



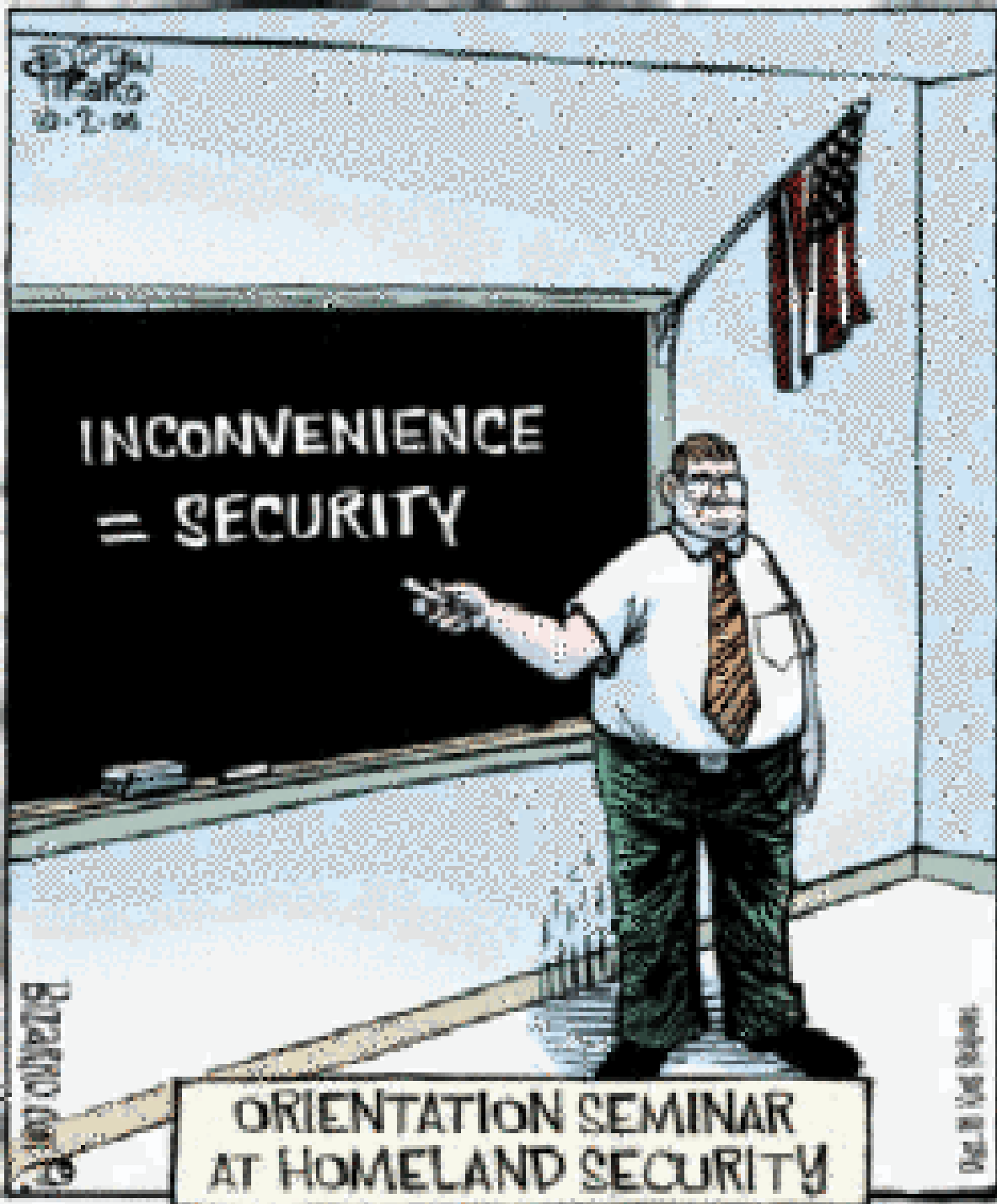
CRISP

SUMMER WEBINAR SERIES



The (Cyber) Dude

How to not be that guy..



