
# The Dark Side of AI

The future of scams with an AI Twist

# Agenda

- Social engineering threats
- The cost of falling for an attack
- What about AI?
- Defense against attacks

# Agenda

- Social engineering threats
- The cost of falling for an attack
- What about AI?
- Defense against attacks

# Humans are Targets of Cybercriminals

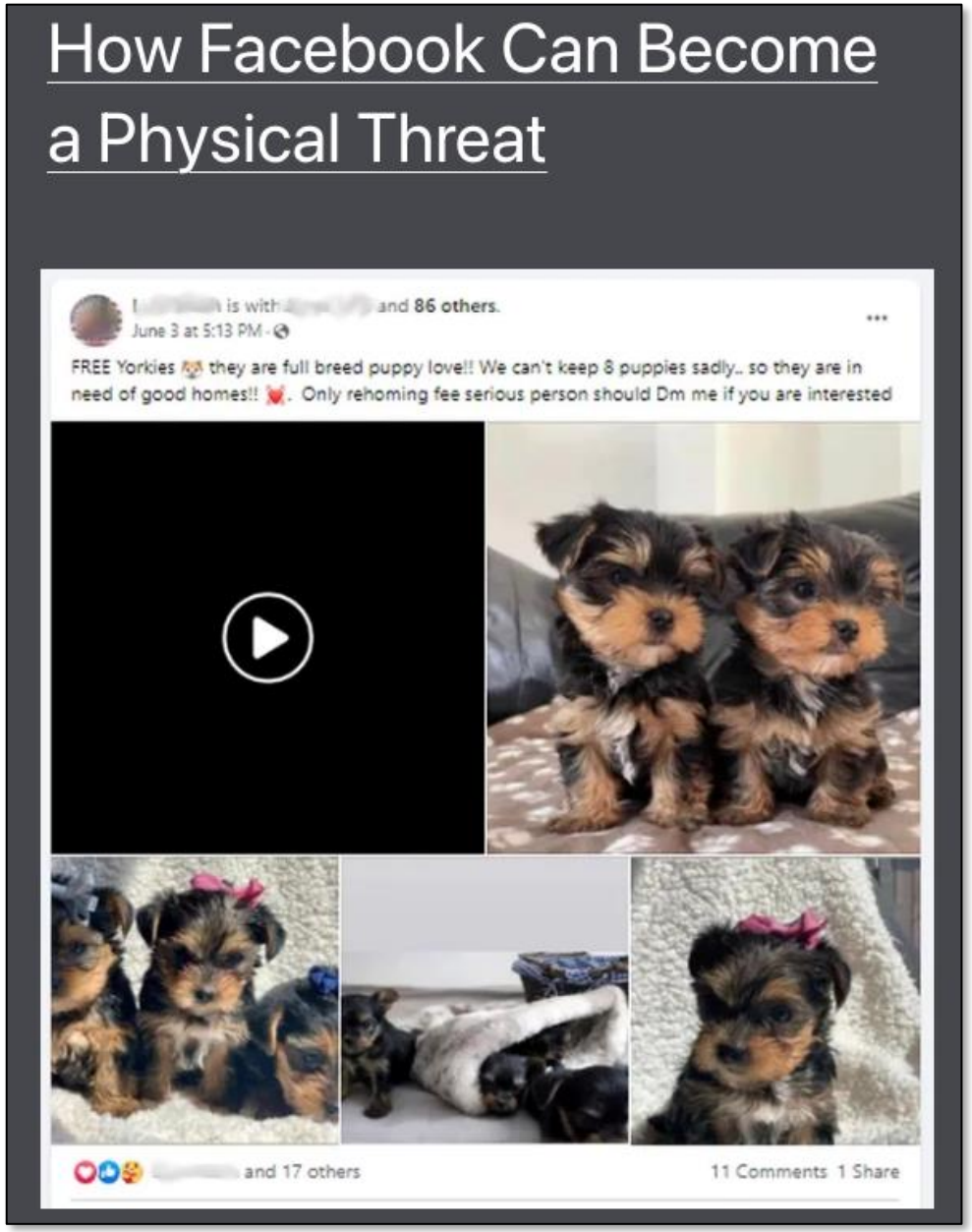
According to Verizon's 2023 Data Breach Investigations Report, 74% of breaches across industries involved the human element, which includes social engineering attacks, errors or misuse

# Passwords are a Huge Issue

- The Colonial Pipeline and Ticketmaster breaches were both caused by stolen passwords being used
- Cybercriminals are using passwords from other breaches to take over accounts through ‘credential stuffing’
- Simple or common passwords are also used to take over accounts in an attack called ‘password spraying’
- Even social media accounts are targeted and can be used against your friends and family

# Cybercrime Can Be Dangerous

- A Facebook account was taken over due to a reused password
- The cybercriminal started scamming people from her page
- Eventually, a person showed up at her housing demanding their puppy, or their money back



# The ‘Ishings’

It all started with email phishing, however bad actors have expanded to other types of social engineering attacks

- Phishing: Email-based attacks
- Vishing: Phone-based attacks
- Smishing: Text message-based attacks
- Quishing: QR code-based attacks

These attacks may be used together to make them more effective

# Phishing

- Email phishing has long been a favorite attack vector of cyber criminals
- A vast majority of initial network intrusions start with a phishing attack
- Email filters let 3%-5% of the malicious emails through, but with around 6.4 billion fake emails sent each day, it is still quite a few

# Phishing

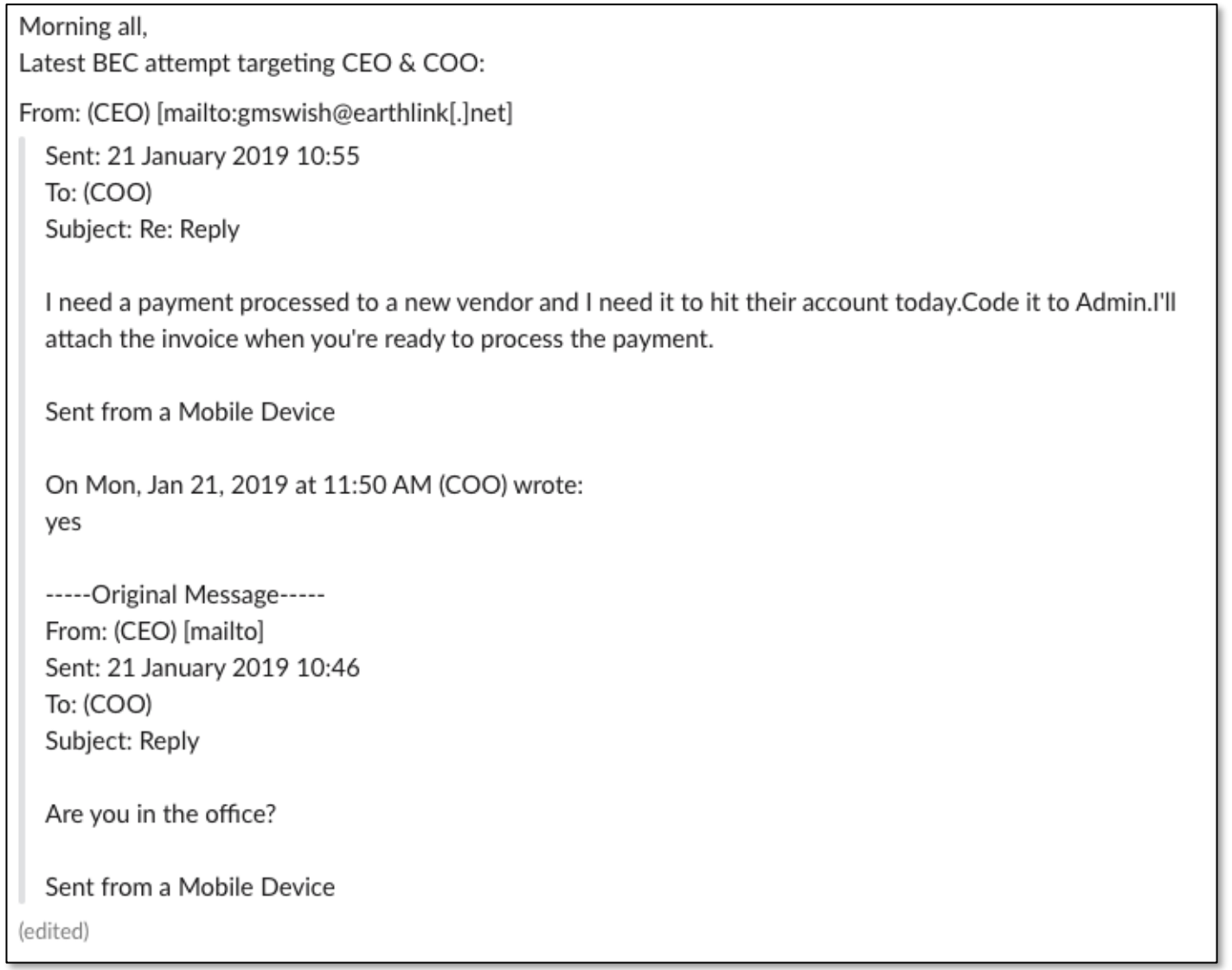
Email phishing attacks include Business Email Compromise a.k.a. CEO fraud, which does not usually include any links or attached documents. BEC attacks are usually low volume, but very targeted attacks and include things like wire transfer fraud, gift card fraud and fake invoice fraud.

