black hat USA 2020
AUGUST 5-6, 2020
BRIEFINGS

Mind Games:

Using Data to Solve for the Human Element

Masha Sedova
Co-founder, Elevate Security

About me

Cyber Analyst for defense community

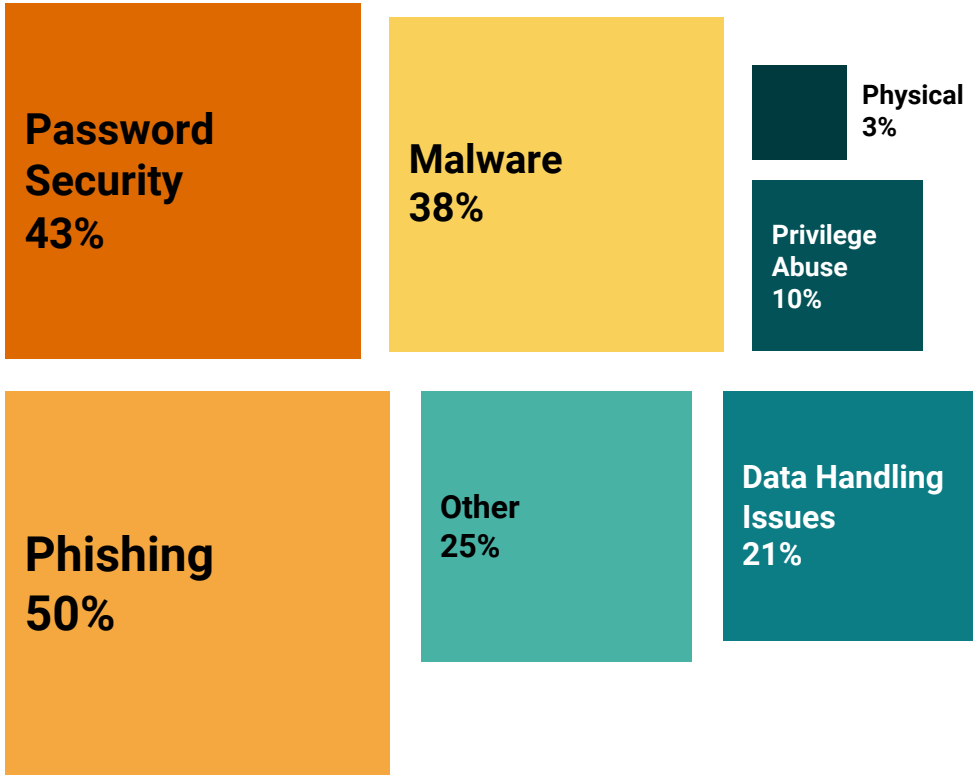
Co-Founder, building the Human Risk Management Platform

