

Mind Games:

Using Data to Solve for the Human Element



Masha Sedova
Co-founder, Elevate Security

About me

Cyber Analyst for
defense community



Co-Founder, building the
Human Risk Management
Platform

Built and ran Salesforce
trust engagement team

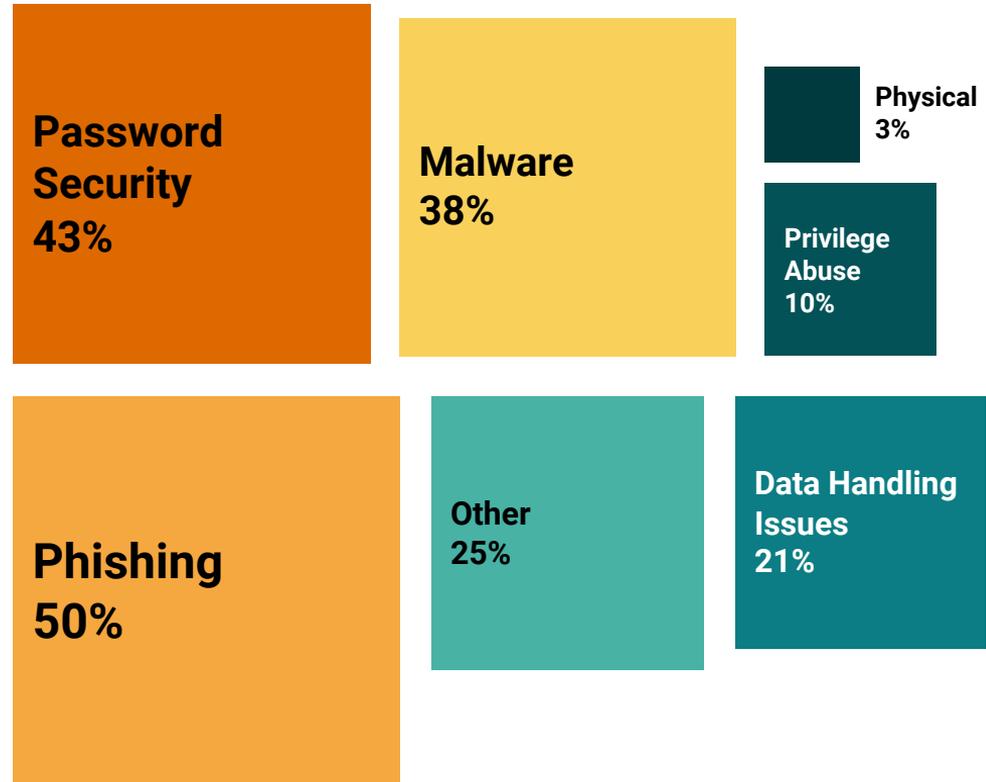


Passionate about the intersection
of security & behavioral science

**The human risk is one of the
largest unsolved problems in
security**



Human risk accounts for 5 of the top 7 breach sources

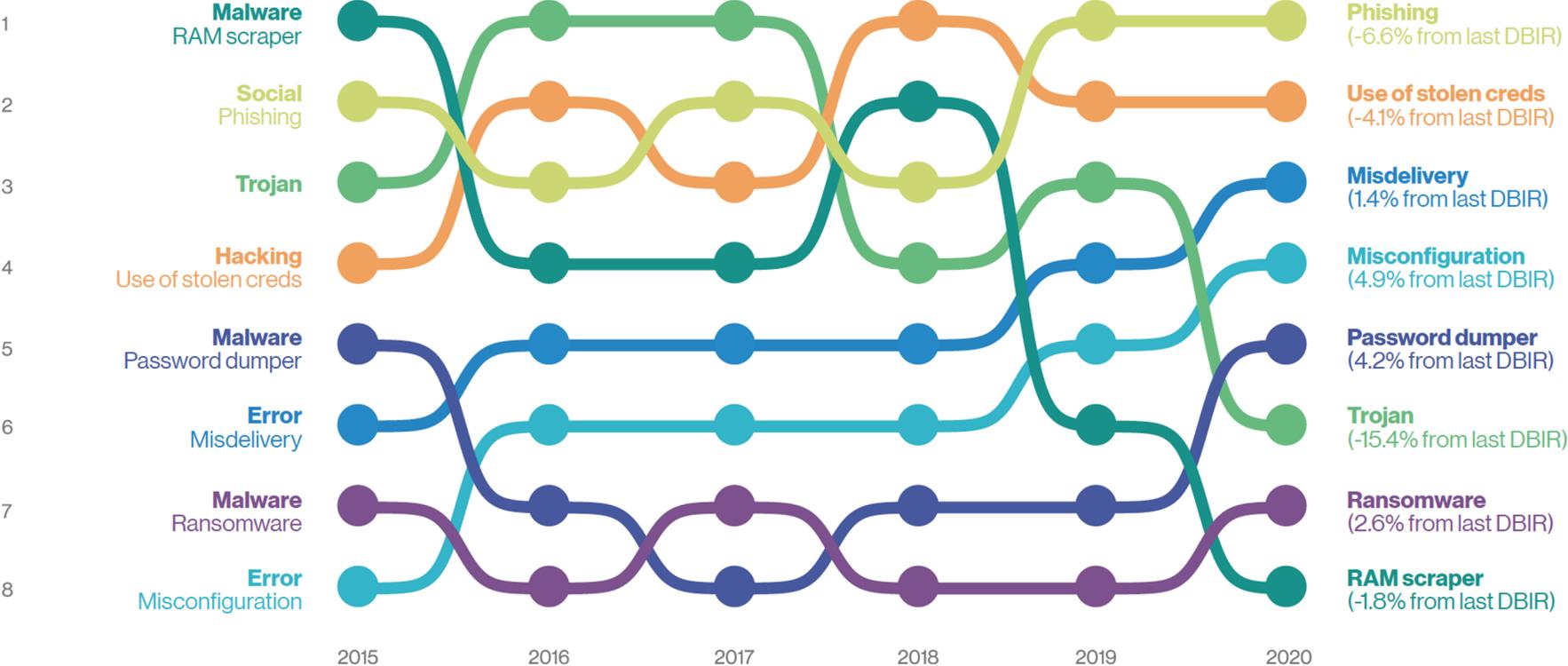


Source: 2020 Verizon Data Breach Report

The % of breaches with attack vector present



Human risks have remained top breach sources in the last 5 years



Source: 2020 Verizon Data Breach Report



**Human risk is the largest
unexplored problem in security**



**Current day approach:
Driven by compliance
Hard to measure impact
One-size-fits all**



This talk will demonstrate how security teams can use their data to:

- Explore the efficacy of accepted best practices.
- Know where to look for human risk.
- Explore a menu of effective remediation techniques.





How does training impact phishing resilience?

The study: Researchers sent 3 spear phishing emails that claimed to have relevant information to 1,500 employees over a few months.

Hypothesis: If users are provided with training immediately following an error in judgment, they will be less likely to make the same error when presented again with a similar judgment.

Expected results:

1. A lower rate of clicking spear phishing links
2. An increase in reporting suspicious emails



Post-compromise training

Spear Phishing



You have just been spear phished. The email that you just read was not actually from the █████ media alert list. It was a spear phishing email designed to raise your awareness regarding spear phishing emails.

This research project is being conducted for a government sponsor and your identity will not be attached to any data results or be provided to █████ management.

Thank you for your time and attention. You may now close the browser.

Control group notification

How to Defend against Spear Phishing



You have just been spear phished! The email that you just read was not actually from the █████ media alert list. It was a spear phishing email designed to help you learn how to protect your co-workers from cyber attackers.

How could you have recognized the spear phishing email you just received?

Spear phishing emails seem professional and legitimate. However, there are several ways to recognize them:

