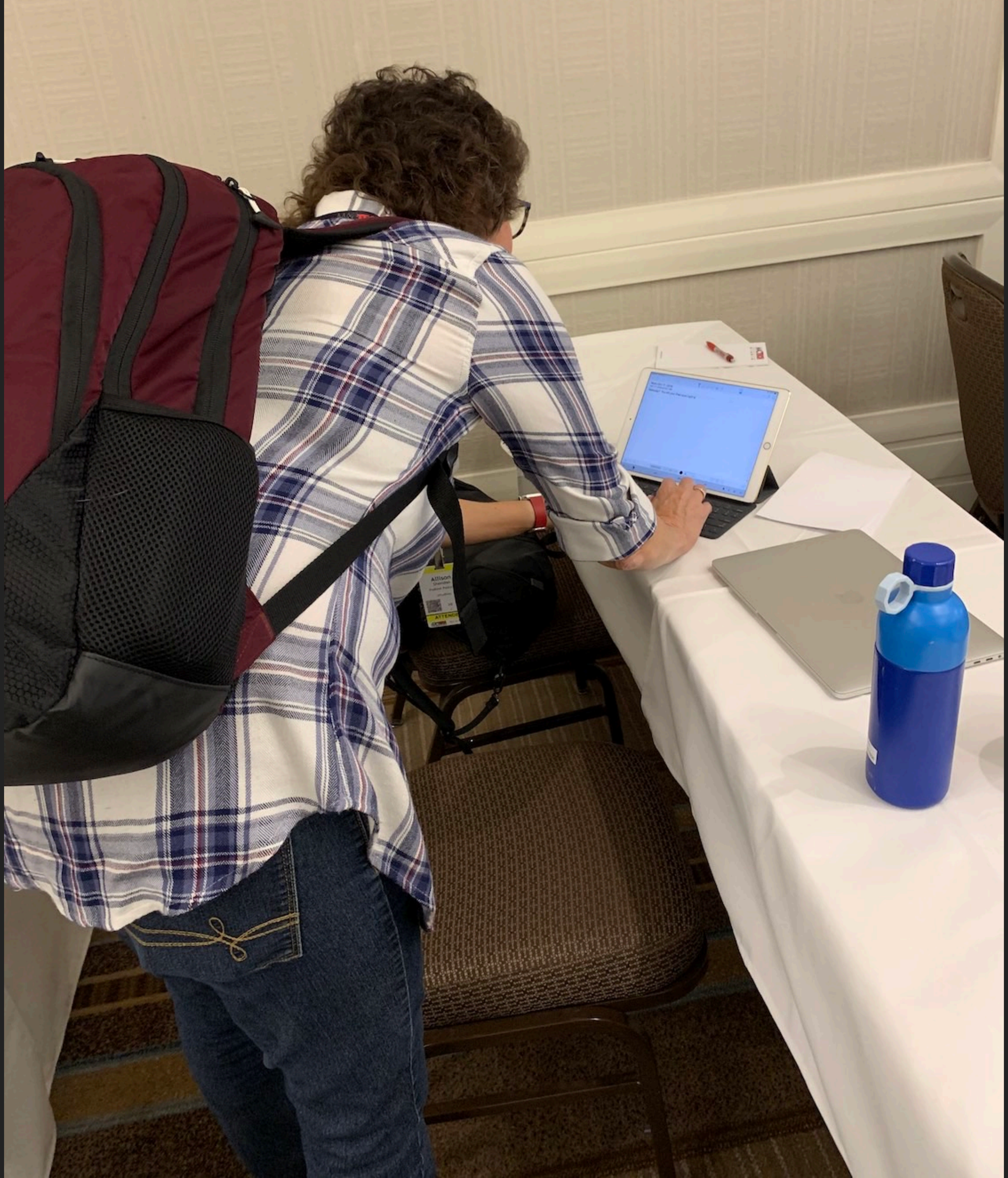


*Photo taken here at MacTech Conference this morning; someone left their device on and walked away

WHAT'S WRONG WITH THIS PICTURE?



*Don't leave your device unlocked and unsupervised! You never know who might see it and what they might do.

WHAT'S WRONG WITH THIS PICTURE?

