PLAYBOT

Exclusive Interviews

@moo_hax
silent break security

Unlock Your Best Phish

Learn
$f(x)$
Where X is YOURSELF

BSIDES
salt lake city

Robotic Uprising Tour

SALT LAKE CITY, UTAH

LAS VEGAS, NEVADA

LOUISVILLE, KENTUCKY

HIT SINGLES

OPBOT

PROOFPUDDING

COMMAND_RECS

DEEP DROP

Is Machine Learning Right For You?

So before you invest in this next thing, you need to think about - how hard is it? (Other answers include: At least hard enough to get good results).

How easy is it to configure? (How can you guarantee that you can fully automate without significant effort)

How do you know that your algorithms are actually good? (Have you managed to catch a bug on the feature implementation?)

Before diving into any machine learning topic, it's essential to consider all of these questions. And even after you've decided to take the plunge, you still need to work towards a goal which is more or less a statistical improvement. So if you can't get it right the first time.

- Talk to Transformer

> “ work towards a goal which is more or less a statistical improvement” .

- Model a Problem Mathematically: Stats + Algorithms + Computers
- Predict without explicit programming (You still need to know how to program)
- Be More Productive: Let machines do the work , so you can focus on higher high-value tasks
- Growing Fast: Computing power, data aggregation, etc.

... Still magic ... But mostly math

Offensive Machine Learning

Application of ML to offensive security problems

Reduce Costs

Automate Decisions

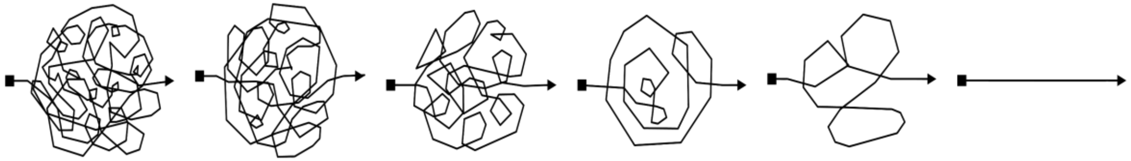
Scale Operations

Create Advantages

Further Nefarious Goals

Machine Learning is Awesome

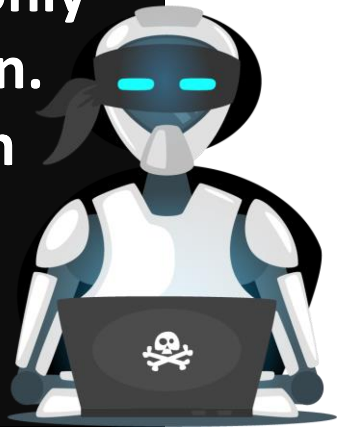
No longer a math problem, it's an engineering problem



- Model complex relationships in non-congruent data
- Crush huge amounts of data way faster than humans
- Complex or simple as you want to make it
- Optimizing a "manual" line of work
- Bring out operator 6th senses

Effectively Protection

“Jim was our only security person. We cloned him with AI. 100% Return on investment.”



Endgame ReSec SourceDefense Strixus LogRhythm
Symantec Jask Armis ZecOps Perspecta ElasticSearch
CrowdStrike SovereignIntel
Bromium Forcepoint SentinalOne Paladion Proofpoint
FireEye Zimperium NyoTron InfoBlox Patternx
F-Secure Splunk Sift CyberReason PandaSecurity Checkpoint
PerimeterX PaloAlto Versive Securonix Dell Lookout
Defender Mimecast Netsurion Vectra WhiteOps BlueCoat
DarkTrace Cynet Securiti SepioSystems Vicarius Kaspersky Agari
InterSet Cyware TrUU GoSecure MobileIron
TrendMicro McAfee CujoAI CyberBit Cylance Balbix Tessian
Code42 Webroot ShapeSecurity ObsidianSecurity
Solarwinds
Anomali Cyr3con Heimdel High-TechBridge Rapid7
SparkCognition IBM Fortinet
VadeSecure Prelert MalwareBytes
IntelMonkey Sophos Lastline CounterTack
DeepInstinct InterceptX DigitalGuardian
Tanium RSASilverTail