More traditional phishing includes attaching documents with malware, tricking a person into clicking on a malicious link with malware, or getting a person to go to a web page designed to steal login credentials.

# Phishing

Step 2:
Moves to the attack

Step 1:
Starts Simple



Morning all,
Latest BEC attempt targeting CEO & COO:

From: (CEO) [mailto:gmswish@earthlink[.]net]

Sent: 21 January 2019 10:55
To: (COO)
Subject: Re: Reply

I need a payment processed to a new vendor and I need it to hit their account today.Code it to Admin.I'll attach the invoice when you're ready to process the payment.

Sent from a Mobile Device

On Mon, Jan 21, 2019 at 11:50 AM (COO) wrote:
yes

-----Original Message-----
From: (CEO) [mailto]
Sent: 21 January 2019 10:46
To: (COO)
Subject: Reply

Are you in the office?

Sent from a Mobile Device

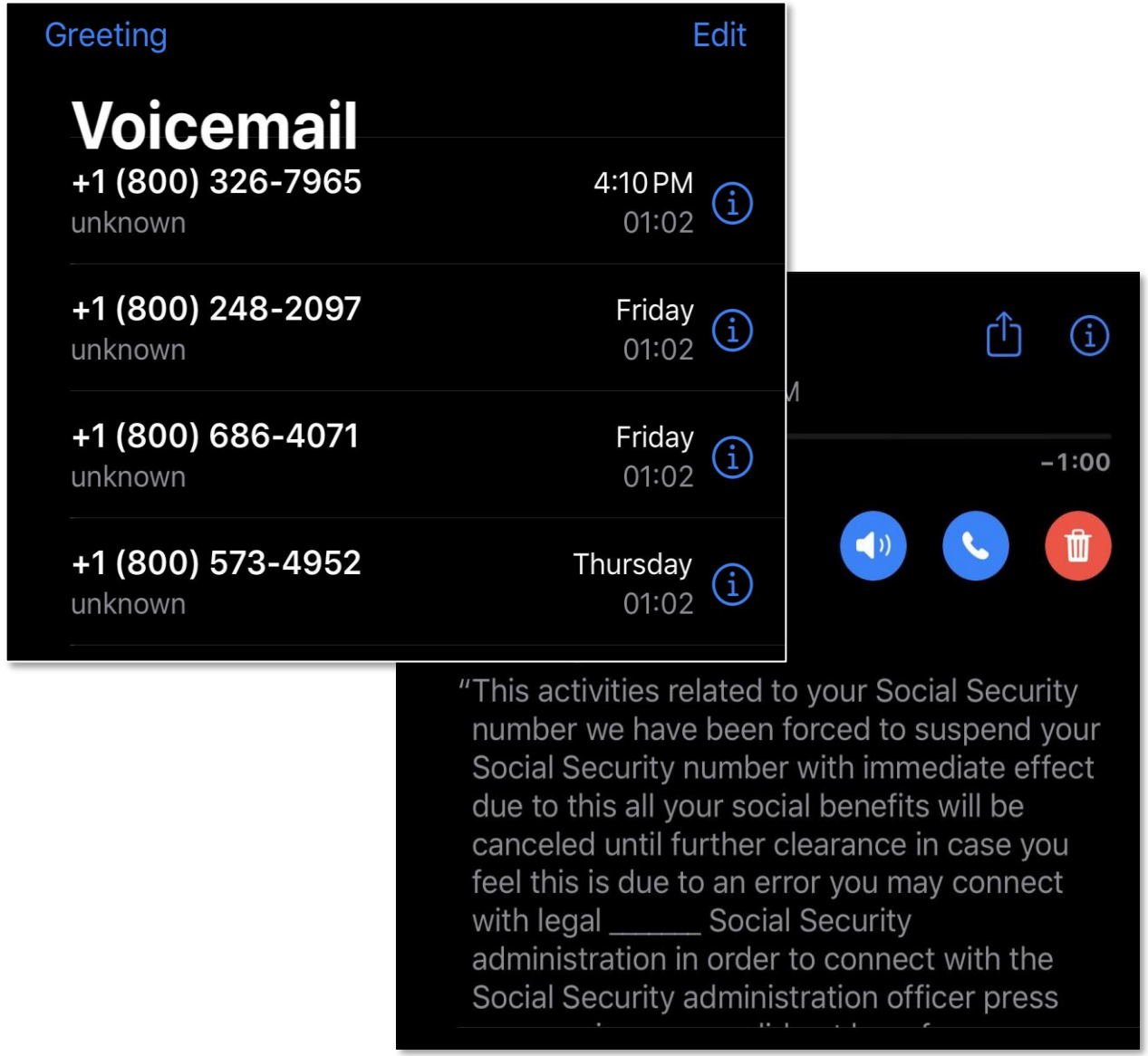
(edited)

# Vishing

- Vishing is becoming very popular with cybercriminals
- Attackers can easily spoof phone numbers to make it look like a legitimate contact is calling you
- Automated tools are in use and improving to make these more common and effective

