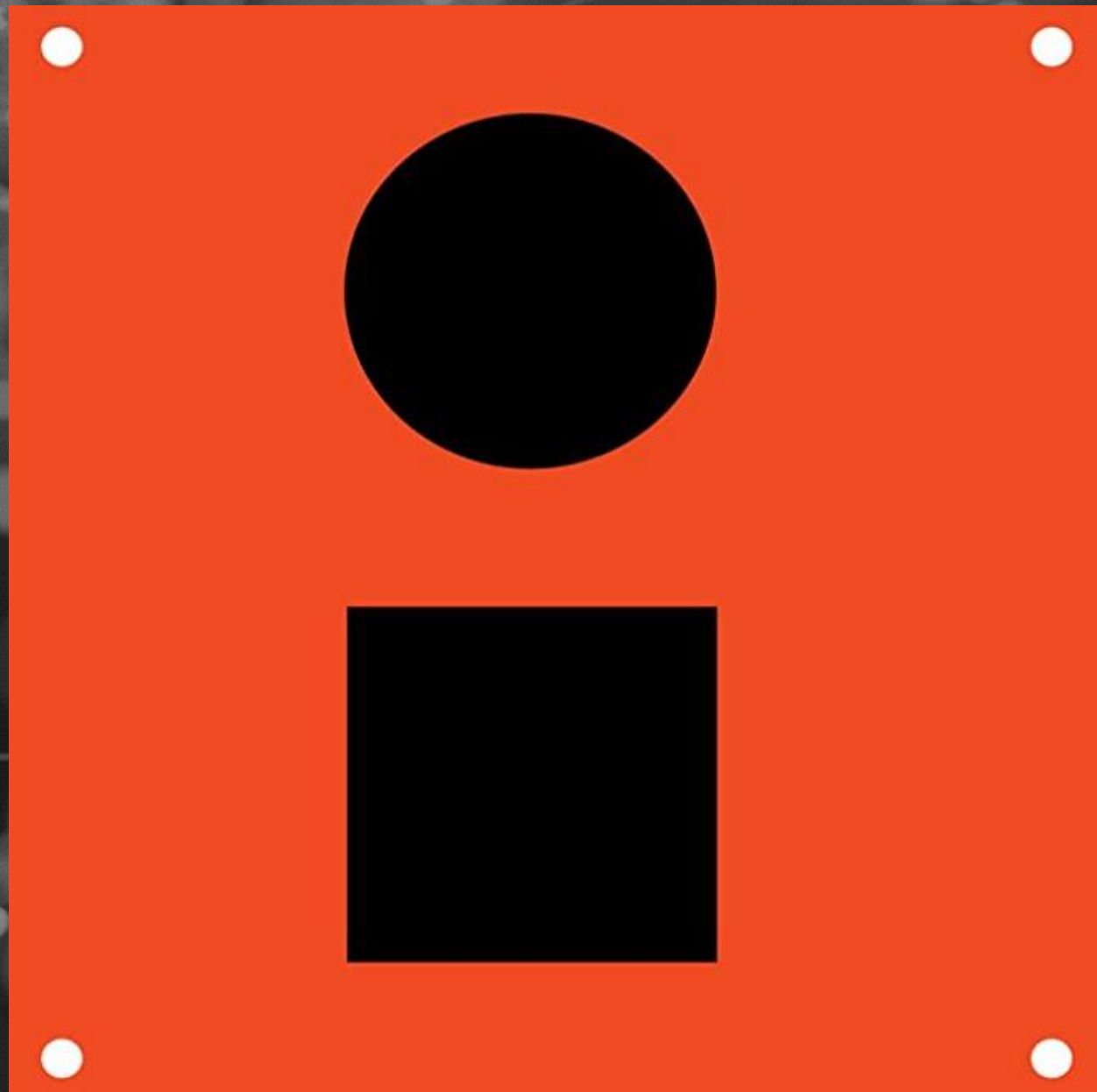
Fun with Cybersecurity?

Fear of getting hacked, swindled, or having data stolen drives much of the attention given to cybersecurity. It truly is a serious issue for small broadband providers and their customers.

But during this session, Steve Riat, Nex-Tech, will share stories about how hackers got caught, look at the dark web and highlight the decisions hackers have made and the consequences for those that got caught.

This is not to make light of the serious nature of the problem, but to help you gain knowledge so that you can be safer in a dangerous online world.



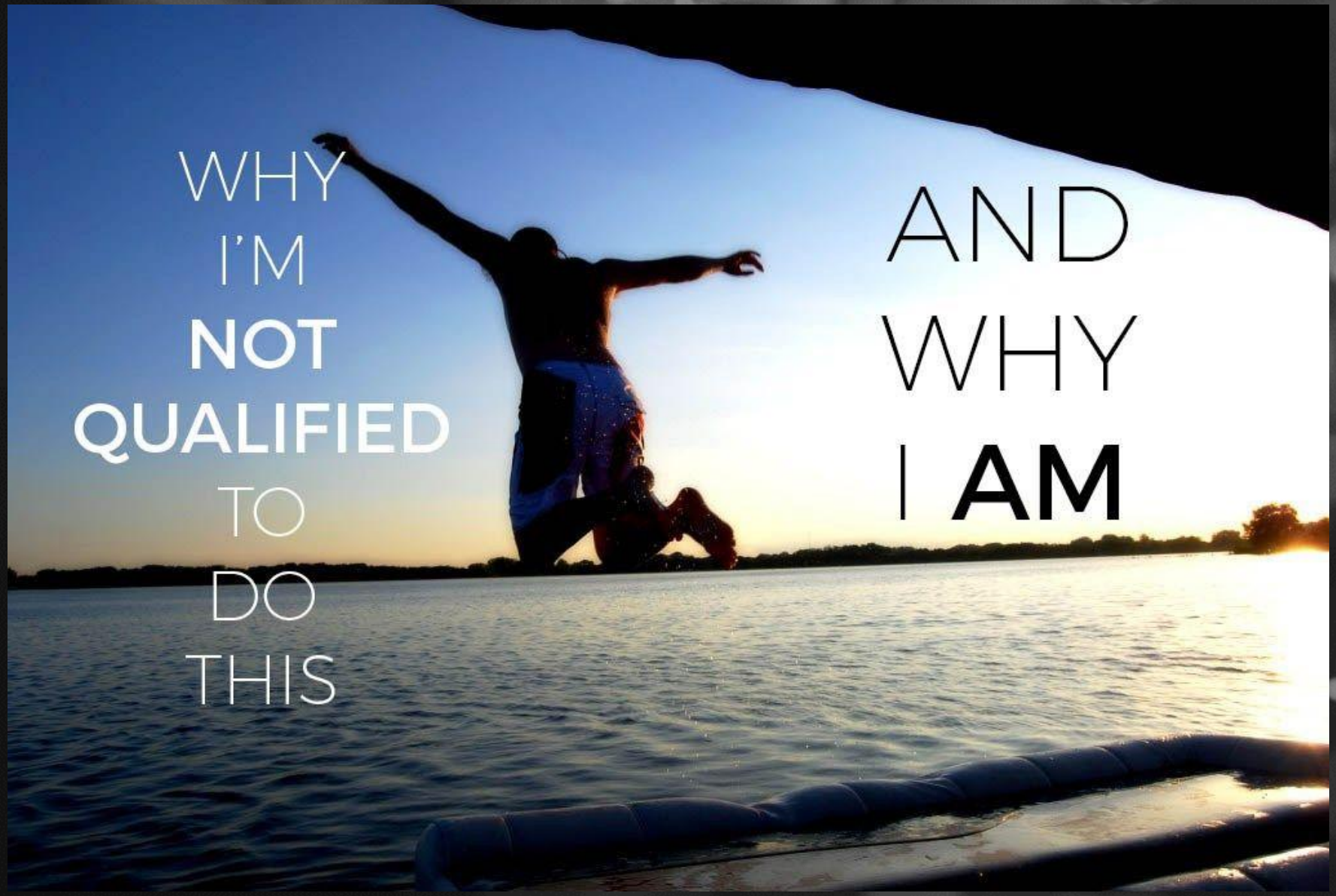
We are fighting an intergalactic Cyber War and people don't care

Really Steve? Intergalactic?

Challenge ↓	Impact ↓
Societal perception of cybersecurity is that it is a technical problem, best handled by technical people.	Societal perception is dominated by fear, uncertainty and doubt. It results in poor engagement with executives, unproductive exchanges and unrealistic expectations. Ultimately, it leads to bad decisions and bad investments in cybersecurity.
Real failures are not getting enough attention to productively change behavior.	Compliance with any regulation does not equal appropriate levels of protection.

Gartner – Urgency to Treat Cybersecurity as a Business Decision August 2021

Why am I qualified to talk to you about Cybersecurity?



People don’t care and here are the major reasons:

- **Immediacy**
- **Short attention span**
- **Numb to breach occurrence**
- **Good detection and recovery (equals mild inconvenience)**

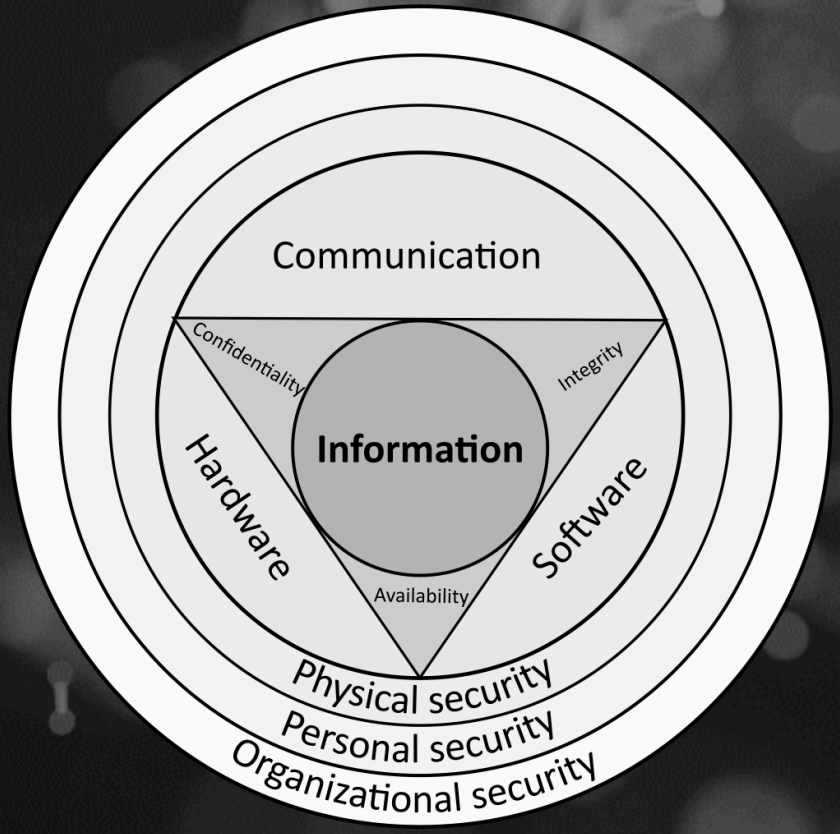
Modern CISO

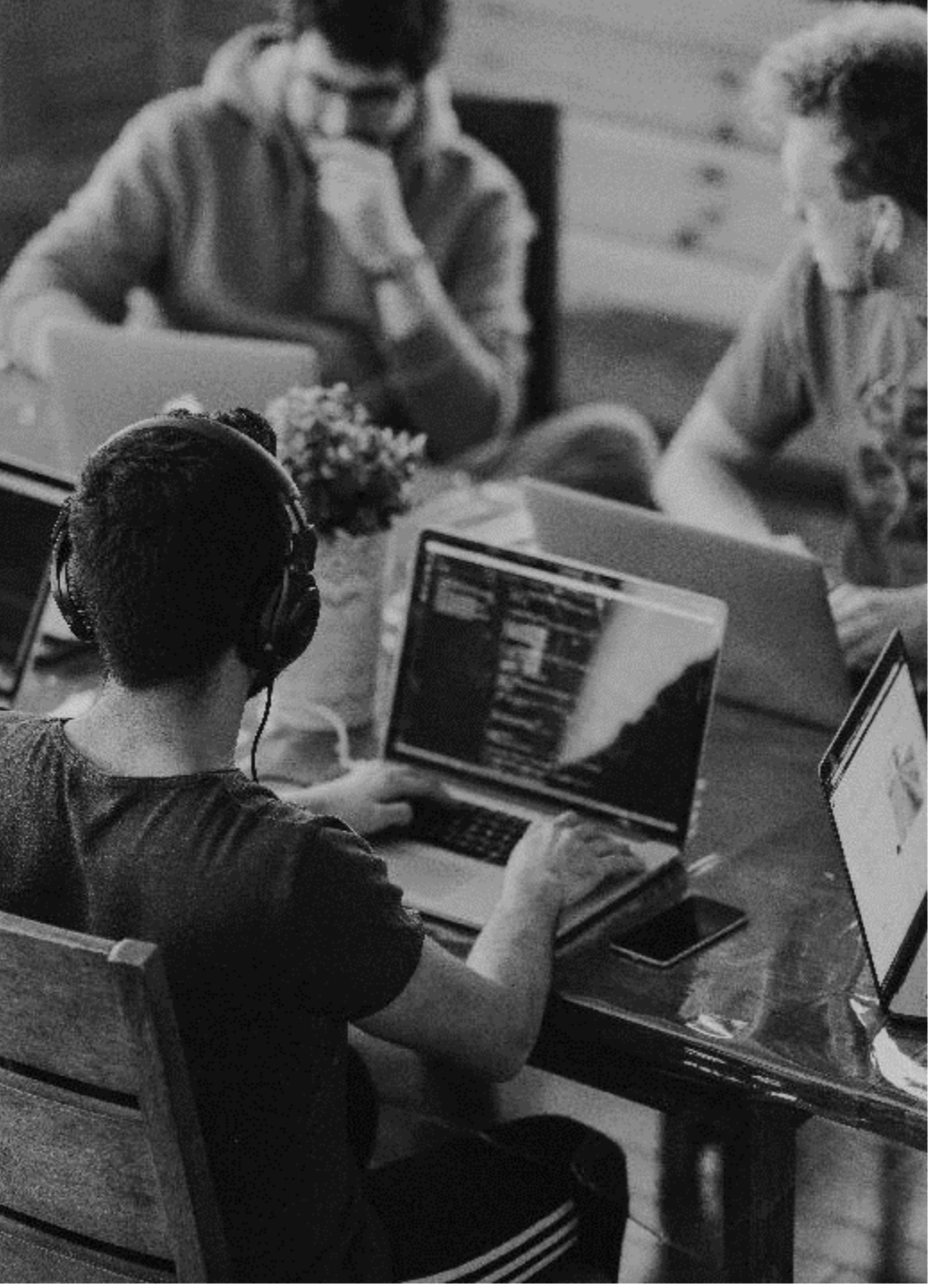
*A Disclaimer

- Systems and tools are very important for protection
- Investment in Cybersecurity is very important
- Having the right vendors and people is very important

Let's take a step back and frame the problem

Then let's look at the first hack (at least in Steve’s life)