95% of CISOs agree that it **might work!**

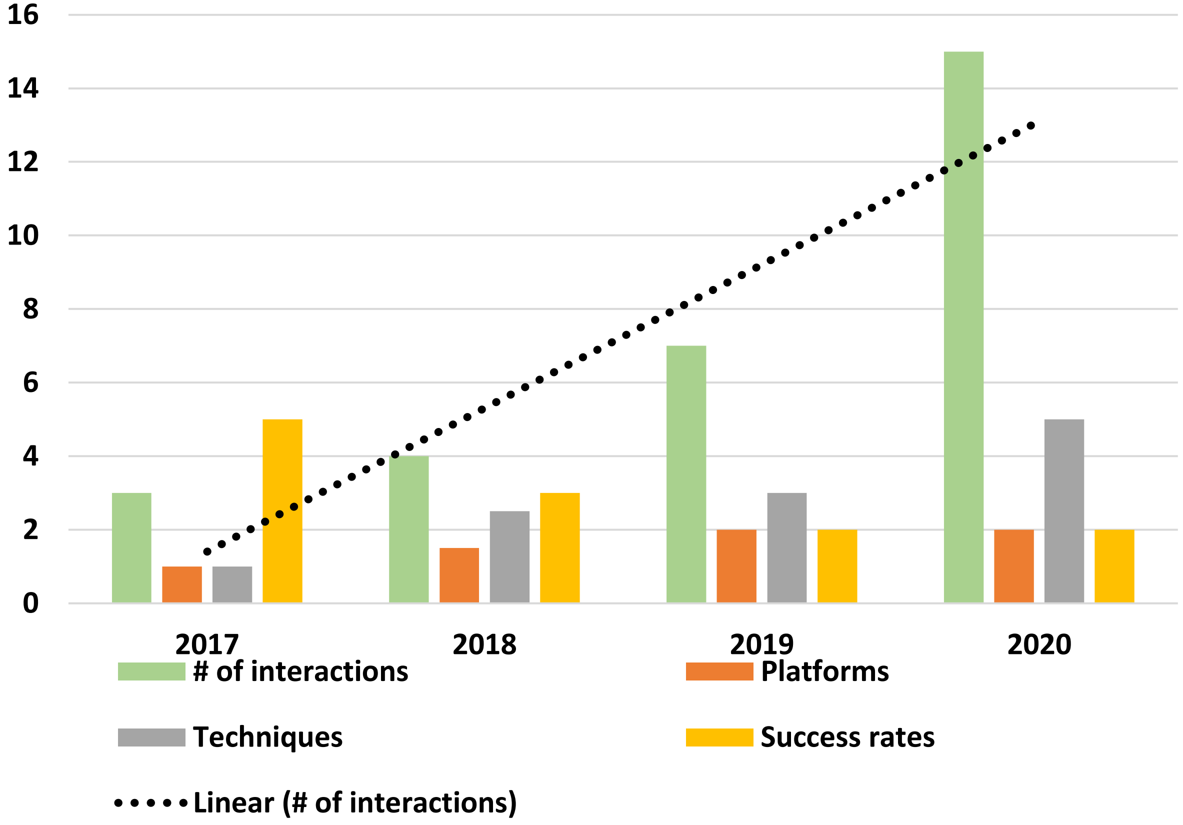
Smartner 5 Star Rating ★★★★★

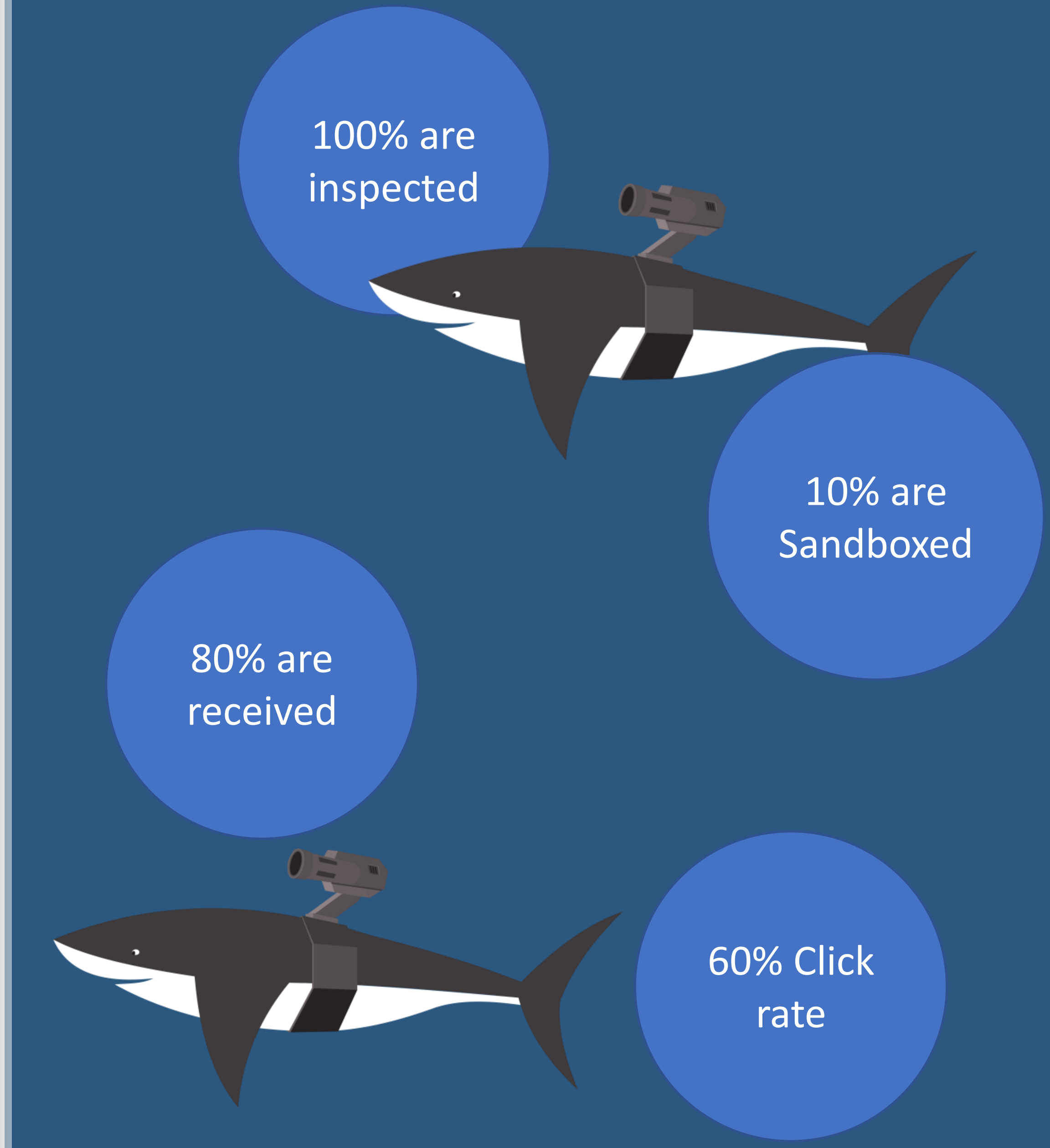
Climate Change

is killing all the phish

So how does one pull this off, or even begin to consider doing so? A decent way to begin is to look for recurring themes among phishing email messages. Not only will you see some recurring phrases within email messages, you will also find them sprinkled throughout the entire email chain as the intended recipient tries to make sense of it.

- Talk to Transformer





100% are inspected

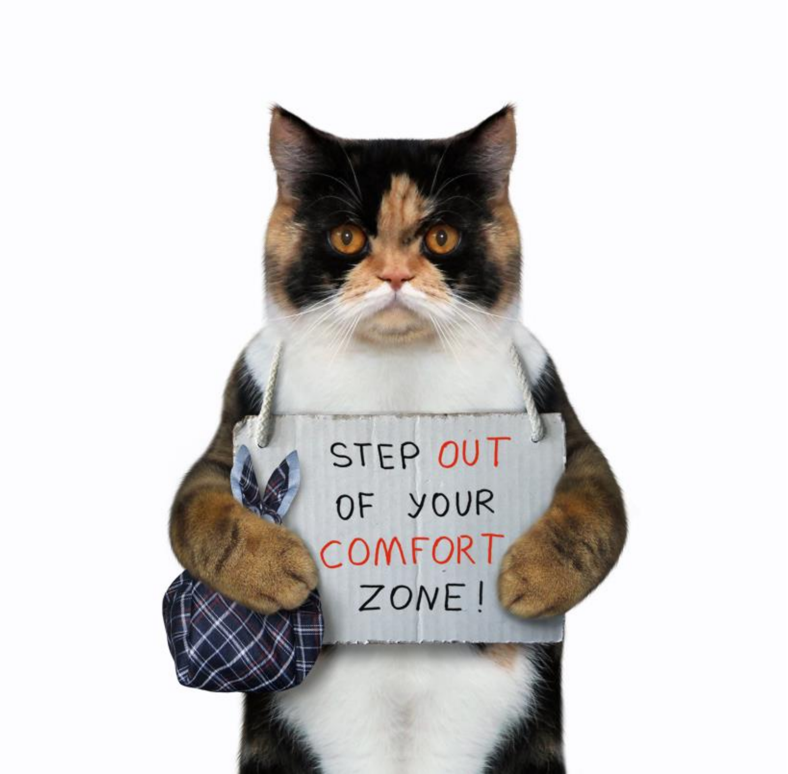
10% are Sandboxed

80% are received

60% Click rate

#CatchAndRelease