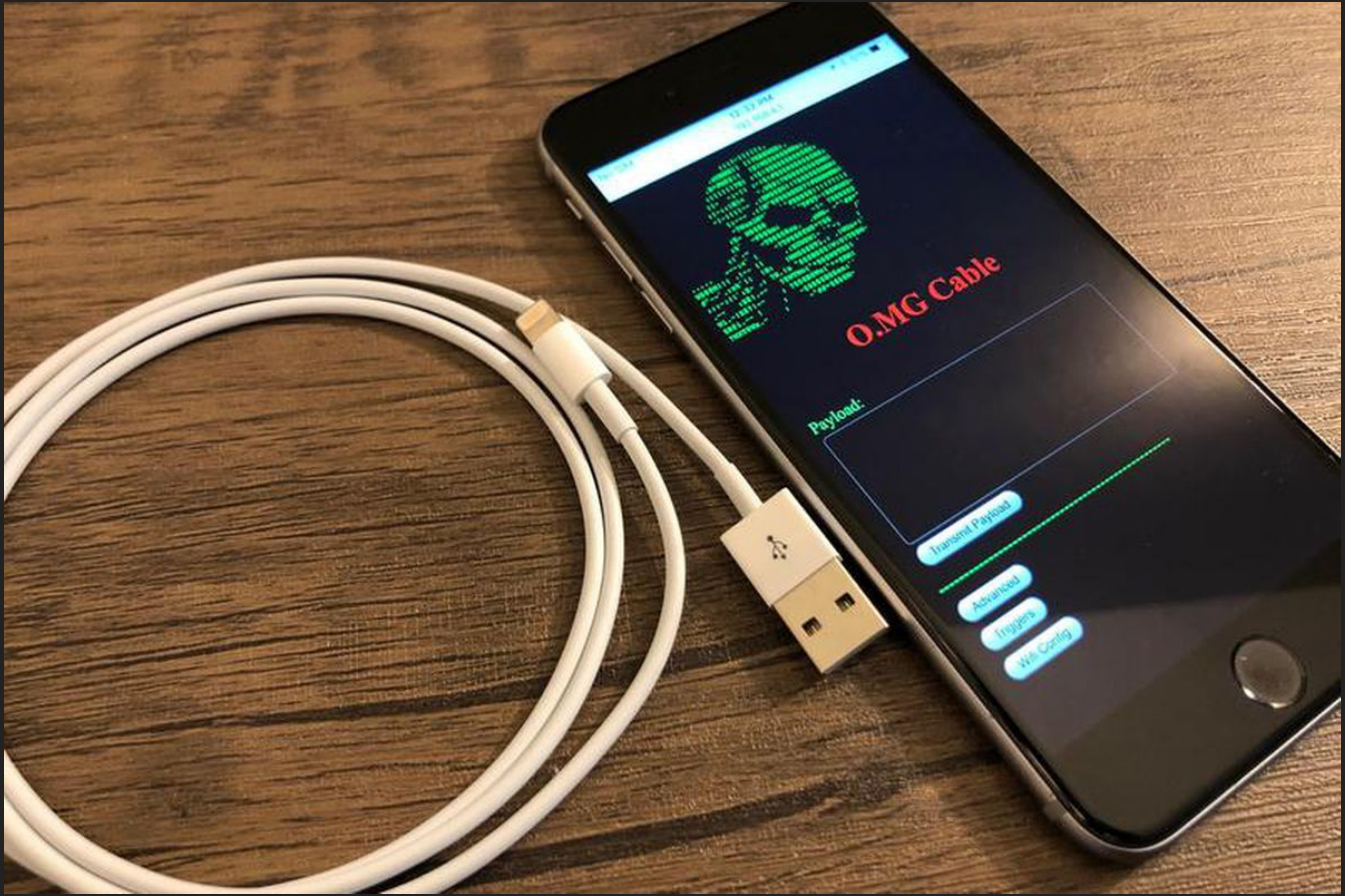
WHAT'S WRONG WITH THIS PICTURE?

*Could contain malware. Could be a "BadUSB" device (with nefarious additional capabilities, like running commands). Could be a "USB killer" device (designed to cause physical, electrical damage).

WHAT'S WRONG WITH THIS PICTURE?