From: owner-media-alert-list@lists.█████.org
on behalf of Rosetti, Mark C. <owner-media-alert-list@lists.█████.org>
Sent: Tue 9/12/2011 12:00 PM
To: Doe, John
Subject: █████ makes "World's 50 Most Innovative Companies" list

Although we dropped to █████ in Fortune Magazine's "100 Best Companies to Work For" this year, we were just ranked #9 in Wired Magazine's "World's 50 Most Innovative Companies" list and you'll never believe why. Here is the link for those interested:

<http://www.wired.com/business/2011/07/innovativecompanies/>

I see this a huge feather in █████ cap.

Mark C. Rosetti
██
██
██
(office)
mrosetti@█████.org

<http://www.██>

Mismatch between name and address in "From:" field

Motivation to take immediate action

Links don't match status bar when mouse is hovered over

Typos, improper grammar, odd spacing

Intuition - overall feeling that something isn't right

1. What is spear phishing?

Spear phishing is a form of cyber attack attempting to infiltrate your system or organization for cyber crime or espionage purposes. Such cyber attackers find inside information specifically relevant to you and craft fake email messages, usually impersonating well-known companies, trusted relationships, or contexts. In order for the attack to succeed, it requires that you take action. For example, by clicking on a link in the email message you could install malicious software on your system.

2. What do your co-workers stand to save when you don't fall for spear phishing attacks?

By not clicking on links within spear phishing emails your co-workers save three things:

- Identity** - Your co-workers save their identity because cyber attackers can't access sensitive details (e.g., logins, passwords, etc.) from their systems.
- Time** - Your co-workers save their time because their systems won't have to be wiped and then restored with the last backup.
- Data** - Your co-workers save data because cyber attackers can't steal sensitive information from their systems.

3. What are simple ways to protect your co-workers?

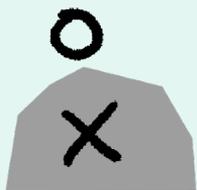
There are several easy things that you can do to protect your co-workers from spear phishing attacks:

- Never click on unanticipated links or attachments within emails or forward/reply to emails asking for private information.
- Always verify contact information by going directly to the source (i.e., using official phone numbers, emails, and websites instead of those provided).
- Report suspicious emails immediately by calling the Help Desk, especially if you have clicked on the links provided.