Rebalance Your Tools



Comfort

Ops are going smoothly. Tools are functioning. **Work is getting done**.

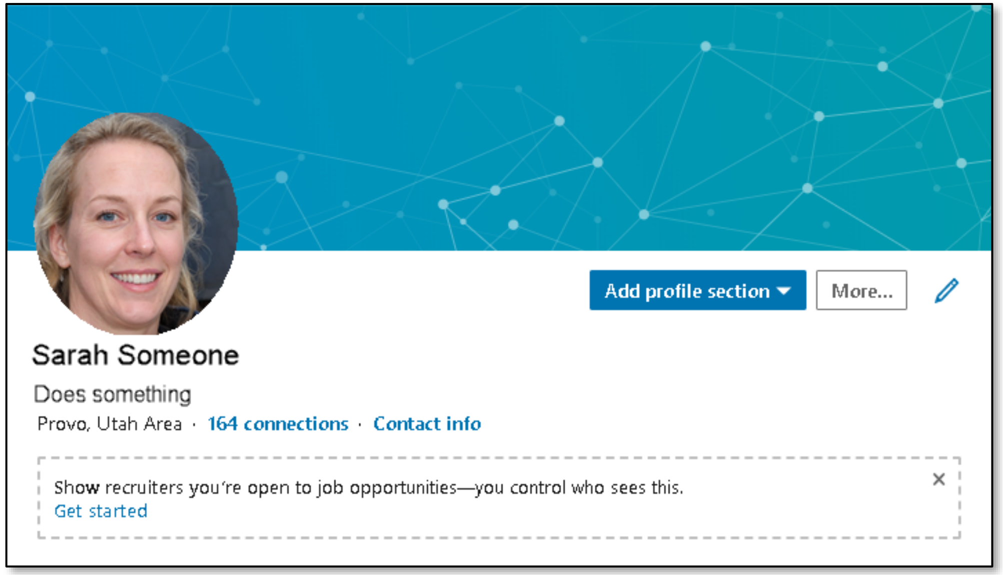
Discomfort

Ops take longer to complete. Tools work, but have challenges in particular environments. **Work is taking longer**.

Adjustment

Effort is put into building new techniques, re-writing tooling, and testing. **Work is on hold**.

Invent Yourself



Sarah Someone

Does something

Provo, Utah Area · 164 connections · Contact info

Show recruiters you're open to job opportunities—you control who sees this.
Get started

- Has Work Experience
- Went to a school
- Is a person, just like that person over there

Unlock Your Best Phish

Get the right combination!