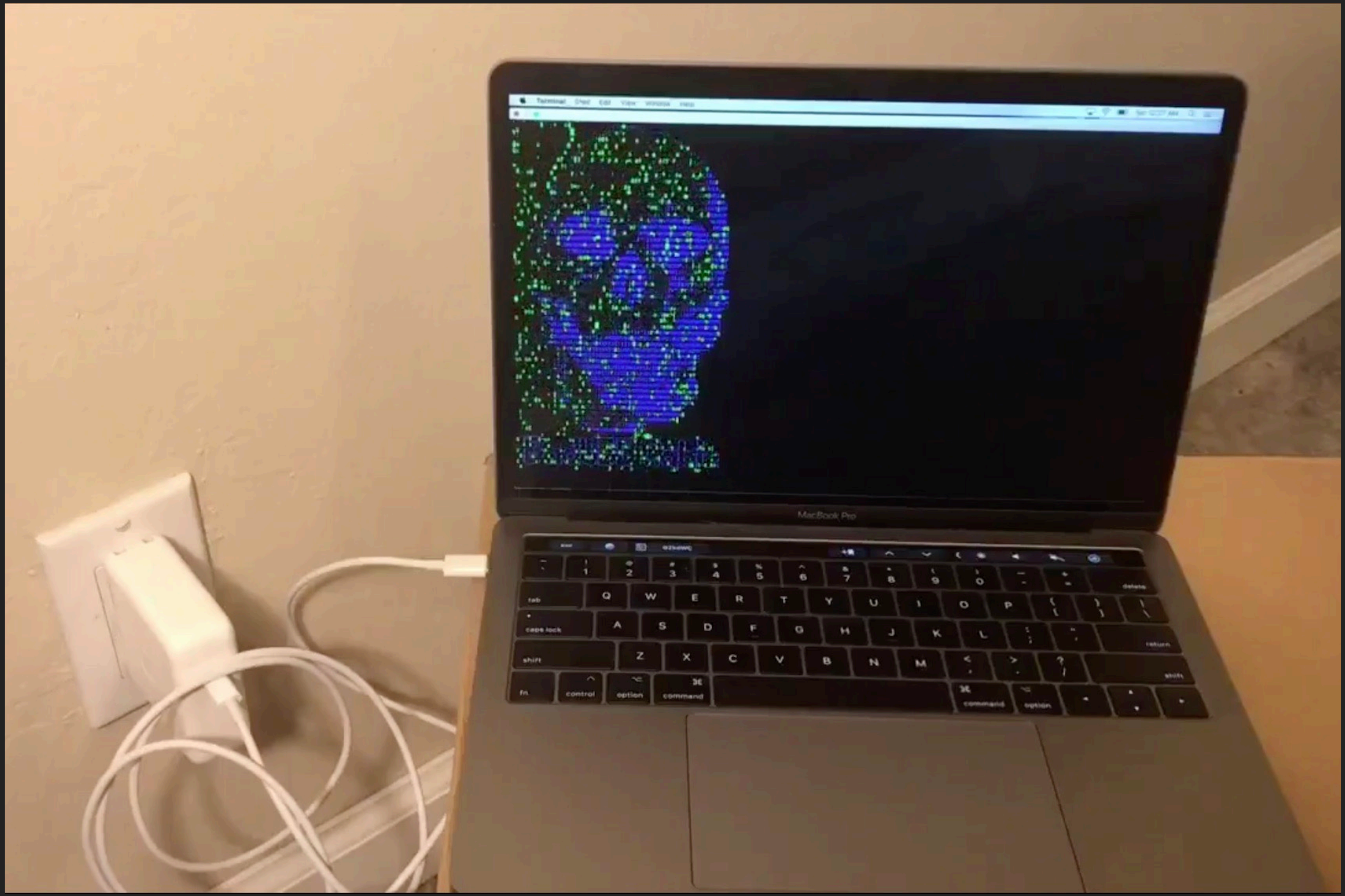
*Scenario: Someone offers to lend you their Lightning, Thunderbolt, or USB-C cable so you can charge your device

WHAT'S WRONG WITH THIS PICTURE?



