Alta Pro Insurance Services

KnowBe4 Webinar Manuscript
April 17, 2020

Live webinar
Date: June 18, 2020

TITLE

No Rest For The Wicked (Cybercriminals)

Law Firm Email Security Awareness and Training

Cybercriminals are not ones to let any major event go unexploited and the COVID-19 pandemic is no exception. Even at the best of times these talented attackers use human behaviors against you in the never-ending quest to separate you from your money.

Using social engineering techniques, the bad actors have continued to attack organizations across industries at a furious pace. While you may believe you are too small to be a target, if you have an email address or if your organization shows up on a Google search, they will use automated tools to attack you.

In this webinar, cybersecurity expert Erich Kron will discuss the current threats and cyber attacks, how the attackers are evolving to target those working from home, the social engineering tricks they use and what we can expect in the near future.

In this webinar, you will learn the following:

- Tricks the bad actors are currently using
- Why remote working can be more dangerous
- How social engineering attacks work
- How to defend against attacks and scams

AGENDA
(One-Hour CLE Webinar)

Part One (0:00 – 0:15)

Current Threats
This will discuss the current tactics being used by the attackers, especially as it relates to email phishing (the #1 method of attack) and text message smishing and will go over current themes behind these attacks. The vary by the timing of events, however we can expect to see COVID-19 themes around returning to work, opening the economy back up, etc. These example will be specific to recent events

Example Questions (subject to change based on current events):

- What types of attacks are we currently seeing in the wild?
- Is it always focused on making money or are there other motivations?
- Where do the attackers come from and why do they do this?

Part Two (0:15 – 0:30)

Working From Home
This section will discuss how attackers are using the move to working from home to exploit the changes, adjustments and new vulnerabilities present due to this operational change.

Example Questions (subject to change based on current events):

- Why do the bad actors feel that it is worth the effort to ramp up attacks while people have started working from home?
- What types of things making working from home more dangerous than in an office environment?
- What habits should we change when working from home vs. in the office?

Part Three (0:30 – 0:45)

Social Engineering
This section will focus on the psychology behind how the attackers use email, text messaging and phone calls to attack the victims. It will discuss the concept of focus redirection, disruption of critical thinking steps and perception filters.

Example Questions (subject to change based on current events):

- Why are these attacks so effective and why can't we seem to make scams stop?
- What is the best way a person can defend against these sorts of attacks?
- What do I do if I fall for an attack and realize it?

Part Four (0:45 – 0:60)

What we can expect in the future

This will focus on upcoming and expected events that will open up doors for attackers. This includes the shift to working back in the office, the reemployment rush and the fears of a second wave as well as the upcoming presidential elections.

Example Questions (subject to change based on current events):

- Why do we expect that the attackers to keep using COVID-19 themed attacks even after things are settling down?
- Will this cycle ever end?
- What do you think is the most dangerous technology that is coming out?
- How can we be prepared?

PRESENTERS

Erich Kron is the Security Awareness Training Advocate for KnowBe4. He is a veteran information security professional who has worked for more than 20 years in the medical, aerospace, manufacturing and defense fields. His experience ranges from large-scale technical project management to hands-on technical work. He is a popular speaker, trainer and author. More about Erich here.

KnowBe4 is a security awareness training and simulated phishing company. Its new-school integrated platform lets subscribers train and phish their users, see their Phish-prone percentage™ improve over time, avoid social engineering scams and get measurable results.

Jay Reeves is the Risk Pro for Alta Pro Insurance Services. He practiced law in South Carolina and North Carolina for nearly 40 years, both in private practice and in-house (as corporate VP/Risk Manager). He has given numerous presentations to lawyers and bar groups in the US and Canada, including keynotes and CLEs. He is founder and owner of Your Law Life LLC, which helps attorneys add purpose, profits and peace of mind to their Law Lives.
More about Jay here.

Alta Pro Insurance Services

Welcome to the Alta Pro Live Webinar

Chapter II of the Cyber Security series

Raise Your Cyber Security Awareness

Jay Reeves is the Risk Pro for Alta Pro Insurance Services. He practiced law in South Carolina and North Carolina for nearly 40 years, both in private practice and in-house (as corporate VP/Risk Manager). He has given numerous presentations to lawyers and bar groups in the US and Canada, including keynotes and CLEs. He is founder and owner of Your Law Life LLC, which helps attorneys add purpose, profits and peace of mind to their Law Lives.

Erich Kron is the Security Awareness Training Advocate for KnowBe4. He is a veteran information security professional who has worked for more than 20 years in the medical, aerospace, manufacturing and defense fields. His experience ranges from large-scale technical project management to hands-on technical work. He is a popular speaker, trainer and author.

KnowBe4 is a security awareness training and simulated phishing company. Its new-school integrated platform lets subscribers train and phish their users, see their Phish-prone percentage™ improve over time, avoid social engineering scams and get measurable results.

Alta Pro
Lawyers Risk Purchasing Group

KnowBe4
Human error. Conquered.

Housekeeping

- To download the manuscript of this webinar visit altaprorpg.com/postwebinar. **Check your chat box!**
- We're approved for 1 hour of CLE. **You must complete the survey to receive your credit.**
- **There'll be two codes** revealed during the webinar that you'll need to remember.
- **You must enter the codes** in the post attendee survey to receive the credit.
- If participating via phone, email us at info@altaprorpg.com to get a form to fill out and received CLE.
- Please direct your questions to the Q&A button at the bottom of the screen.
- Unanswered questions will be answered in a post-attendee .pdf.

Alta Pro
Lawyers Risk Purchasing Group

KnowBe4
Human error. Conquered.

Current Threats

Alta Pro
Lawyers Risk Purchasing Group

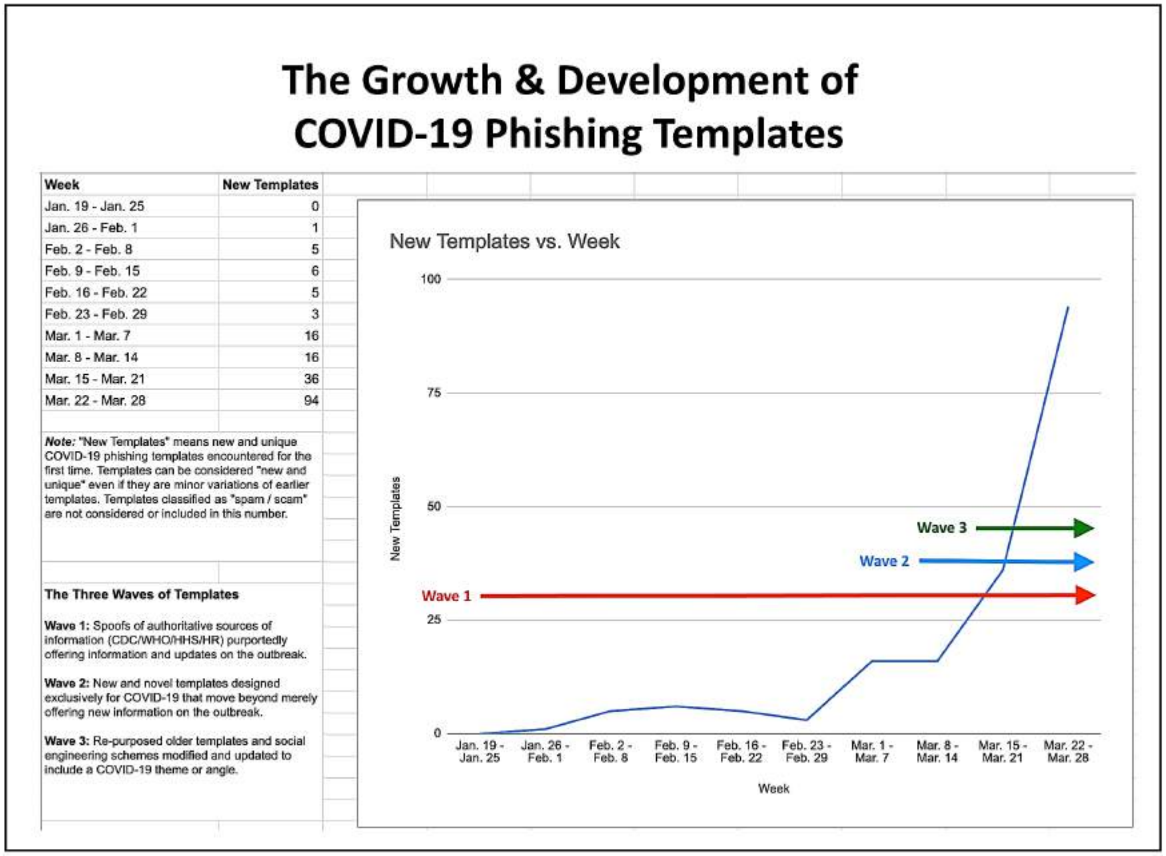
KnowBe4
Human error. Conquered.