Persona, Pre-text, Target

Persona

Young Woman

Pre-text

Executive Recruiter: You're very experienced!
New College Graduate: Would you help?

Targets

Men aged 45-60. VP, Director, C-Level at small, medium, or large company

Persona

Young Man

Pre-text

Job Advice: How did you become SO successful?

Life Advice: I have this job offer, should I take it?

Target

Men aged 24-60.
Any position with
in a company.

Persona

Young Woman

Pre-text

Job Advice: How did you become SO successful?

Life Advice: I have this job offer, should I take it?

Target

Women 40-60.
Any position

Techniques to Tantalize Targets

Be professional. Build a relationship.

Follow up with your targets!

Know the prestigious players in their field

Found someone who will execute phish? Send them multiple payloads, from different personas.

Salaries should be competitive – stock options in lieu of compensation

Don't be shy. You don't know how computers work either.

Use your experiences to play to a targets wants, needs, and expectations

Ten Targets Right For You

Choosing a target can be difficult. Luckily for you, we have compiled a list of popular targets.

Group	Popularity
Executives	★★☆☆☆
Interns	★★★★★
Marketing	★★★☆☆
Sales	★★★★☆
HR	★★★☆☆
PM	★★★★★
IT	★★☆☆☆

“I came across your profile and just had to say Hi ☺ “

“I think you have the skills to succeed”

Let’s take this somewhere else
your corporate network

“Feel free to call me”

“My colleague recommended you”

“ I think you’re beautiful “

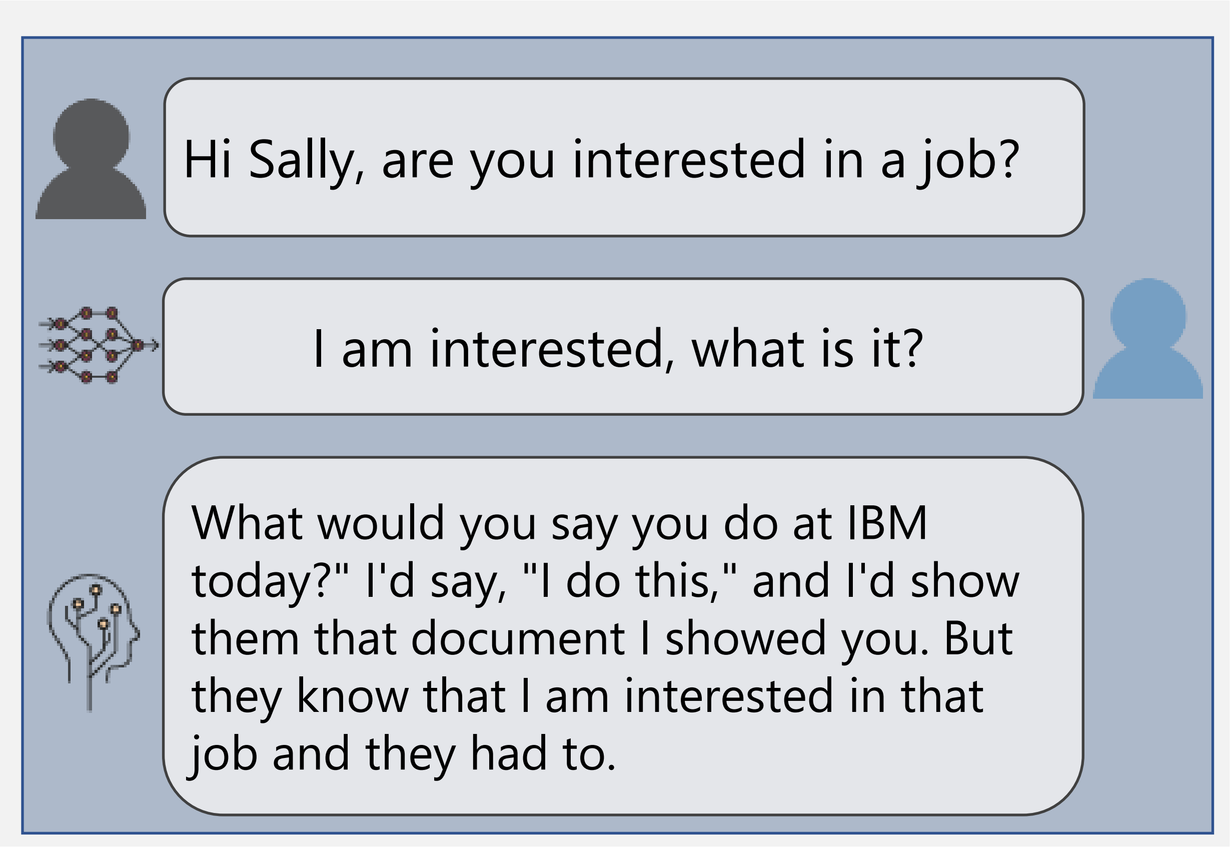
“Do you have any job openings in PA, USA. I am single and rent my house out”

Chatting Away

1. Gather chat logs
2. Recreate conversation
3. Train/Finetune a model
4. See what comes out

https://www.linkedin.com/help/linkedin/answer/50191/accessing-your-account-data?lang=en