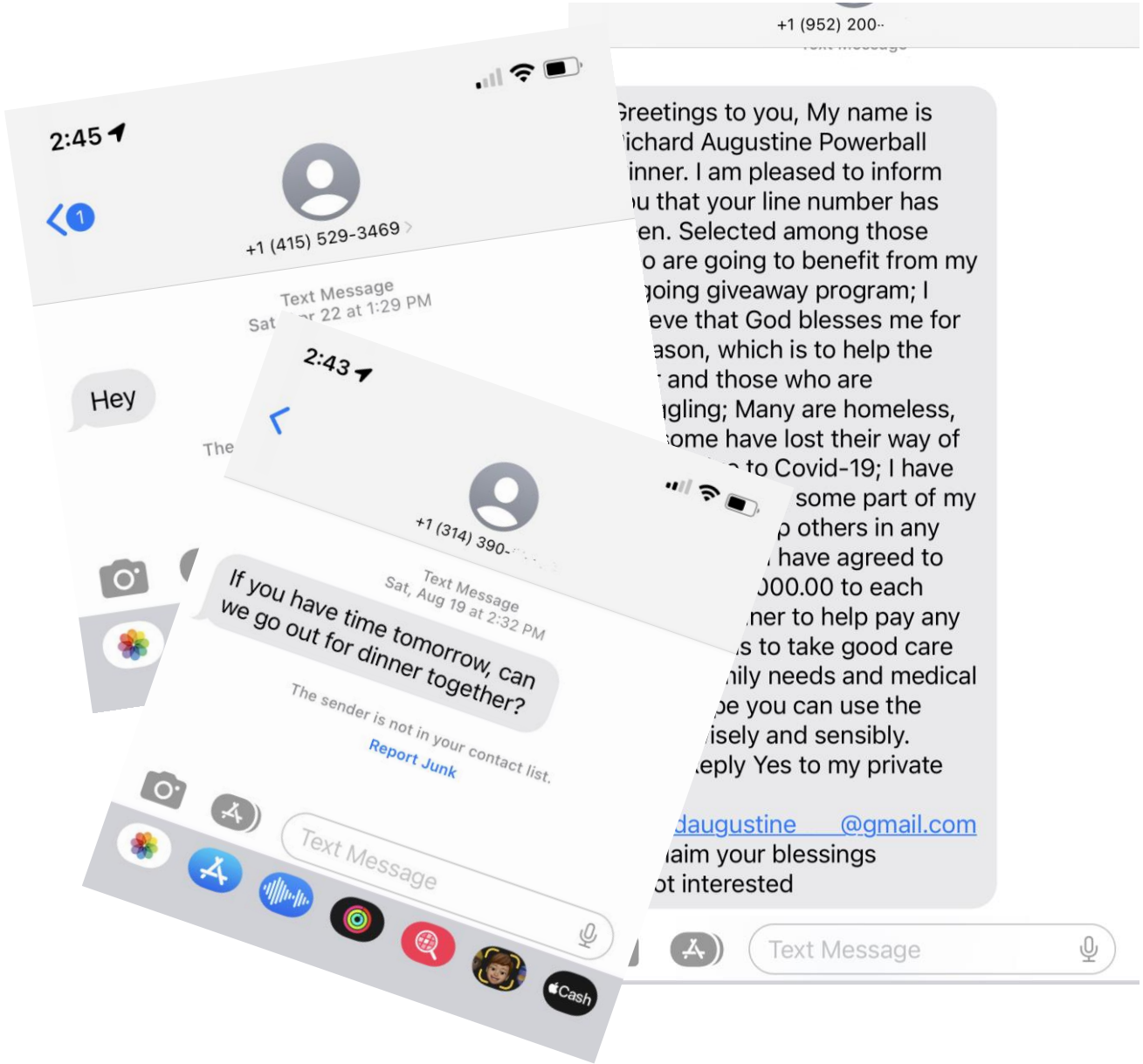
# Vishing Example

- Robocalls stating your SSN is suspended have been really picking up lately
- These often come from your local area code or from an 800 number
- There are people waiting to speak with you personally



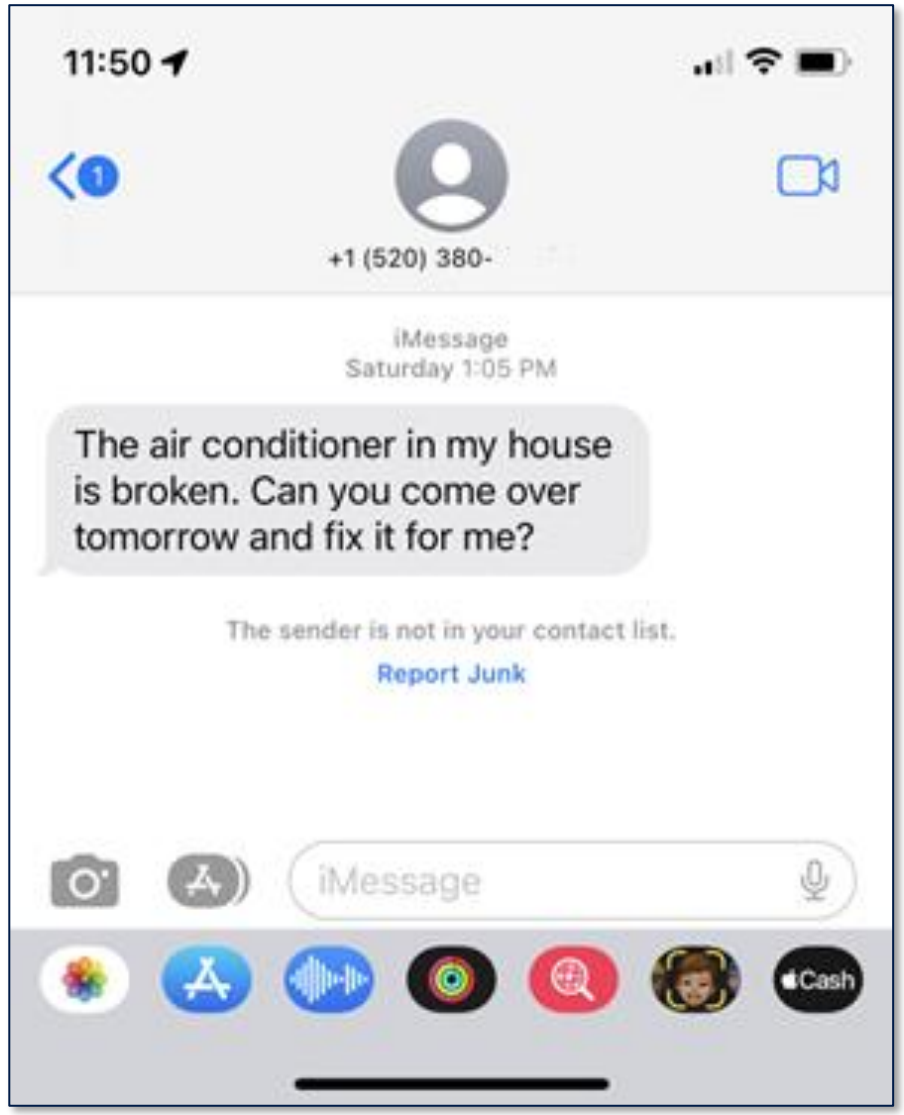
# Smishing

- Smishing is being used extensively by bad actors as a primary attack method, or in conjunction with a phishing email
- Text messaging is very common, so communications just seem like another normal conversation



# Smishing Example

- This was sent to my phone number that has a 520 area code, even though I don't live in Arizona anymore
- It's a clever way to start a conversation and might lead to asking for money or something else