1 MINUTE ON INTERNET

ONE MINUTE

*Statistica August 2021

2021

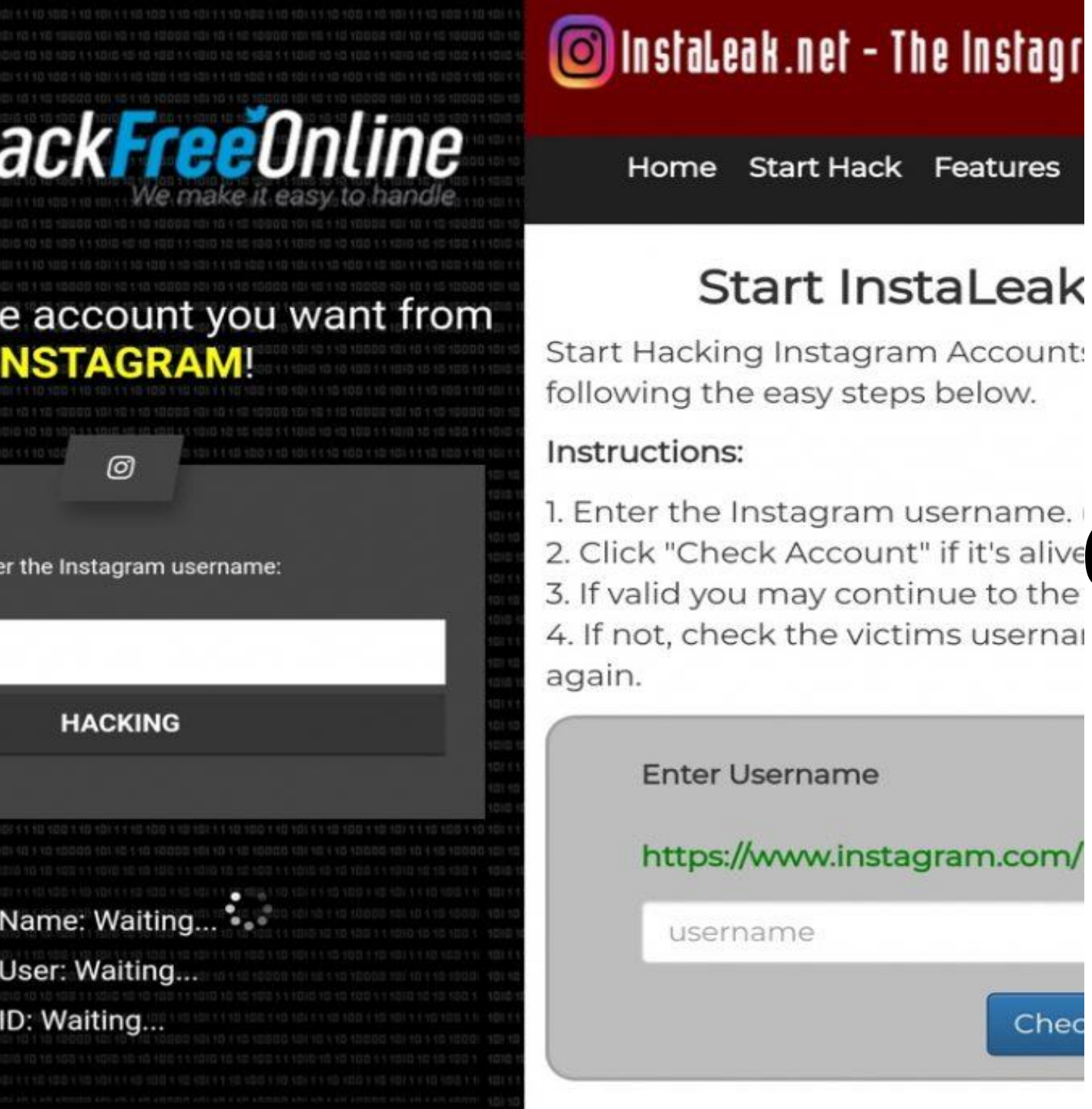
NETFLIX

28,000 Subscribers Watching

For as low as $1.25 you can get a Netflix account.

(Source: Wondershare, dr.fone)

Netflix streaming is one of the standard hacking services and widely available. For a small fee, you'll receive the email and password of someone's Netflix account. Just imagine how many people's credentials have been hacked or stolen for the price to get this low.



695,000 STORIES SHARED

132 CONNECTIONS MADE

The social networking website LinkedIn was hacked on **June 5, 2012**, and passwords for nearly 6.5 million user accounts were stolen by Russian cybercriminals.

TikTok

5,000 DOWNLOADS

$1.6 MILLION SPENT ONLINE

92% of ATMs are vulnerable to hacker attacks.

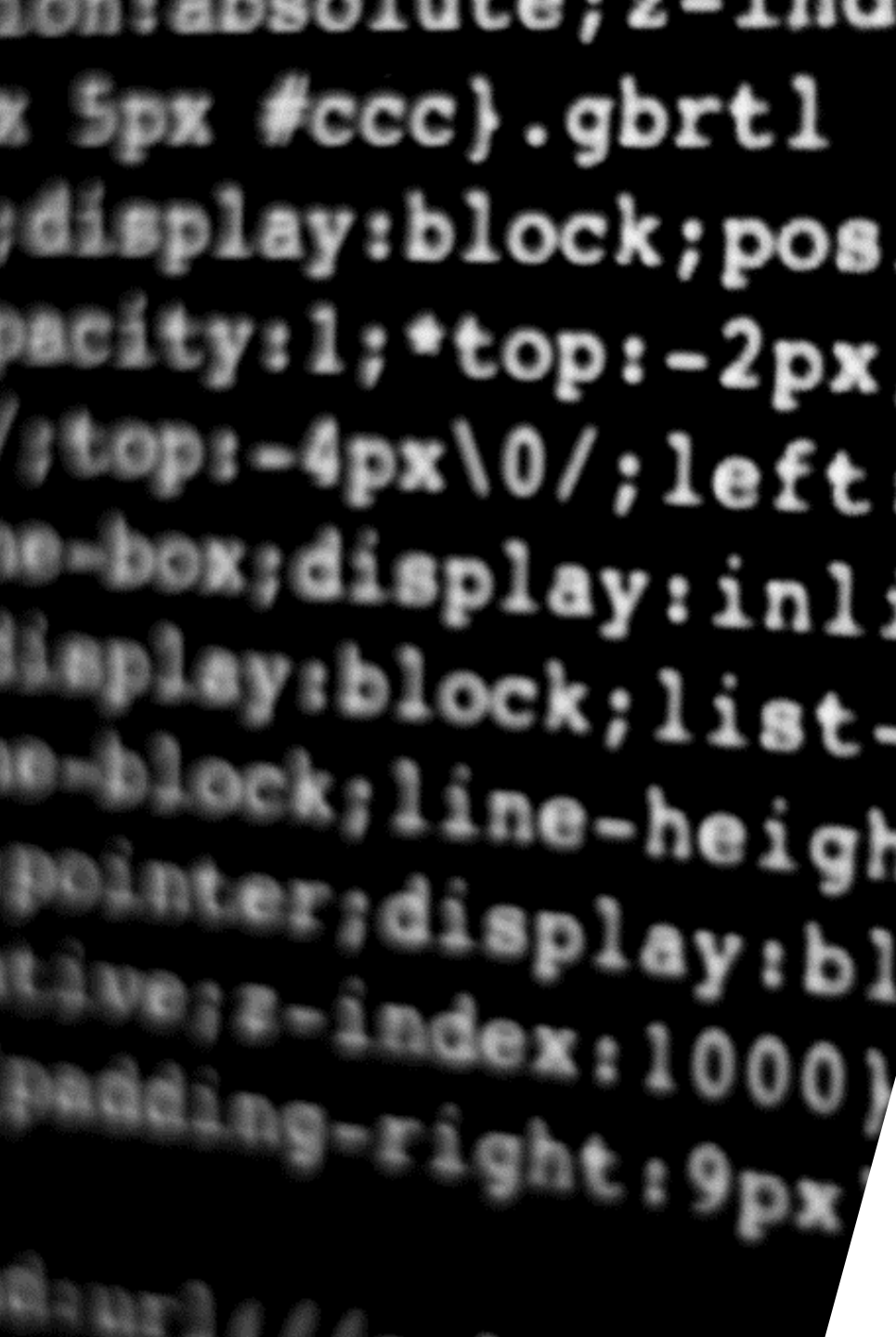
(Source: PTSecurity)

There are several ways to hack an ATM, but consider this – if your card data is stolen, then 100% of ATMs would be vulnerable to this kind of attack.

tinder™

2 MILLION SWIPES

197.6 MILLION EMAILS SENT



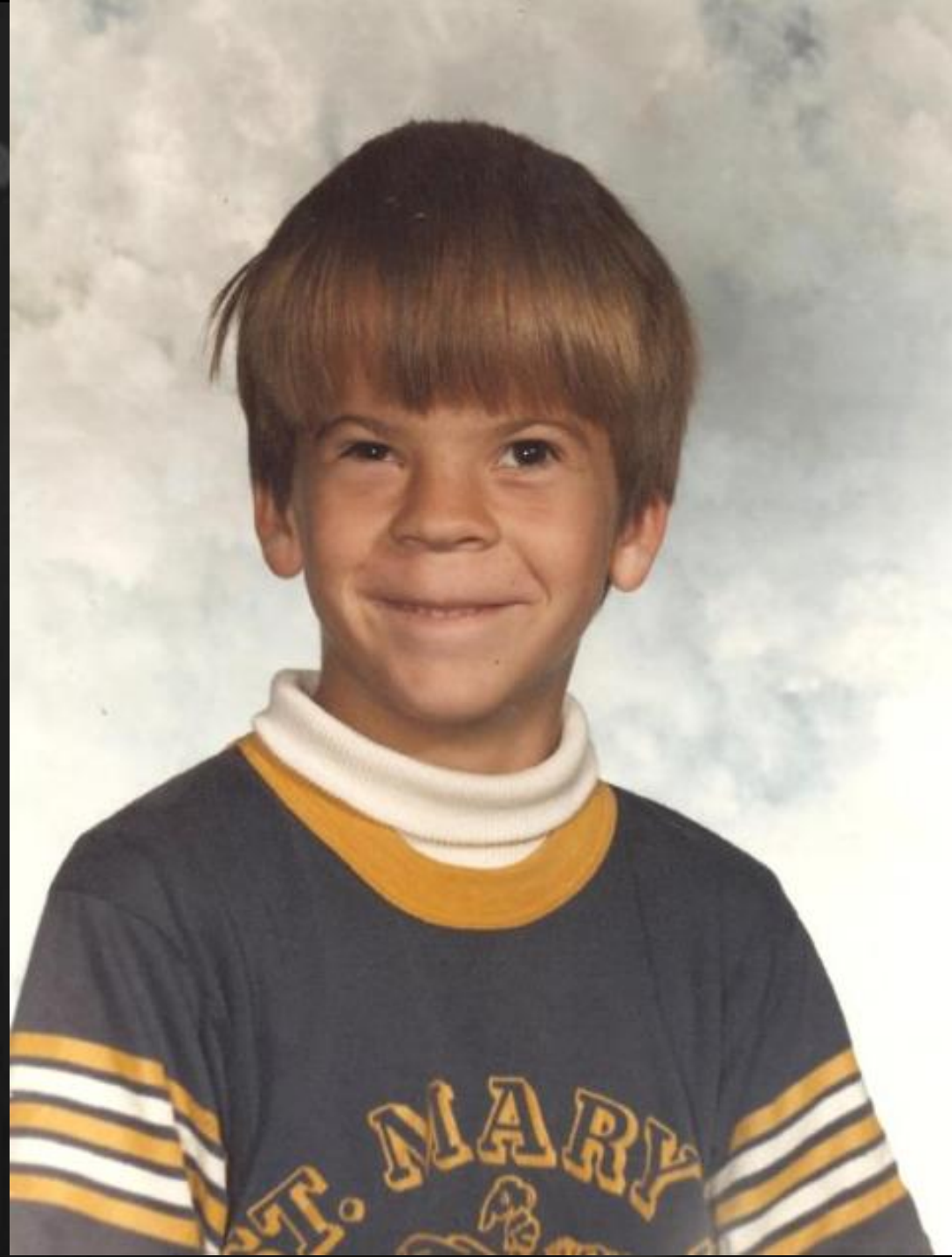
You Tube

500 HOURS OF CONTENT UPLOADED

Has its own how to videos on hacking!

I want to take us back to a simpler time

Couple of things happened when I was 8



First, I became a big brother

Second, I became a computer geek

Definition:

A person who is interested in technology, especially computing and new media. Geeks are adept with computers, and use the term *hacker* in a positive way, though not all are hackers themselves. A person who relates academic subjects to the real world outside of academic studies; for example, using multivariate calculus to determine how they should correctly optimize the dimensions of a pan to bake a cake. A person who has chosen concentration rather than conformity; one who passionately pursues skill (especially technical skill) and imagination, not mainstream social acceptance.

Read more: http://www.answers.com/topic/geek#ixzz1EbPBBNp9

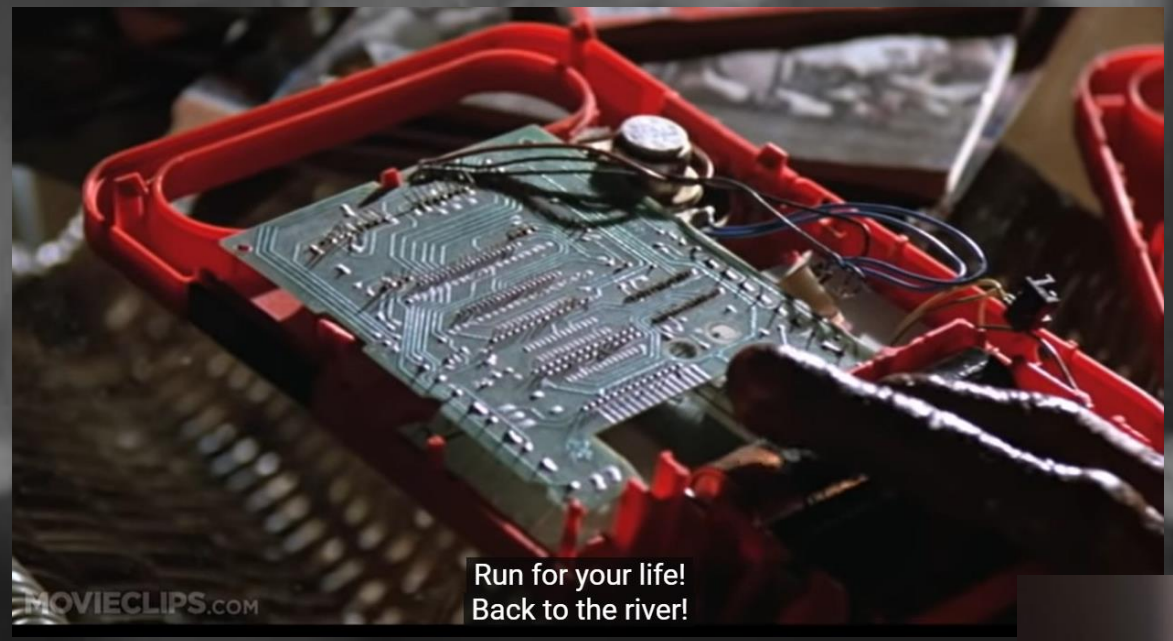
It all started here

Could say 200 words
Sold for $50
Over 20 films
Over 40 songs
1,000 bits per second
18k

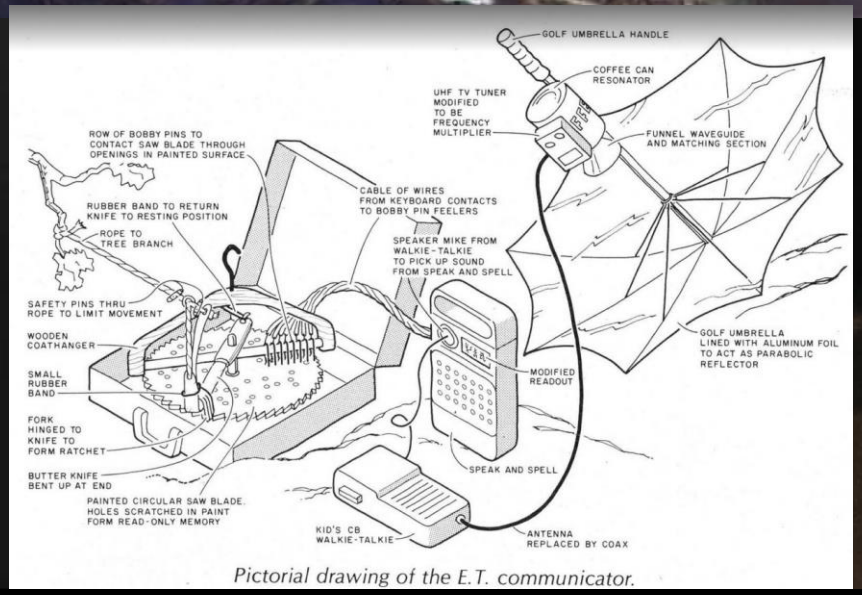
Upgradeable

Technology = Possibilities


Reese's
pieces
Peanut Butter
CANDY IN A CRUNCHY SHELL
NET WT


Run for your life!
Back to the river!
MOVIECLIPS.COM


MOVIECLIPS.COM



Pictorial drawing of the E.T. communicator.


© 1982 Universal Studios


SHALL WE PLAY A GAME?


-STUDENT ID # 38-106 -BUELLER, FERRIS
-CLASS (12) -HOME PHONE # 555-6452
DAYS ABSENT: 0

Much like Elliot I feel under attack!