This research project is being conducted for a government sponsor and your identity will not be attached to any data results or be provided to █████ management. For more comprehensive █████ awareness material on spear phishing, ██████████ ██████████.

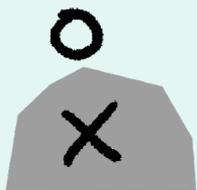
Thank you for your time and attention. Now that you have finished the training please close the browser.

Post-compromise training



Results

- 1) **All or none:** Many employees either clicked all the links or not at all across multiple emails.
- 2) **Initial results foreshadowed future performance:** Employees who clicked an initial spear phishing email were more likely to click subsequent spear phishing emails; those who didn't click an initial spear phishing email were less likely to click subsequent spear phishing emails.
- 3) **Training didn't matter:** Being given training had no significant effect on the likelihood that a participant would click a subsequent spear phishing email.
- 4) **Skipping the content:** Almost every employee ignored the training materials.



Taking these findings further

- 1) All or none
- 2) Initial results foreshadowed future performance



Can we predict who will be a good and bad security performer across security behaviors?

- 1) Training didn't matter
- 2) Skipping the content

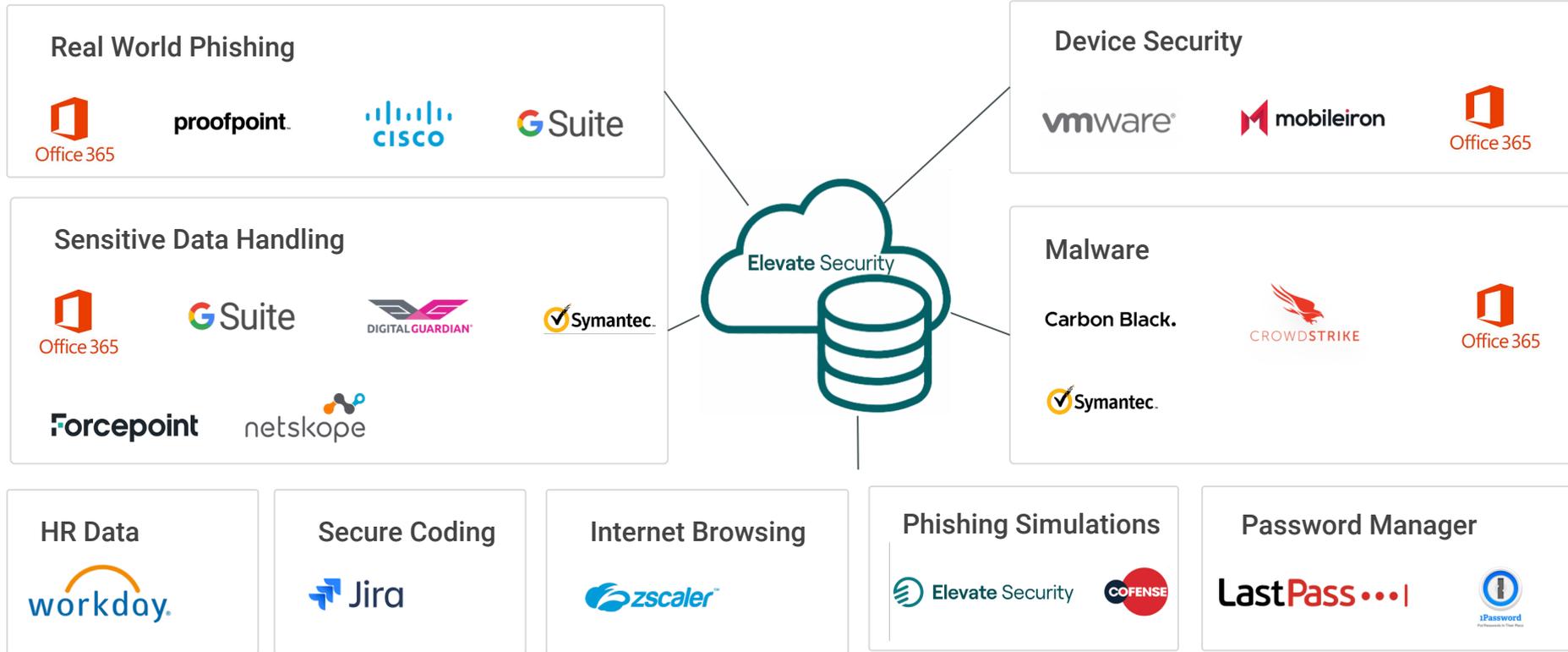


How do we design more effective interventions?