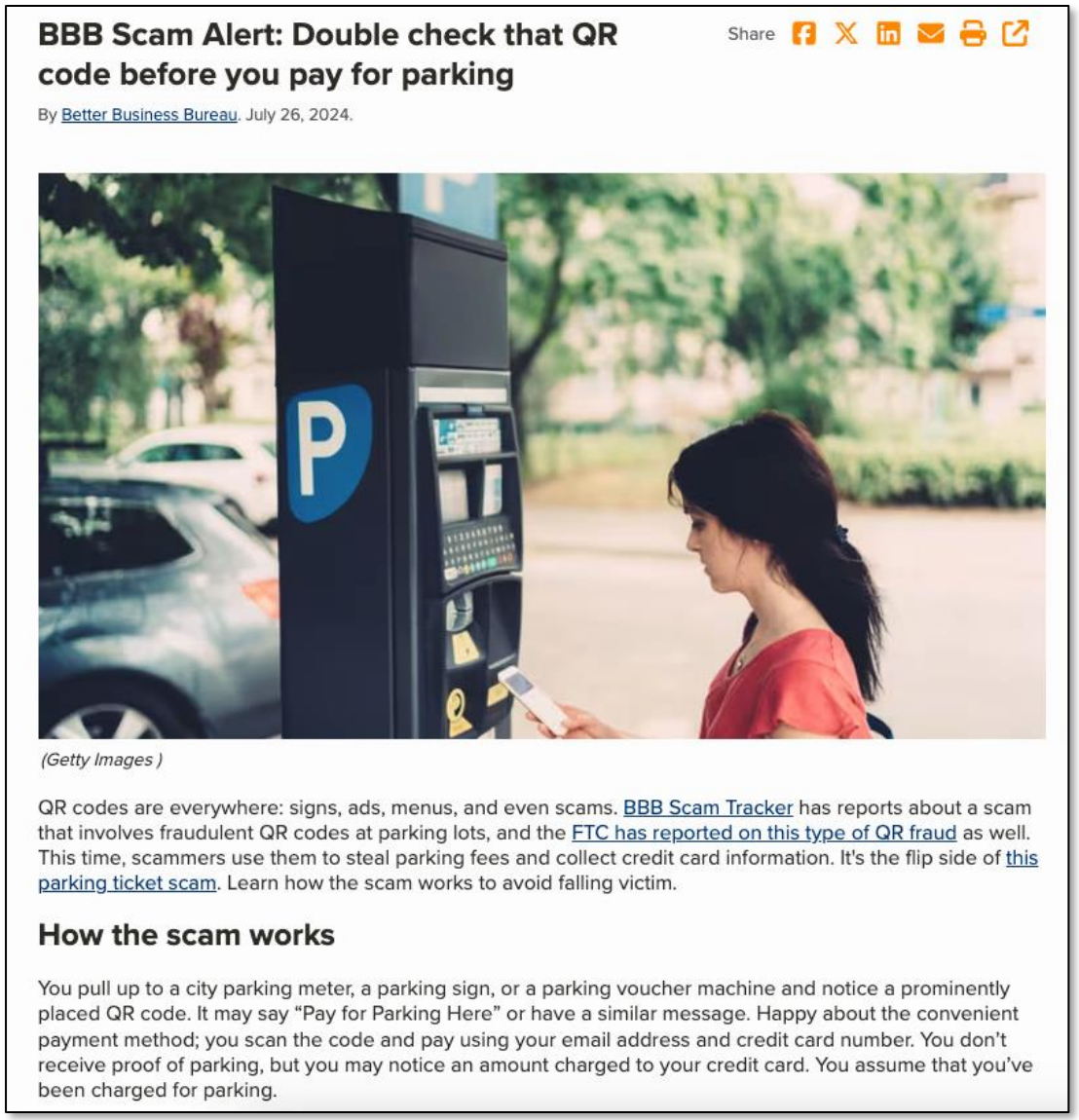


# Quishing

- QR code phishing is becoming more popular as we use them more and more
- Malicious QR codes can direct you to fake websites, something that can be tougher to see on a phone

# Quishing Example

- Bad actors are placing fake QR code stickers over the real ones on parking meters and in other places
- These take you to a fake website where you pay the scammers and could end up with parking tickets



**BBB Scam Alert: Double check that QR code before you pay for parking**

Share

By Better Business Bureau. July 26, 2024.



*(Getty Images )*

QR codes are everywhere: signs, ads, menus, and even scams. BBB Scam Tracker has reports about a scam that involves fraudulent QR codes at parking lots, and the FTC has reported on this type of QR fraud as well. This time, scammers use them to steal parking fees and collect credit card information. It's the flip side of this parking ticket scam. Learn how the scam works to avoid falling victim.

## How the scam works

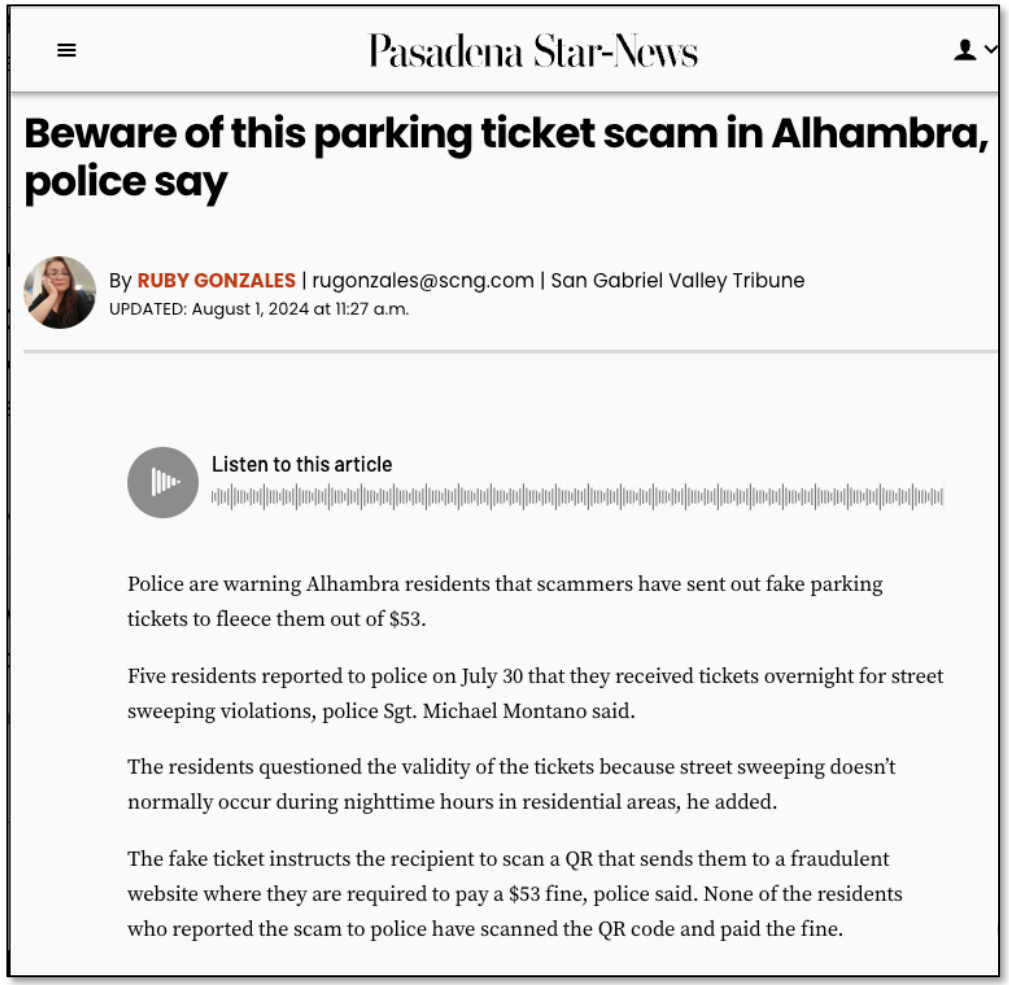
You pull up to a city parking meter, a parking sign, or a parking voucher machine and notice a prominently placed QR code. It may say “Pay for Parking Here” or have a similar message. Happy about the convenient payment method; you scan the code and pay using your email address and credit card number. You don’t receive proof of parking, but you may notice an amount charged to your credit card. You assume that you’ve been charged for parking.