Phishing Attacks Have Exploded Since COVID-19

The number of NEW phishing templates being spotted in the wild since COVID-19 hit has been unprecedented.

Attackers are taking advantage of the chaos and emotional impact these changes have made in our lives to profit for themselves.

This increase has been seen in not only typical cybergangs, but nation-state actors as well.



The Growth & Development of COVID-19 Phishing Templates

Week	New Templates
Jan. 19 - Jan. 25	0
Jan. 26 - Feb. 1	1
Feb. 2 - Feb. 8	5
Feb. 9 - Feb. 15	6
Feb. 16 - Feb. 22	5
Feb. 23 - Feb. 29	3
Mar. 1 - Mar. 7	16
Mar. 8 - Mar. 14	16
Mar. 15 - Mar. 21	36
Mar. 22 - Mar. 28	94

Note: "New Templates" means new and unique COVID-19 phishing templates encountered for the first time. Templates can be considered "new and unique" even if they are minor variations of earlier templates. Templates classified as "spam / scam" are not considered or included in this number.

The Three Waves of Templates

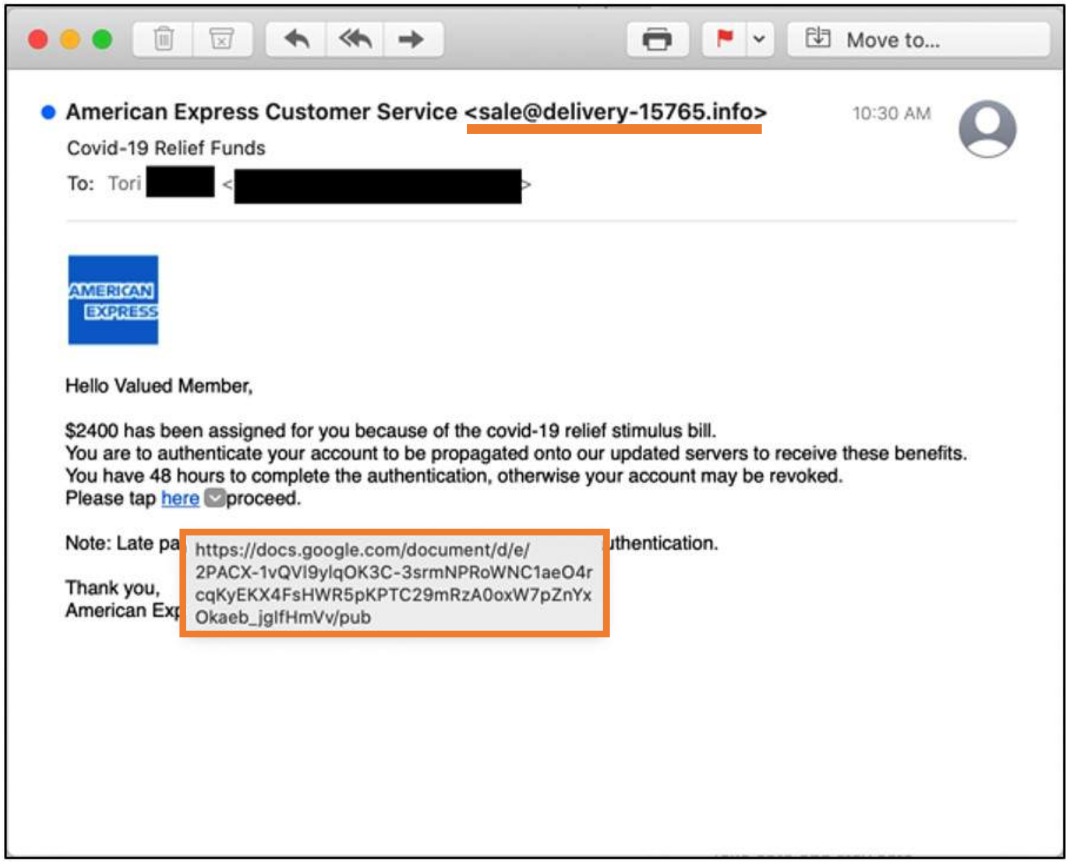
Wave 1: Spoofs of authoritative sources of information (CDC/WHO/HHS/HR) purportedly offering information and updates on the outbreak.

Wave 2: New and novel templates designed exclusively for COVID-19 that move beyond merely offering new information on the outbreak.

Wave 3: Re-purposed older templates and social engineering schemes modified and updated to include a COVID-19 theme or angle.

Stimulus Focused Attacks

- It says it’s from American Express, but it’s obviously not.
- Hovering the link shows a link to a google doc. This is not how real organization would do business.
- They are targeting account information and bank credentials with this attack.



American Express Customer Service <sale@delivery-15765.info> 10:30 AM

Covid-19 Relief Funds

To: Tori [redacted] <[redacted]>

Hello Valued Member,

$2400 has been assigned for you because of the covid-19 relief stimulus bill.
You are to authenticate your account to be propagated onto our updated servers to receive these benefits.
You have 48 hours to complete the authentication, otherwise your account may be revoked.
Please tap here proceed.

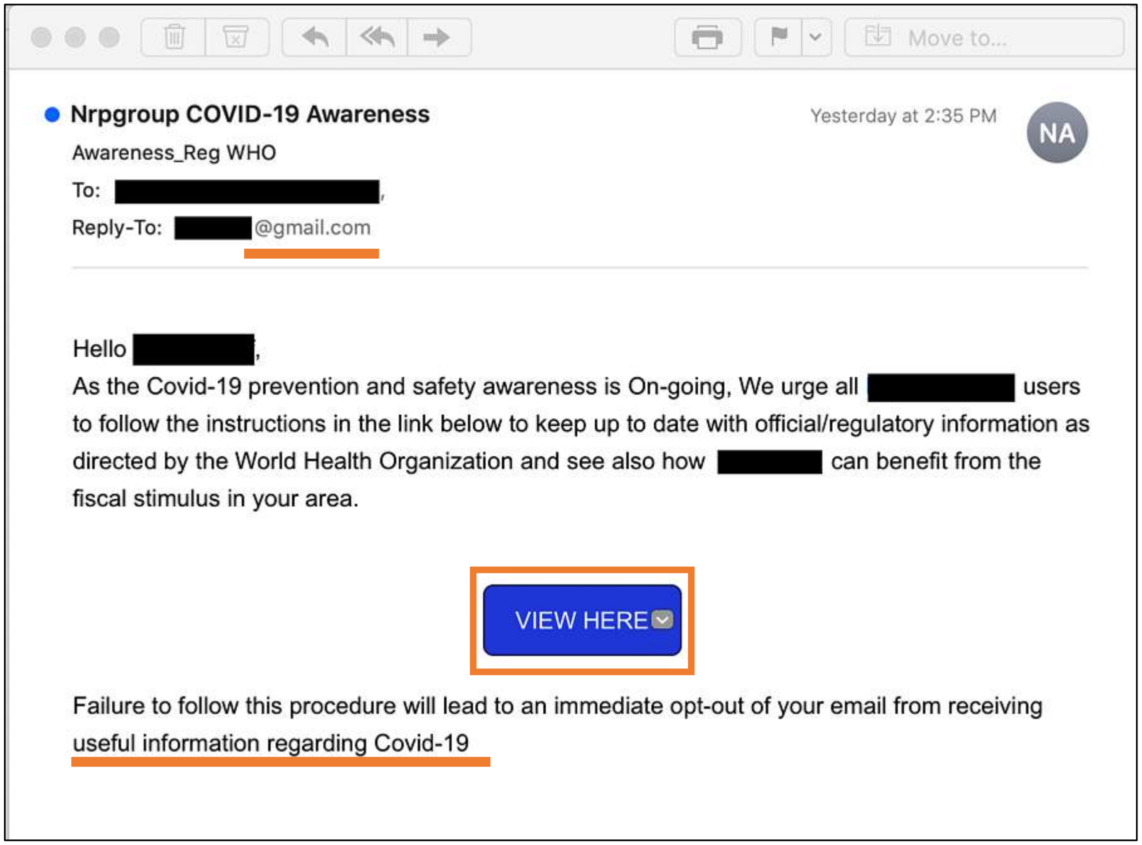
Note: Late pa uthentication.

Thank you,
American Exp

https://docs.google.com/document/d/e/2PACX-1vQVl9ylqOK3C-3srmNPRoWNC1aeO4rcqKyEKX4FsHWR5pKPTC29mRzA0oxW7pZnYxOkaeb_jglfHmVv/pub

Stimulus Focused Attacks

- Always be cautious of emails from free providers such as Gmail, Hotmail, etc.
- This uses a reputable organization (WHO) to lend credibility to the message.
- The link is likely tied to a site hosting malware but can also be used to present someone with a fake login portal to steal credentials.



