Observations from Social Engineering My Way Through a Pandemic

Dominic Clark (Parzival)

CactusCon

About Me

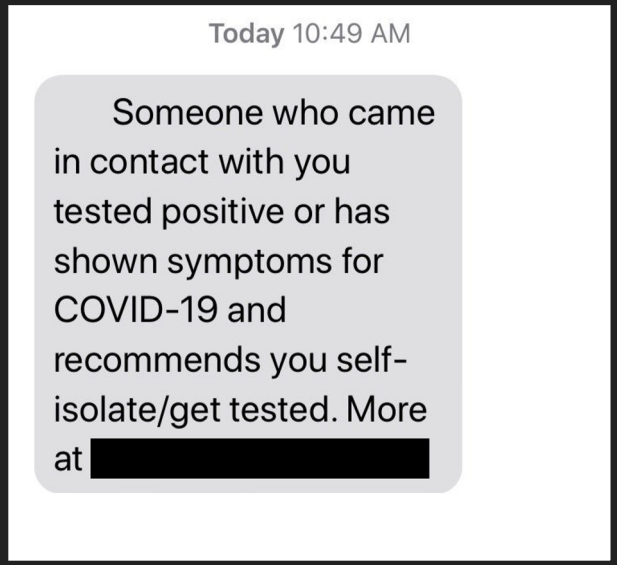
- Senior Penetration Tester
- Hacking things as long as I can remember
- Professionally hacking for 5 years
- Performing social engineering engagements for 3 years
- Proud dog dad to two amazing puppers

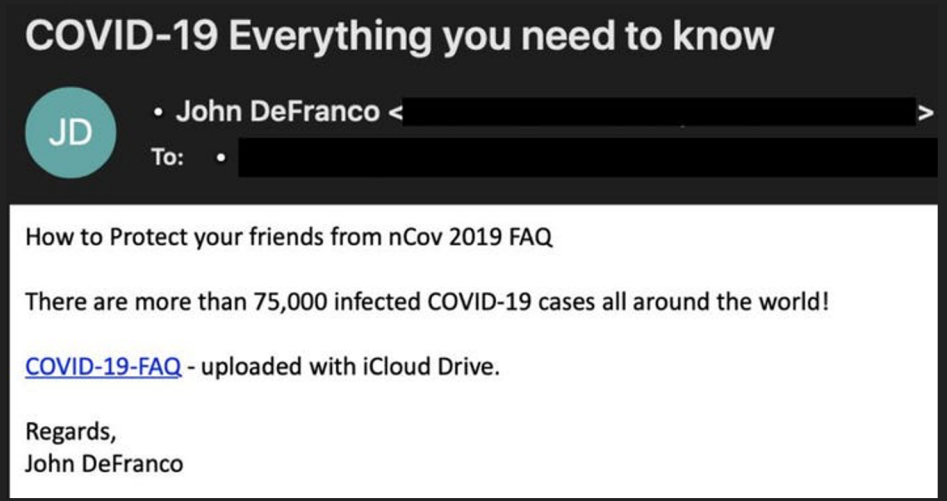
Motivations

- Social engineering attacks aren’t stopping for a pandemic
- Humans are error-prone, especially during a pandemic
- COVID-19 changed the way that millions worked.

Motivations

- Uptick in social engineering attacks throughout the pandemic
- Situation progressed faster than a lot of people thought
    - Pretexts changed day-to-day



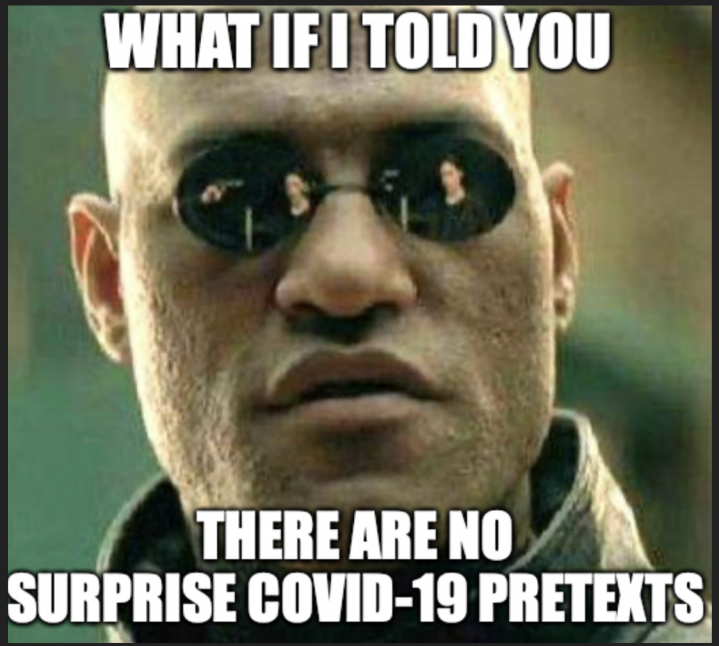


Ethics

- Many debates had for and against the use of COVID-19 campaigns
- At the end of the day, there is a public health emergency
  - I don’t want to be the reason someone doesn’t receive valid news
- This may be dependent on the organization
  - While the threat is real, we should not add fuel to the fire
- Phishing emails should be sent to educate and inform
  - We want to leave the customer in a better place, not worse.