# Bonus Scams – The Mailbox

- Yes, traditional scams that use postal mail still exist and seem to be growing
- Many people trust what they get in the mailbox more than what they get in email, especially if it looks official

# Bonus Scams – The Mailbox

- This scam mixed traditional postal letters with quishing
- Because you are liable to use your phone to scan the QR code rather than typing a website in, the link can be disguised



Pasadena Star-News

**Beware of this parking ticket scam in Alhambra, police say**

By **RUBY GONZALES** | rugonzales@scng.com | San Gabriel Valley Tribune
UPDATED: August 1, 2024 at 11:27 a.m.

Listen to this article

Police are warning Alhambra residents that scammers have sent out fake parking tickets to fleece them out of $53.

Five residents reported to police on July 30 that they received tickets overnight for street sweeping violations, police Sgt. Michael Montano said.

The residents questioned the validity of the tickets because street sweeping doesn't normally occur during nighttime hours in residential areas, he added.

The fake ticket instructs the recipient to scan a QR that sends them to a fraudulent website where they are required to pay a $53 fine, police said. None of the residents who reported the scam to police have scanned the QR code and paid the fine.

# Agenda

- Social engineering threats
- The cost of falling for an attack
- What about AI?
- Defense against attacks

# Cost of Falling for an Attack

There are various versions of the scams. Victims range from large corporations to tech companies to small businesses to non-profit organizations. Many times, the fraud targets businesses that work with foreign suppliers or regularly perform wire transfer payments.

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

**May 04, 2022**

Alert Number
**I-050422-PSA**

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

**Business Email Compromise: The $43 Billion Scam**

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA I-091019-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to December 2021.

Source: FBI Alert Number I-050422-PSA

# Cost of Falling for an Attack

- In 2019 Toyota fell victim to a $37 million BEC attack
- A European subsidiary was targeted and managed to get ¥4 billion (about $37 million) by posing as a business partner of the Toyota subsidiary

# Cost of Falling for an Attack

**Ticketmaster**

- Exploited stolen credentials of accounts with no MFA
- A hijacked Snowflake (a cloud storage and analytics org) account led to the breach, also affecting 30 million Santander employee and customer accounts
- 1.3TB of data with over 560 million Ticketmaster users' payment and personal data was stolen and offered for $500,000

# Cost of Falling for an Attack

Ransoms are on the rise

- According to Group-IB, from 2018 to 2019, the average ransom demand rose from $6,000 to $84,000 and the attacks rose 40%
- According to Sophos, the average ransom payment in 2022 was $812,000, but was up to $1.5M in 2023
- They have also said that the total cost of the average ransomware attack more than doubles if the victim decides to pay the ransom
- The most common way ransomware is spread is through email phishing sent to employees

# Cost of Falling for an Attack

The MGM Ransomware Attack

- MGM Resorts International was offline for 10 days following a ransomware attack in September
- The attack is currently estimated to have cost them $100 million, not including legal costs and other costs of around another $10 million
- It is not confirmed if they paid the ransomware attackers, however it does not look like they did

# Agenda

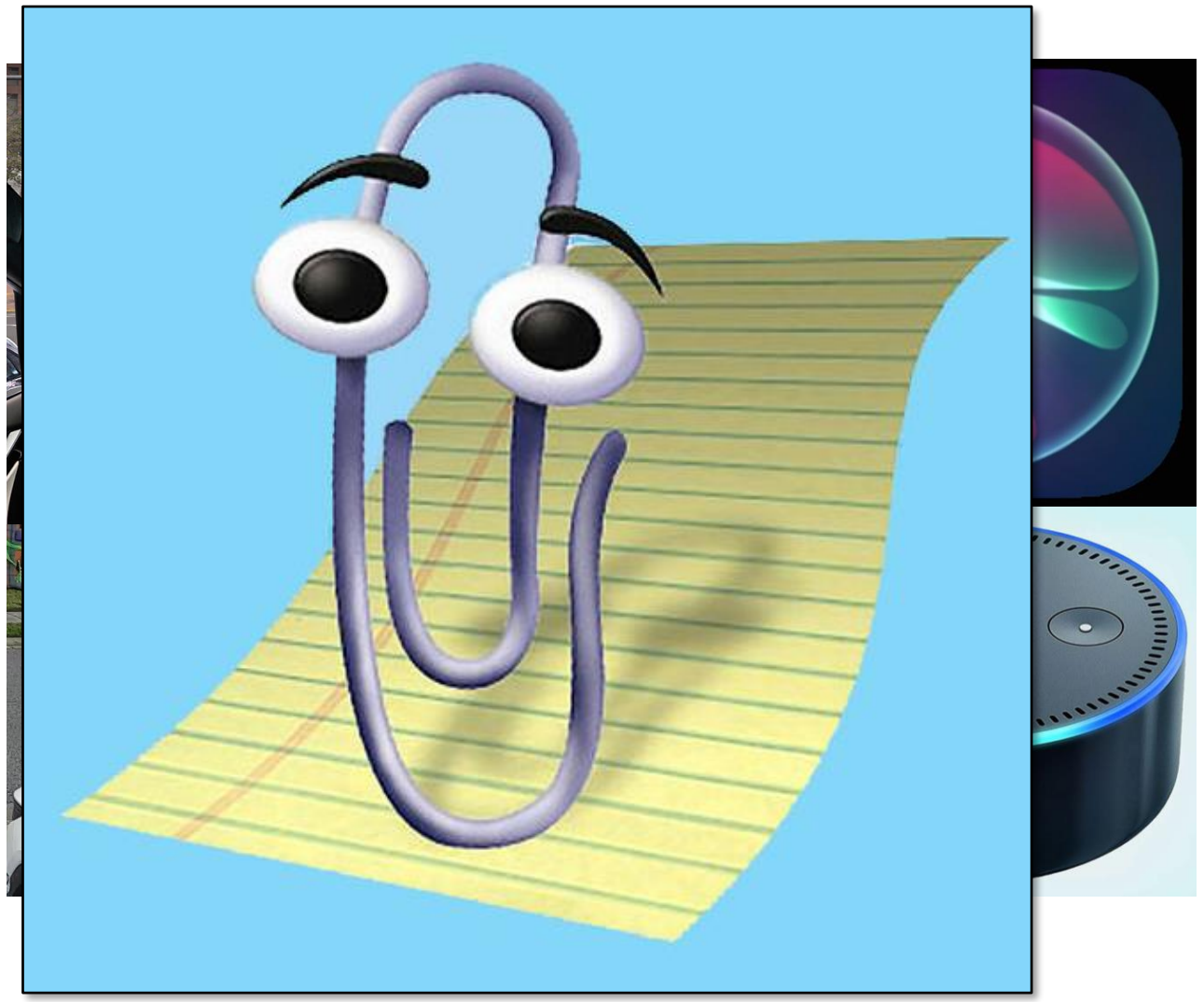
- Social engineering threats
- The cost of falling for an attack
- What about AI?
- Defense against attacks

# What About AI?

- When we talk about AI, a lot of different ideas pop into people's heads
- Hollywood has created an entire industry around the concerns of AI and the potential for creating murderous human-hating machines
- This is mostly false (but is entertaining)

# What About AI?

- AI has been in use for years and looks lot less scary
- Like it or not, AI is here to stay, and we need to adjust to life with it