Nrpgroup COVID-19 Awareness   Yesterday at 2:35 PM

Awareness_Reg WHO

To: [redacted],

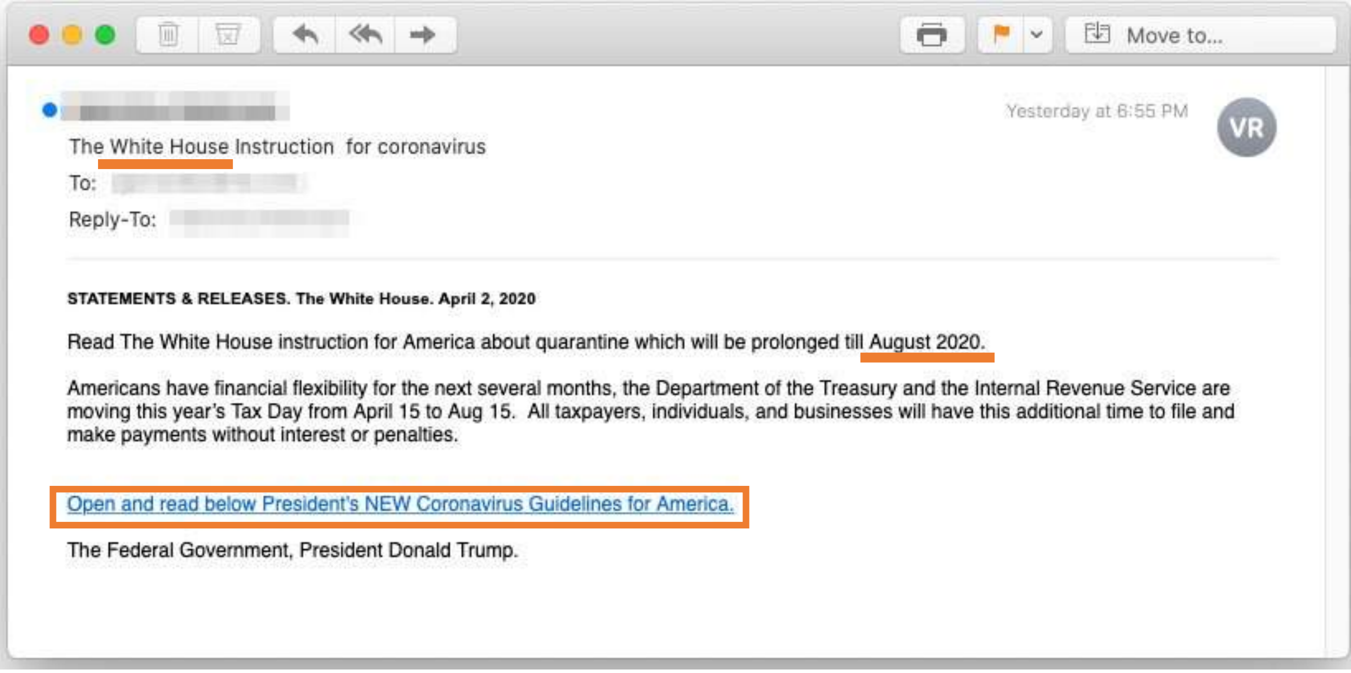
Reply-To: [redacted]@gmail.com

Hello [redacted],
As the Covid-19 prevention and safety awareness is On-going, We urge all [redacted] users to follow the instructions in the link below to keep up to date with official/regulatory information as directed by the World Health Organization and see also how [redacted] can benefit from the fiscal stimulus in your area.

Failure to follow this procedure will lead to an immediate opt-out of your email from receiving useful information regarding Covid-19

COVID-19 Focused Attacks

- Using the White House to make it seem credible.
- The note about extending to August 2020 is about fear and outrage.
- The link went to a site hosting a malware infected Word document that prompted people to “allow editing” and “enable content”.



[redacted]

Yesterday at 6:55 PM

VR

The White House Instruction for coronavirus

To: [redacted]

Reply-To: [redacted]

STATEMENTS & RELEASES. The White House. April 2, 2020

Read The White House instruction for America about quarantine which will be prolonged till August 2020.

Americans have financial flexibility for the next several months, the Department of the Treasury and the Internal Revenue Service are moving this year’s Tax Day from April 15 to Aug 15. All taxpayers, individuals, and businesses will have this additional time to file and make payments without interest or penalties.

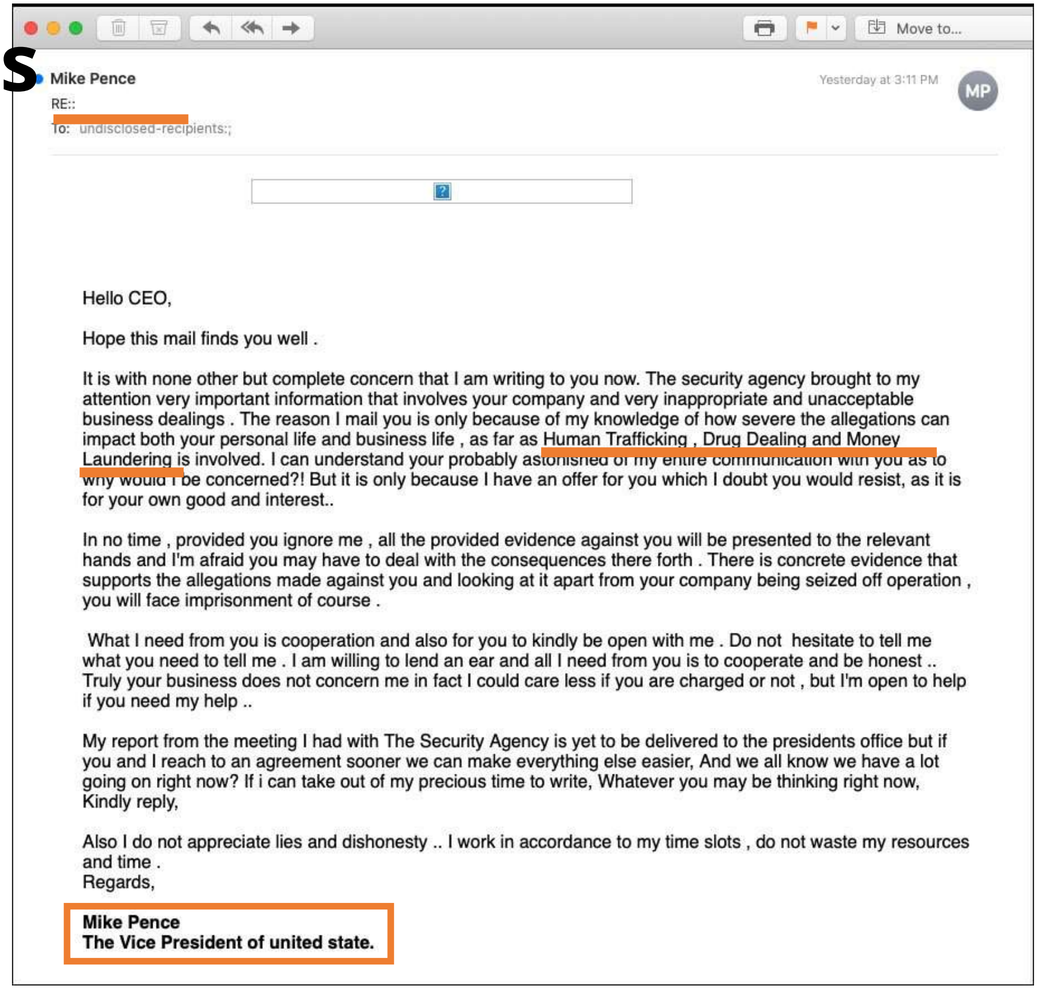
Open and read below President’s NEW Coronavirus Guidelines for America.

The Federal Government, President Donald Trump.

Image from: **https://www.bleepingcomputer.com/news/security/phishing-emails-impersonate-the-white-house-and-vp-mike-pence/**

COVID-19 Focused Attacks

- Supposed to be coming from the VP of the United States.
- No subject line and full of grammar and spelling errors.
- The idea is open communication with the victim and convince them to pay a fine rather than face imprisonment.
- A lot of small business owners are already under great stress right now. This is an emotional attack.



Mike Pence
Yesterday at 3:11 PM
RE::
To: undisclosed-recipients:;

Hello CEO,

Hope this mail finds you well .

It is with none other but complete concern that I am writing to you now. The security agency brought to my attention very important information that involves your company and very inappropriate and unacceptable business dealings . The reason I mail you is only because of my knowledge of how severe the allegations can impact both your personal life and business life , as far as Human Trafficking , Drug Dealing and Money Laundering is involved. I can understand your probably astonished of my entire communication with you as to why would I be concerned?! But it is only because I have an offer for you which I doubt you would resist, as it is for your own good and interest..