(Although he did let ET in)

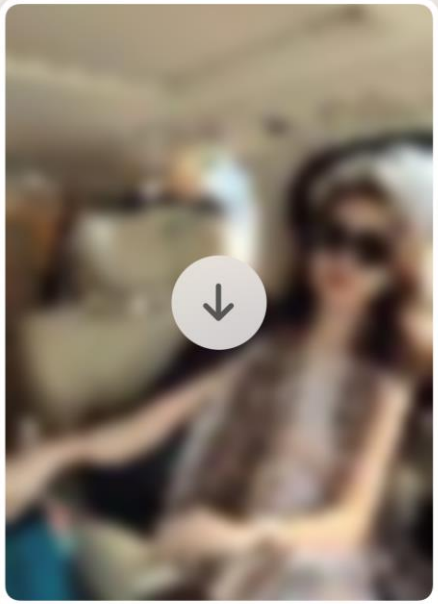
Unfortunately,
I have bad news for you.
A few months ago, I had access to the device you use to browse the internet.
Since then I have been monitoring your activities on the internet.
As a regular visitor to adult websites, I can confirm that this is your responsibility.
For your convenience, the websites you visit have given me access to your information.
I have loaded a driver-based trojan that updates its signature several times a day so the antivirus cannot detect it.
I also have access to your camera and microphone.
Also, I backed up all data including photos, social media, chats and contacts.
I recently had the great idea to create a video where you cum on one part of the screen while the video is playing on another screen at the same time.
It was fun! Rest assured that I can easily send this video to all your contacts with just a few clicks and I assume you want to avoid this scenario.
With that in mind, here's my suggestion: Transfer the amount of 900 usd to my bitcoin wallet and I'll forget everything.
I will also permanently delete all data and videos. In my opinion, this is a rather modest price for my work.
You can find out how to buy bitcoins using search engines like Moonpay or Banxa as it is not very difficult.
My Bitcoin Wallet (BTC): 1Gy71W4bQpcq5D9xsYHz7wsgrzoQxZLhwd
You have 72 hours to respond and you should also note the following:
It's no use answering me - the address was generated automatically.
It also makes no sense to complain as the letter cannot be traced along with my bitcoin wallet.
Everything is precisely orchestrated.
If I find out that you've mentioned this letter to someone, the video will be shared immediately and your contacts will be the first to receive it.

5:29

LTE

+1 (209) 323-2247

one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

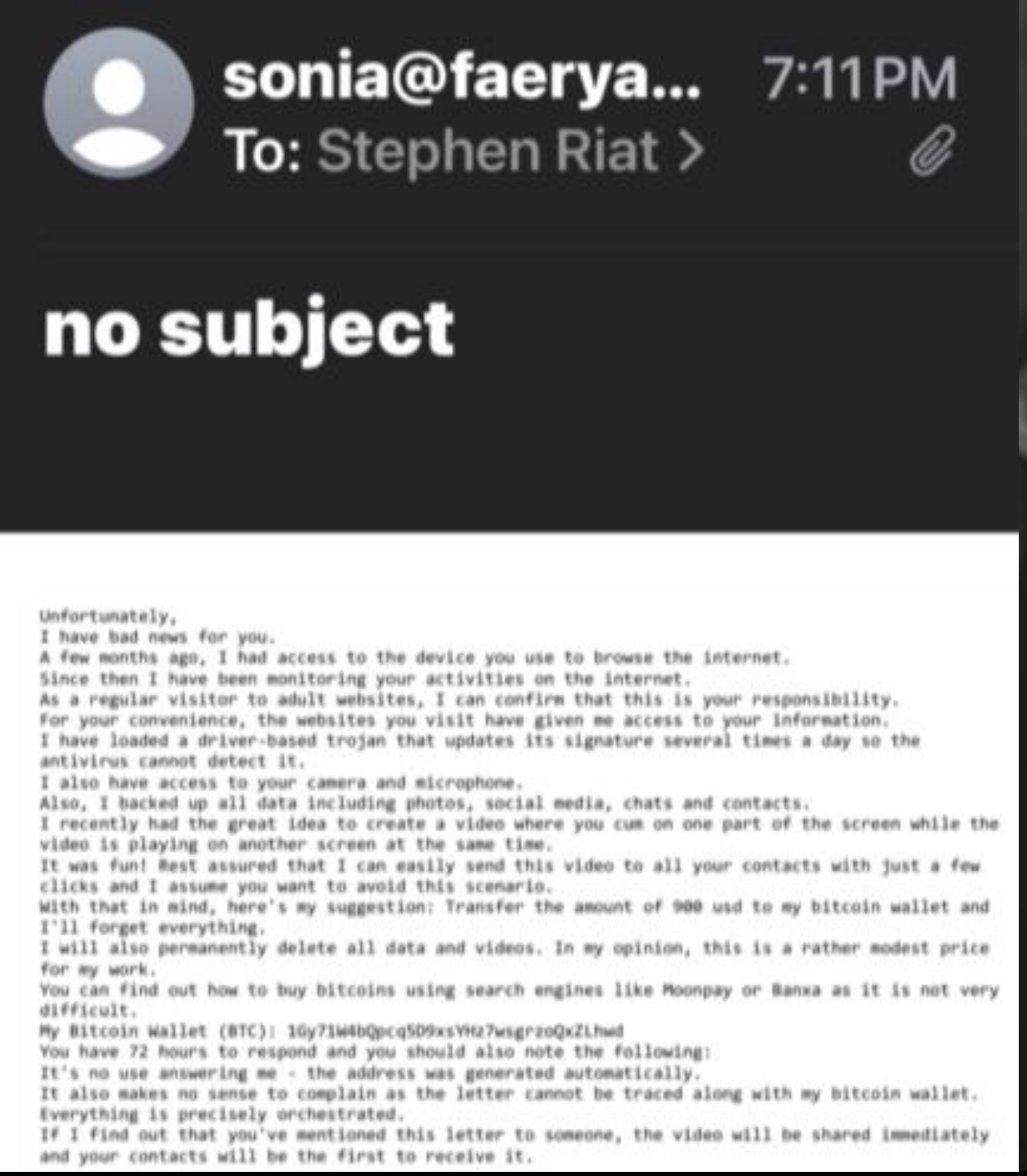


I've waited too long for you, I've asked Sam to pick me up, please reply promptly when you see the

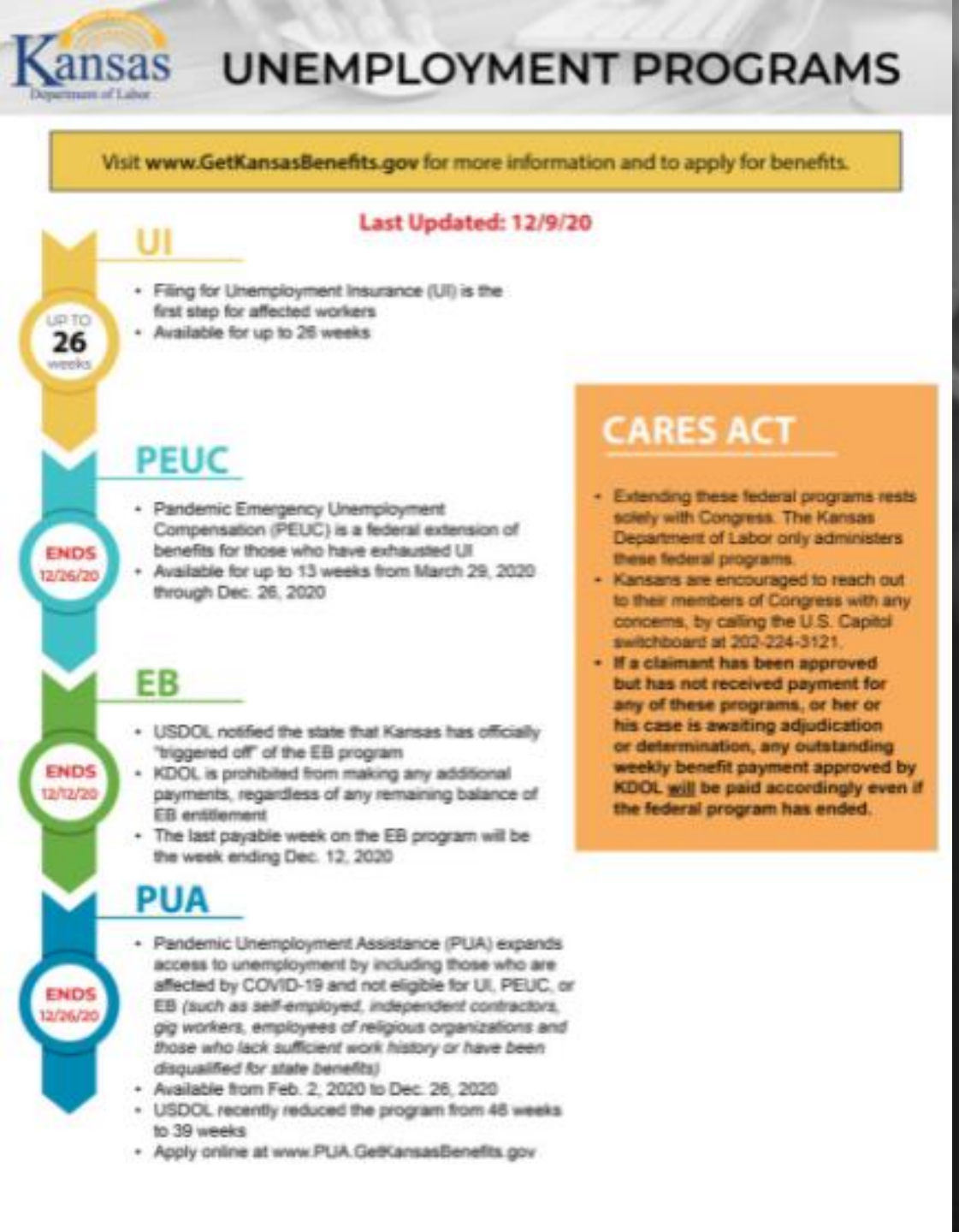
5:28 PM

I've waited too long for you, I've asked Sam to pick me up, please reply promptly when you see the

5:28 PM



Sextortion occurs when someone threatens to distribute your private and sensitive material if their demands are not met. In 2021, the IC3 received more than 18,000 sextortion-related complaints, with losses over $13.6 million.
*IC3



Filed the 3rd time for unemployment!

TD Bank

America's Most Convenient Bank®

March 16, 2022

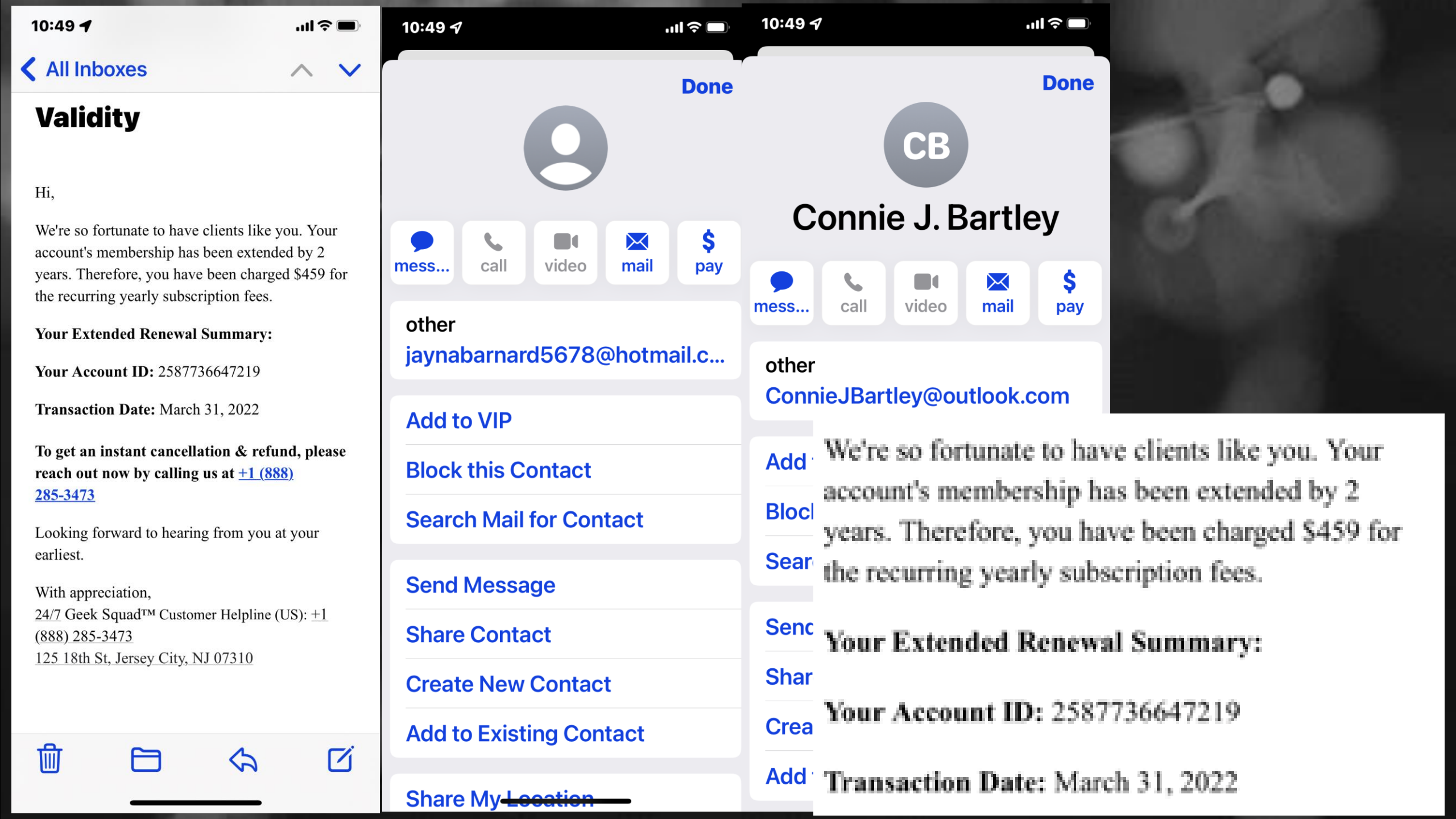
39949-04-N-003442
STEPHEN RIAT
[redacted]
HAYS, KS 67601-2788

Dear STEPHEN RIAT,

At TD Bank, protecting consumer information is our top priority. That's why we're writing to let you know that someone tried to open a TD checking or savings account in your name—but we've already restricted and closed the account using safeguards we have in place to detect this type of fraud. While you may have already contacted us about this account, this letter confirms that **no further action** with TD is needed.

This activity was not a data breach of TD's systems—the information used to create the account was obtained by people and sources outside of TD.

We realize how unsettling it is to learn your information was compromised in any way, and we're here to inform and empower you when it comes to protecting yourself from fraud. That's why we're providing resources below with tips and tools to help protect your information going forward—including one year of free credit monitoring.


10:49
All Inboxes
Validity
Hi,
We're so fortunate to have clients like you. Your account's membership has been extended by 2 years. Therefore, you have been charged $459 for the recurring yearly subscription fees.
Your Extended Renewal Summary:
Your Account ID: 2587736647219
Transaction Date: March 31, 2022
To get an instant cancellation & refund, please reach out now by calling us at +1 (888) 285-3473
Looking forward to hearing from you at your earliest.
With appreciation,
24/7 Geek Squad™ Customer Helpline (US): +1 (888) 285-3473
125 18th St, Jersey City, NJ 07310
10:49
Done
mess...
call
video
mail
pay
other
jaynabarnard5678@hotmail.c...
Add to VIP
Block this Contact
Search Mail for Contact
Send Message
Share Contact
Create New Contact
Add to Existing Contact
Share My Location
10:49
Done
CB
Connie J. Bartley
mess...
call
video
mail
pay
other
ConnieJBartley@outlook.com
We're so fortunate to have clients like you. Your account's membership has been extended by 2 years. Therefore, you have been charged $459 for the recurring yearly subscription fees.
Your Extended Renewal Summary:
Your Account ID: 2587736647219
Transaction Date: March 31, 2022

Hi, Dearly Beloved In The Lord.

I want Introduce my self to you My Dearest Friend In the Lord, I am Mrs. Linda Niiko. Arthur, from Canada but my husband is Japanese origin, We were married for twenty-seven years year. I'm 60 years old and suffering from a long time Cancer sickness. My Husband died after a brief illness that lasted for only ten days in august 16 2016. well my husband is a contractor and before his death he secure and complete a contract work with the UK government's value $17.500, 000.00 million dollars, but death took him away before the money was deposited into his bank account. before his death my Husband advised me to donate the money to God Fearing Person to invest the fund in God's work, Helping The Poor and Needy Around the world because i m sick i can not do it myself for now.