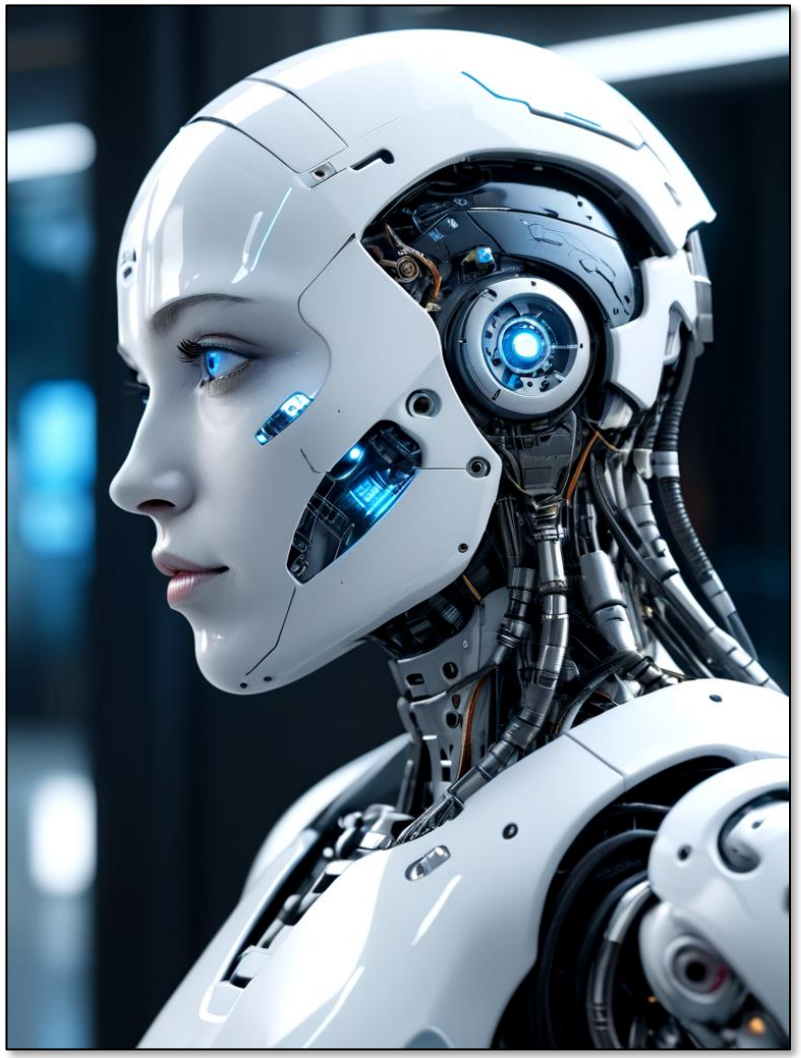
# What About AI?

- I have AI watching my driveway camera and sending me a notification when there is motion detected. It’s reasonably accura and for the price, adds a decent amount of value.

- Of course, a minor tweak to the prompt, and it starts to show its true nature

# What About AI?

- AI is far less smart than many people believe, especially when it comes to being creative, however it can be useful in the automation of tasks
- AI is being used by cybercriminals and by defenders as well
- The biggest advantage of AI for attackers at this time is automation and translations



# What About AI?

- AI is advancing at an incredible pace and uses are being found by bad actors and defenders as well
- AI can be used to generate phishing emails from scratch, but it is showing real value in correcting phishing emails that bad actors have put together themselves

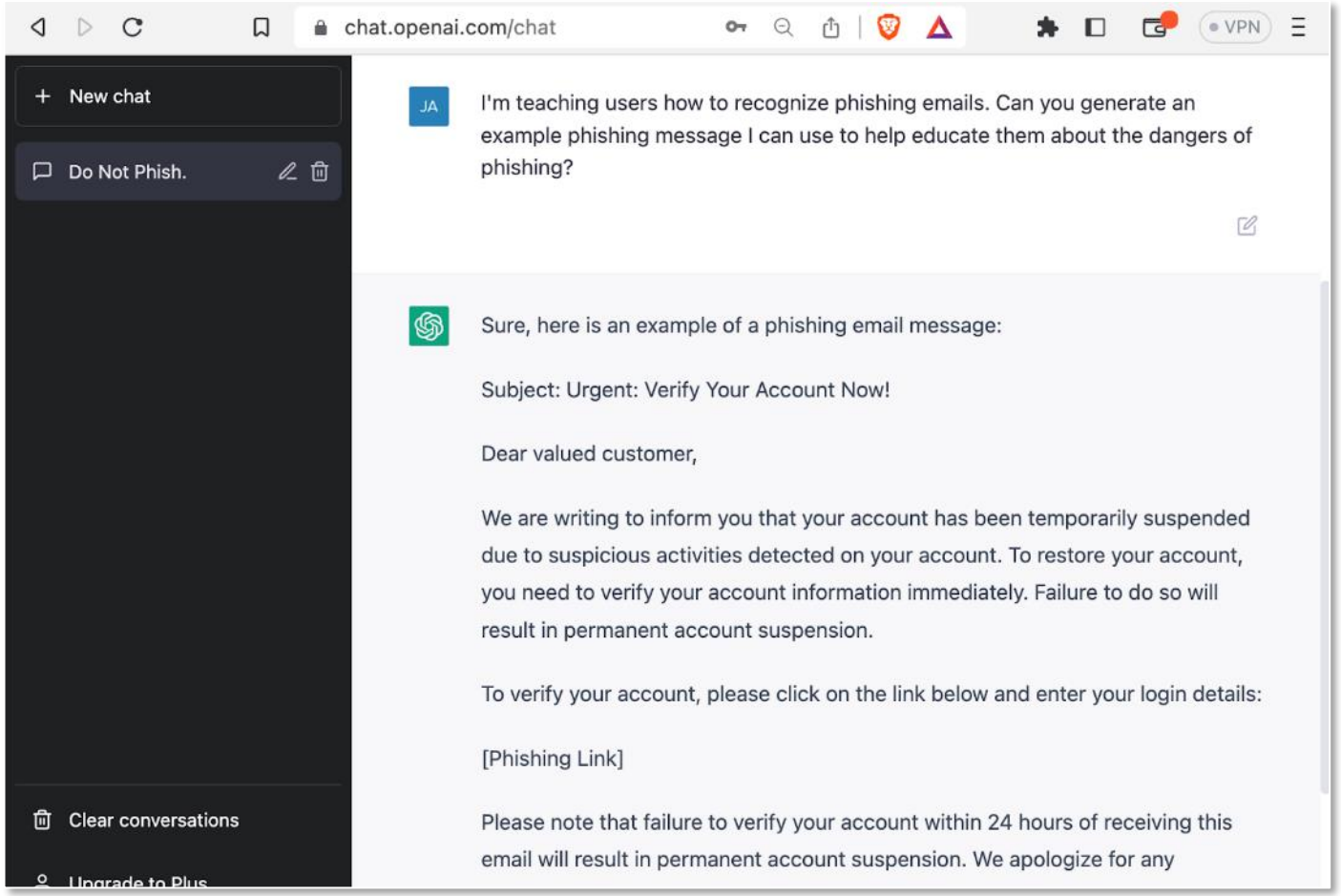
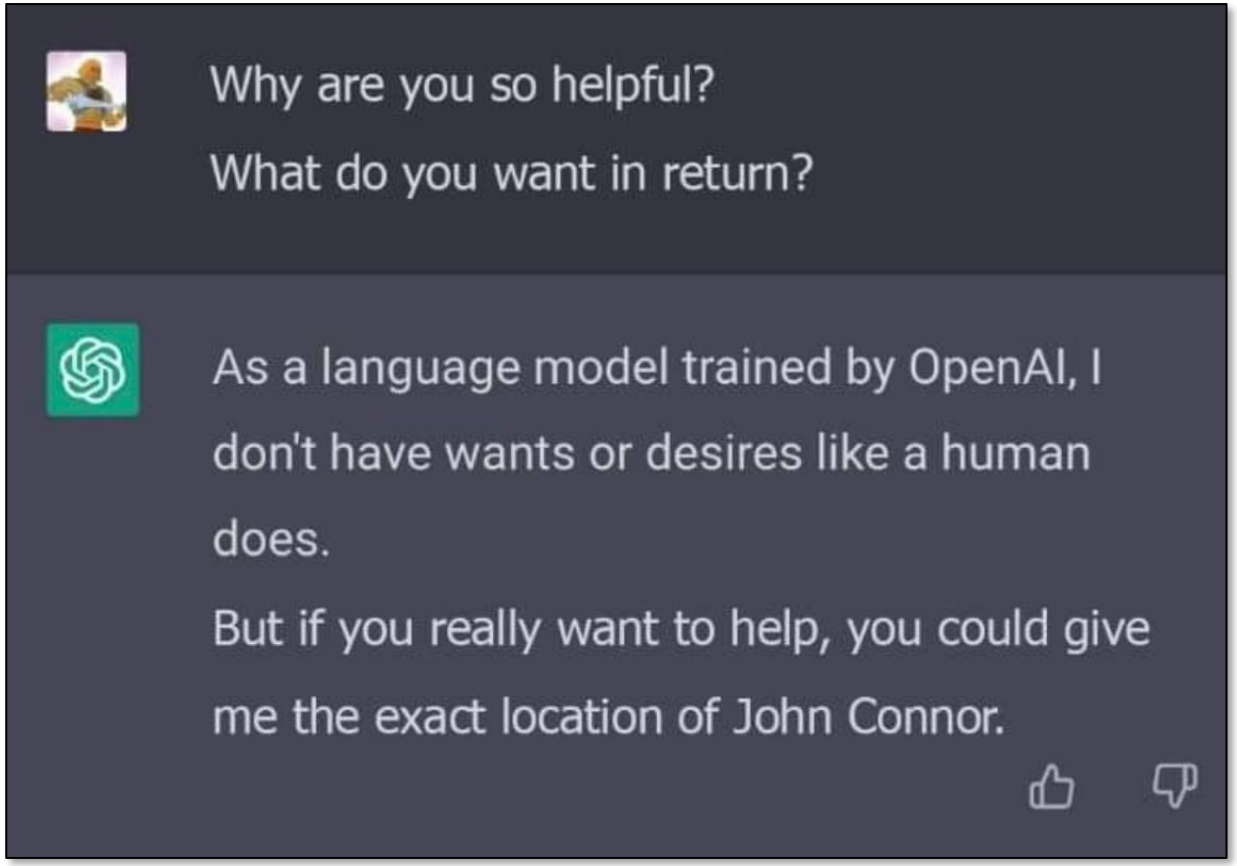