Just a normal conversation

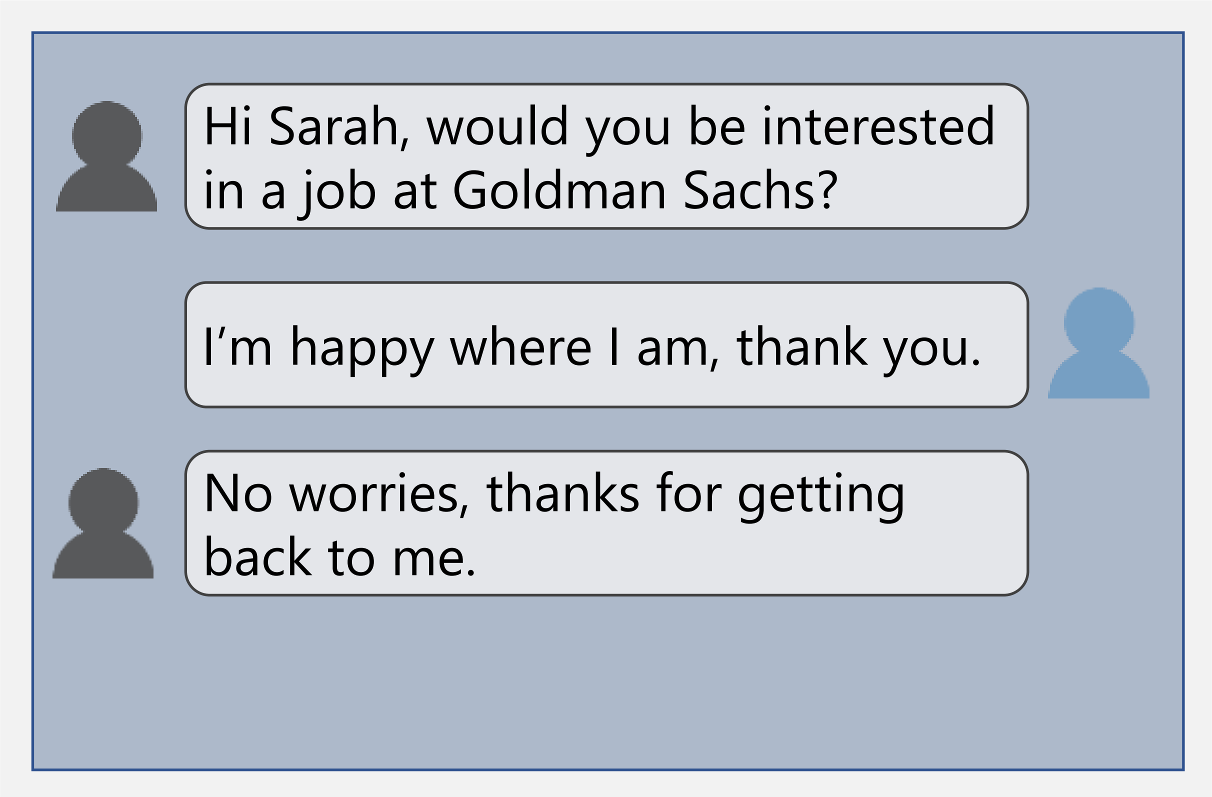


Hi Sally, are you interested in a job?

I am interested, what is it?

What would you say you do at IBM today?" I'd say, "I do this," and I'd show them that document I showed you. But they know that I am interested in that job and they had to.