**Can we predict who
will be a good and
bad security
performer across
security behaviors?**



Mapping human risk through security actions of employees

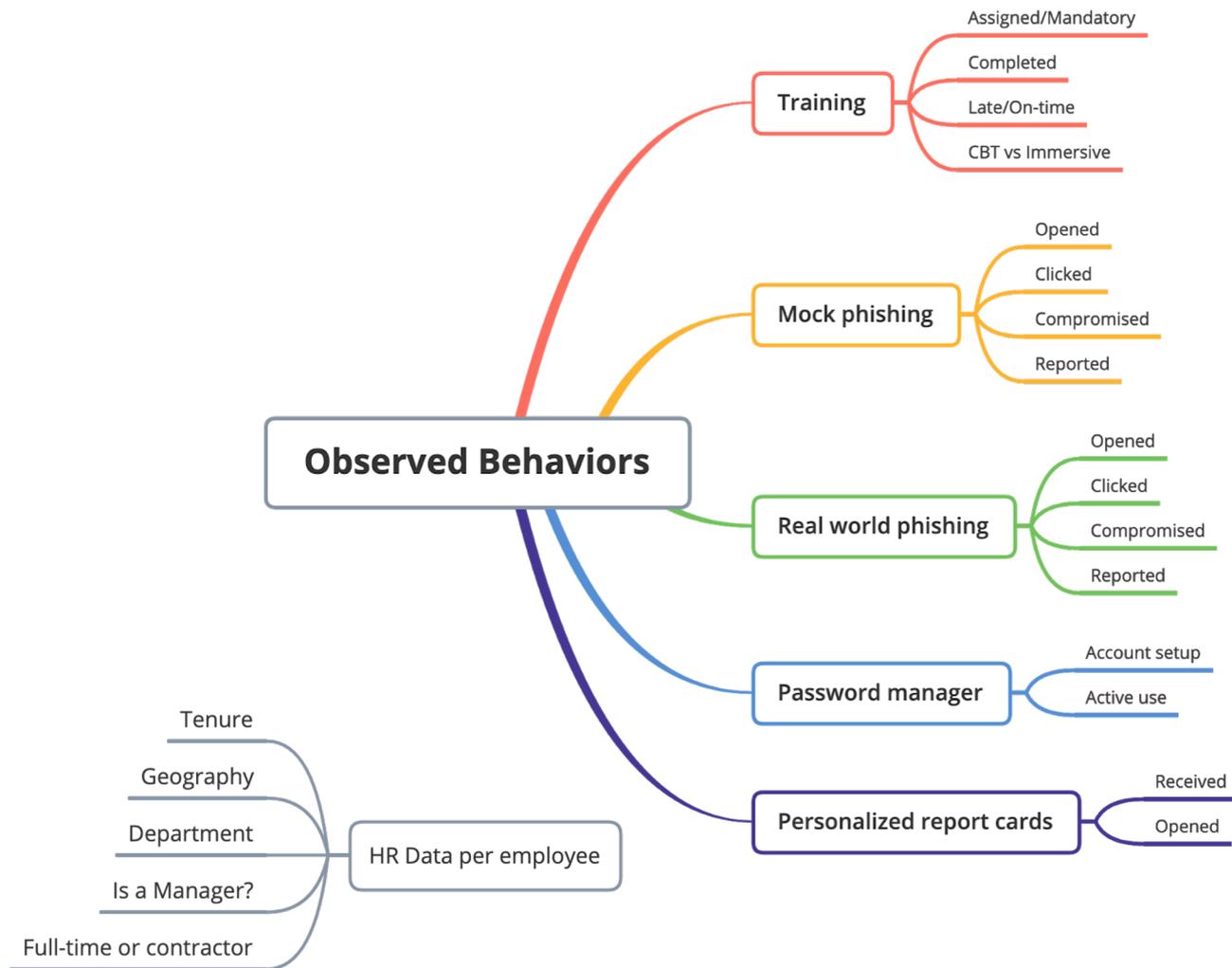


Mapping your orgs strengths and weaknesses



The data set

Over 1M behavioral actions of 80,000+ employees observed over 18 months

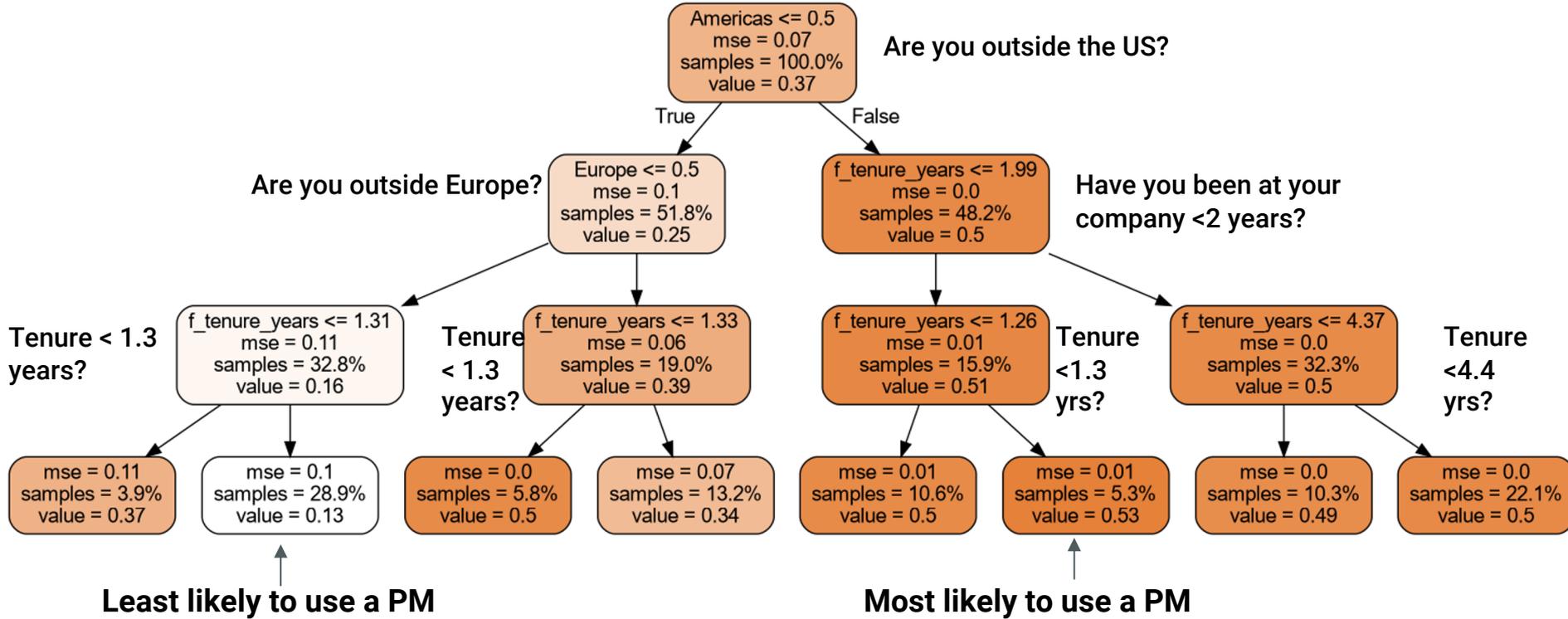


Predictors based on HR data



Who is most likely to use a password manager?