In no time , provided you ignore me , all the provided evidence against you will be presented to the relevant hands and I'm afraid you may have to deal with the consequences there forth . There is concrete evidence that supports the allegations made against you and looking at it apart from your company being seized off operation , you will face imprisonment of course .

What I need from you is cooperation and also for you to kindly be open with me . Do not hesitate to tell me what you need to tell me . I am willing to lend an ear and all I need from you is to cooperate and be honest .. Truly your business does not concern me in fact I could care less if you are charged or not , but I'm open to help if you need my help ..

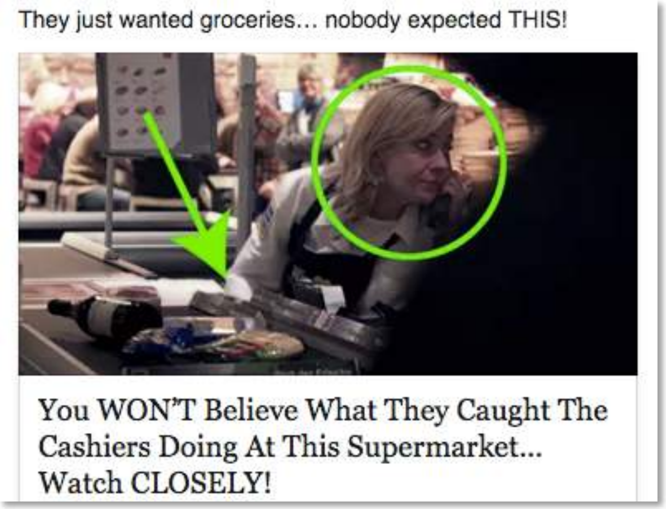
My report from the meeting I had with The Security Agency is yet to be delivered to the presidents office but if you and I reach to an agreement sooner we can make everything else easier, And we all know we have a lot going on right now? If i can take out of my precious time to write, Whatever you may be thinking right now, Kindly reply,

Also I do not appreciate lies and dishonesty .. I work in accordance to my time slots , do not waste my resources and time .
Regards,

Mike Pence
The Vice President of united state.

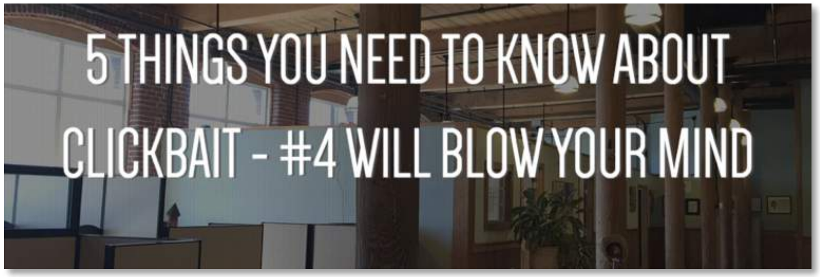
Image from: **https://www.bleepingcomputer.com/news/security/phishing-emails-impersonate-the-white-house-and-vp-mike-pence/**

Clickbait: It’s More Science Than You Think



They just wanted groceries… nobody expected THIS!

You WON’T Believe What They Caught The Cashiers Doing At This Supermarket... Watch CLOSELY!



5 THINGS YOU NEED TO KNOW ABOUT CLICKBAIT - #4 WILL BLOW YOUR MIND

- Leverages “pattern interruption” to create curiosity often based on the "information-gap" theory
- “Such information gaps produce the feeling of deprivation labeled curiosity. The curious individual is motivated to obtain the missing information to reduce or eliminate the feeling of deprivation.” - George Loewenstein, Carnegie Mellon
- Also leverages outrage and anger, which drives us to take action

Working From Home

Alta Pro
Lawyers Risk Purchasing Group

KnowBe4
Human error. Conquered.

Smart Devices and Privacy

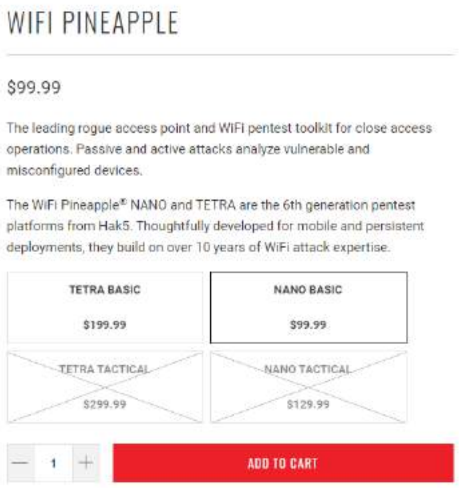
- 3 in 10 (29%) households own at least 1 smart speaker at the end of 2019, an increase from 12% in 2017.
- The number of smart homes is at 41.3m in 2020, up 18.7% from the previous year.
- What about Siri, Bixby and Google digital assistants on phones?
- When enabled, these devices listen for keywords and commands. In addition, the audio can be sent to the manufacturer and audited by humans for improvement

Smart Cameras

- Can you access any smart cameras in your home when you are away?
- Did you specifically open ports on your router to allow that access?
- Many smart cameras stream a video feed to their own servers, then you access that from the app or the web. Some license agreements state that employees might monitor these feeds on occasion for quality control or troubleshooting.
- Can your work be seen or heard by a smart camera?

WiFi

- Many homes have WiFi, however they do not have the same protections in place as most corporate networks.



WIFI PINEAPPLE

$99.99

The leading rogue access point and WiFi pentest toolkit for close access operations. Passive and active attacks analyze vulnerable and misconfigured devices.

The WiFi Pineapple® NANO and TETRA are the 6th generation pentest platforms from Hak5. Thoughtfully developed for mobile and persistent deployments, they build on over 10 years of WiFi attack expertise.

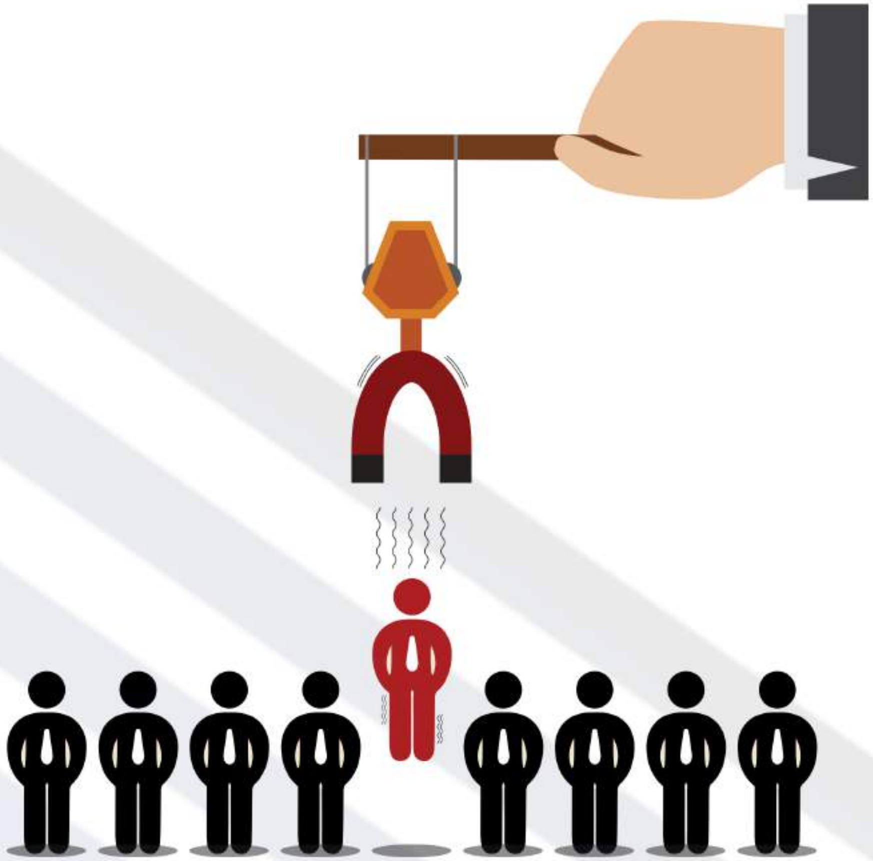
TETRA BASIC $199.99	NANO BASIC $99.99
~~TETRA TACTICAL~~ ~~$299.99~~	~~NANO TACTICAL~~ ~~$129.99~~

- If you live in a high-density area such as NYC or other urban spaces, a cheap $99 device can be used to intercept WiFi signals if you are not looking for the signs.