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

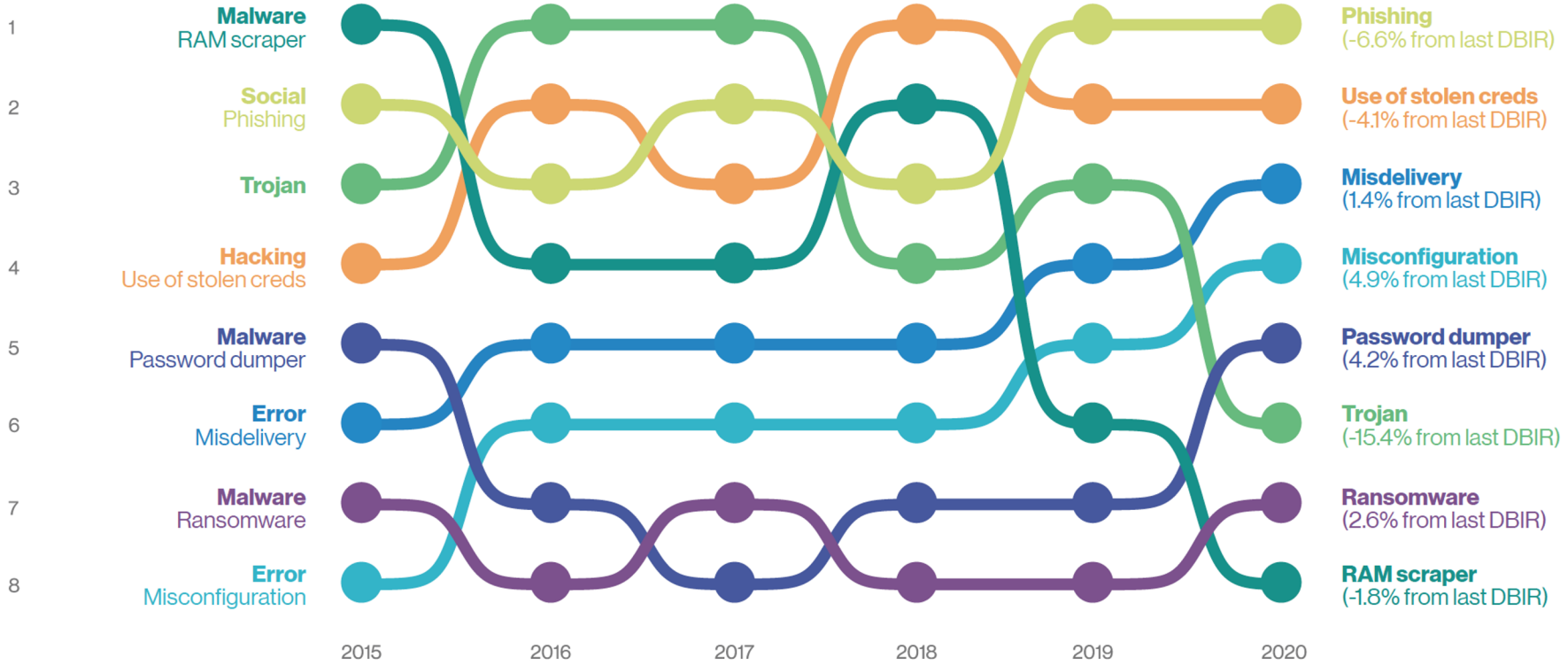
Human risk accounts for 5 of the top 7 breach sources



The % of breaches with attack vector present

Source: 2020 Verizon Data Breach Report

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.

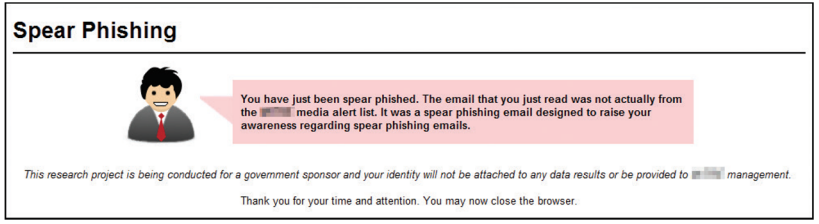
Hypothesis: If users are provided with training immediately following an error in judgment, they will be less likely to make the same error when presented again with a similar judgment.

Expected results:

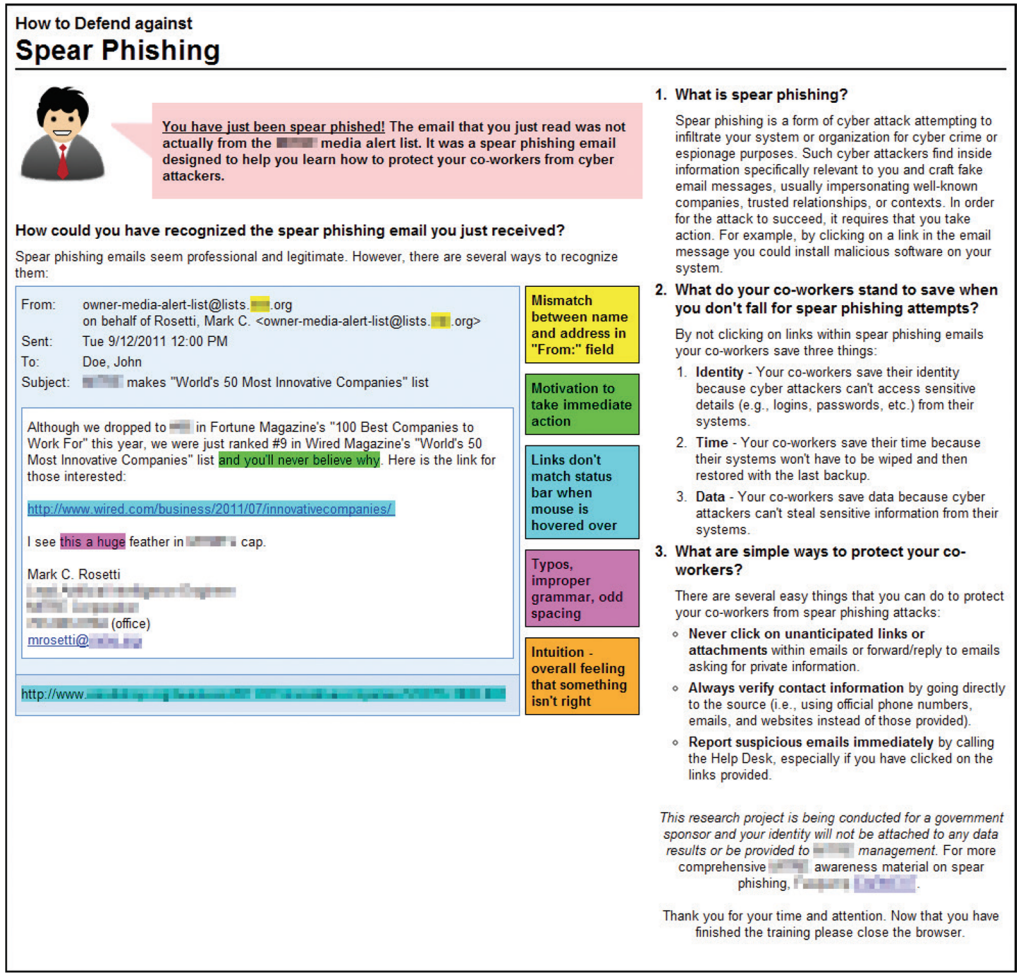
1. A lower rate of clicking spear phishing links
2. An increase in reporting suspicious emails