Introduction

Summer Webinar Series

Jesse Mayer (The guy down there)

Cyber Security Architect for CRISP

There will be Memes and Pop Culture References

Why do we do training? What's it for? Why make a password so complex?

#D0n7b3F00l3D

What is it.. Really..

Image and Perception

What you think we do



What we really do





What people think we do

T h e R e a l C y b e r

Cyber Security is all about creating what I call a “Culture of Cyber.”

Build a holistic, well rounded balance between people, processes and technology that creates a comprehensive wall of defensive components at every level.

Training and Awareness is critical to the puzzle.

“There is no patch for human stupidity” – Cyber Mantra



Let's talk about Tim

A day in the life of a doctor and ULP
user



Meet Tim

Dr. Tim Timmies

Tim is one of the many ULP users who has his own practice!

Great doctor, loved by his patients

Uses his private practice email for ULP access

DrTIMRox@gmail.com



GET UP TO 1,000
FREE
4x6 PHOTO
PRINTS

No subscriptions. No commitments.
Just free prints!

★★★★★
5 STAR RATED APP

The deal of the century appears

Tim wants to Redecorate

P I C T U R E T I M E !

Tim signs up for the service using his personal email account

He gets 1,000 free prints!

Dr. Tim's clinic has now been renovated with a ton of pictures of his adventures around the world.

So did his office..

And his house....

And his neighbors' house.....



A person's hands are holding a tablet computer. The screen shows a finance application with a line graph and the word 'FINANCE' in large letters. The background is a blurred image of a person's face and a coffee cup on a table.

Oops.

Enter the Disaster

During lunch a few months later, Dr. Tim discovers a news article regarding his photo company.

They were breached, and his credentials have been floating on the internet somewhere for almost 2 months.

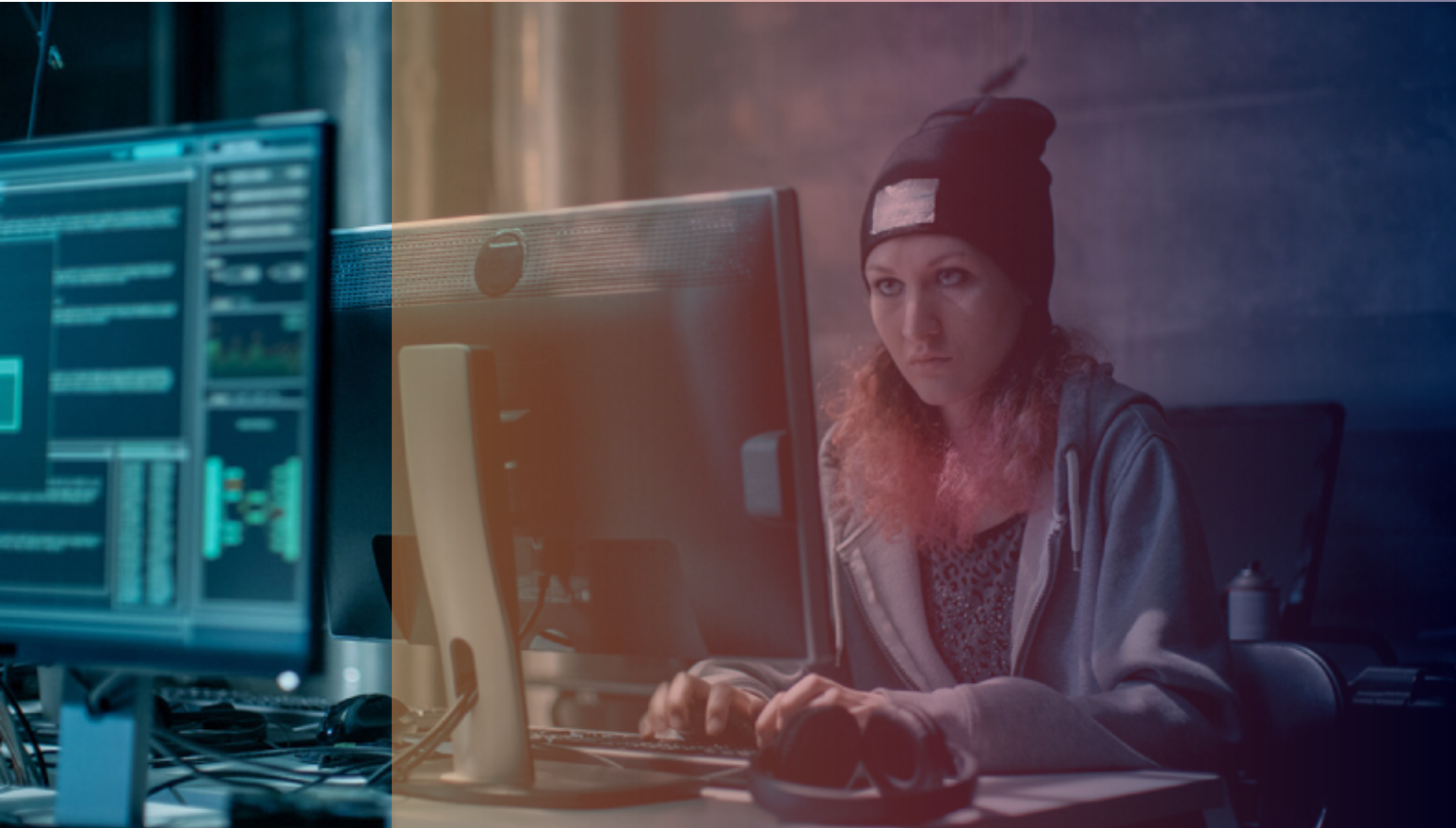
It's just 2 months.. What's the **worst** that could happen..