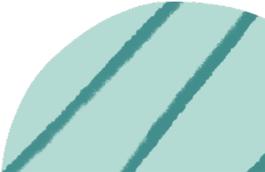
Yes \longleftrightarrow No



Learnings of likelihood to adopt a password manager

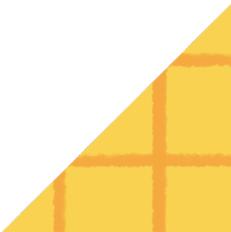
Least likely

Employees in APAC, with the company longer than 1.3 years.



Most likely

Employees in the US, with the company longer than 1.3 years.



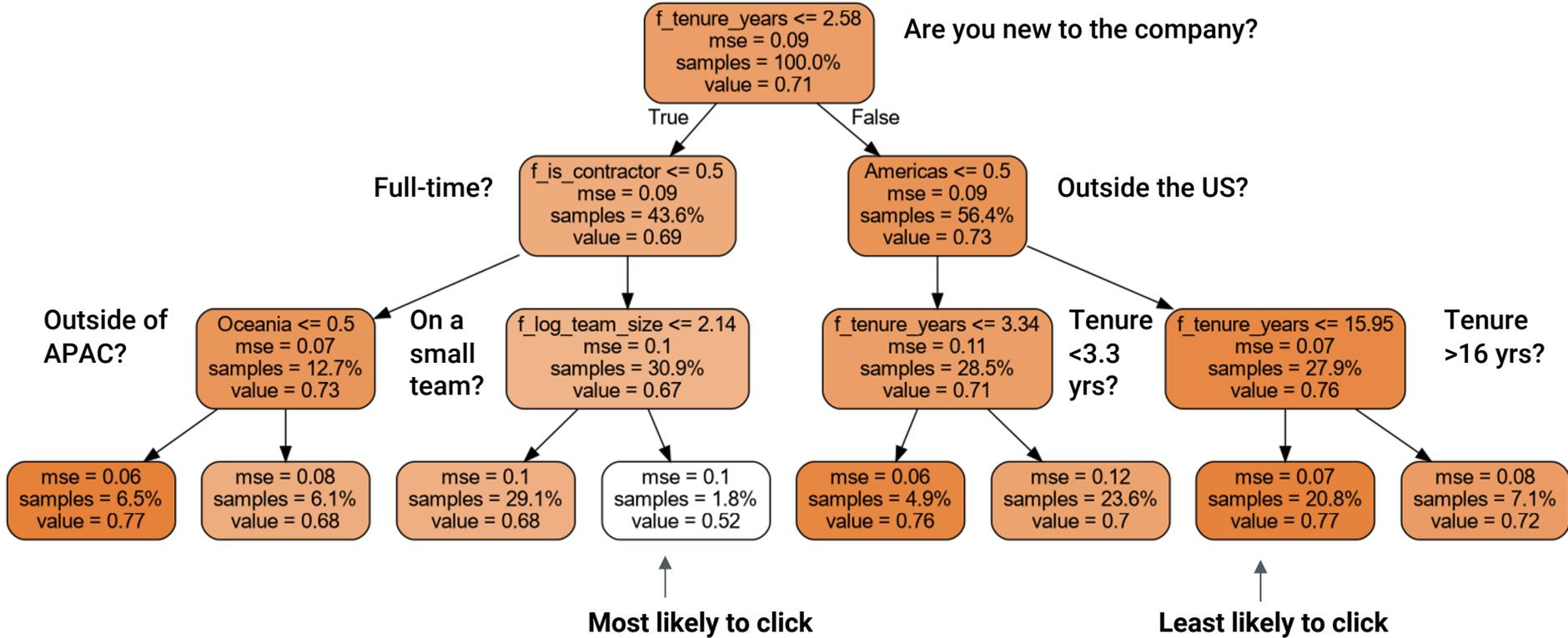
Geography was the strongest indicator of likelihood.