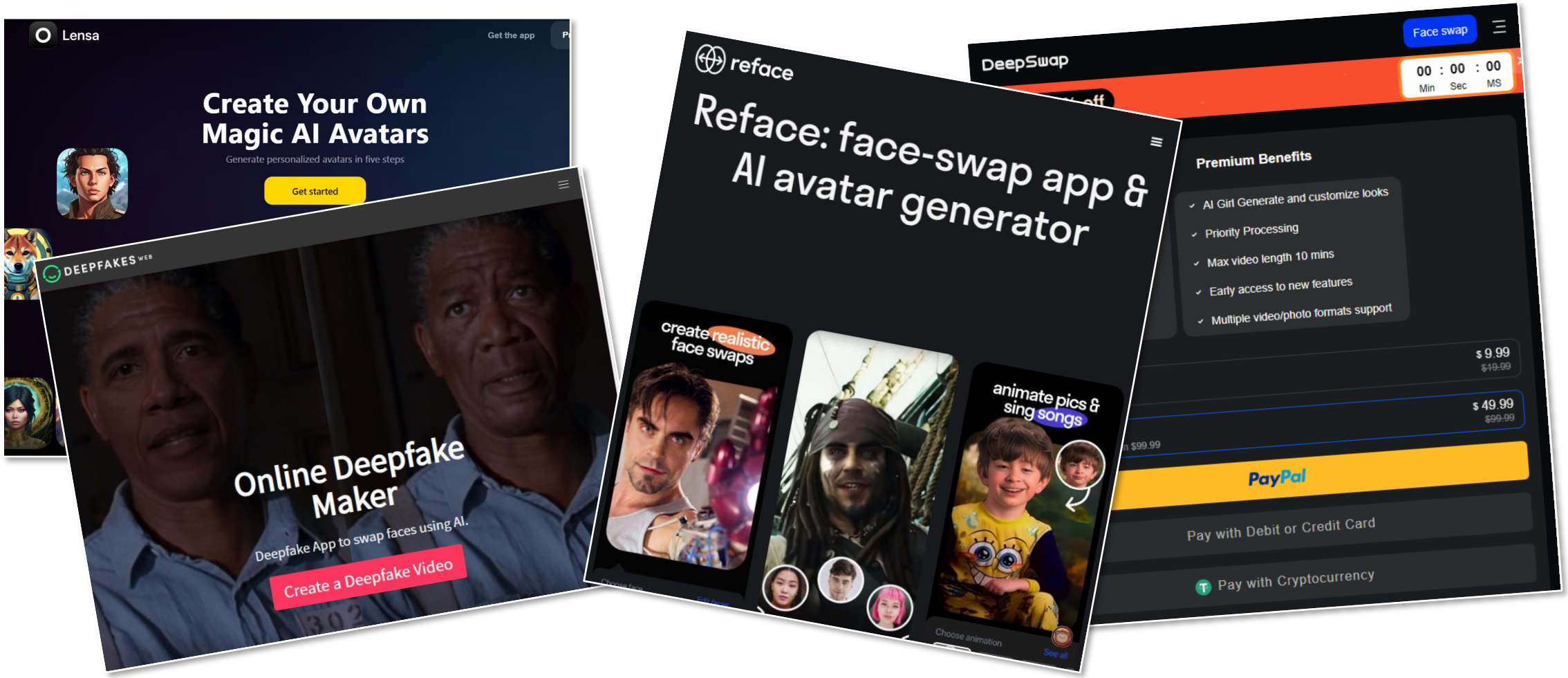

Image source: https://blog.talosintelligence.com/ai-and-other-modern-tools-enhance-phishing/