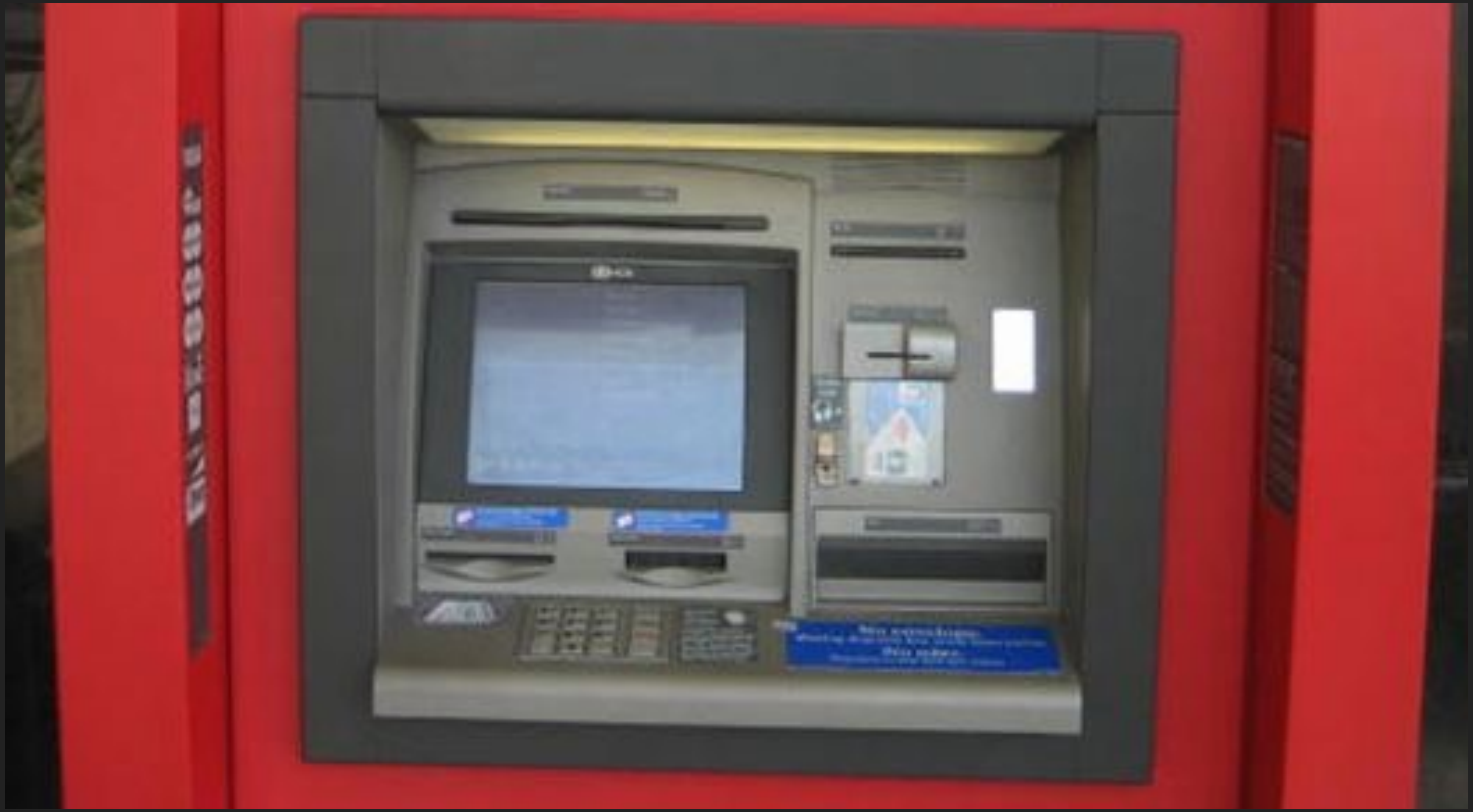
*It might be an O.MG cable (or something like it); charging and data transfer like a real Apple cable, but also a wireless hotspot through which an attacker can send commands.

WHAT'S WRONG WITH THIS PICTURE?