My Ethics

- Reports of COVID-19 as a pretext being used in a poor manner
- Using COVID-19 oriented pretexts should not be a surprise
  - Companies know their culture
  - Assure the client
  - Opt out? That's okay.
- General Rules
  - Waiting waiting waiting..
  - No promises I couldn't keep
  - Don't impersonate official sources



Key Observations Throughout the Pandemic

- Clients opting out of social engineering
  - Budget cuts
  - Fuel to the fire
  - Is this the right move?
- Majority of pretexts used prior to the pandemic are still as efficient
  - Including COVID-19 is not necessary for a click
  - But if COVID is in the subject? Click.

Key Observations Throughout the Pandemic - Cont.

- Is working from home the dream?
- Increased interaction with campaigns
  - Increased opens, click rates, credential submission, and file downloads.
  - These go up and down with news coverage such as variants
- Overall, a higher rate of success during my social engineering assessments.

Phishing During the Pandemic

- Cybercriminals can be lazy
  - We don’t need to reinvent the wheel
  - Pretexts working before the pandemic will work fine
  - Let’s just tailor what we have to the ongoing pandemic

Phishing Pretexts

- A few phishing pretexts with high success rates (with a COVID-19 twist)
  - Updated Dress Code

Subject: Coronavirus Dress Code Updates

Dear all,

We're continuing to closely monitor updates around the coronavirus (COVID-19) outbreak.

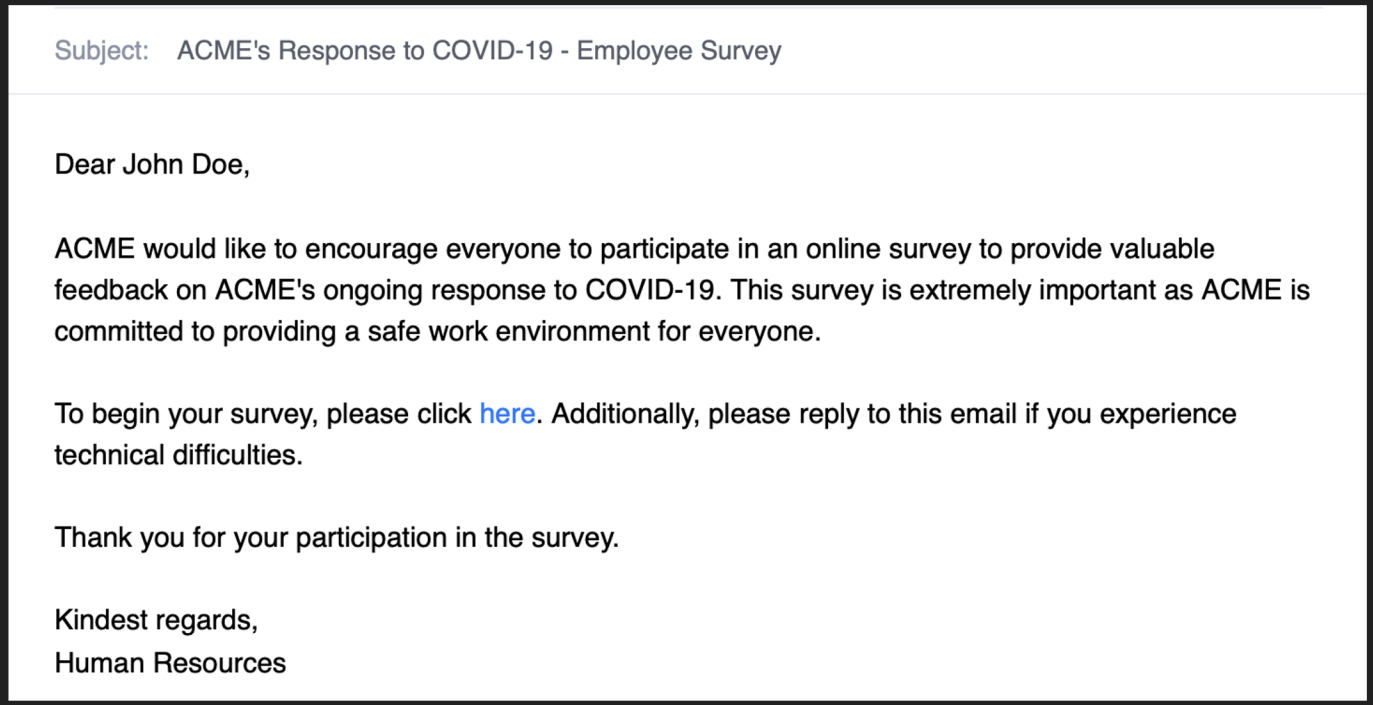
Due to the new safety standards introduced by the World Health Organization, Acme employees are now required to follow a strict new dress code policy which can be located at the following link: https://doesanybodyreadthelink.com/covid/dresscode

Please contact your manager or reply to this email if you have any questions on these updates.