Enter the Dude

Darkweb Shopping trip

- **Literally like picking up milk**
- Hundreds of thousands of records for sale in batches
- PHI data is one of the most expensive and sought after groups of compromised data
- A patient can cancel their Credit Card
 - They can't cancel their SSN



Meet Misha

Misha found Tim's credentials on the dark web when she purchased an access pack.

She knows through LinkedIn and a simple google search that Dr. Tim owns a clinic in Maryland.

She logs into his ULP account and starts to exfiltrate patient data to sell on the dark web.

Cyber Christmas

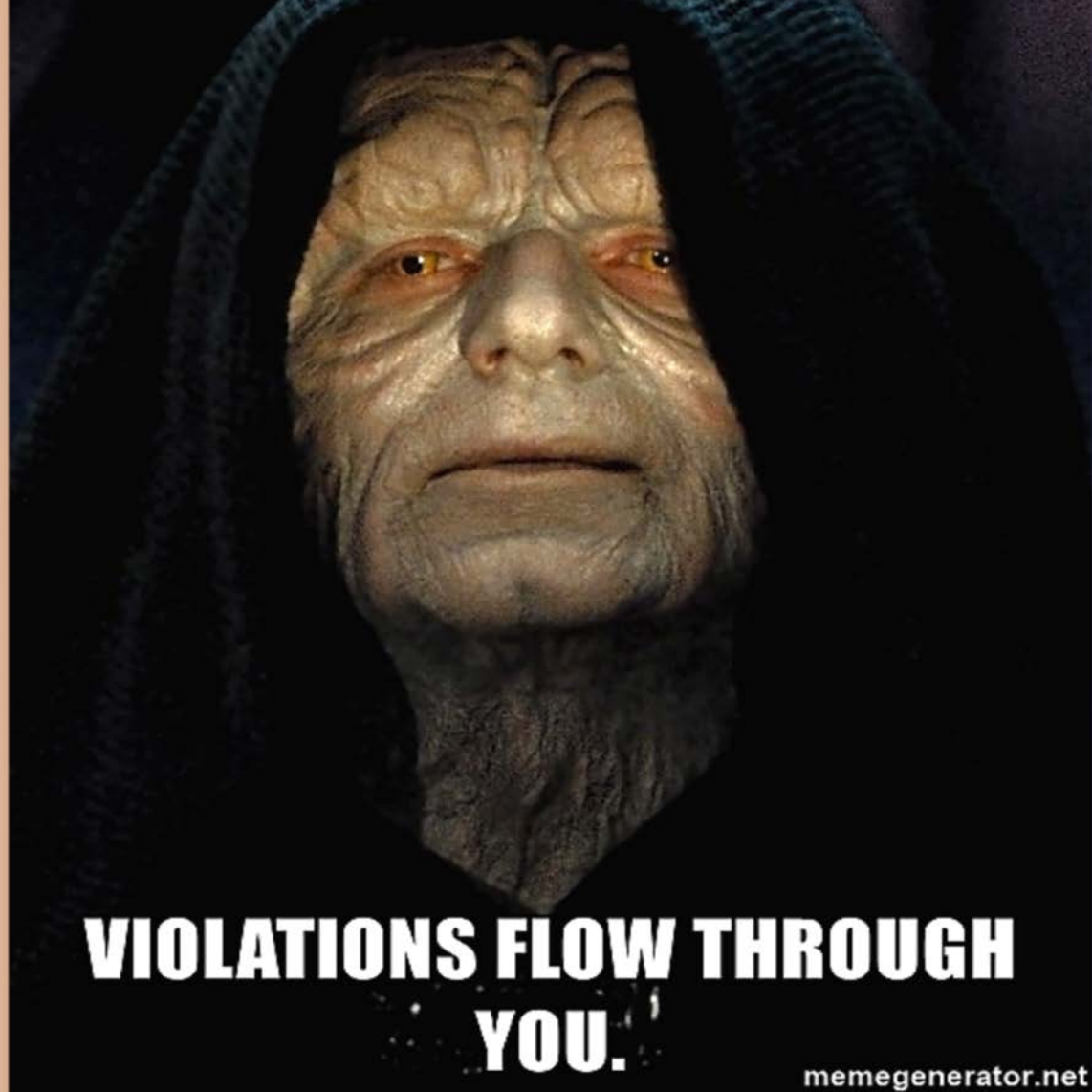
Dr. Tim was consistently bad.

- Dr. Tim's ULP Credentials are now in the hands of Misha
- She resets them, and discovers some other nifty information..
 - Bank of America
 - Wells Fargo Business Account
 - Personal Healthcare Account
 - Retirement Fund

Misha Resets all of Tim's accounts, changes his google password and two factor authentication to her own phone.

Tim is now pwnd, Misha is celebrating Christmas early now that she has sold all of the ULP patient data, at current going rate of \$450 per record.

**GOOD.. GOOD.. LET THE
INFOSEC**



**VIOLATIONS FLOW THROUGH
YOU.**

memegenerator.net

Fix the Puzzle

What pieces were missing?

Authentication and Authorization

Complexity

Password Complexity Requirements are significantly important. Let's compare the following at a 5 character password

Characters	Count	Total Combinations
a-z	26	11,881,376
A-Z, a-z	52	380,204,032
A-Z, a-z, 0-9	62	916,131,832
A-Z, a-z, 0-9, !@#\$%&*	69	1,564,031,349

At a 7 character requirement, there are a total of 7.4 Trillion combinations

Diversify your Protection

Change your password every 90 days.

Do NOT share passwords between services (ULP and Google).

Follow the Complexity Requirements.

If you can google yourself and a part of your password, chances are it's not secure.

2FA

- 2FA ensures that there is an additional step to confirm that the who is logging into your account.