Tenure only slightly affected the predictions.



Who is most likely to fall for a phishing attack?

Yes \longleftrightarrow No



Learnings of likelihood to fall for a phish

Most likely

Short-tenured contractors
on large teams.

Least likely

Employees in the US who
have been with the
company more than 3
years but less than 16.

**Tenure was the strongest
indicator of phishing
resiliency.**



Predictors based on behavioral data



Employees who complete security trainings late are more likely to click on phishing and not report than those who complete it on-time

	Trainings completed on time	Trainings completed late	Delta
Phishing attack detection rate	91.4%	89.2%	2.2%
Phishing reporting rate	48%	42.2%	5.8%



How do we design more effective interventions?



Knowing Isn't Enough

WE UNDERSTAND WHAT
GOOD PASSWORD BEHAVIOR
SHOULD LOOK LIKE



59%

know a secure
password is
important



91%

understand the
risk of reusing
passwords



YET WE CONTINUE TO EXHIBIT
POOR PASSWORD HABITS

41%

choose a password
that is easy to
remember



61%

use the same or
similar passwords





Motivation

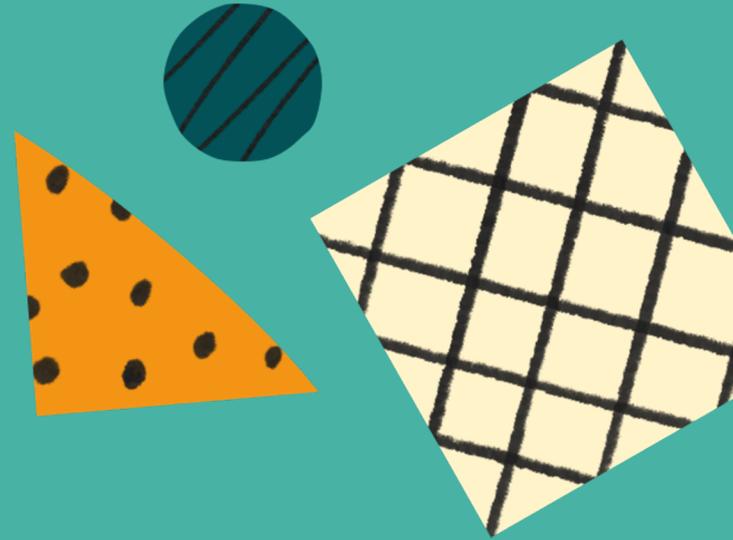
**3 elements are
required for
behavior
change**

B = **M A P**
Behavior happens when **Motivation & Ability & Prompt**
converge at the same moment



Motivation Hack #1

Social Proof



The power of social proof

Customer Reviews

★★★★☆ 1,975
4.5 out of 5 stars ▾

5 star	<div style="width: 79%;"></div>	79%
4 star	<div style="width: 8%;"></div>	8%
3 star	<div style="width: 4%;"></div>	4%
2 star	<div style="width: 3%;"></div>	3%
1 star	<div style="width: 6%;"></div>	6%

[Rate this item](#) ★★★★★

[Write a review](#)

The Little Prince

by Antoine de Saint-Exupery

Format: Kindle Edition | [Change](#)
Price: ~~\$6.99~~



Malone Lodge Hotel & Apartments ★★★★★

Very good **8.2**
1,379 reviews

Queens Quarter, Belfast – [Show on map](#) (1.2 miles from centre)

6 people are looking at this moment
In high demand! Booked 41 times in the last 24 hours

Great Value Today

One-Bedroom Apartment 👤👤 **£71**
includes taxes and charges

In high demand - only 6 rooms left on our site!

[See our last available rooms >](#)

Last Month Neighbor Comparison

You used **92% MORE** energy than your efficient neighbors.