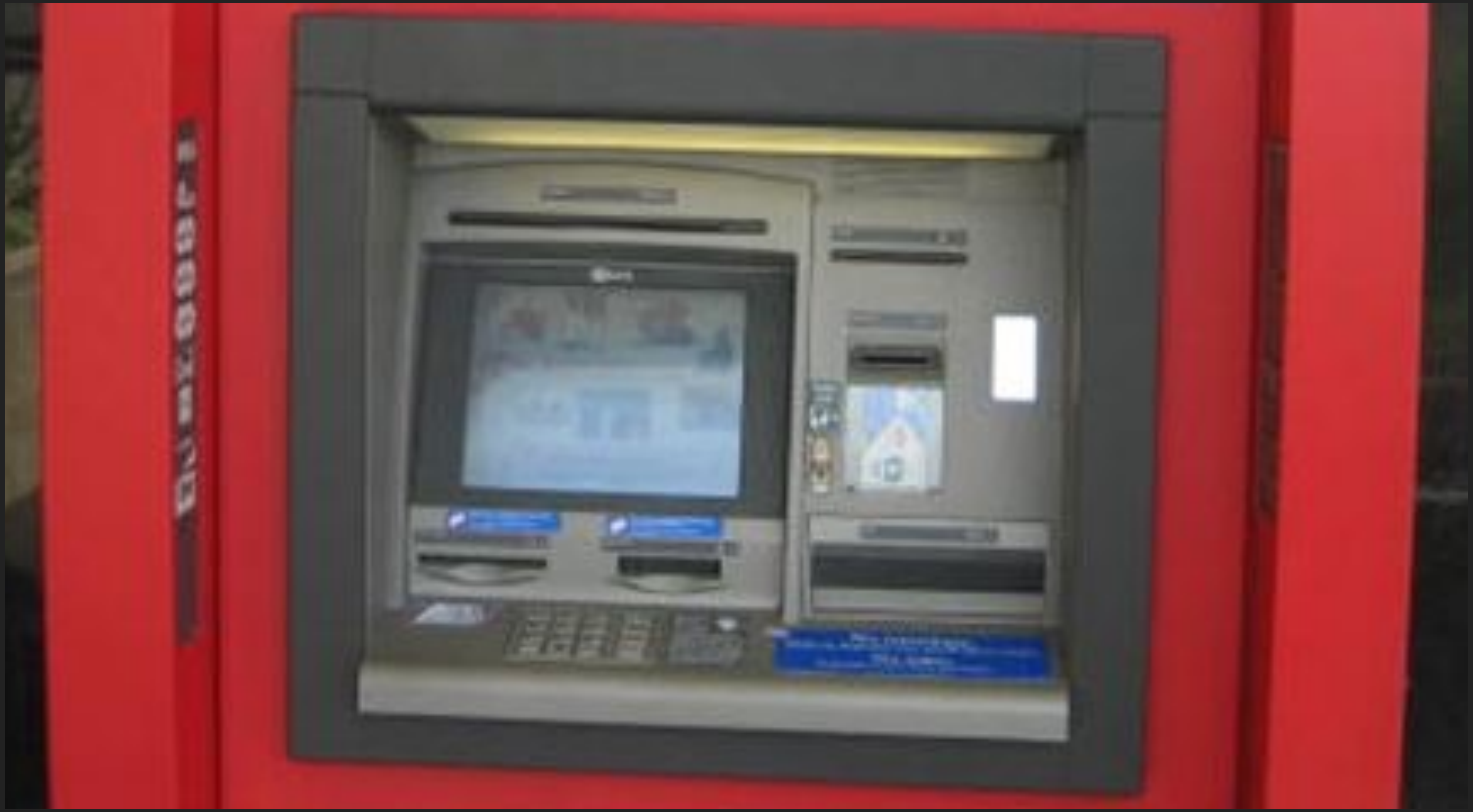


*The creator of the O.MG Lightning cable
has also made a proof-of-concept USB-C cable.

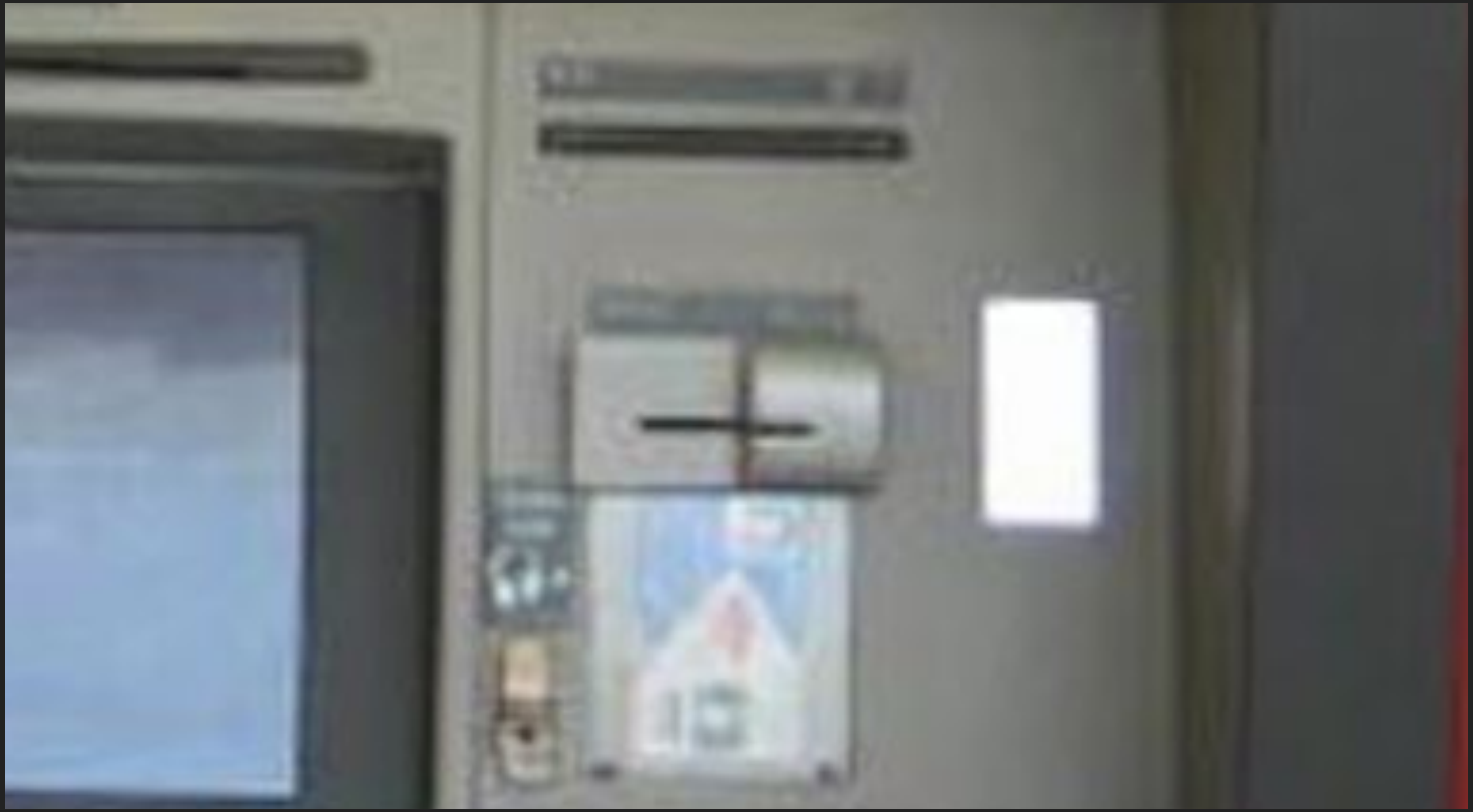
WHAT'S WRONG WITH THIS PICTURE?