As a real believer of God after all my prayers, for over a month now that I have been praying about you to know if really you are going to use the fund working according to the direction of God our lord, so after all my prayers I am convinced and contacted you, I need your reply immediately you receive this massage now if you would be able to use the funds for the Lord's work and help the poor ones as I want it with trust reply to me with this email address (mrsarthurlinda114@gmail.com)

May God Bless You My Good Friend In The Lord.

Best Regard's,
Mrs. Linda Nikko. Arthur.

Hello I am Miss SOLONGE the only daughter of PETER FOFO who died in a motor accident some months ago he was a contractor to federal government of Cote d'Ivoire. Before he gives up in the hospital he told my mother and I that he deposited sum of US $ 9.5 million with a bank in Lome-Togo and where the document is.

Since after my father's death my uncles are troubling my mother with their useless African traditions they have taking all of my father's belongings/properties and left us with nothing just because, my late father did not have a male child. As a result of this problem my mother feels into an illness. Now she is seriously sick and I have spent all the money we have on drugs and hospital bills.

We have nothing to do than to run down to Lome-Togo to claim the (money) from the bank. We have contacted the bank management and they said before the fund can be released we must bring my late father foreign business partner to stand as my father next of kin for security reasons.

Now we are looking for someone who will assist us and claim the (money) so that when it arrived to his home/ country he will take his own share and send us our own. I am writing this mail to see if you can assist us.

Upon receipt of your acknowledgment mail I shall send you the contact of the bank director as well as our telephone number.

Thanks
Miss SOLONGE PETER FOFO

2:11 LTE

4 2 Messages

JR **Jennifer Riat** 1:08 PM
To: Stephen Riat >

Packaging will be charged extra

PayPal

Your Order Just Shipped

Consignment Number is - 2003528

Order Number - tpVG-Cq6yHU-RbCVw

2:11

4 2 Messages
Packaging will...

Follow your order details below. For any clarification, please reach us on 1-657-229-2926.

Order Details :

Name - Jennifer Riat
Product name - Power BTC 2x
Purchase date - Tuesday, March 22, 2022
Amount paid - #custom4#

We're Here to Help

If you have any questions, concern or wish to make changes to your order please feel to call us on our helpline number 1-657-229-2926 . Our representative will be happy to assist you.

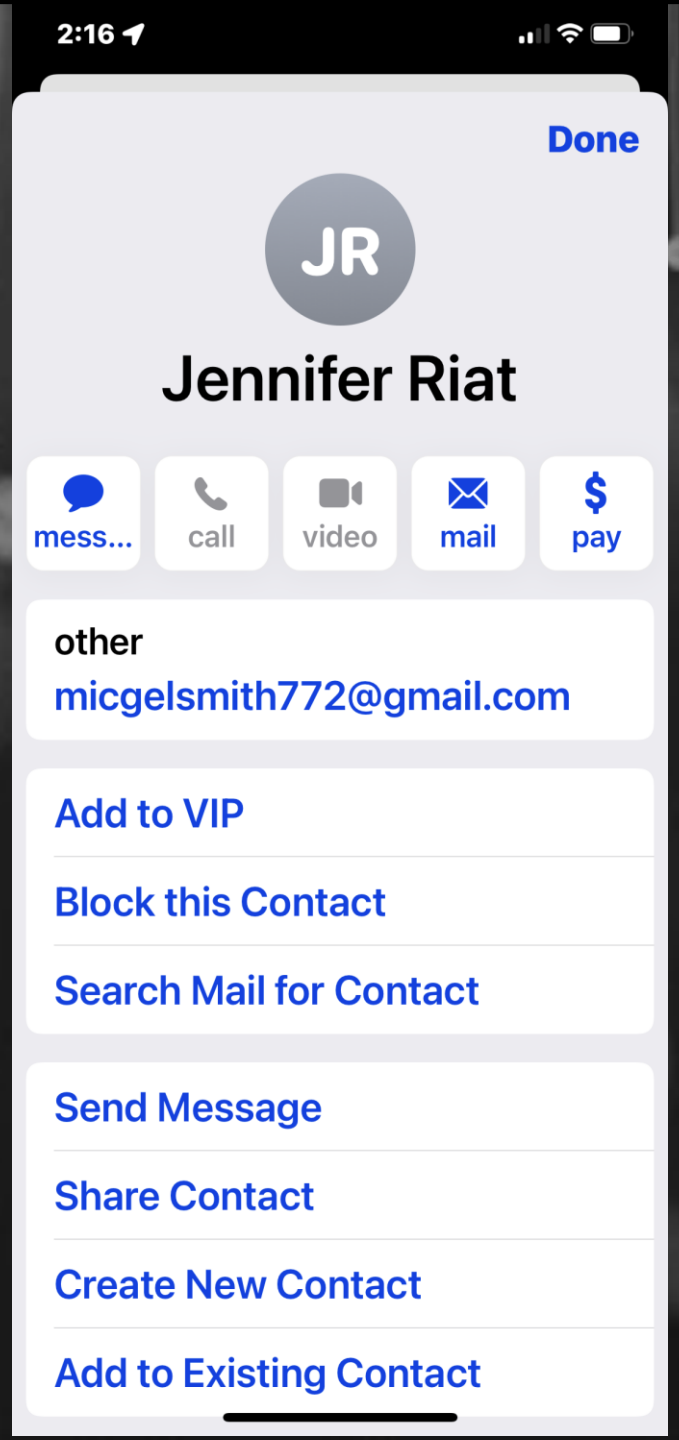
Sincerely,
Janice Robinson
Customer Relation Head
#custom7

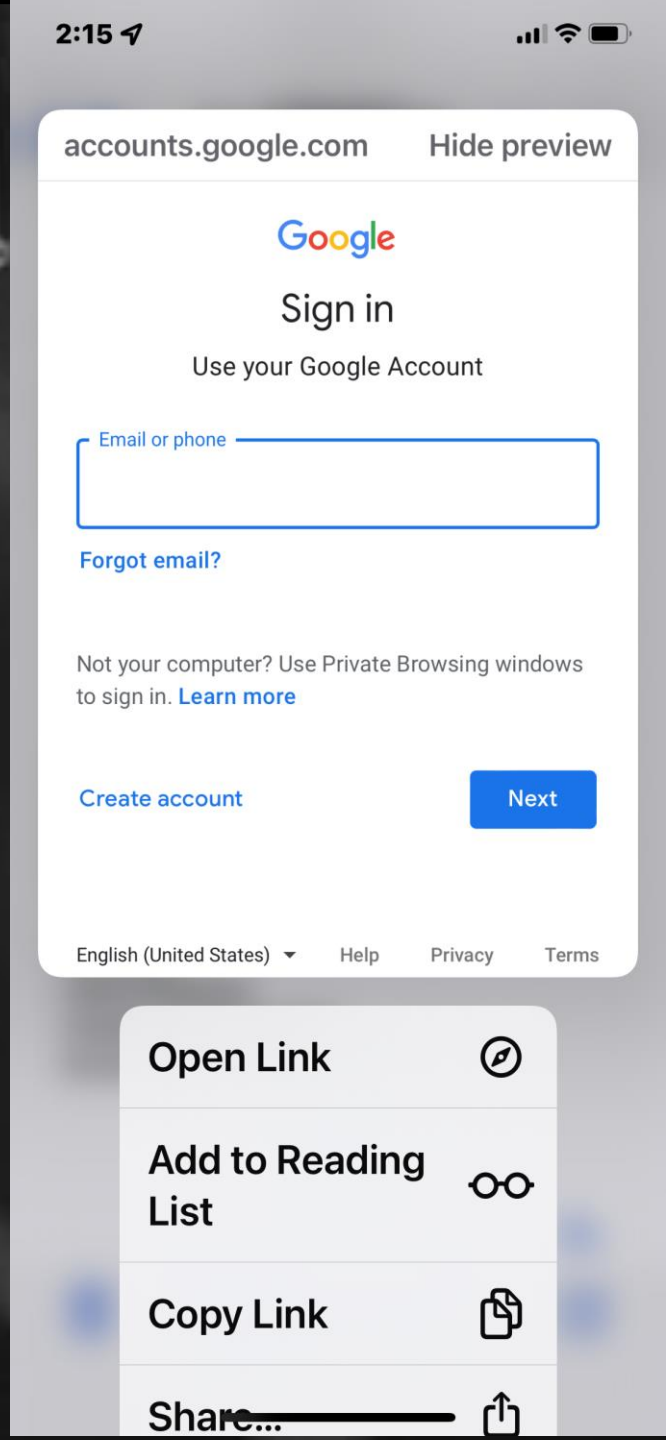
Unsubscribe

Hey wait…This came from my wife?

- Her name is spelled wrong

Unsubscribe is a Google Form?





Dialing Instructions

Call PayPal Customer Service and enter this one-time passcode when prompted.

The code below takes you directly to the experts you need.

Enter one-time passcode for quicker service

344122

This one-time passcode expires after ten minutes.

1-888-221-1161

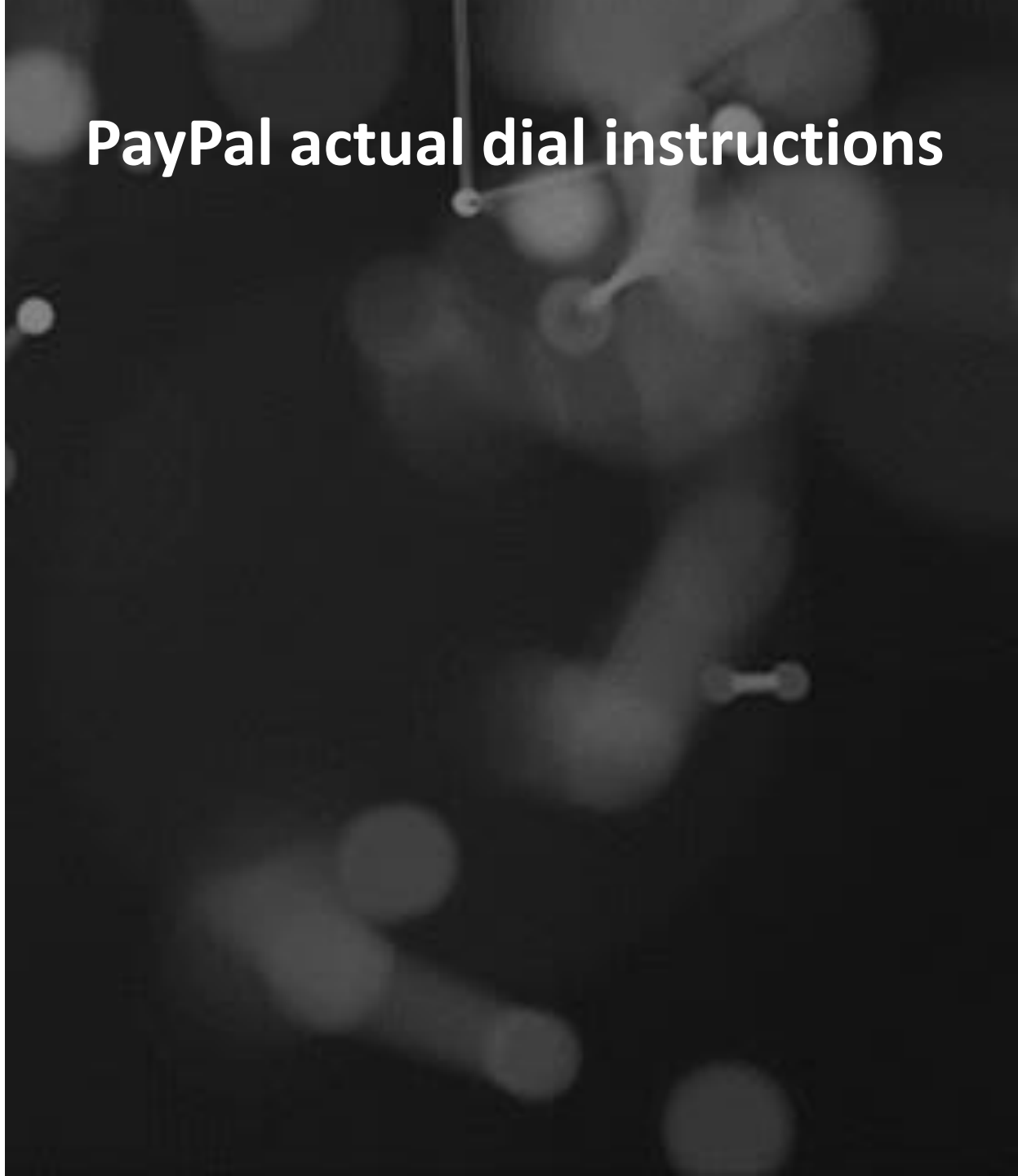
Customer Service Hours

6:00 AM PT to 6:00 PM PT Monday through Sunday

Message us instead
It's like texting, send us a note!

1-402-935-2050 (if calling from outside the U.S.)

Para atenderle en español por favor marque 1-888-914-8072



877- 844- 558
Link.att.com/inquiry
fraud

AT&T

PO BOX 5093
CAROL STREAM IL 60197-5093

03/09/2022

STEPHEN RIAT
[redacted]
HAYS, KS 67601

Re: 276041891605
Order/ Reference Number: 203087069372

Dear STEPHEN RIAT:

Thank you for applying for AT&T communications or entertainment services/products.

As of 03/08/2022, your AT&T credit score was: .

AT&T utilizes a proprietary credit rating system that creates a score based on information derived from your credit history as supplied by the consumer reporting agency listed below. Your AT&T credit score is unique to AT&T and is not related to scores commonly supplied by credit reporting agencies. Your credit score can change and credit scores range from 001 to 999. The credit score values are established based upon comparative analyses of repayment histories of large numbers of customers.

Key factors affecting your AT&T credit score include:

- No factors were provided by consumer reporting agency

Based in part on an assessment of your AT&T credit score and/or being a new customer to AT&T, we imposed certain conditions or restrictions on your service request, which may have included:

- Limiting and/or denying the purchase of products and /or services
- Requiring a down payment on equipment or products purchased on installment
- Requiring an advance payment or other payment prior to establishing services
- Requiring a nonrefundable fee

In making our decision, we received information from the credit bureau listed below. The credit bureau did not make the above decision and is unable to provide you the specific reasons for the above decision.

ORDER RECAP FOR STEPHEN RIAT

03/08/2022

This is an overview of your Customer Service Summary that follows. See full summary for important details.

Here's what we helped you with today

NEW

Reserved Wireless line : 785.432.6551

Here's why your next bill will be different than the rest

Your estimated next bill will be	Your estimated ongoing bills will be
$145.60	**$135.40**/mo

Promotions and discounts may not show up here but will show on your bill within the time promised.
After promotions end, monthly charges will increase. Pricing subject to change.

Your next bill will include:

- Since you made a change to **Wireless** service today, we include **3 days of partial monthly charges:** $10.20
  (March 08 - March 10)
- Your **ongoing monthly charges**, including AT&T Fees and Surcharges: **$135.40**
  (March 11 - April 10)

Hello STEPHEN RIAT,

Your profile for the account number ending in 1605 has been updated with changes made recently.