Efficient Neighbors	<div style="width: 488%;"></div>	488*
YOU	<div style="width: 939%;"></div>	939
All Neighbors	<div style="width: 1,101%;"></div>	1,101

How you're doing:

Great 😊 😊

GOOD 😊
More than average

* This energy index combines electricity (kWh) and natural gas (therms) into a single measurement.

Control



Keep Your Account Safe

You can use security settings to protect your account and make sure it can be recovered if you ever lose access.

[Improve Account Security](#)

Social context



Keep Your Account Safe

108 of your friends use extra security settings. You can also protect your account and make sure it can be recovered if you ever lose access.

[Improve Account Security](#)

Social proof in security

**1.36x more successful
when using social proof**

Using social proof

Compromised



Good job! You're **much less likely** to fall for a phish and submit your credentials than the rest of your department!



Detection Badge
You earned a badge!

Compromised



Oh no! You are **much more likely** to fall for a phish and submit your credentials than people in your department. You can do better!

[Strengthen Skills](#)

Password Manager

Password managers are the best way to have unique and strong passwords across all your accounts.

ACME CEO John Doe uses Lastpass, too!

50% of your department has installed Lastpass.



Password Manager installed

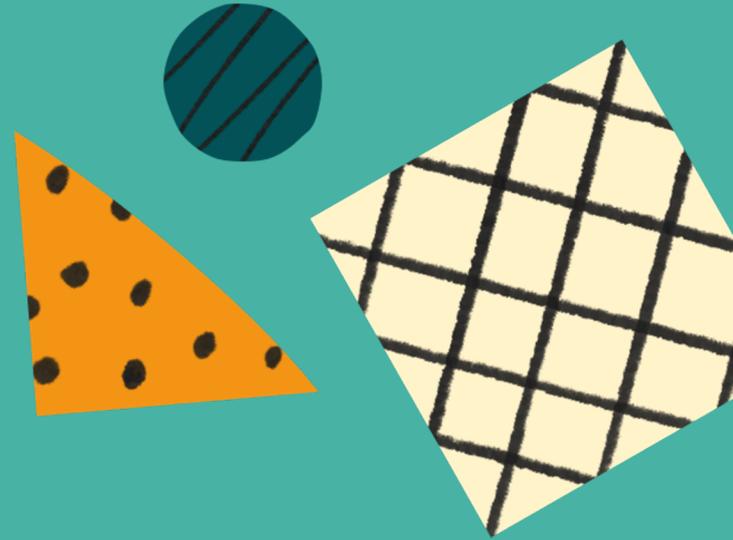


Password Protected
You earned a badge!



Motivation Hack #2

Gamification



Gamification



**It's Not About Playing
Games at Work**



**Gamification is the use of Game Mechanics in
Non-Gaming environments to improve
Engagement, Motivation and Business Results**



Gamification principles

AUTONOMY | We Like Having Choices

MASTERY | We Like to Get Better at What We Do

FEEDBACK | We Like Getting Feedback on our Progress

PURPOSE | Meaning Amplifies What We Do

SOCIAL | All This Means More With Others



Fly your way to up to 12,000 bonus points.*



1X ROUND TRIP

2,000 points



2X ROUND TRIP

+4,000 points



3X ROUND TRIP

+6,000 points

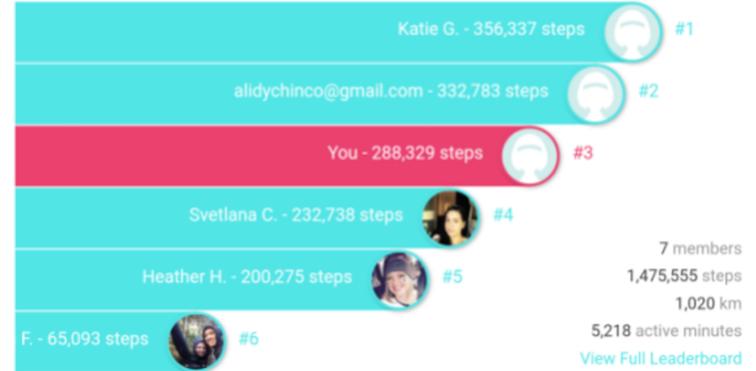


12,000 points

*Anytime or Business Select® fares only.

IMAGE: SOUTHWEST AIRLINES

Steps in April



Profile Strength: Intermediate



Add a profile photo to help others recognize you

Members with a photo get up to 21x more profile views

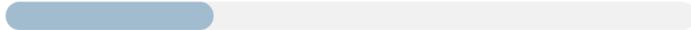
Add photo



Applying Gamification

Keep Improving!

You're **Tenuous**. The rest of your company is Sturdy. You've still got a few things to do to improve your security skills.