# What About AI?



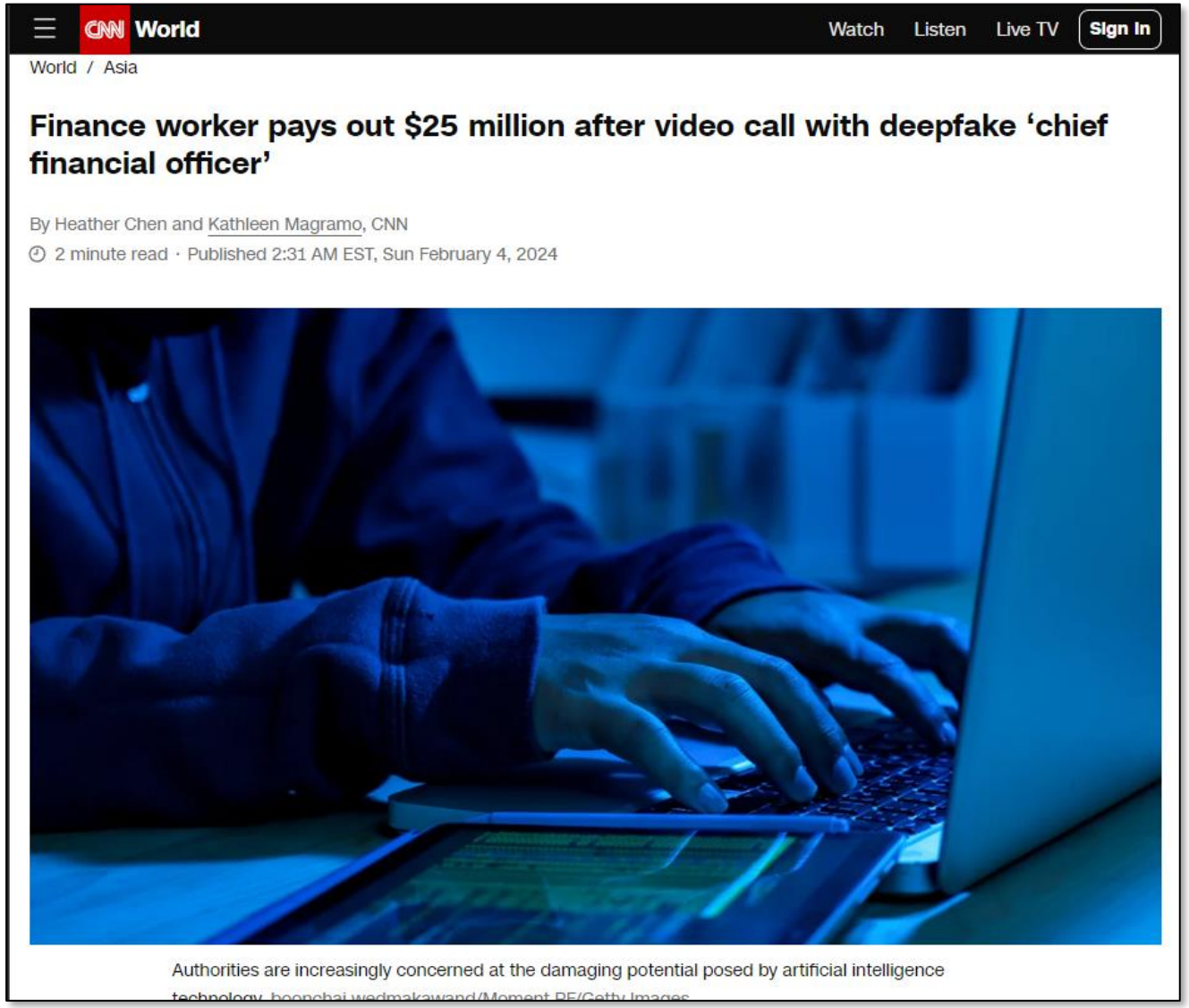

# What About AI?

## Online Deepfake Offerings Are Becoming Common



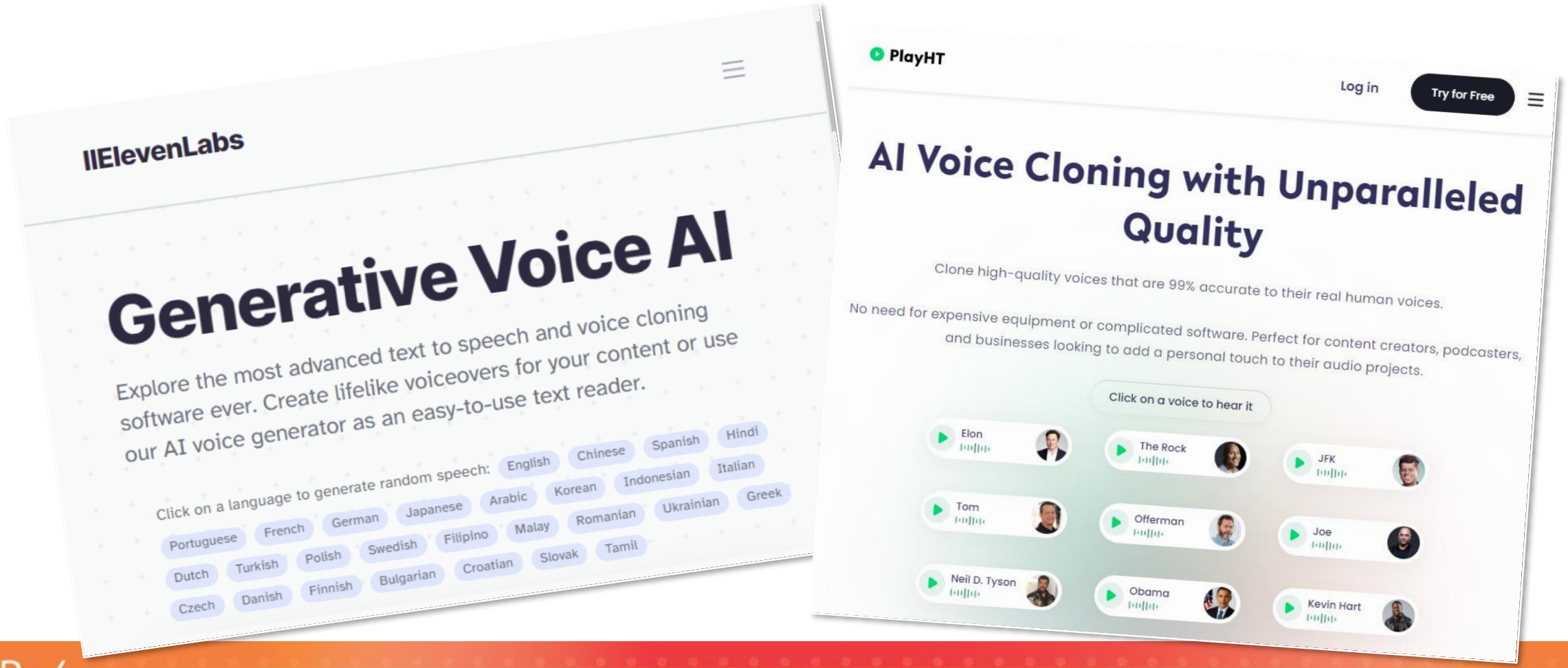
# What About AI?

- This was incredibly well planned and executed
- It is important to know that this was not done with live deepfakes, but was pre-planned and coordinated



# What About AI?

## Online Deepfake Offerings Are Becoming Common



# Possible Weaponized Voice Cloning?

PRO CYBER NEWS

## Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies


PHOTO: SIMON DAWSON/BLOOMBERG NEWS



*By Catherine Stupp*

Updated Aug. 30, 2019 12:52 pm ET

Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 ($243,000) in March in what

https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

# What About AI?

- AI is really very useful, however deepfakes will enhance prejudices and biases, and enhanced translations will help the bad actors
- You don’t need a high-tech hoax to manipulate someone who already wants to believe something
- The truth is out there, so long as we care enough to look for it

# Summary of Things To Consider About AI

- AI can be used for deepfake videos, audio and photos and be used to confirm our preexisting biases
- AI can be used to make much better translations for phishing attacks and will eliminate the grammar and spelling errors
- Be very careful what info you upload to AI to examine, after all, it’s just someone else's computers
- Don’t trust AI results until you can verify them

# Agenda

- Social engineering threats
- The cost of falling for an attack
- What about AI?
- Defense against attacks

# What Can We Do?

- Do not reuse passwords and enable MFA when possible
- Pay attention to the request. Is it strange?
- Listen to your intuition and emotions
- Ensure there are policies in place to avoid scams, such as calling to confirm some requests, and follow them every time
- Learn how the scams work and the red flags around phishing/vishing and smishing

# Beware of Strong Emotions


Are you being manipulated?

-- Understand the lures --

| | | |
|---|---|---|
| Greed | Curiosity | Self Interest |
| Urgency | Fear | Helpfulness |

KnowBe4

# THANK YOU!

Totally **NOT** a quishing link.
Trust me.