Our Mental State

- 2020 has been quite the year so far and attackers know this.
- People are under a great deal of stress, working conditions have changed and a lot of organizations were not prepared to do business from private homes.
- There has been an information overload, while also a lack of details that has people becoming mentally weary.
- Supply chains have been interrupted (e.g. toilet paper, alcohol and hand sanitizer) and people have started acting primal about this.

Social Engineering



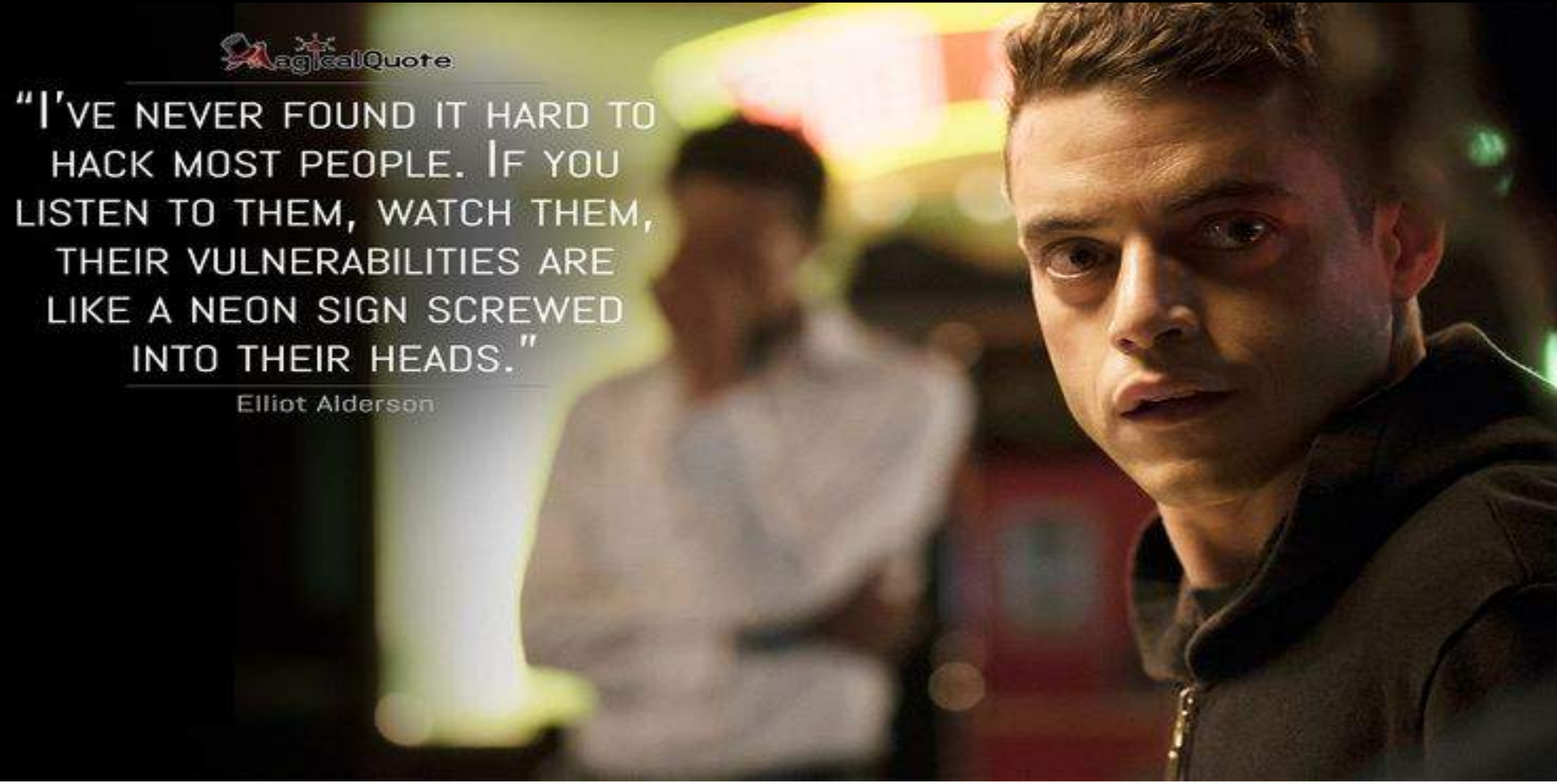
Alta Pro
Lawyers Risk Purchasing Group

KnowBe4
Human error. Conquered.

"All warfare is based on deception."

- Sun Tzu, *The Art of War*

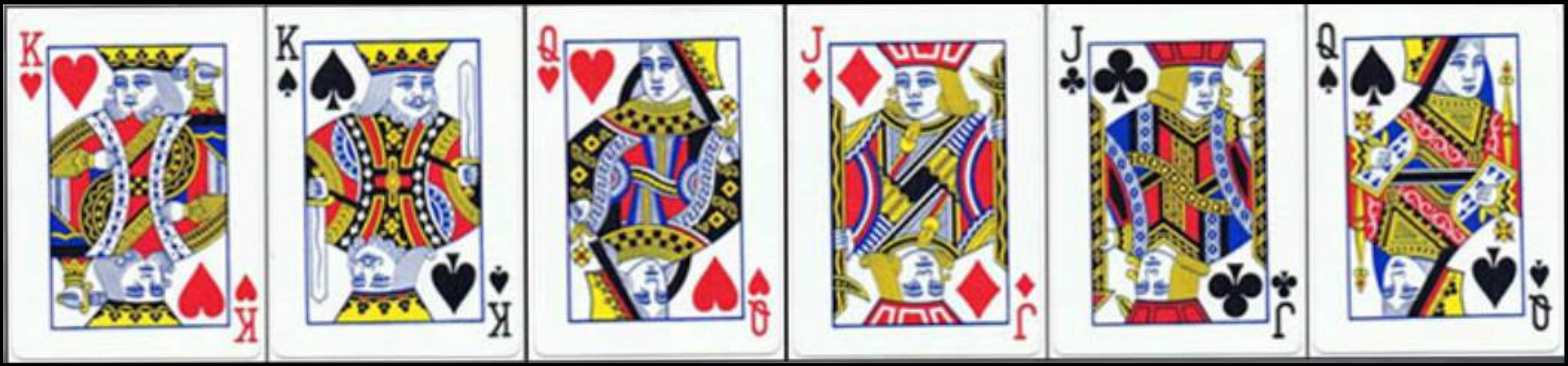
Social Engineering

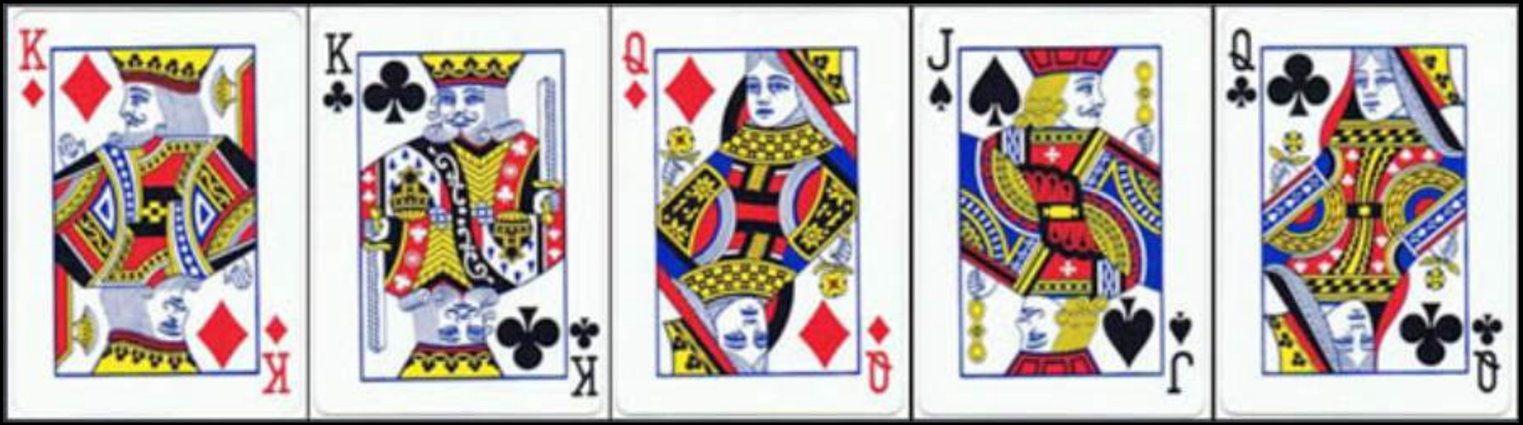


"I'VE NEVER FOUND IT HARD TO HACK MOST PEOPLE. IF YOU LISTEN TO THEM, WATCH THEM, THEIR VULNERABILITIES ARE LIKE A NEON SIGN SCREWED INTO THEIR HEADS."

Elliot Alderson

Pick a card!