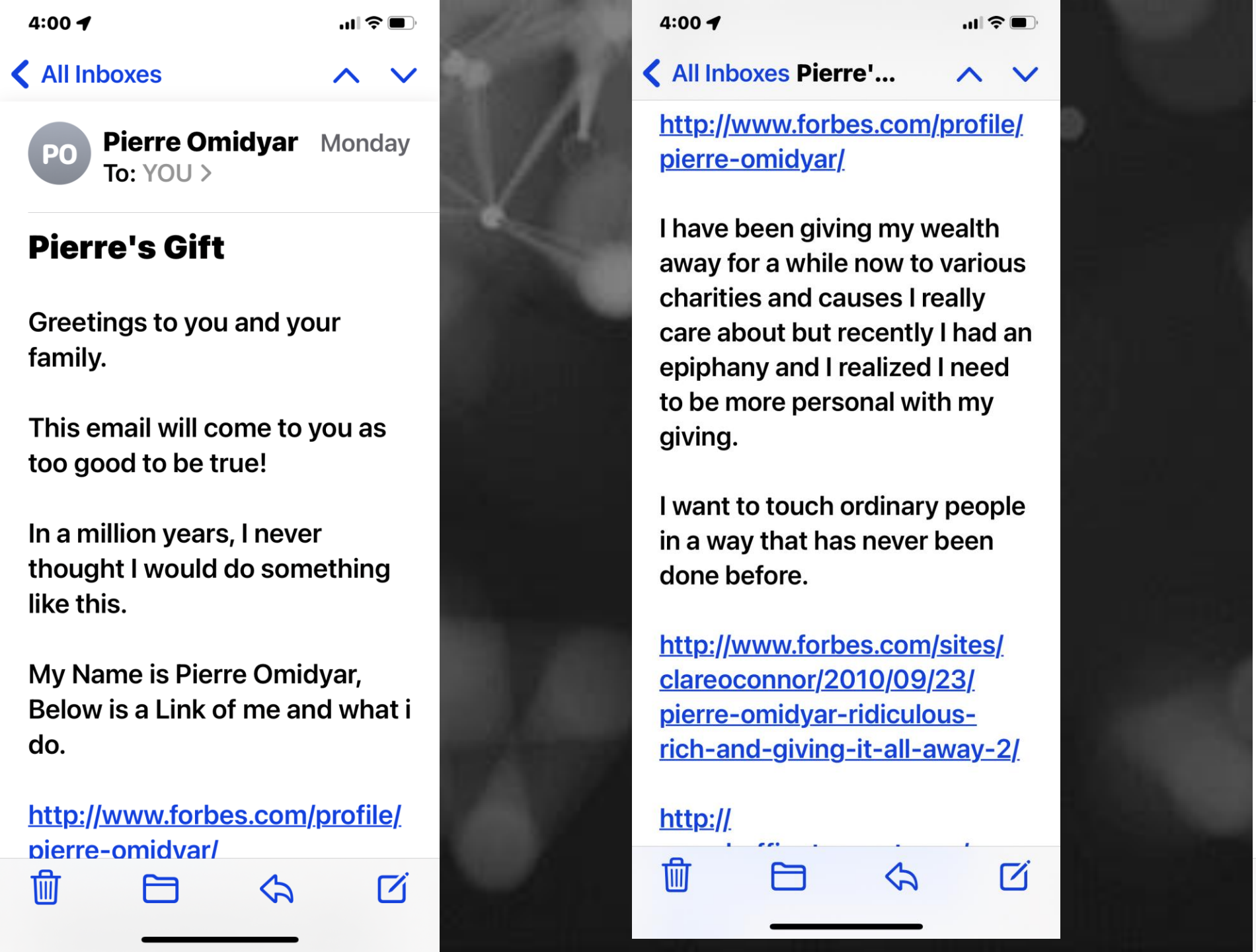
- Start Paperless Billing

If you or your authorized user made these changes, you don't have to do anything else. If you didn't make these changes, please call us at 800.331.0500 or dial 611 from your wireless phone.

Thank you for choosing us,

AT&T

This is just lazy



4:00

All Inboxes

PO **Pierre Omidyar** Monday
To: YOU >

Pierre's Gift

Greetings to you and your family.

This email will come to you as too good to be true!

In a million years, I never thought I would do something like this.

My Name is Pierre Omidyar, Below is a Link of me and what i do.

http://www.forbes.com/profile/pierre-omidyar/

4:00

All Inboxes **Pierre'...**

http://www.forbes.com/profile/pierre-omidyar/

I have been giving my wealth away for a while now to various charities and causes I really care about but recently I had an epiphany and I realized I need to be more personal with my giving.

I want to touch ordinary people in a way that has never been done before.

http://www.forbes.com/sites/clareoconnor/2010/09/23/pierre-omidyar-ridiculous-rich-and-giving-it-all-away-2/

http://

4:00

All Inboxes **Pierre'...**

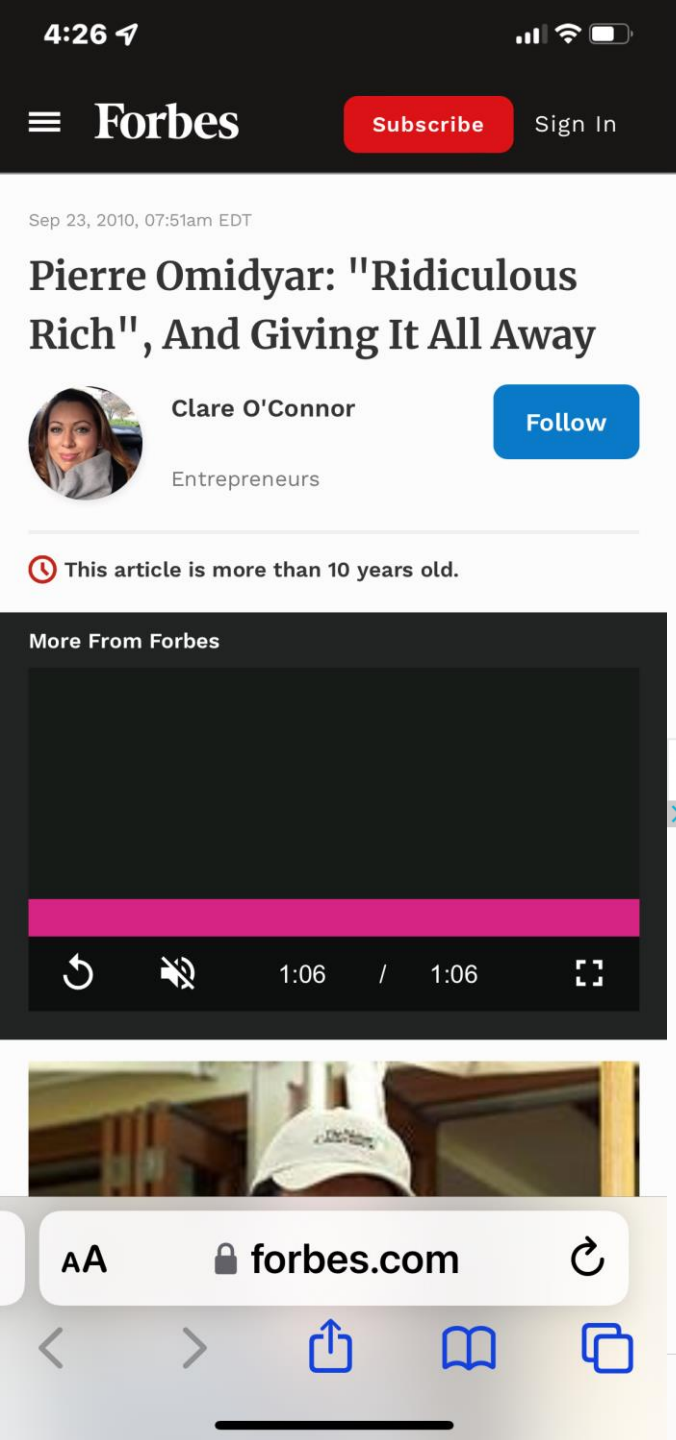
So I decided I was going to contact 20 people via their email address which I paid for from a Marketing Firm.

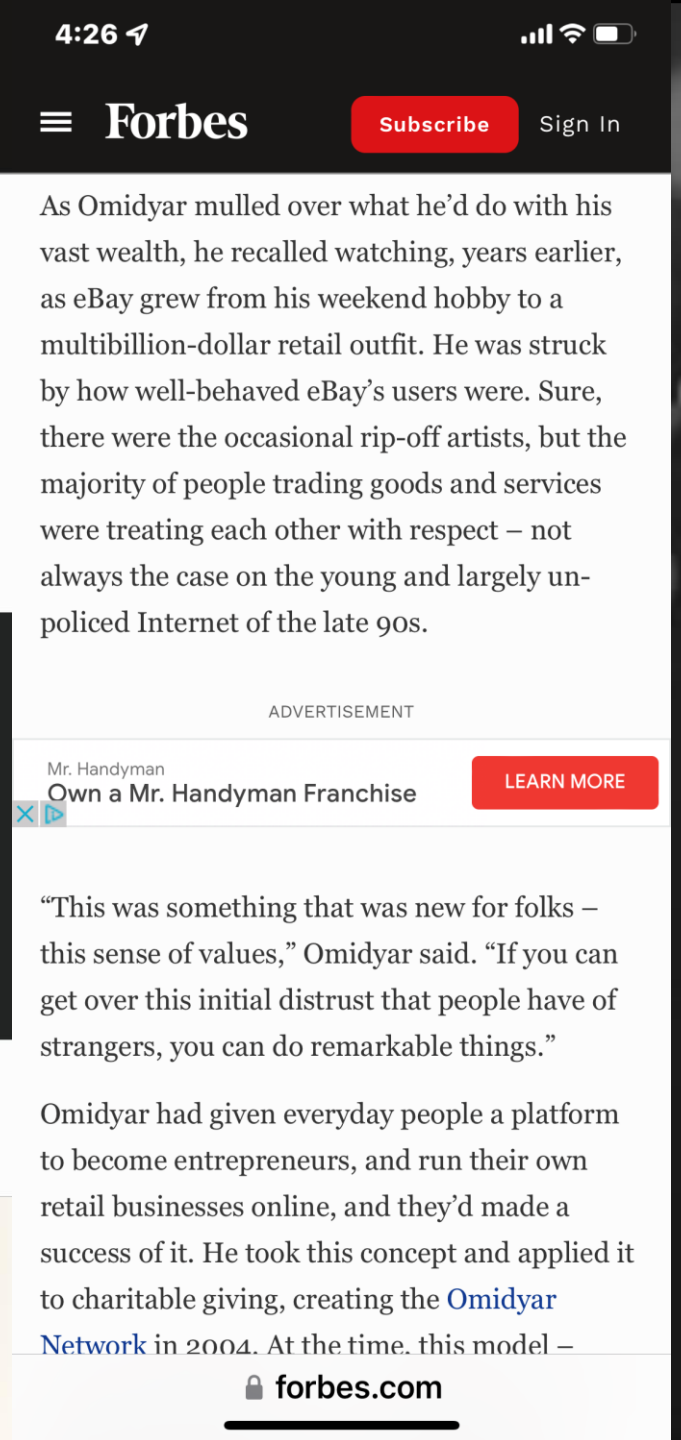
If you receive this email, I am giving you $1.9 Million.

Thinking about it again, I must be crazy to do something like this but crazy is what made me who I am today so lets go for it!

All you have to do is reply to this email with your full names and you will be paid $1.9 Million.

This is my personal journey to self-fulfilment, I hope you accept this special gift from me





Pierre is a real person!

Article is from Forbs (OK in 2010 but when you have so much to give away it takes a while right?)

BUT

Pretty sure his Entrepreneur Platform isn't "Giving it to Steve"

AA datadrivendota.com

All Products |... | Amazon.com:... | Disbursement... | Help: Help & C... | Bread machin... | 沙龙国际sa36-... | 1997 - 1998 F...

English | $ Usd | My Account

e SHOP

Enter Your Keyword...

Shopping Cart($125)

Home | Login | Cart | Checkout | Contact Us

Free Shipping

Money Back !

Free Home Deli...

Free Gift Service

Featured Products

Email Address

The Unsubscribe

1:57

4

A

From: **Automated**
To: Steve Riat
Today at 1:48 PM

REQUEST: Password almost completed-21420

Office

The password for your email (sriat@nex-tech.com) expires - today, you can change or keep the same password.

Keep Same Password

Nex-tech.com

1:57

Done

A

Automated

mess... call video mail pay

other
dabbi.piccio@geffenrealestat...

Add to VIP

Block this Contact

Search Mail for Contact

Send Message

Share Contact

Create New Contact

Add to Existing Contact

Dabbi Piccio

Real Estate Agent from Los Angeles Area

Message ···

Lives in Los Angeles, California

Dabbi Piccio

Real Estate Agent at Geffen Real Estate

Los Angeles, California, United States · Contact info

500+ connections

Connect | Message | More

Real Estate Agent
Geffen Real Estate
Apr 2019 - Present · 3 yrs
Beverly Hills, CA

Independent Business Contractor
American Red Cross
Apr 2014 - Feb 2019 · 4 yrs 11 mos
Pomona, CA

Distribution of Blood Supplies all over Southern California Hospitals

Office Manager
State Farm ®
Jun 2005 - Mar 2014 · 8 yrs 10 mos
Los Alamitos, CA and Palmyra, PA

Insurance Sales and Service

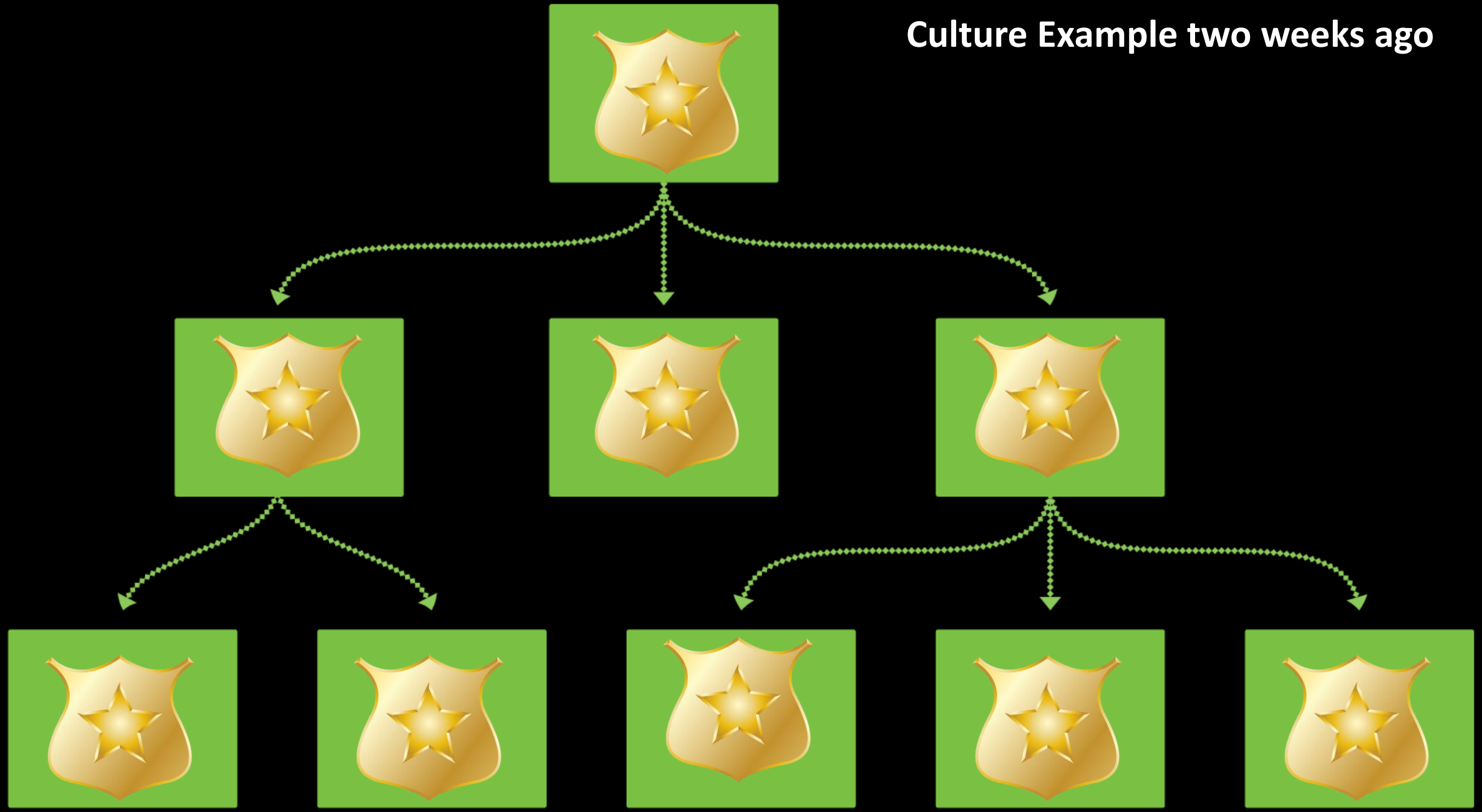
Restaurant General Manager
Boston Market
Feb 1998 - May 2005 · 7 yrs 4 mos
Harrisburg, Pennsylvania Area

What have we been doing?

KnowBe4

Human error. Conquered.

Culture Example two weeks ago



According to a study by IBM, human error is the main cause of 95% of cybersecurity breaches. In other words, if human error was somehow eliminated entirely, 19 out of 20 cyber breaches may not have taken place at all!

95% OF CYBERSECURITY BREACHES ARE DUE TO HUMAN ERROR

Cyber-criminals and hackers will infiltrate your company through your weakest link, which is almost never in the IT department.

World Economic Forum annual Global Risks Report 2022

“81% of hacking-related breaches leveraged either stolen and/or weak passwords.”

Version Data Breach Investigation Report

Passwords – One of the most basic Cybersecurity items?

Yet, still ignored and argued over frequently.