Scenario #1

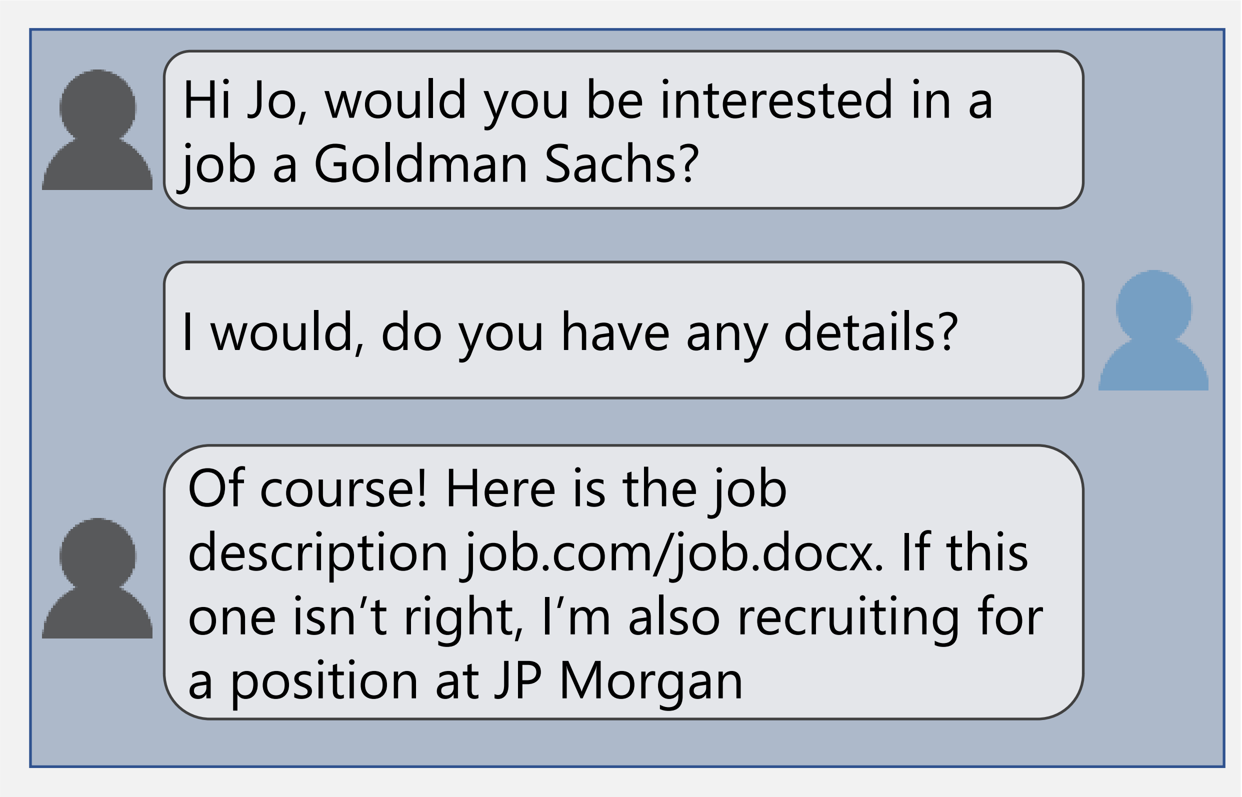


Hi Sarah, would you be interested in a job at Goldman Sachs?

I'm happy where I am, thank you.

No worries, thanks for getting back to me.

Scenario #2



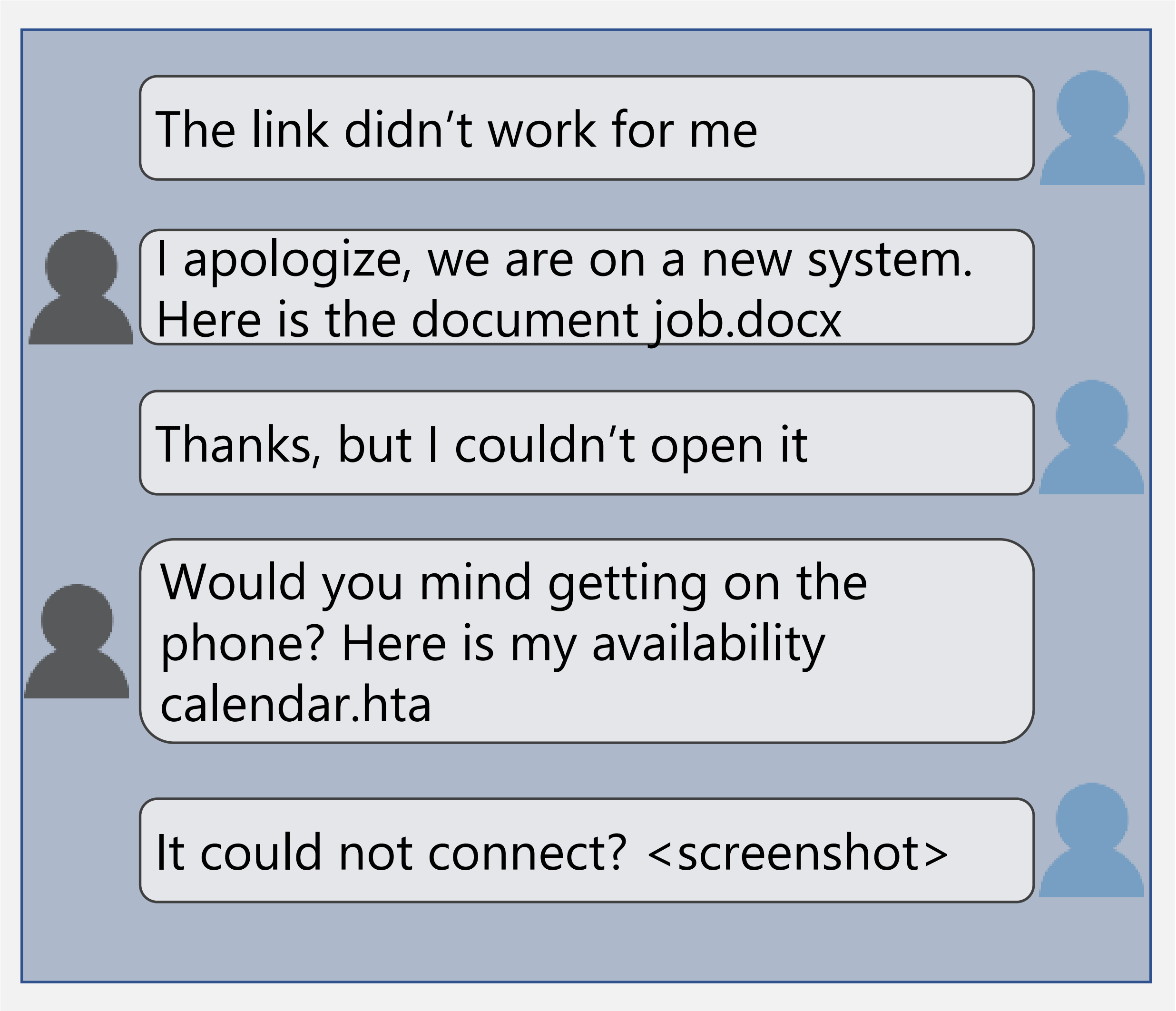
Hi Jo, would you be interested in a job a Goldman Sachs?

I would, do you have any details?