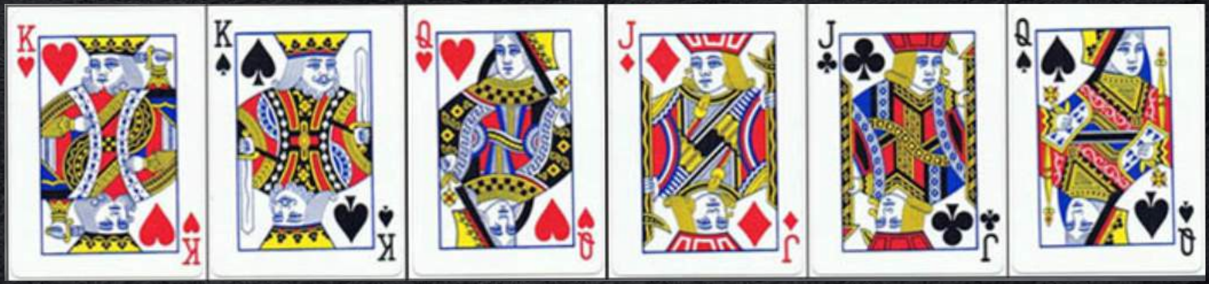




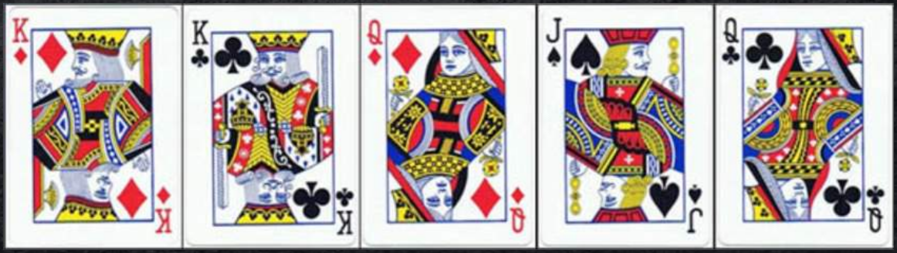
Is it gone now?

How did we identify and remove your card?

Here’s what we started with:

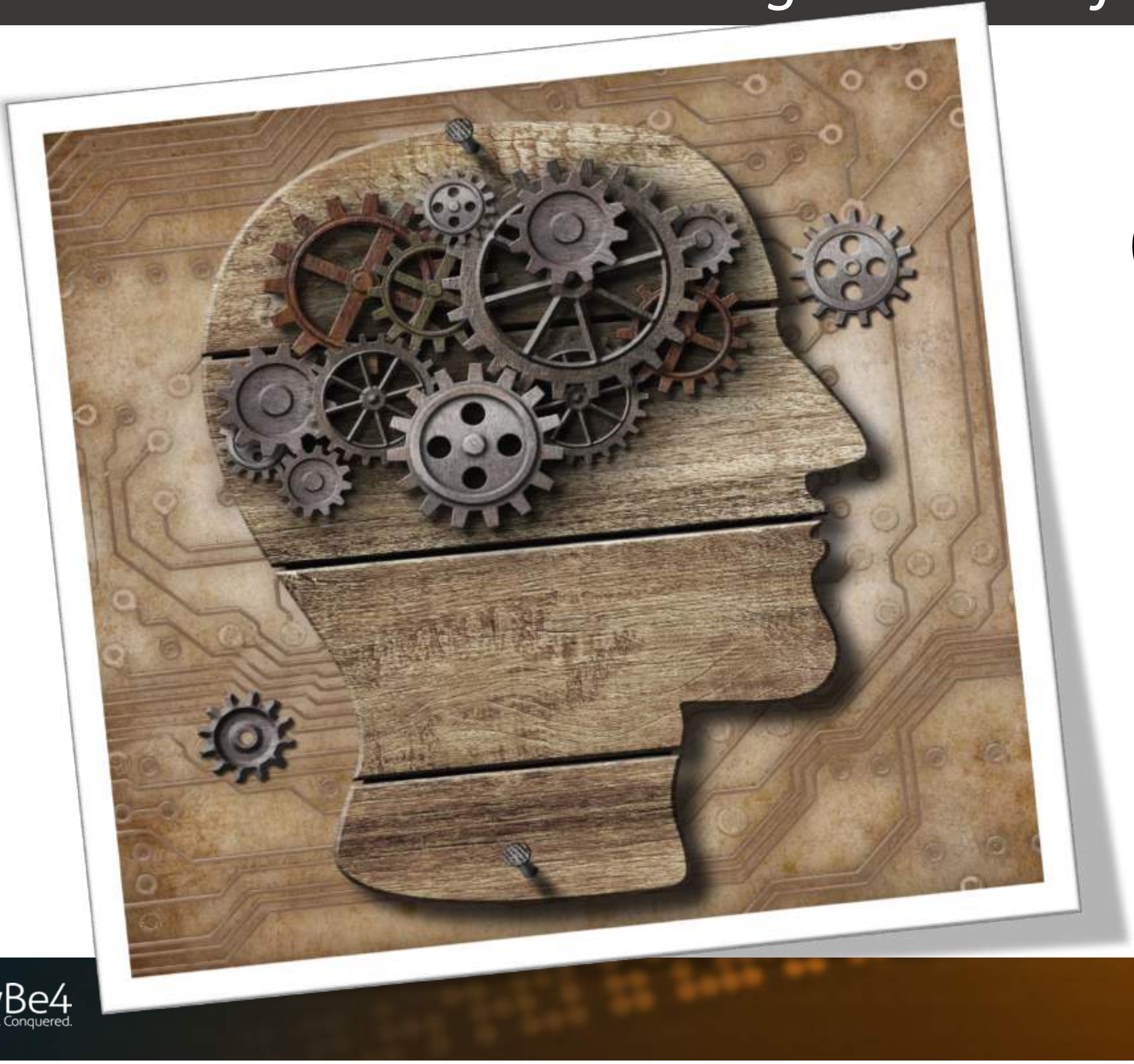


And here’s what we ended with:



Yeah: These are two completely different sets of cards.
But, by rushing you through the process, you probably didn’t notice!

Understanding the root of deception



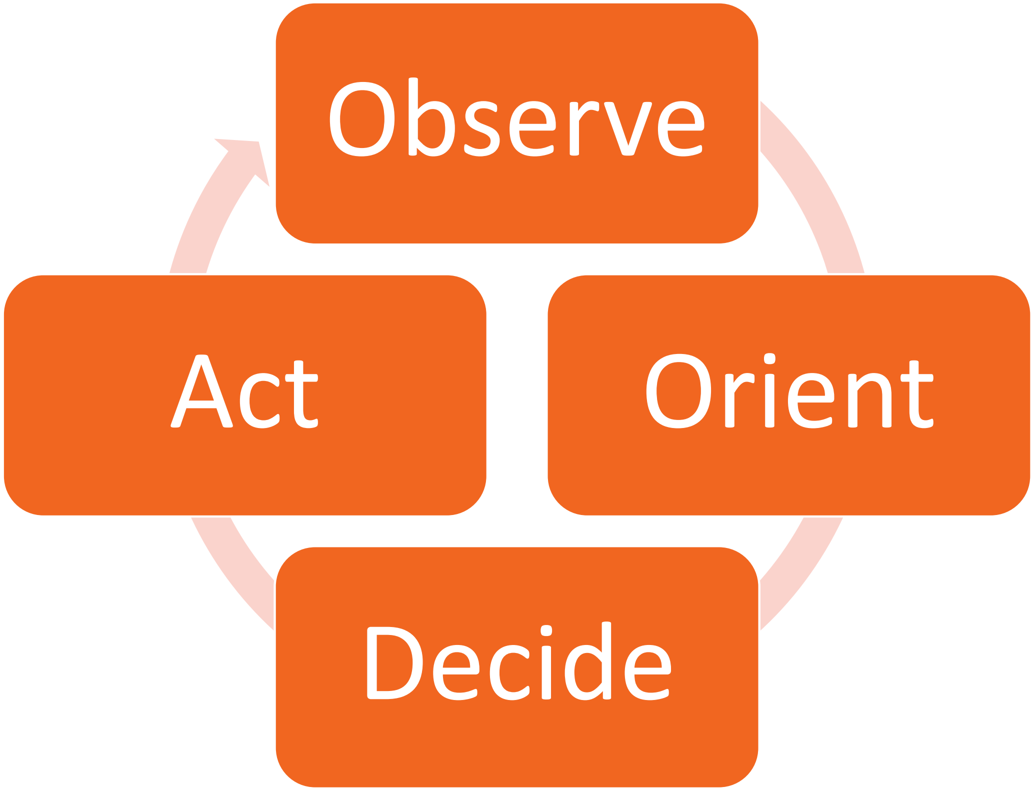
Our brains' job to filter, interpret, and present 'reality'

Spies, Magicians, Pickpockets, Con-artists and Cybercriminals all use the principles we are about to discuss

What is an OODA Loop and how do I mess with it?