Going Spear Phishing: Exploring Embedded Training and Awareness by Deanna Caputo et al, 2014

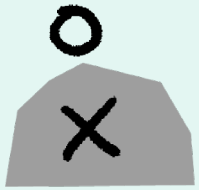
Post-compromise training



Control group notification

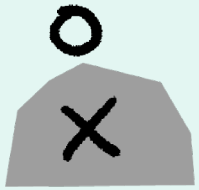


Post-compromise training



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

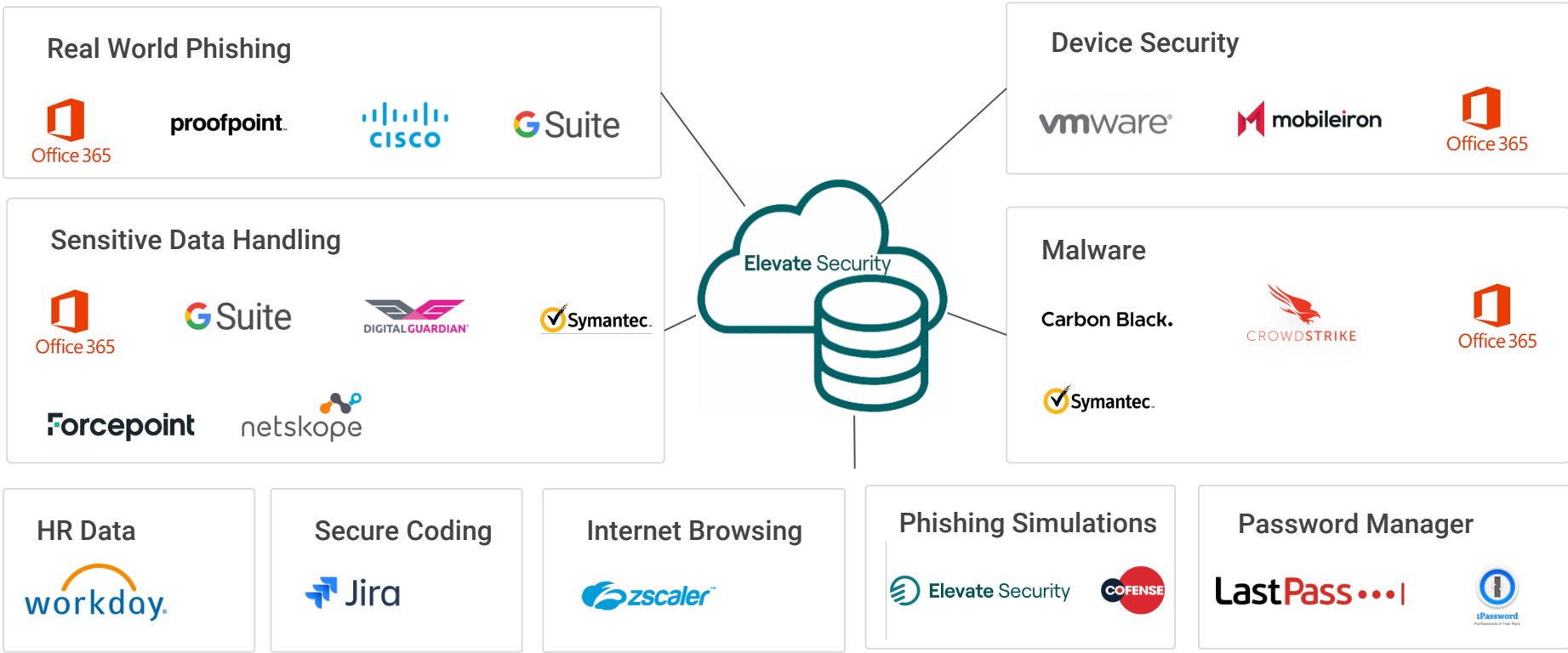
→ **Can we predict who will be a good and bad security performer across security behaviors?**