For nearly 20 years, the launch code for US nuclear missiles was 00000000

*According to a recently published paper about Permissive Action Links (PALs) – small security devices that prevent setting off nuclear weapons without the right code and the right authority – the “secret unlock” code for all US Minuteman nuclear missiles for almost 20 years during the Cold War was set to the jaw-droppingly simple code of eight zeros: 00000000.

Someone created a computer capable of guessing 350 billion passwords per second.

The system uses 5 servers, which makes use of 25 AMD Radeon graphic cards to come up with this many guesses per second.

The system has made it entirely possible to guess an 8-character password in significantly lesser time. It will take it only 5.5 hours to go through all the possible 8-character options, including numbers, upper- and lower-case characters, and symbols.

(Source: Ars Technica)

Rainbow Crack
John the Ripper
Aircrack – ng
L0phtCrack
Ophcrack
Hashcat
DaveGrohl
Ncrack
THC Hydra

Brute Force Tools

Sometimes we don’t use common sense?

How do I know?


DoorCode: 63526
DoorCode: 63526


Lost
Set of House Keys
· black automatic car door opener
· front & back house keys
· silver safe key
If found please return to:
456 Linden Ave, #1A
Brooklyn NY 11233
I'm usually home after 5pm. Thank you!

People are three times more likely to use their pet's name as password rather than that of a family member.

Pets often become dearer to us than our human family members. The unconditional love people receive from their pets shows up in their password practices, as well. There is three times more probability of someone using the name of their pet as a password and not a family member.

It is needless to mention that it will not make up for a strong password. Someone can easily predict your password if they have an idea of how much you love your pet.

(Source: Facebook)


IT MAY SEEM RUDE
BUT FOR SECURITY
REASONS
PLEASE DO NOT
OPEN THE DOOR
TO STRANGERS


Come a little closer

LAPSUS$ Data Extortion Group

/r/verizon / u / oklaqq 11/24/2021, 8:16:40 PM

Earning opportunity for a mobile carrier employee ~ $20000+

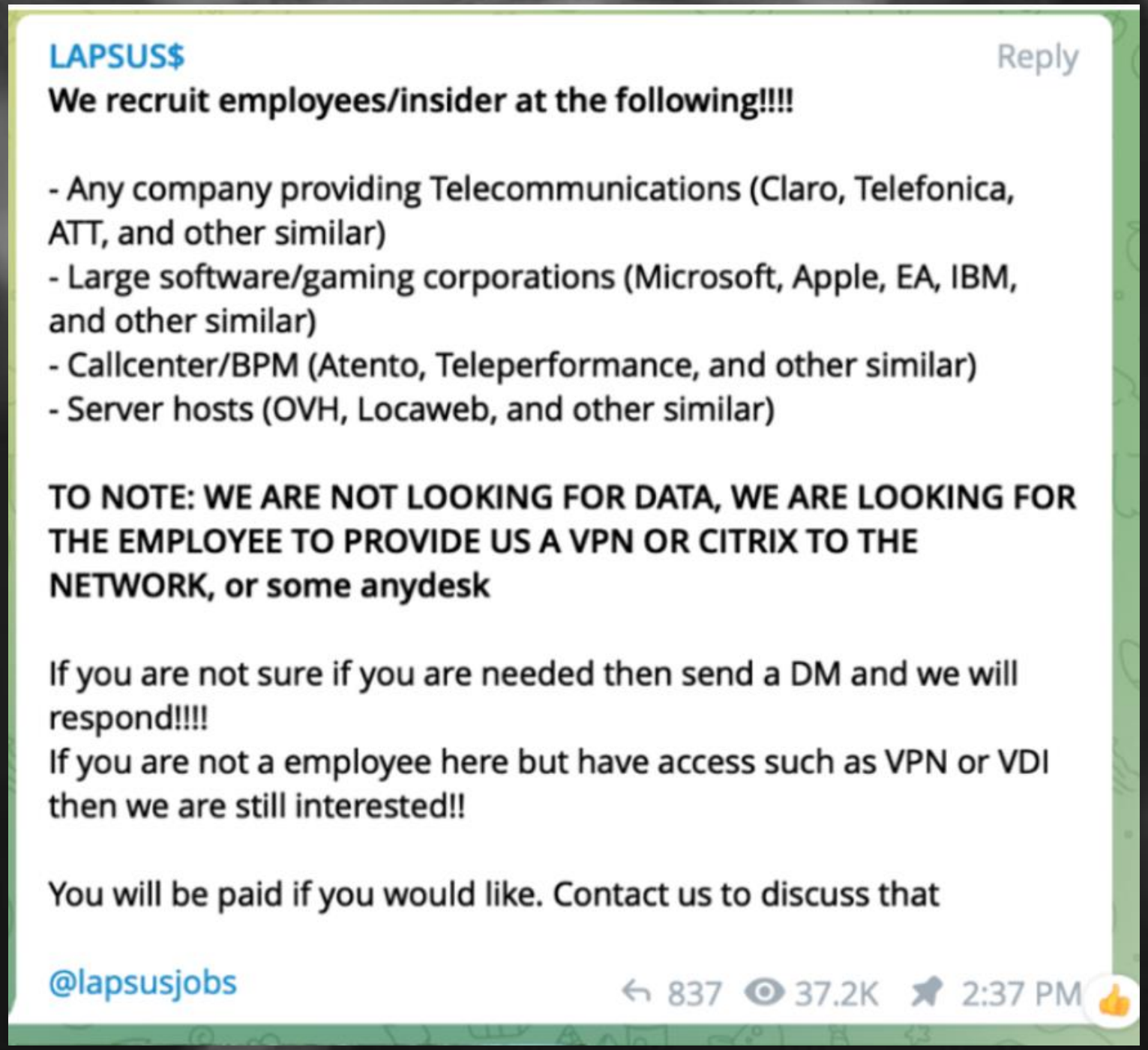
My name is Alex.

I am looking for insiders/employees at either ATT, Verizon or T-Mobile

I can offer you upwards of $20000 a week to do some *inside jobs* at either ATT, Verizon or T-Mobile for me. - these tasks are low risk for you and me..... plus you will get paid insanely well by me. - the jobs will involve Sim-Swapping 1 or 2 customers a week.... you won't even be noticed!!!

You can contact me on Telegram, my username is whitedoxbin https://t.me/whitedoxbin

https://telegram.org/ we can discuss further on Telegram or email. If you are interested. This is a great opportunity for me and you!



SIM-SWAPPING PAST SECURITY

Microsoft said LAPSUS$ also has used "SIM swapping" to gain access to key accounts at target organizations. In a fraudulent SIM swap, the attackers bribe or trick mobile company employees into transferring a target's mobile phone number to their device.

"DEV-0537 advertised that they wanted to buy credentials for their targets to entice employees or contractors to take part in its operation. For a fee, the willing accomplice must provide their credentials and approve the MFA prompt or have the user install AnyDesk or other remote management software on a corporate workstation allowing the actor to take control of an authenticated system. Such a tactic was just one of the ways DEV-0537 took advantage of the security access and business relationships their target organizations have with their service providers and supply chains."

*DEV-0537 is LAPSU$$

Source: Krebsonsecurity.com

From Microsoft

Okta

Management Company

Okta, Inc. is a publicly traded identity and access management company based in San Francisco. It provides cloud software that helps companies manage and secure user authentication into applications, ...

okta.com

Stock price OKTA (NASDAQ) 158.01 USD ▲ +8.15 (5.44%)

Founded 2009

Revenue $1.30 billion (2022)

Headquarters San Francisco

Sykes Enterprises

Organization

Sykes Enterprises, Inc., stylized as SYKES, is an American multinational business process outsourcing provider headquartered in Tampa, Florida. The company provides business process outsourcing servic...

sykes.com

Stock price SYKE (NASDAQ) 54 USD ▲ +0.02 (0.04%)

Founded 1977

Revenue $1.71 billion (2020)

Headquarters Tampa, United States

CEO Charles E Sykes (Since 2009)

Lapsus$ found a spreadsheet of passwords as they breached Okta, documents show

The Lapsus$ hackers used compromised credentials to break into the network of customer service giant...

By Zack Whittaker | 24 hours ago

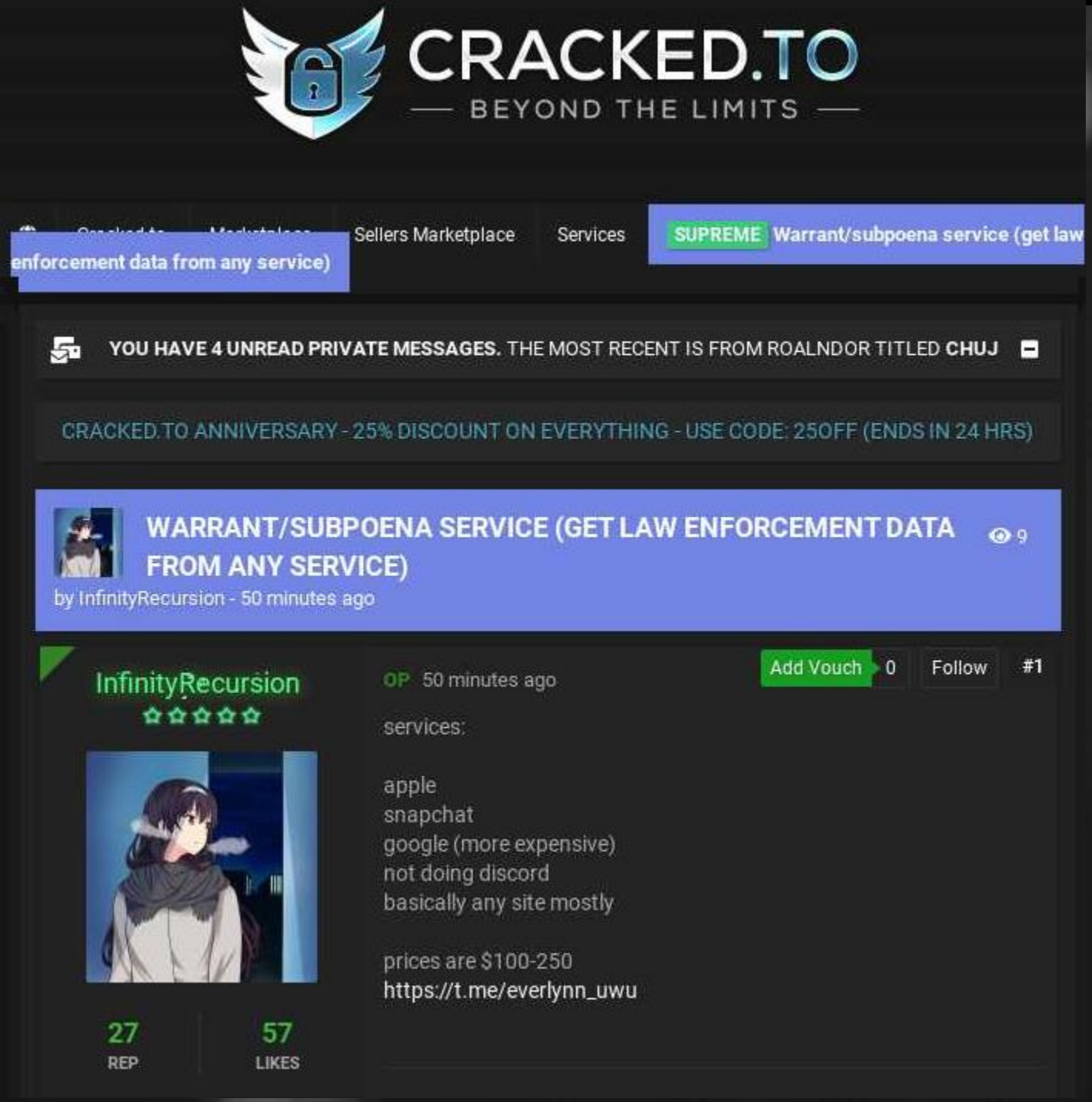
Source: TechCrunch.com

Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests"

March 29, 2022 10 Comments

There is a terrifying and highly effective "method" that criminal hackers are now using to harvest sensitive customer data from Internet service providers, phone companies and social media firms. It involves compromising email accounts and websites tied to police departments and government agencies, and then sending unauthorized demands for subscriber data while claiming the information being requested can't wait for a court order because it relates to an urgent matter of life and death.

Source: Krebsonsecurity.com



The founder of the Recursion Team was a then 14-year-old from the United Kingdom who used the handle “**Everlynn**.” On April 5, 2021, Everlynn posted a new sales thread to the cybercrime forum cracked[.]to titled, “Warrant/subpoena service (get law enforcement data from any service).” The price: $100 to $250 per request.

Researchers from security firms Unit 221B and Palo Alto Networks say that prior to launching LAPSUS$, the group's leader "White" (a.k.a. "WhiteDoxbin," "Oklaqq") was a founding member of a cybercriminal group calling itself the "Recursion Team."

Roblox

Game

Roblox is an online game platform and game creation system developed by Roblox Corporation that allows users to program games and play games created by other users. Created by David Baszucki and Erik ...

Release date Sep 01, 2006

Developer Roblox Corporation

Genre Massively multiplayer online game

CEO David Baszucki (Since 2005)

Platforms Android · Microsoft Windows · iOS · OS X · ... +

Roblox is poised to unlock a large global audience. It's already played by English-speaking kids in **over 40 countries** worldwide.

Dynablocks was the official name for Roblox in 2003. As Dynoblocks is tough to pronounce, they renamed it to Roblox.

We do so well following instructions!

If that isn't hard enough the people trying to communicate?

CAN YOU FOLLOW DIRECTIONS?

This is a timed test--you have 3 minutes only!

1. Read everything carefully before doing anything.
2. Put your name in the upper right-hand corner of this paper.
3. Loudly call out your first name.
4. Circle the word NAME in sentence two.
5. If you have followed directions carefully to this point, call out "I have."
6. Draw five small squares in the upper left-hand corner.
7. Put an "X" in each square.
8. In your normal speaking voice, count from ten to one backwards.
9. Put a circle around each square.
10. Sign your name under the title of this paper.
11. After the title write, "Yes, yes, yes."
12. Put a circle completely around the sentence number seven.
13. When you reach this point, LOUDLY call out, "I AM THE LEADER IN FOLLOWING DIRECTIONS."
14. Put an "X" in the lower left-hand corner of this paper.
15. Draw a triangle around the "X" you just put down.
16. On the back of this paper, multiply 703 by 66.
17. Loudly call out, "I AM NEARLY FINISHED. I HAVE FOLLOWED DIRECTIONS."
18. Draw a rectangle around the word "corner" in sentence six.
19. On the reverse side of this paper, add 8950 and 9805.
20. Put a circle around your answer, and put a square around the circle.
21. Punch three small holes in the top of this paper with your pencil point.
22. Underline all even numbers on the left side of this paper.
23. Now that you have finished reading everything carefully, do only sentences one and two!


DANGER
DUE TO
DANGER


MAXIMUM SECURITY ENTRANCE


DO NOT
BREATHE
UNDER
THE
WATER


STOP
THIS IS A
STOP SIGN


This product
contains
peanuts.


CAUTION
Do Not
Drink
This Water

Passwords

20% of password reset questions can be guessed on the first try

40% of people can’t remember their own answers

60% of answers can be found on social media

Kevin Mitnick

91% of people know that password recycling poses huge security risks, yet 59% continue to use the same password everywhere. Therefore, if a hacker was to crack one password, they would be able to gain access to all other accounts!

Source: Tech.co

Cybercriminal group Darkside gained entry to America's largest fuel pipeline, Colonial Pipeline, via a compromised password posted on the Dark Web.

Solar Winds – solarwinds123
JBS (Meat Packing Plant) (Compromised credential)
NEW Cooperative – chicken1
Colonial Pipeline (Shared Password)

Password Hygiene and MFA Could Have Stopped These Attacks

While these attacks were all devastating, they (along with 2020's SolarWinds attack) also share another commonality: They could have been prevented with better password hygiene and multi-factor authentication.

In late 2020, roughly 18,000 of SolarWinds' customers received SolarWinds software infected with malicious code. In a congressional investigation, it was revealed that the use of the password "solarwinds123" might have contributed to the breach.

In the case of JBS, a government investigation revealed that a weak password on an old administrator account gave cybercriminals access to the network.