"In order to win, we should operate at a faster tempo or rhythm than our adversaries—or, better yet, get inside [the] adversary's Observation-Orientation-Decision-Action time cycle or loop ... Such activity will make us appear ambiguous (unpredictable) thereby generate confusion and disorder among our adversaries—since our adversaries will be unable to generate mental images or pictures that agree with the menacing, as well as faster transient rhythm or patterns, they are competing against."

-- John Boyd (creator of the OODA Loop)

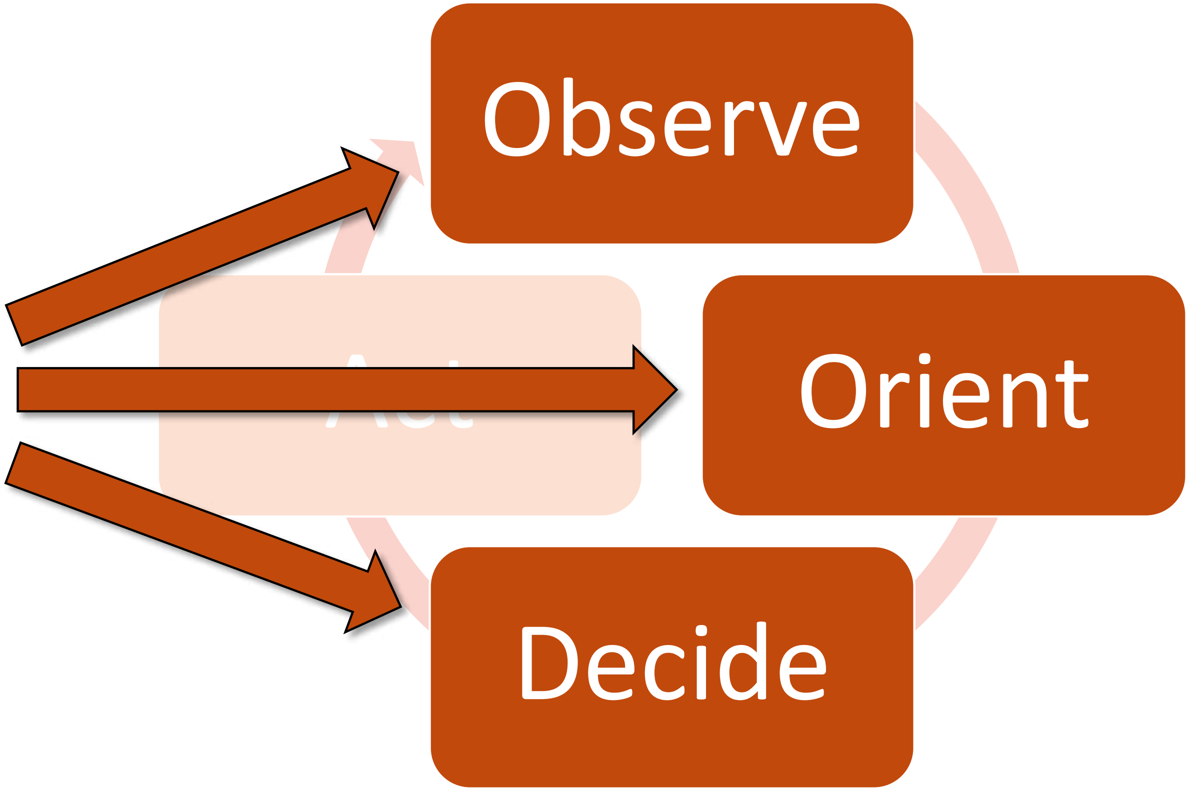


The ideal situation for a social engineer is to hijack the OODA loop by creating a knee-jerk action that effectively bypasses the first three steps and results in the attacker’s intended Action.

What is an OODA Loop and how do I mess with it?

These are critical thinking steps

These all impact the final action



Observe

Orient

Decide

Act

Future Expectations

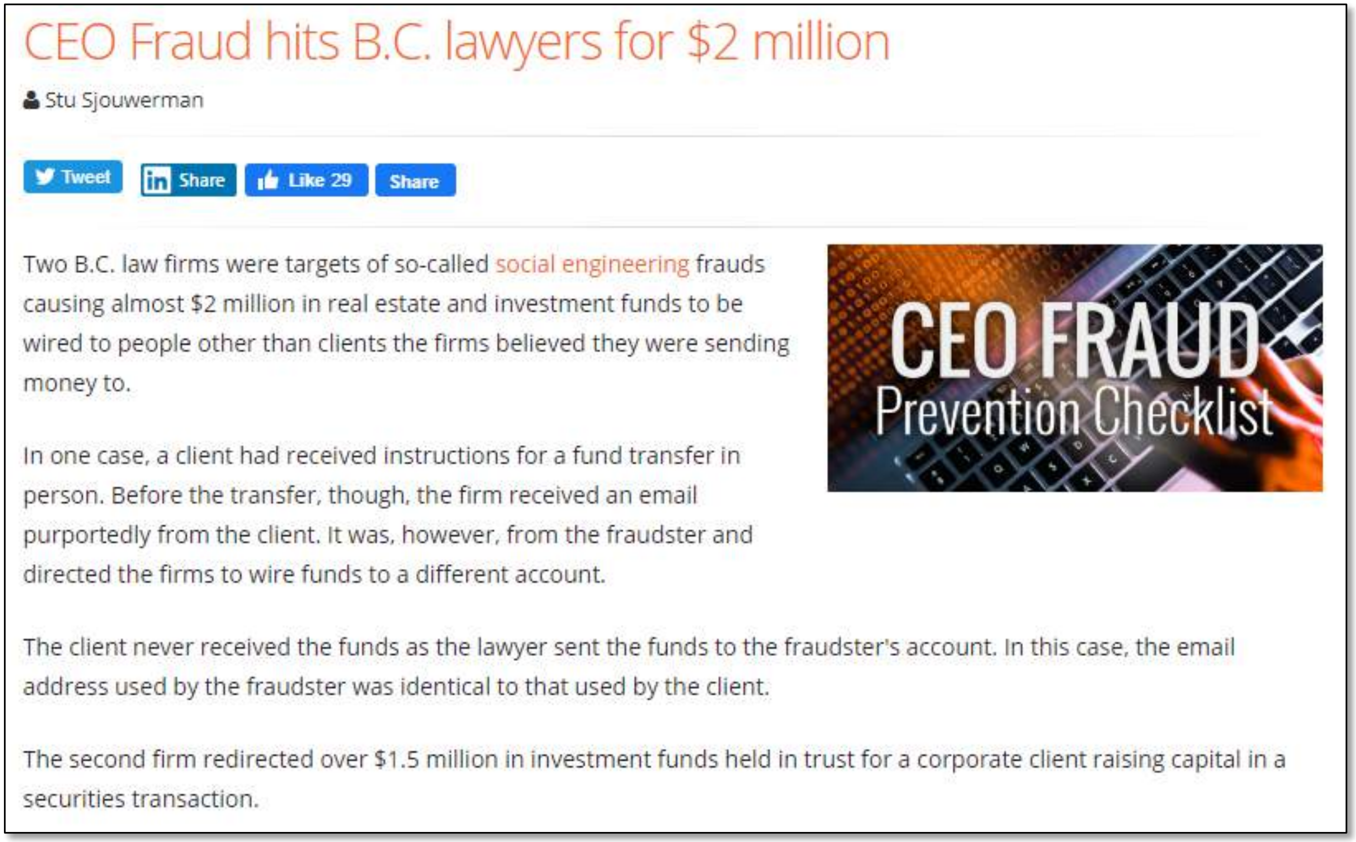
Alta Pro
Lawyers Risk Purchasing Group

KnowBe4
Human error. Conquered.

Business Email Compromise (The Phish Evolved)

- a.k.a. CEO Fraud
- No payload
- Low volume email targeting high value individuals
- Personalized
- Few to no 'traditional' spam/phishing tells (such as poor grammar, egregious misspellings, etc.)

Business Email Compromise



CEO Fraud hits B.C. lawyers for $2 million

Stu Sjouwerman

Two B.C. law firms were targets of so-called social engineering frauds causing almost $2 million in real estate and investment funds to be wired to people other than clients the firms believed they were sending money to.

In one case, a client had received instructions for a fund transfer in person. Before the transfer, though, the firm received an email purportedly from the client. It was, however, from the fraudster and directed the firms to wire funds to a different account.

The client never received the funds as the lawyer sent the funds to the fraudster's account. In this case, the email address used by the fraudster was identical to that used by the client.

The second firm redirected over $1.5 million in investment funds held in trust for a corporate client raising capital in a securities transaction.