Flimsy Tenuous Sturdy Fortified Indestructible

**This Department
Has Worked**

297 DAYS

Without a Claim

**The Best Previous
Record Was**

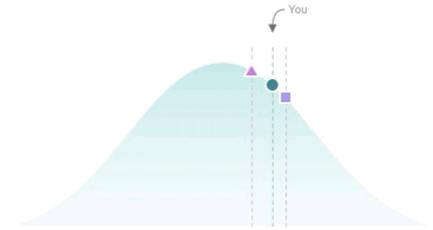
297 DAYS

The Best Company Record Is

297 DAYS

Leaderboard: Ranked 15th (out of 32)

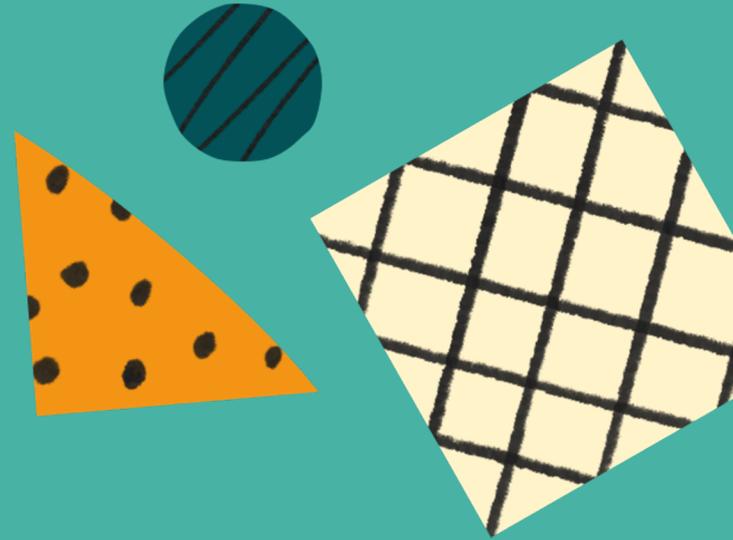
Rank	Name	Department
14	Tess Bard-Laredo	Marketing
15	You	Quality Assurance
16	Vince Amaretta	Finance

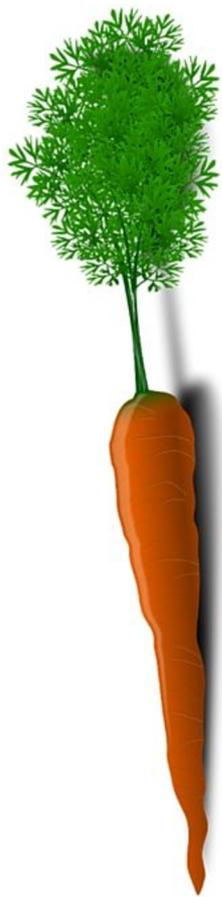


Motivation Hack #3

Positive

Reinforcement





VS.



Negative Reinforcement

Strengthen a behavior that avoids or removes a negative outcome



Positive Reinforcement

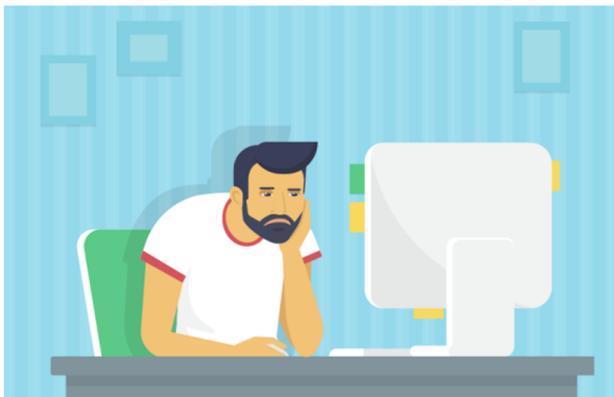
Introduce a reinforcing stimulus following
a specific behavior



Reinforcement in Phishing

Negative reinforcement

“You clicked on a link, now take training.”



Positive reinforcement

“You detect attacks well and report them quickly. Kudos!”



Punishment can also be an effective tool for improving efficiency and effectiveness, It often has the downside of reducing morale;

On the other hand, verbal **positive reinforcement** is effective in both **increasing the likelihood of desired behavior** and encouraging enthusiasm, engagement, and satisfaction among staff.

(Wei & Yazdanifard, 2014).



Changing behaviors by leveraging motivation

Phishing Compromises
over 9 months

✓ 83%

Employee Reporting
over 9 months

▲ 32%

Password Manager Adoption
over 5 months

▲ 87%

Key learnings



Security actions can be predicted based on HR and behavioral data

Tenure was the strongest indicator of phishing resiliency. Employees with the company less than 3 years or more than 16 performed the worst.

Geography was the strongest indicator of likelihood of adopting a password manager.

Late training completion predicted higher click rates and lower reporting rates.



Effective interventions are a combination that address both ability and motivation.

- Leverage motivation to get employees to *want* to change behaviors and engage in training
- Use techniques like social proof, gamification, and positive reinforcement to achieve behavior change



Stay on top of our latest research:

www.elevatesecurity.com/learning-hub



Thank you

Questions?
masha@elevatesecurity.com