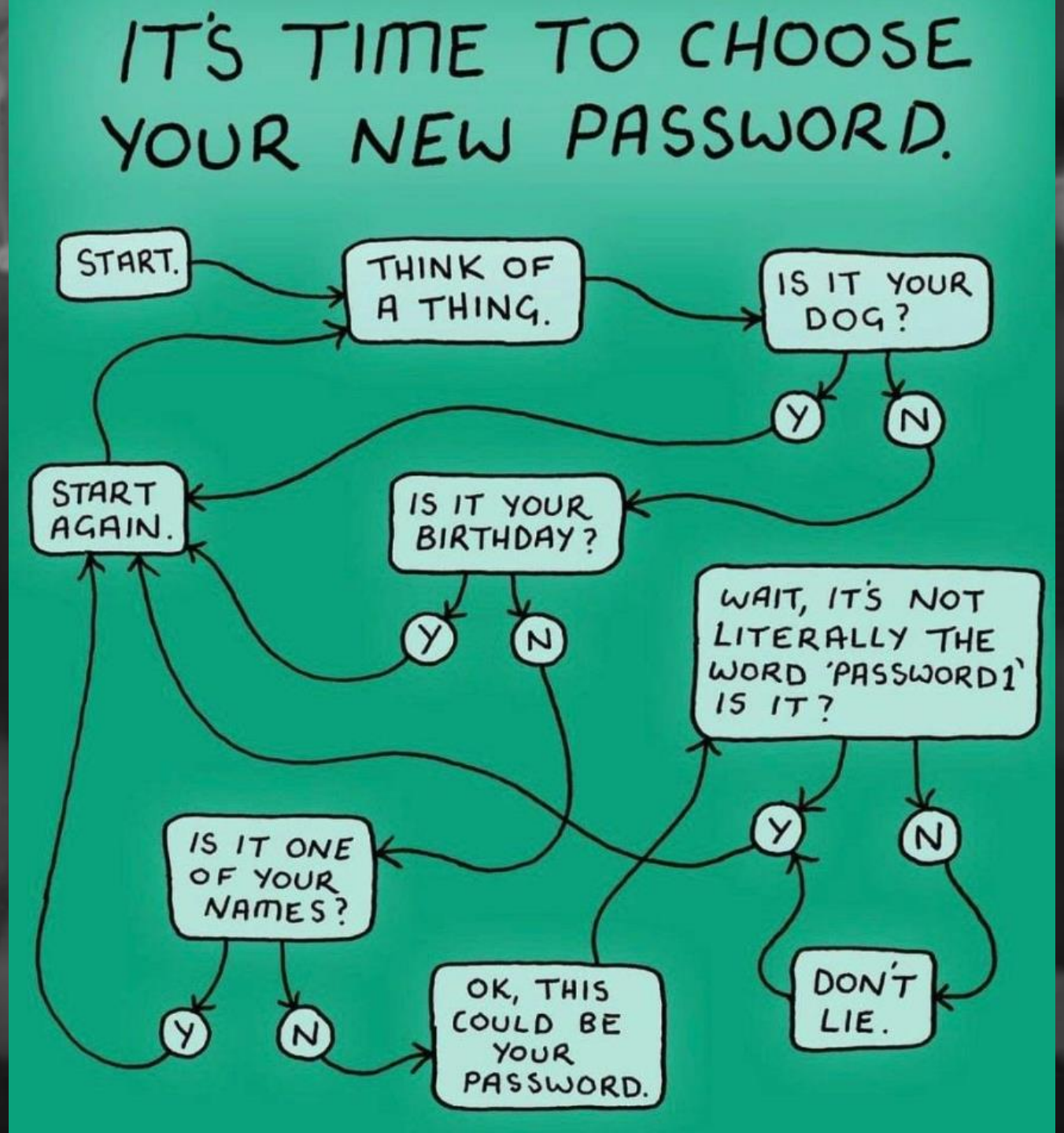
The Colonial Pipeline breach could almost certainly have been prevented with the use of two-factor authentication.

For NEW Cooperative, the reuse of a weak password — "chicken1" — on at least 10 different accounts across the company's 120 employees resulted in one of two outcomes: either an employee reused this password on an unrelated site that was breached and leaked to the Dark Web, or the use of brute-force attacks allowed the password to be easily guessed.

While cyberdefense has become more sophisticated and specialized over time, in some cases the simplest prevention is still some of the best.

A person usually changes the password every 2.5 to 3 years

(Source: Resource Techniques)


IT'S TIME TO CHOOSE YOUR NEW PASSWORD.
START.
THINK OF A THING.
IS IT YOUR DOG?
Y
N
START AGAIN.
IS IT YOUR BIRTHDAY?
Y
N
WAIT, IT'S NOT LITERALLY THE WORD 'PASSWORD1' IS IT?
Y
N
IS IT ONE OF YOUR NAMES?
Y
N
OK, THIS COULD BE YOUR PASSWORD.
DON'T LIE.

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

› Learn about our methodology at hivesystems.io/password

Compromised passwords are responsible for 81% of hacking-related breaches

Source: Verizon Data Breach Investigations Report.

66% of people use only 1 or 2 passwords for all their accounts

40% of organizations store passwords in a Word document or a spreadsheet

2020, the average number of accounts per user is 207

Fintech Startup Offers $500 for Payroll Passwords

May 10, 2021 38 Comments

How much is your payroll data worth? Probably a lot more than you think. One financial startup that's targeting the gig worker market is offering up to $500 to anyone willing to hand over the payroll account username and password given to them by their employer, plus a regular payment for each month afterwards in which those credentials still work.

The average person reuses each password as many as 14 times.

Microsoft recently announced that a staggering 44 million accounts were vulnerable to account takeover due to compromised or stolen passwords.

73% of users duplicate their passwords in both their personal and work accounts.

The Hidden Cost of Ransomware: Wholesale Password Theft

January 6, 2020 40 Comments

Organizations in the throes of cleaning up after a ransomware outbreak typically will change passwords for all user accounts that have access to any email systems, servers and desktop workstations within their network. But all too often, ransomware victims fail to grasp that the crooks behind these attacks can and frequently do siphon every single password stored on each infected endpoint. The result of this oversight may offer attackers a way back into the affected organization, access to financial and healthcare accounts, or — worse yet — key tools for attacking the victim's various business partners and clients.

It seems the younger generation doesn’t pay much attention to password security.

A survey said that 76% of the people aged between 18 to 24 years are likely to reuse a password. It was the highest percentage for any age group.

The same fraction for people aged above 65 years was 62%. The stat is surprising in many ways since one expects the younger tech-savvy generation to be more careful about their online security.

Source: Digital Guardian

90% of passwords can be cracked in less than 6 hours

Think you have a strong password? Think again…

Hackers are continuing to become more sophisticated and have a variety of ways in which they can crack your passwords to gain access to your online accounts. One way to help keep secure is to understand the methods they use, here are four:

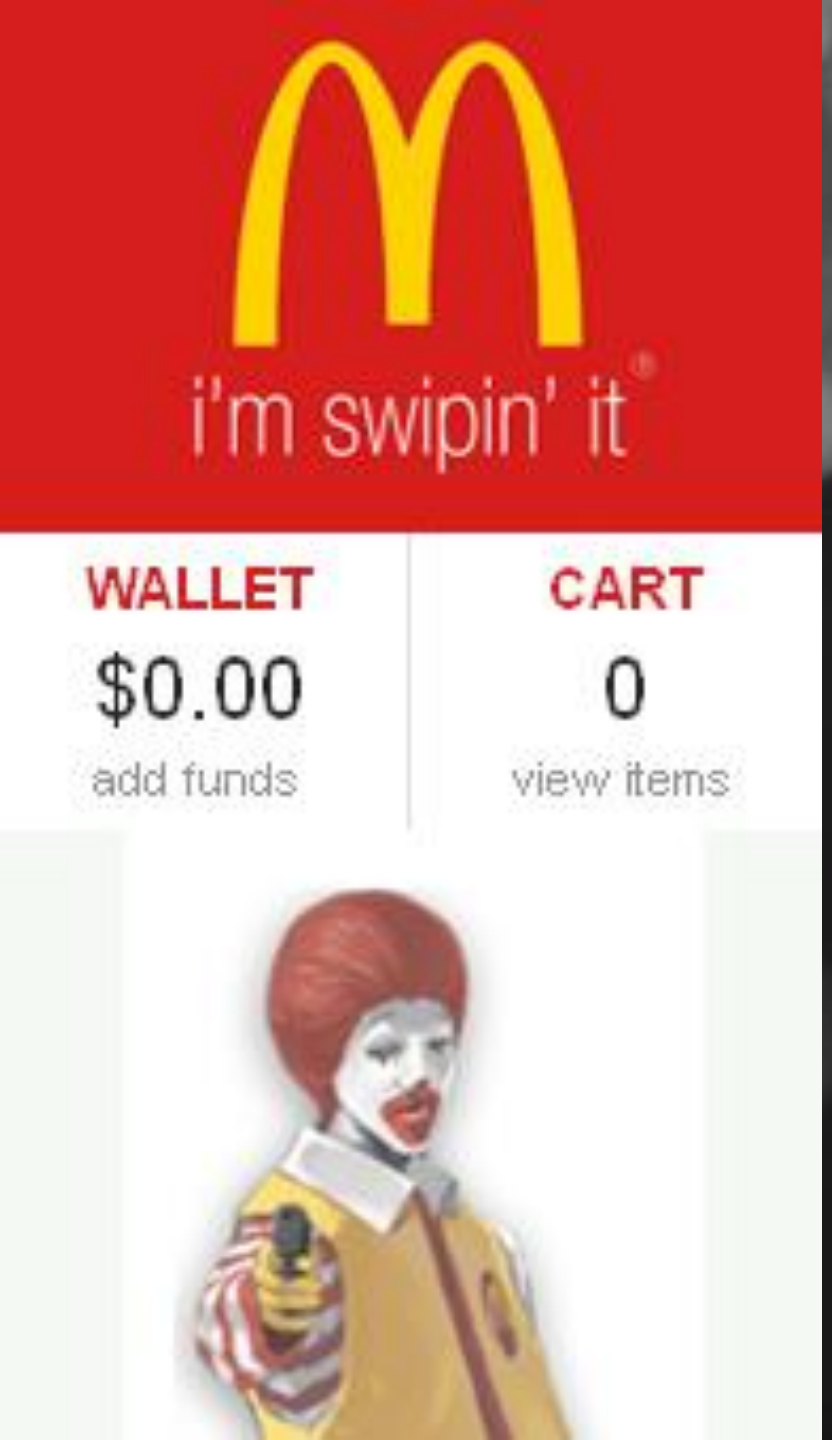
1. **Dictionary attack** – A dictionary attack is a method that systematically enters words that can be found in a dictionary. Hence, the name. The only reasons this kind of attack works is because users are remaining to rely on easy-to-guess words for their passwords.
2. **Brute-Force attack** – A brute-force attack is when hackers have a software that tries to guess every possible combination until it hits yours. They often begin with the most commonly used passwords first and then move onto more complicated phrases.
3. **Credential stuffing** – Credential stuffing proves the dangers of re-using usernames and passwords for numerous accounts. It works where credentials obtained from a data breach on one platform are used to attempt log ins on other platforms.
4. **Social engineering** – Phishing has remained on of the top social engineering methods used by hackers to crack passwords. They do this by appearing as a trusted source and concoct a scenario for handing over login credentials or other sensitive personal data.

Source:Info Security Group

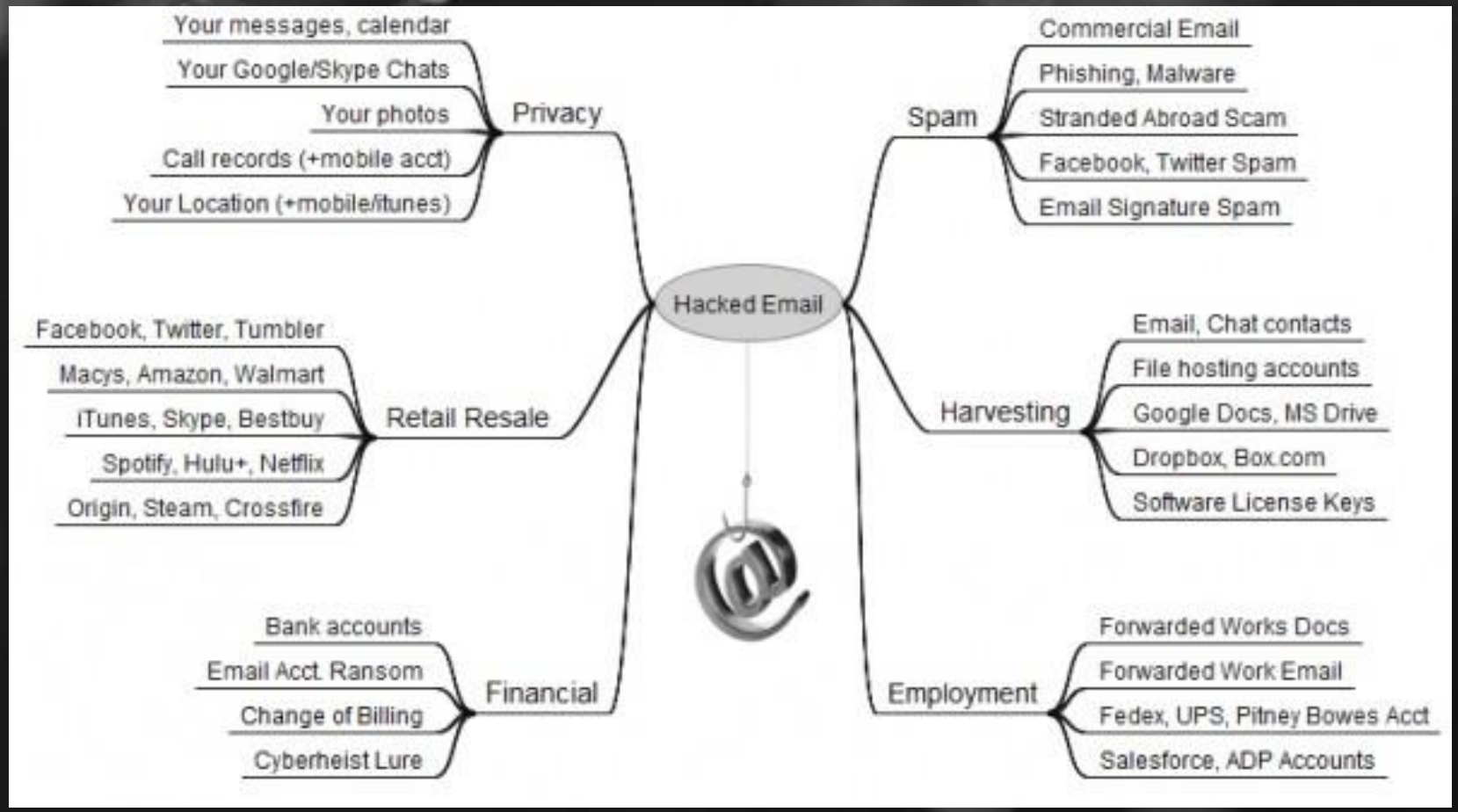
Cybercrime is the greatest threat to every company in the world.

Last year, Ginni Rometty, IBM's chairman, president and CEO, said: **"Cybercrime is the greatest threat to every company in the world."** And she was right. During the next five years, cybercrime might become the greatest threat to every person, place and thing in the world. With evolving technology comes evolving hackers, and we are behind in security.

Understanding the cyber terminology, threats and opportunities is critical for every person in every business across all industries.