WHAT'S WRONG WITH THIS PICTURE?



WHAT'S WRONG WITH THIS PICTURE?



*ATM with skimmer

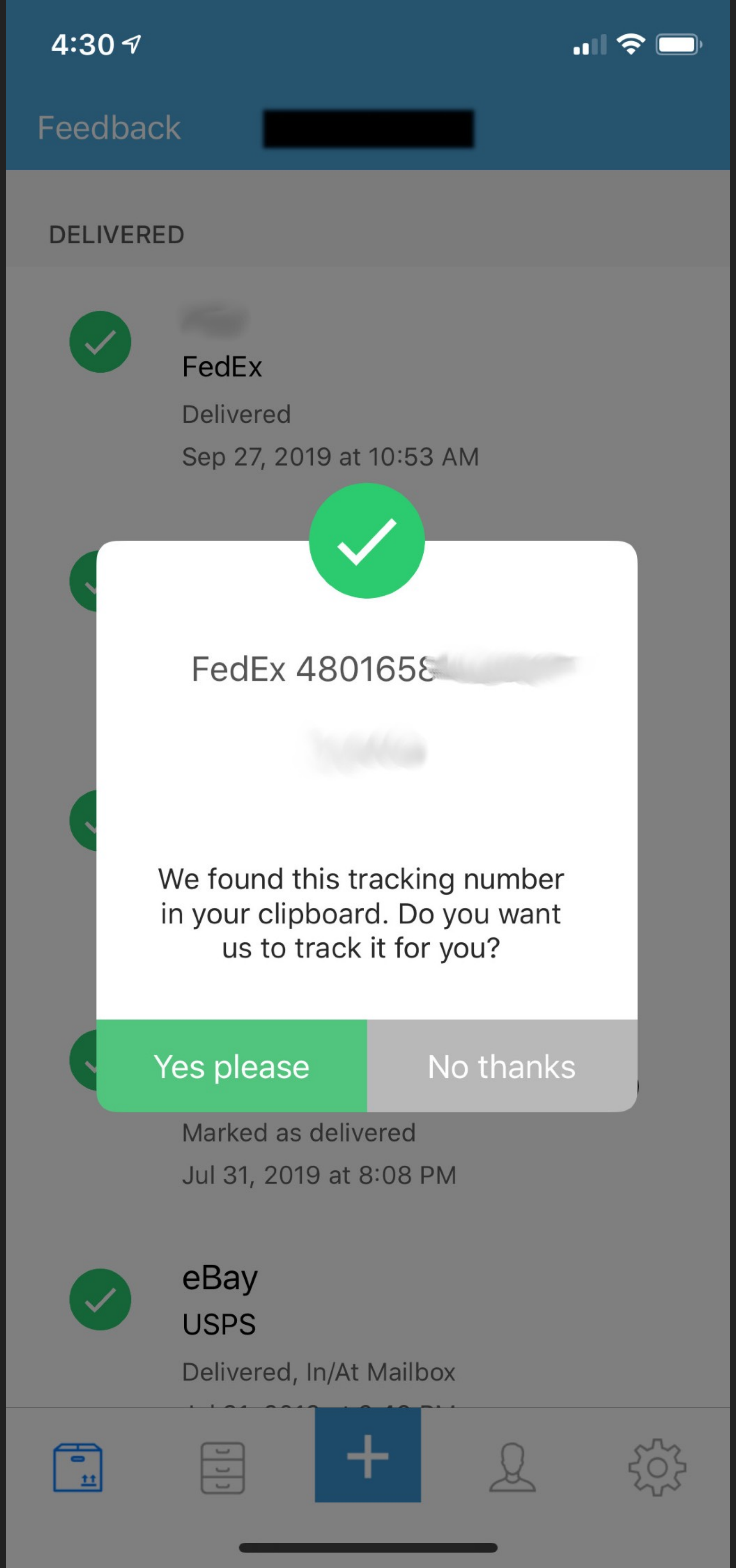
intego

MACTECH CONFERENCE 2019

WHAT'S WRONG WITH THIS PICTURE?

*ATM without skimmer

WHAT'S WRONG WITH THIS PICTURE?