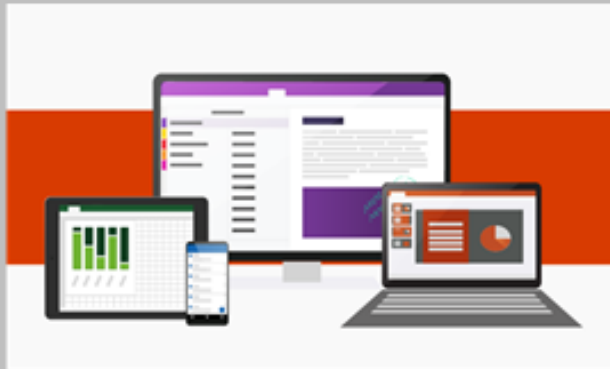
Phishing



(I)Legitimate Emails

- Phishing Emails can be cleverly crafted to look like a standard email you may receive from a vender, partner or service you subscribe to.
- Often difficult to tell at first glance whether or not it is Legitimate or Illegitimate

Look before you Leap



[REDACTED], Your payroll details need updating, please click below to start the update.

**UPDATE YOUR ACCOUNT
DETAILS**

Dear **[REDACTED]**

We have recently upgraded our ACE payroll system, as a security measure we need you to re-confirm your bank routing number details for your account nominated to receive your salary. Please review and enter your routing number details at the link above **[REDACTED]** - by clicking on the "Update Your Account Details" button above.

<http://portal.payrolltooling.com/?id=qe/p/pi6a+l1yi10jnda+jnelmjwguyhc5ru+zfoylnzqu0tebxylr2vyqnyiq7q1718wc1ighctkslj7uckkebd4p7qkatqyi9uco0rnxf7k3kyfsbxevgxhqtoljvwzswudl70abhtoc0m+k8gb29w3lxwjcnszl659t8un1wtv7wu6ymmmppbpdmdtr2lzz8ohdd8mdxnpuyuxzz9iygoc40o/pu0m+jpcgun6devpsapfnsazbgspsw/0o9zmwczhvwzpt6dhp5w/il2wzbdmdhellaaihtjyenpmgduaywhovyjc/2psdq/oi>
Click or tap to follow link.