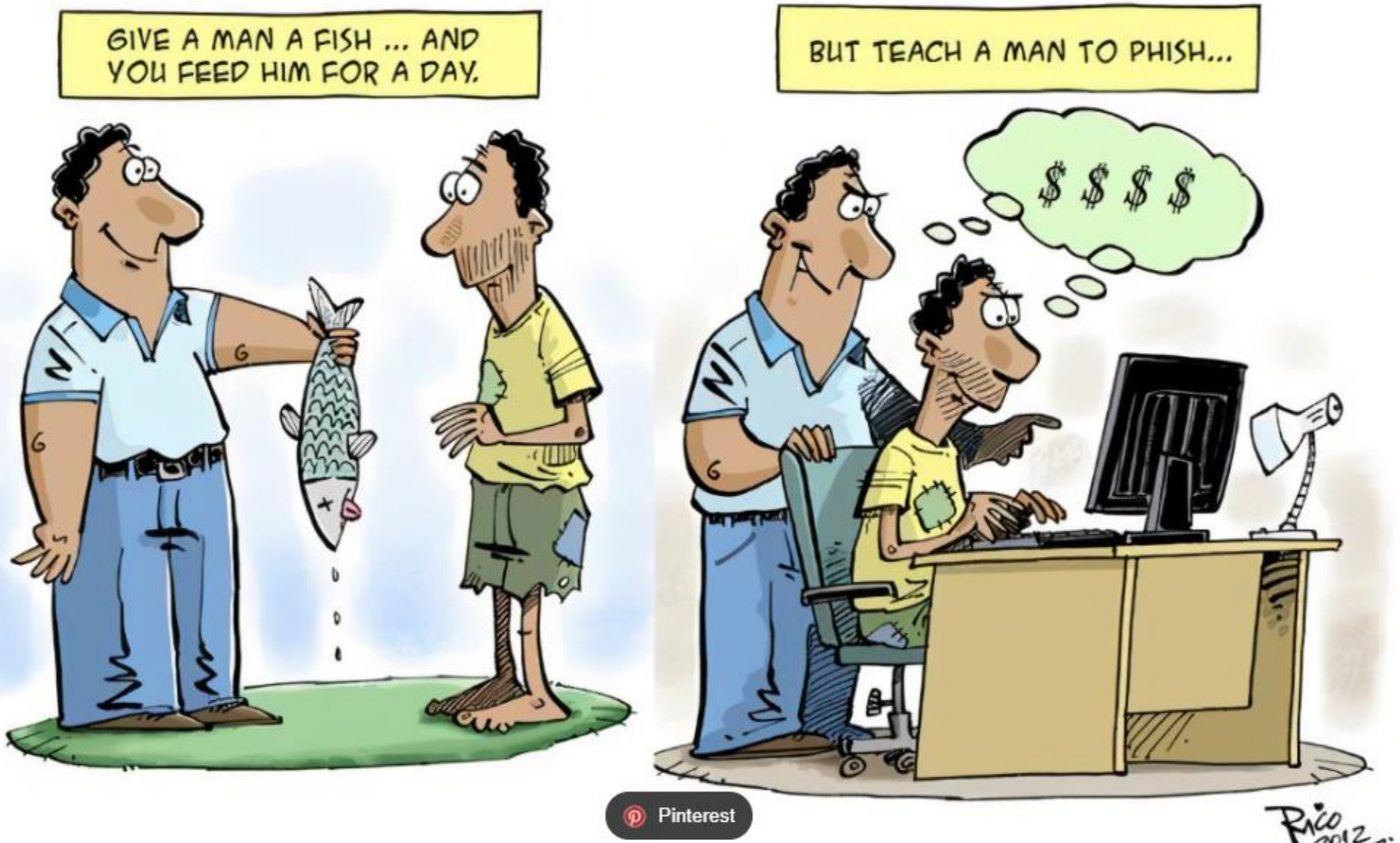
The Tor network had more than 2.2 million users in 2017.
(Source: Europol)
The dark web hosted almost 60,000 unique onion domains,
and around 57% of them hosted illegal content.



Source – Krebs on Security

FUNNY BUSINESS

BY RICO



Phishing Goes Old School

Over the past several years, we've observed numerous phishing emails imitating correspondence from Amazon or medical authorities. But in 2021, the FIN7 group, responsible for the BlackMatter and Darkside ransomware operations, decided to carry out a version of these campaigns the old-fashioned way.

According to an FBI alert, starting in August, this group used UPS and USPS to snail-mail ransomware to U.S. businesses in the insurance, transportation and defense industries.

Targets received one of two packages: One, purportedly from Amazon, arrived in a gift box accompanied by a thank-you letter, a fake gift card and a USB drive. The other, disguised as a package from the U.S. Department of Health and Human Services, included a page of guidance regarding COVID-19 and a USB drive.

If plugged in, these drives — which are loaded with "BadUSB" attacks — are able to register themselves as keyboards, emulate keystrokes, execute commands and install malware, ultimately creating an entry point for ransomware, commonly BlackMatter or REvil.

THE VERGE TWITTER FACEBOOK

HACKERS SET UP A NETWORK OF TWITTER ACCOUNTS AND A CYBERSECURITY BLOG

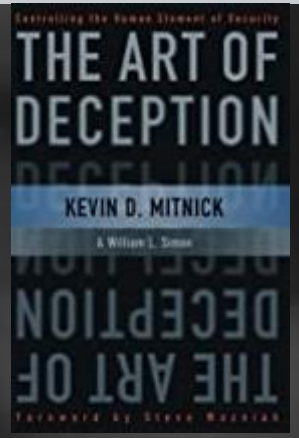
According to Google, the hackers set up a cybersecurity blog and series of Twitter accounts in an apparent attempt to build and amplify credibility while interacting with potential targets. The blog focused on writing up vulnerabilities that were already public. Meanwhile, the Twitter accounts posted links to the blog, as well as other alleged exploits. At least one of the purported exploits was faked, according to Google. The search giant cites several cases of researchers' machines having been infected simply by visiting the hackers' blog, even when running the latest versions of Windows 10 and Chrome.

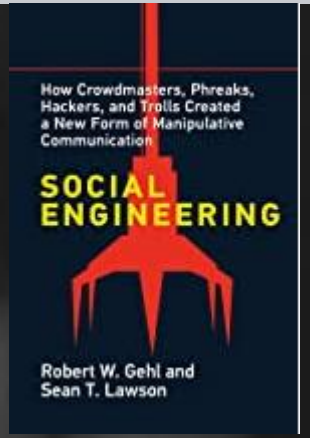
As *The Copper Courier* originally reported, GoDaddy sent an email phishing "test" to its employees promising much-needed money: "2020 has been a record year for GoDaddy, thanks to you!" it said. "Though we cannot celebrate together during our annual Holiday Party, we want to show our appreciation and share a $650 one-time Holiday bonus!"

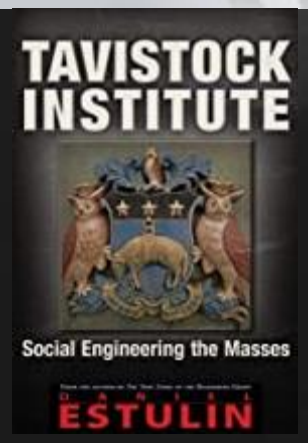
The employees who clicked the link then reportedly received an email two days later telling them they failed the test. Instead of receiving a holiday bonus, they'd instead be required to take a training course on social engineering.

Social Engineering

The clever **manipulation** of the natural human tendency to trust!







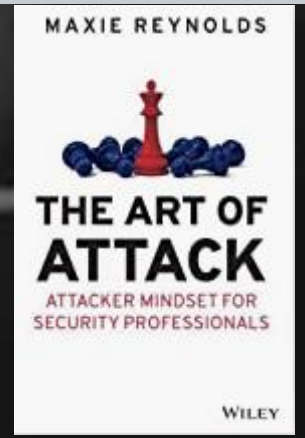
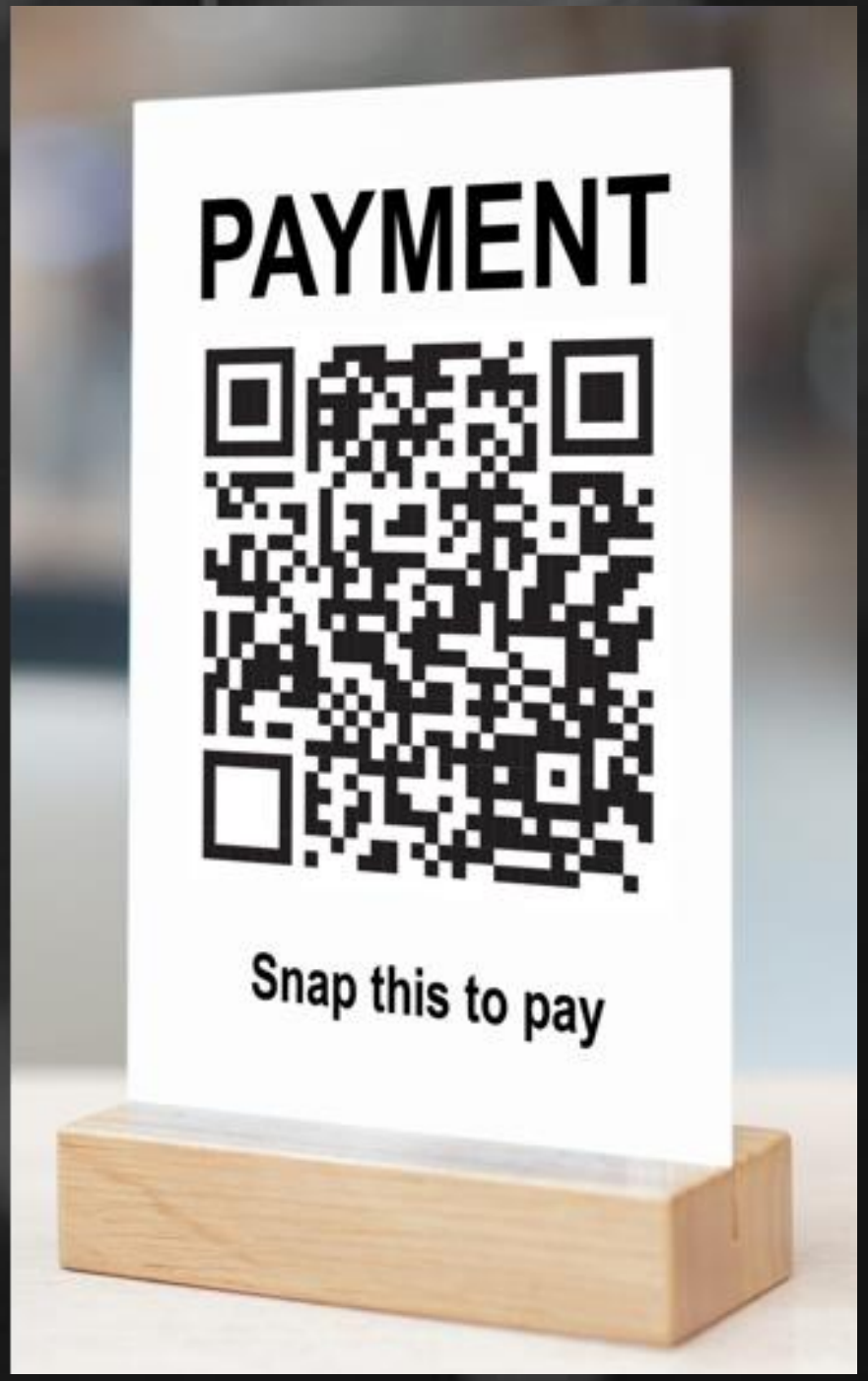



TABLE
11


PAYMENT
Snap this to pay

1. Malware attacks. Cybercriminals might embed malicious URLs in publicly present QR codes so that anyone who scans them gets infected by malware.

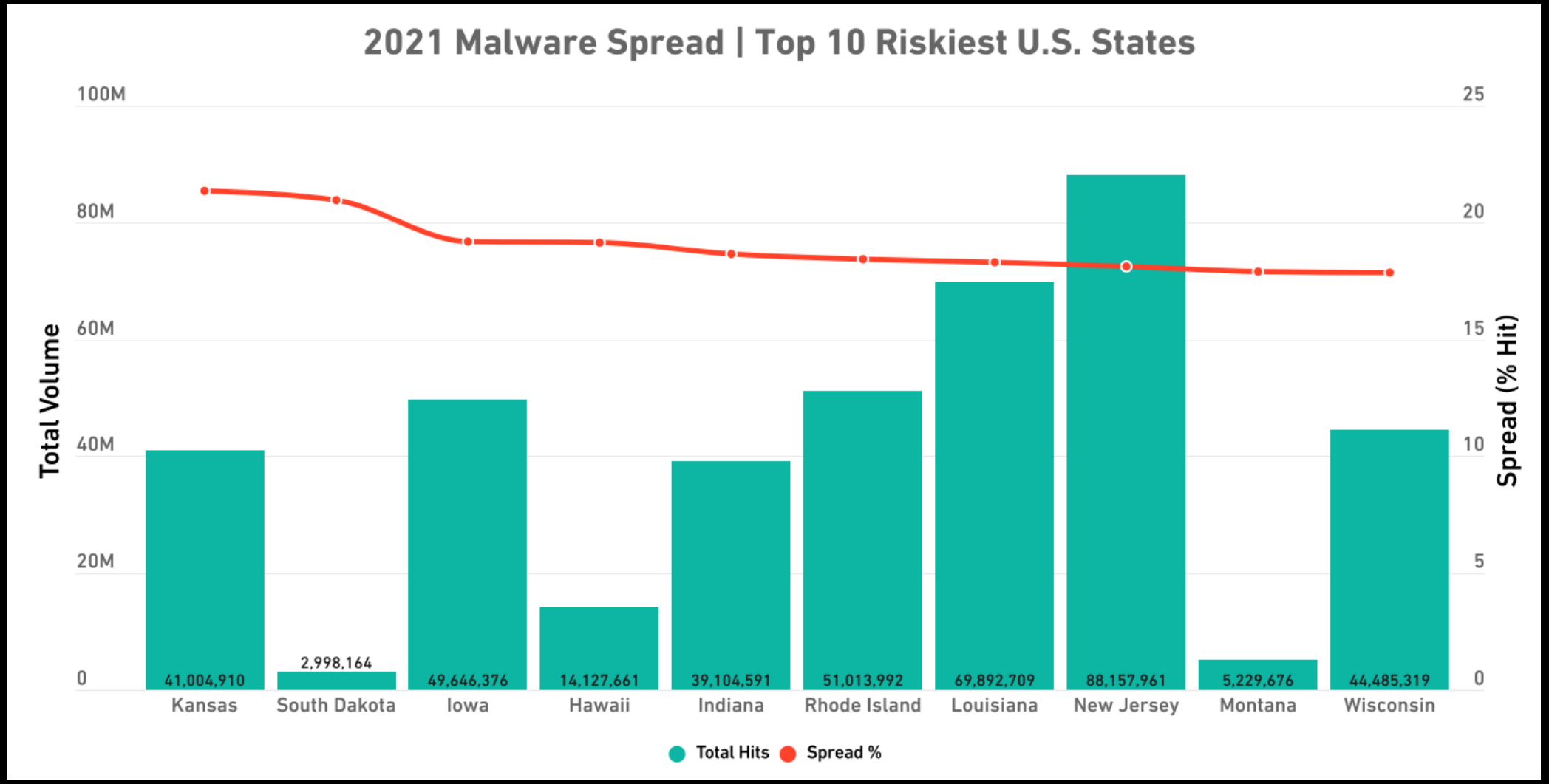
2. Phishing Attacks. QR codes are also used to serve in phishing attacks, a problem known as QPhishing.

3. Bugs in QR codes. At times it may also not be a threat actor working to exploit users. A mere bug within a QR code reader application.

4. Financial theft. QR codes have long since been an efficient manner of carrying out transactions and paying bills

In fact, with 304.7 million attempts, the first half of 2021 had more ransomware than all of 2020 — but the second half would prove to be even worse, reaching 318.6 million.

For the second year in a row, it's Kansas, where roughly 21.4% of SonicWall sensors saw a malware hit. Fortunately for those in the Sunflower State, however, this is down from the 26.7% recorded last year. (In other words, slightly more than 1 in 4 saw a hit in 2020; in 2021 it was closer to 1 in 5.



2022 SonicWall Cyber Threat report

Can User Training Prevent Phishing?

Although **95% of organizations provide phishing awareness training**, **30% trained just a portion of their user base**, according to the 2020 State of Phish Annual Report.

Additionally, **78%** of organizations say their **security awareness training activities resulted in measurably lower phishing susceptibility**, but **31% of employees failed a phishing test**.

Cloudwards March 2022

The rate of cybercrime increased by 600% during the COVID-19 pandemic.

Everyone must embrace Cybersecurity:

- **Cyber Bullying**
- **It is about control**
- **It is about image**
  - **Personal**
  - **Professional**

Perception:

- **Cop behind you driving**
- **On his way to protect your family**
- **Like breaks on a car**
- **Enable you to do more business (Go faster)**

5 Things to protect yourself and your company (spoiler alert they are the same)

1. PASSWORDS
   - Do not duplicate
   - User a Password Manager
   - Complexity matters
   - Multifactor
2. Don’t Click
   - Or swipe or connect or allow (I know right?)
   - Getting tricked – go to #3
   - Or scan (QR Codes)
3. Call them back
   - Separate email
   - Call a known number
   - Verify THEIR identity
4. Share
   - Your own examples
   - Make it a game of finding new bad actors
   - Hacker of the day post
   - Privately punish
5. Lock your credit
   - Call Experian at (888) 397-3742 or request a freeze online at the Experian Freeze Center.
   - Call Equifax at (888) 298-0045 or create/access an online account to manage your freeze manually.
   - Call TransUnion at (888) 909-8872. You will be creating a pin that you will need to access, freeze and unfreeze your account, so make sure to keep it in a safe place!


“Be good.”

Thank You!

sriat@nex-tech.com
@sriat