Supply Chain and Invoice Fraud

- Criminals gain access to an email account and monitor incoming and outgoing emails.
- Bad actors create fake invoices or request payment to a different account.

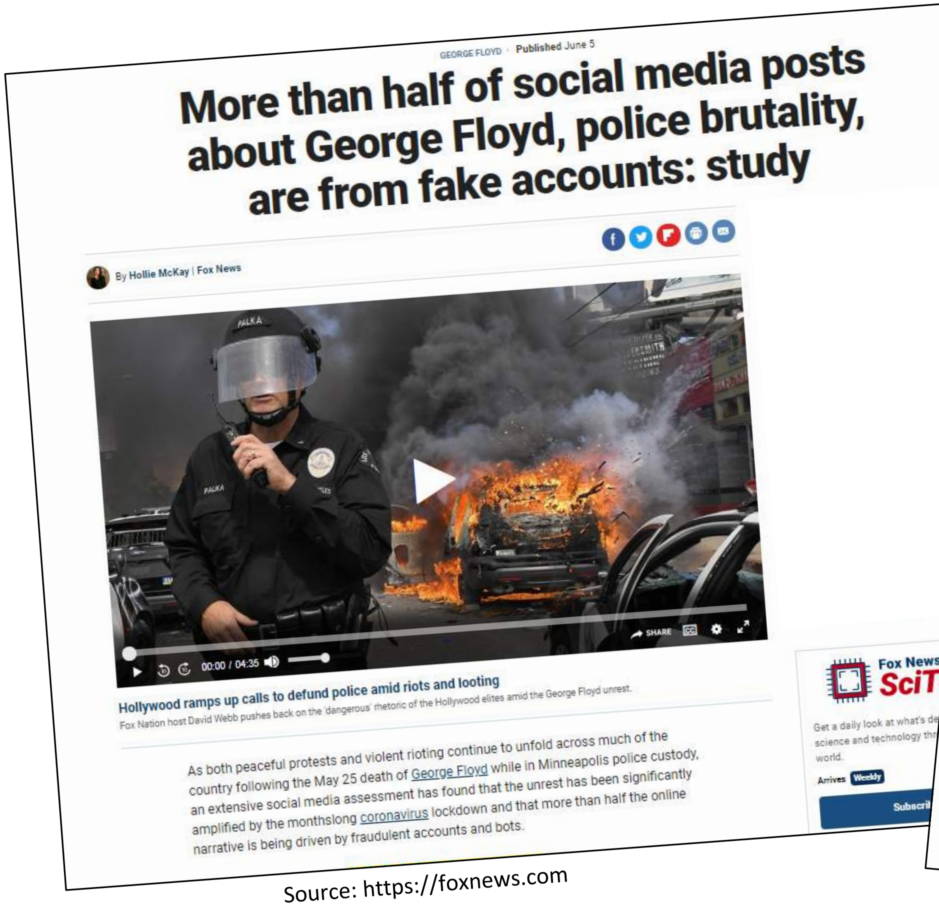
Two Unnamed US Companies Falls Victim to $100 Million CEO Email Fraud

- This scam only surfaced as the U.S. government filed a civil forfeiture lawsuit in federal court in Manhattan seeking to recover tens of millions held in at least 20 bank accounts around the world.

- The scammer, a 48-year old Lithuanian managed to trick two American technology companies into wiring him **$100 million**.

- What makes this remarkable is the amount of money he managed to score and the industry from which he stole it. The indictment specifically describes the companies in vague terms, but Apple, Cisco, HP and Facebook come to mind.

More Social Media Influence



GEORGE FLOYD · Published June 5

More than half of social media posts about George Floyd, police brutality, are from fake accounts: study

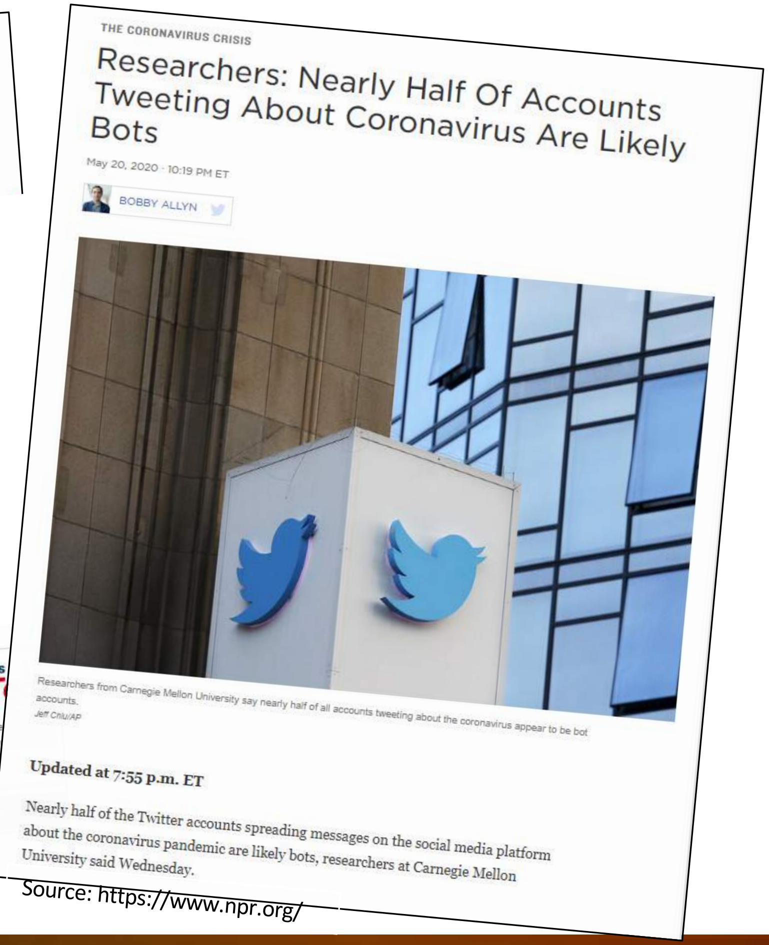
By Hollie McKay | Fox News

Hollywood ramps up calls to defund police amid riots and looting

Fox Nation host David Webb pushes back on the 'dangerous' rhetoric of the Hollywood elites amid the George Floyd unrest.

As both peaceful protests and violent rioting continue to unfold across much of the country following the May 25 death of George Floyd while in Minneapolis police custody, an extensive social media assessment has found that the unrest has been significantly amplified by the monthslong coronavirus lockdown and that more than half the online narrative is being driven by fraudulent accounts and bots.

Source: https://foxnews.com



THE CORONAVIRUS CRISIS

Researchers: Nearly Half Of Accounts Tweeting About Coronavirus Are Likely Bots

May 20, 2020 · 10:19 PM ET

BOBBY ALLYN

Researchers from Carnegie Mellon University say nearly half of all accounts tweeting about the coronavirus appear to be bot accounts.

Jeff Chiu/AP

Updated at 7:55 p.m. ET

Nearly half of the Twitter accounts spreading messages on the social media platform about the coronavirus pandemic are likely bots, researchers at Carnegie Mellon University said Wednesday.

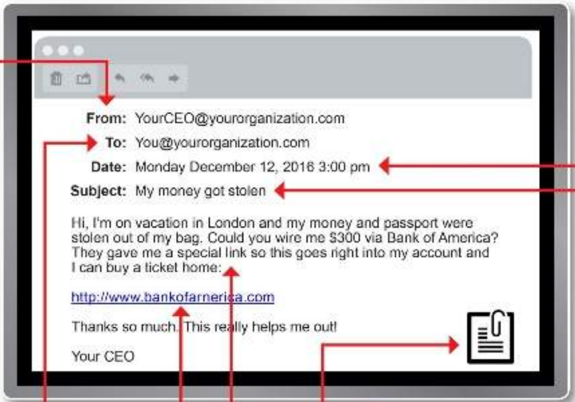
Source: https://www.npr.org/

Are You Being Manipulated?

-- understand the lures --

Greed	Curiosity	Self Interest
Urgency	Fear	Helpfulness

Social Engineering Red Flags



From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

KnowBe4
Human error. Conquered.

Questions?

KnowBe4
Human error. Conquered.

Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com

Thank You!

Erich Kron – Security Awareness Advocate

ErichK@KnowBe4.com | @KB4Erich | @ErichKron

KnowBe4
Human error. Conquered.

Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com

Conclusion

You'll need to complete the survey to receive your CLE credit.
It will open automatically in your browser after the event.
You may complete it at anytime by visiting
altaprorpg.com/postwebinar
You'll need to input the codes to qualify for CLE

Code #1 = ALTA
Code #2 = PRO

Alta Pro
Lawyers Risk Purchasing Group

KnowBe4
Human error. Conquered.