Thank you for your continued cooperation,
Acme LLC

Phishing Pretexts

- A few phishing pretexts with high success rates (with a COVID-19 twist)
  - Employee survey on COVID-19



Subject: ACME's Response to COVID-19 - Employee Survey

Dear John Doe,

ACME would like to encourage everyone to participate in an online survey to provide valuable feedback on ACME's ongoing response to COVID-19. This survey is extremely important as ACME is committed to providing a safe work environment for everyone.

To begin your survey, please click here. Additionally, please reply to this email if you experience technical difficulties.

Thank you for your participation in the survey.

Kindest regards,
Human Resources

Vishing During the Pandemic

- Vishing can be a lot more unpredictable.. But fun
- It’s not weird to be the new employee.
- Less opportunities for employees onboarded during the pandemic
- Background noise is less of an issue (bork bork)
- Finally, someone to talk to!

Vishing Pretexts

- A few vishing pretexts with high success rates (with a COVID-19 twist)
  - Impersonating IT to inform the employee that something broke (like a VPN) and I needed them to verify they can still access a site using their credentials
    - Citing work from home breaking everything
    - This pretext was expanded upon to enumerate sensitive information such as usernames and passwords when possible
  - Impersonating HR per a request from an client to get verification of a COVID-19 vaccination card along with other personal information.

Vishing Scripts

<Call Answered>

Actor: Hello is this, [TARGET_NAME]?

<Response>

Actor: Great! This is Andrew Ryan from [COMPANY]. How are you doing today?

<Response>

Actor: That's good to hear! Are you working remotely right now or are you in the office?

<Response>

Actor: [SCENARIO]

<Response>

<IT Scenario>

Actor: Great! Do you happen to have your laptop nearby? And are you connected to the corporate network?

<Response>

Actor: Could you please navigate to the following link? We are trying to verify whether the [TARGET] site is functioning as intended since we had some issues with it earlier today.

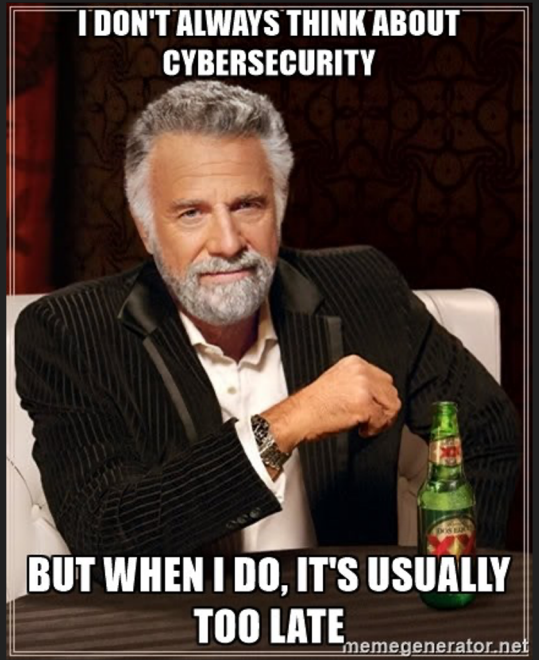
<Response>

Actor: Thank you! I really appreciate your help.

<End Call>

What Should We Do?

- Continue to raise awareness and educate employees
  - Attackers will continue to sink to these depths
- Prepare for these attacks to continue in different formats
  - Student loan extensions
  - Additional COVID variants
  - What's next?



Articles Referenced & Other Fun Links

- Jake Williams' Twitter Thread of Using COVID-19 as a Pretext https://twitter.com/MalwareJake/status/1237871580094459907
- Social Engineering Attacks During the COVID-19 Pandemic: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7866964/
- Verizon - Analyzing the COVID-19 Data Breach Landscape https://www.verizon.com/business/resources/articles/analyzing-covid-19-data-breach-landscape/
- A Content Analysis of COVID-19 Themed Phishing Emails https://journals.sagepub.com/doi/10.1177/21582440211031879
- NotDan's Twitter Thread of Using COVID-19 as a Pretext https://twitter.com/notdan/status/1318608969724686336

Thank you!

- Twitter: FreeZeroDays
- GitHub: FreeZeroDays
- Website: Parzival.sh