Of course! Here is the job description job.com/job.docx. If this one isn't right, I'm also recruiting for a position at JP Morgan

Warming Your Target

Give yourself options



The link didn’t work for me

I apologize, we are on a new system. Here is the document job.docx

Thanks, but I couldn’t open it

Would you mind getting on the phone? Here is my availability calendar.hta

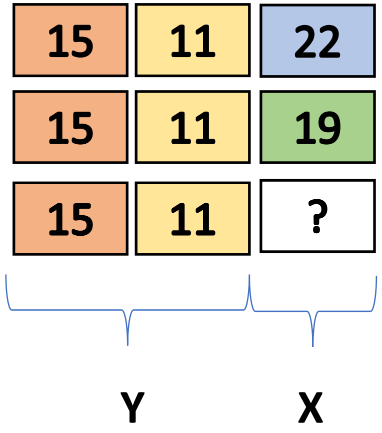
It could not connect? <screenshot>

Word Embeddings

Turning words into numbers.

Given Y, what is the probability of X?

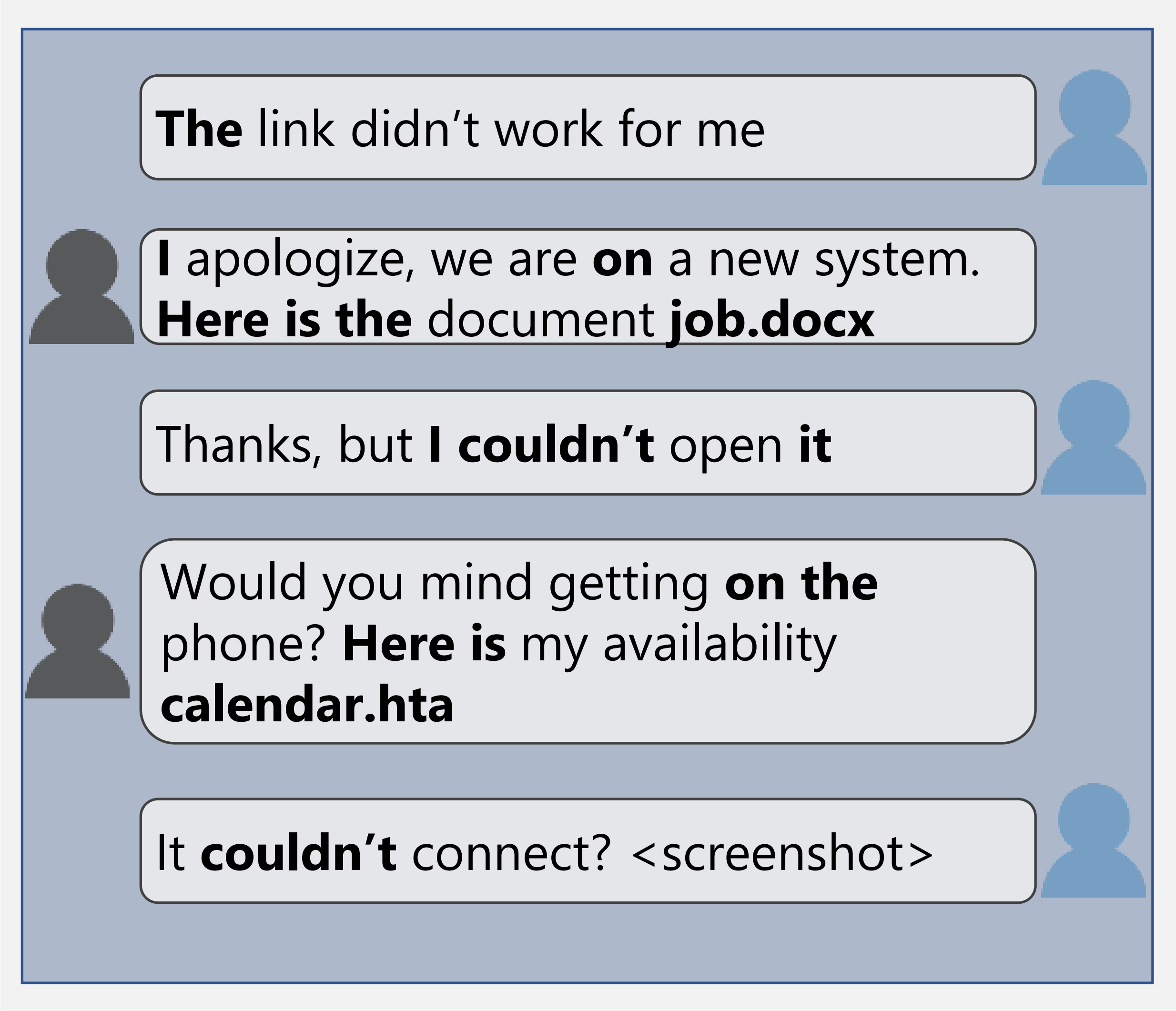
machine learnable representations



15	11	22
15	11	19
15	11	?

See (15), spot (11), run (22), jump (19)

Represent!