CRISP Cyber Security

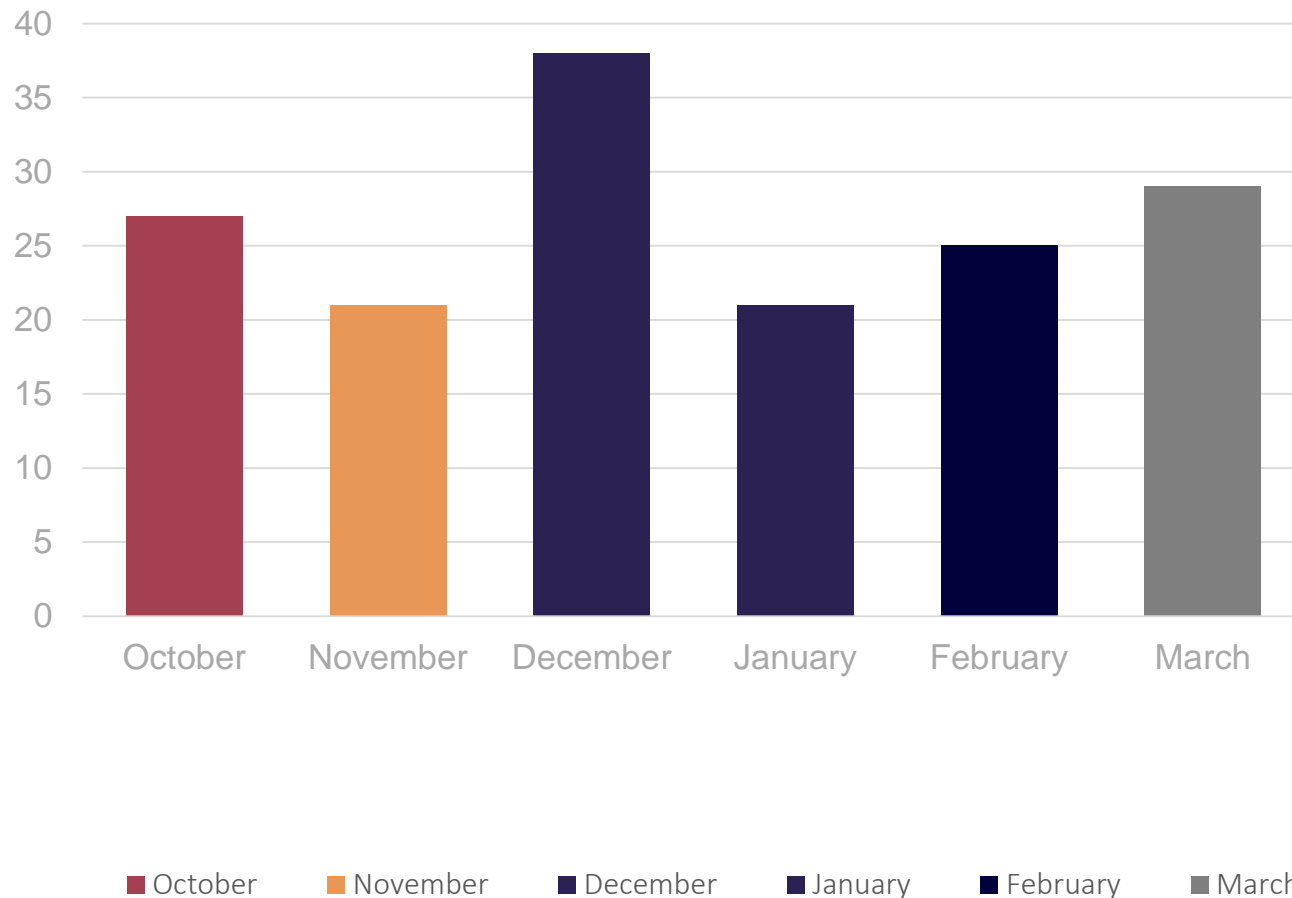
What are we doing

- Security and Encryption requirements on all segments of our architecture that touch any PHI
- Thorough vetting of all incoming data sets to ensure security and integrity of data is at highest standard
- Requiring all access to our internal data center to go through secured, single access data points
- Testing and Processing that have granted us HITRUST accreditation
- Password Complexity Requirements be met
- Two Factor Authentication for all enterprise level global administrators

What's Coming

- Two Factor Authentication in pilot and rollout stages
- Dynamic Data Loss Prevention solution in test phases
- Bi-monthly Phishing training against all CRISP employees
- Active Black Box / Grey Box / White Box penetration tests by a trusted third party