DELIVERED

FedEx

Delivered

Sep 27, 2019 at 10:53 AM

FedEx 4801658

We found this tracking number in your clipboard. Do you want us to track it for you?

Marked as delivered

Jul 31, 2019 at 8:08 PM

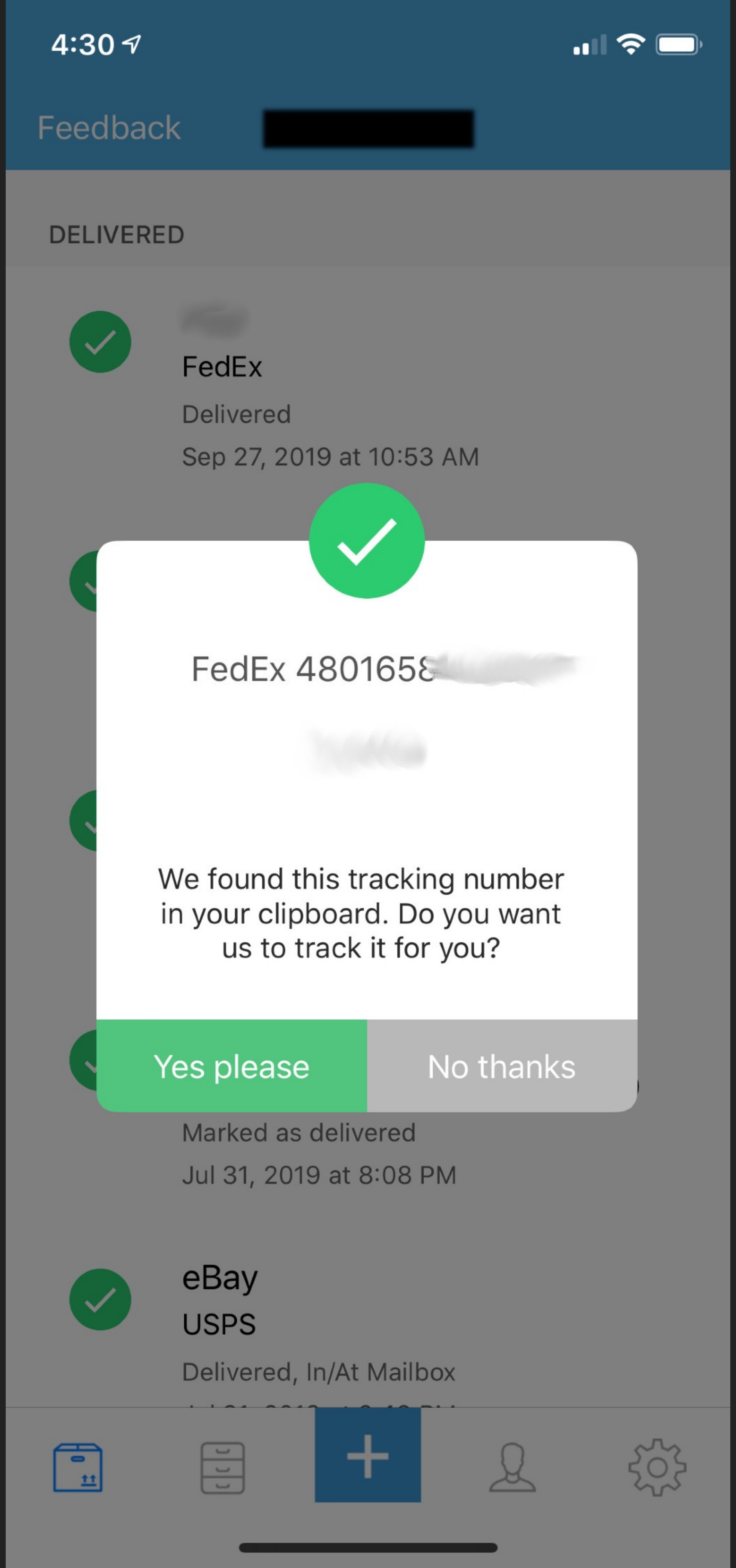
eBay

USPS

Delivered, In/At Mailbox

*We've mostly been looking at physical-world attack scenarios. But what about software?

WHAT'S WRONG WITH THIS PICTURE?



4:30

Feedback [redacted]

DELIVERED

[redacted]
FedEx
Delivered
Sep 27, 2019 at 10:53 AM

FedEx 480165[redacted]

[redacted]

We found this tracking number in your clipboard. Do you want us to track it for you?

Marked as delivered
Jul 31, 2019 at 8:08 PM

eBay
USPS
Delivered, In/At Mailbox

*Just because something is in the App Store doesn't mean it's perfectly secure or that it adequately respects your privacy. What exactly happens to data from my clipboard when I switch to this app? Does it go to their server? Is it transmitted securely? Do they store that data? What else do they do with it? What if I had a password or something else sensitive on my clipboard when I switched to the app?