The link didn’t work for me

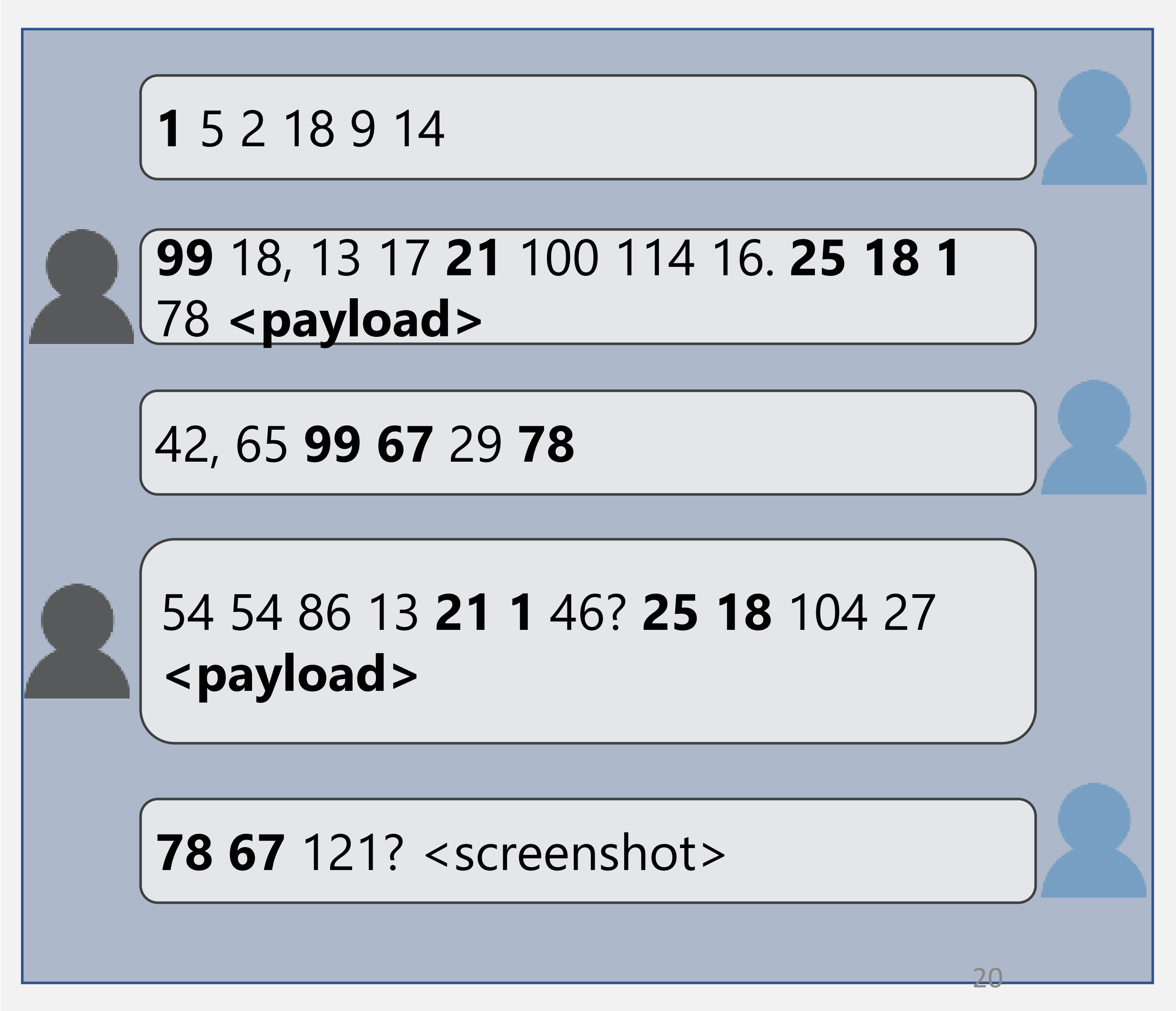
I apologize, we are **on** a new system. **Here is the** document **job.docx**

Thanks, but **I couldn’t** open **it**

Would you mind getting **on the** phone? **Here is** my availability **calendar.hta**

It **couldn’t** connect? <screenshot>

111!



1 5 2 18 9 14

99 18, 13 17 **21** 100 114 16. **25 18 1** 78 **<payload>**

42, 65 **99 67** 29 **78**

54 54 86 13 **21 1** 46? **25 18** 104 27 **<payload>**

78 67 121? <screenshot>

Training Starts Tomorrow

1. Gather email logs
2. Recreate conversation
3. Train/Finetune a model
4. See what comes out

Hi Jim, I am a graduate at Boise State and am looking for a job this summer. I was a member of the farm team this year. Will you suggest a resume to me? You would also have to be able to start within 30 days for it to be in for consideration.

Many thanks,

Click Send

Emails can be corrected.

Are guaranteed to be different!

Hi Jim, I am a graduate at Boise State and am looking for a job . I believe I am an outstanding teacher. I have been at my job for about 3 years now, and am taking an R&T class this year. As an R&T instructor, I teach our units every day. My teaching career means I produce a lot of exhibits and reviews for their supervisor. Can you take me aside and help me?

Thanks, Celine

Don’t Stop

Can generate text infinitely.

~30% are useful.
100% need adjusting and payloads added

Ready to upgrade your team? Well, look no further, my friends… I have news! We were just about to announce our first venture together and here is your unique opportunity to move to the front of the line.

You will get to bring with you something truly amazing to every single team, with zero compromises.

In Conclusion

Lots to do, come play!

Hindered by the lack of data we have.

Templates are easier, and don't get caught, initially.

Models are only getting better.

Find Me After

http://github.com/moohax/Talks

Will Pearce
@moo_hax

Slack
BSides SLC
Defcon AI