Healthcare Breaches

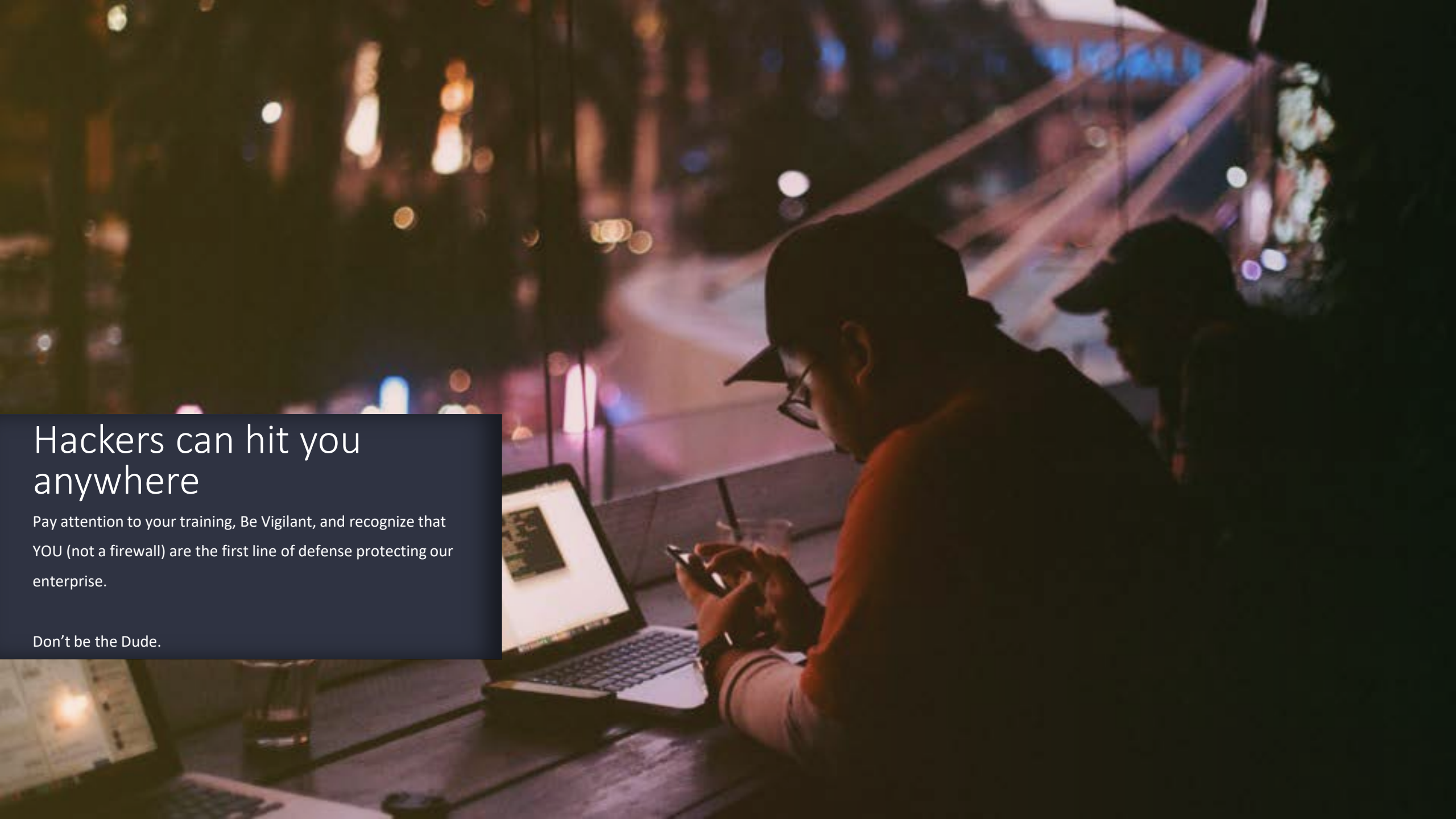


It actually happens
And more than we want to admit

The Verizon Data Breach Investigations Report confirmed that the healthcare industry is the only one where more data breaches are caused by insiders than hackers.

2018 compromises have been on the rise, with Unauthorized access/disclosures, loss of devices/records, and improper disposal incidents behind 19 of the 29 (65.5%) incidents reported in March.

PEBKAC – Problem Exists Between Keyboard and Chair

A person wearing a black cap and glasses is sitting at a wooden table, working on a laptop. The laptop screen displays some code or data. The person is holding a smartphone in their left hand. The background is a blurred city street at night, with warm lights from buildings and street lamps creating a bokeh effect. Another person is partially visible in the background, also working.

Hackers can hit you anywhere

Pay attention to your training, Be Vigilant, and recognize that YOU (not a firewall) are the first line of defense protecting our enterprise.

Don't be the Dude.

THANK YOU

Any questions?



Jesse Mayer



Security@CRISPhealth.org