HOW TO TRAIN OTHERS

CONSIDERATIONS FOR TRAINING OTHERS

- Convince the top-level bosses; get them fired up!
- Use multiple training techniques; examples:
    - Mandatory yearly meeting & onboarding training
    - “Phish” them before they *really* get phished
    - Posters (by phones, entrances, in lunch rooms, etc.)
    - Boss memos mention security initiatives
    - Reserve 1 minute in regularly scheduled meetings

MORE CONSIDERATIONS FOR TRAINING OTHERS

- Repetition is a key to learning (consider frequency)
- Reward successful training efforts!
- Security mindset can take time to develop
- Not everyone is as savvy as you; manage your expectations
- Never shame anyone–keep training until they "get it"

RESOURCES: TRAINING

- Duo Security - Free security awareness & education tools & activities
  https://duo.com/security-123
- PagerDuty - Free security training for everyone & for engineers
  https://sudo.pagerduty.com
- SANS - Newsletter, blog, poster, questions to ask vendors
  https://www.sans.org/security-awareness-training/resources
- SecureWorld - Free webinars, posters, videos, fact sheets
  https://www.secureworldexpo.com/industry-news/free-security-awareness-training-tools
- InfoSec Institute - Security Awareness & Training Resource Center
  https://www.infosecinstitute.com/resource-center/

RESOURCES: VIDEOS

- Bruce Schneier: The Security Mindset (YouTube) – 8 min
  https://youtu.be/eZNzMKS7zjo

- “Hacking the Grid” (Amazon Prime Video) – 16 min
  https://bit.ly/hackingthegrid
  aka “Watch hackers break into the US power grid” (YouTube)
  https://youtu.be/pL9q2lOZ1Fw

- “This Is How Easy It Is To Get Hacked” (YouTube) – 3 min
  https://youtu.be/G2_5rPbUDNA?t=484
  Patrick Wardle & Mikhail Sosonkin hack VICE News Producer

RESOURCES: FURTHER LEARNING OPPORTUNITIES

- Book: Beyond Fear: Thinking Sensibly About Security in an Uncertain World by Bruce Schneier http://bit.ly/beyondfearbs
- The Mac Security Blog and e-mail newsletter https://www.intego.com/mac-security-blog
- Podcasts:
  - Intego Mac Podcast https://podcast.intego.com
  - Security Now https://twit.tv/shows/security-now

REMEMBER THIS…

Think different.

*Think like an attacker.

QUESTIONS?
DISCUSSION?

What experiences do you have?

What have you found that you were surprised by?

IMAGE CREDITS

- Apple logo, “Think different.”, & “I'm a Mac” (©Apple) https://appleinsider.com/articles/19/05/27/actor-justin-long-reveals-why-jobs-rejected-over-200-im-a-mac-ads
- Trust No One (X-Files, ©Fox) https://knowyourmeme.com/photos/1183656-x-files
- Locked gate by stair rails https://imgur.com/gallery/9W2wEsf
- Gate that's a ladder https://www.reddit.com/r/CrappyDesign/comments/9tyjg8/when_your_security_gate_is_a_ladder/
- Vandal-proof camera https://www.lorextechnology.com/articles/Lorex-Vandal-Proof-Security-Cameras
- Silly-stringed security camera https://imgur.com/KwLMN
- USB drive in parking lot https://blog.idwatchdog.com/index.php/2016/08/02/dont-use-usb-flash-drives-found-on-the-ground/
- Public kiosk, CC BY-SA 4.0, Joshua Long (taken at MacTech Conference 2019)
- Charging station, CC BY-SA 4.0, Joshua Long (taken at MacTech Conference 2019)
- Aquarium QR, CC BY-SA 4.0, Joshua Long (taken at MacTech Conference 2019)
- QR code sticker over another QR code https://zengo.com/qr-code-degenerators/
- Screenshot of scanning an “irs.gov” QR code in iOS 11, CC BY-SA 4.0, Joshua Long
- Smart home assistants https://www.wertgarantie.de/Home/Themen/Blog/Smart-Home/smart-speaker-im-dreikampf-apple-homepod-amazon-echo-und-google-home-im-vergleich.aspx
- Lightning cable https://www.shopwudn.com/products/industrial-paracord-iphone-lightning-cable
- O.MG/BadUSB cables https://mg.lol/blog/omg-cable & https://mg.lol/blog/badusb-cables/
- ATM skimmer https://www.pymnts.com/news/security-and-risk/2017/atm-skimming-gets-a-tech-upgrade/attachment/atm-skimm/
- Hacker/attacker CC BY-SA 4.0, Magnus916 https://commons.wikimedia.org/wiki/File:Hacker-1_(1).jpg