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

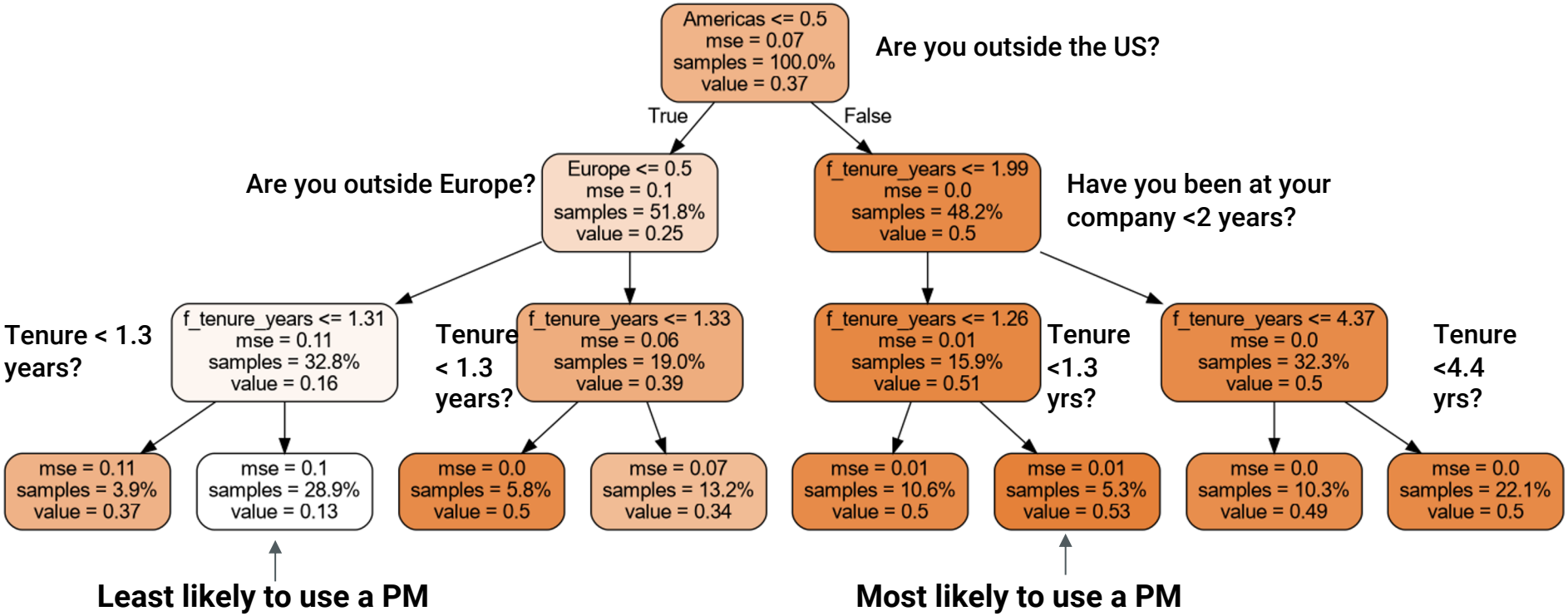
The data set

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 ⟷ No



Learnings of likelihood to adopt a password manager

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

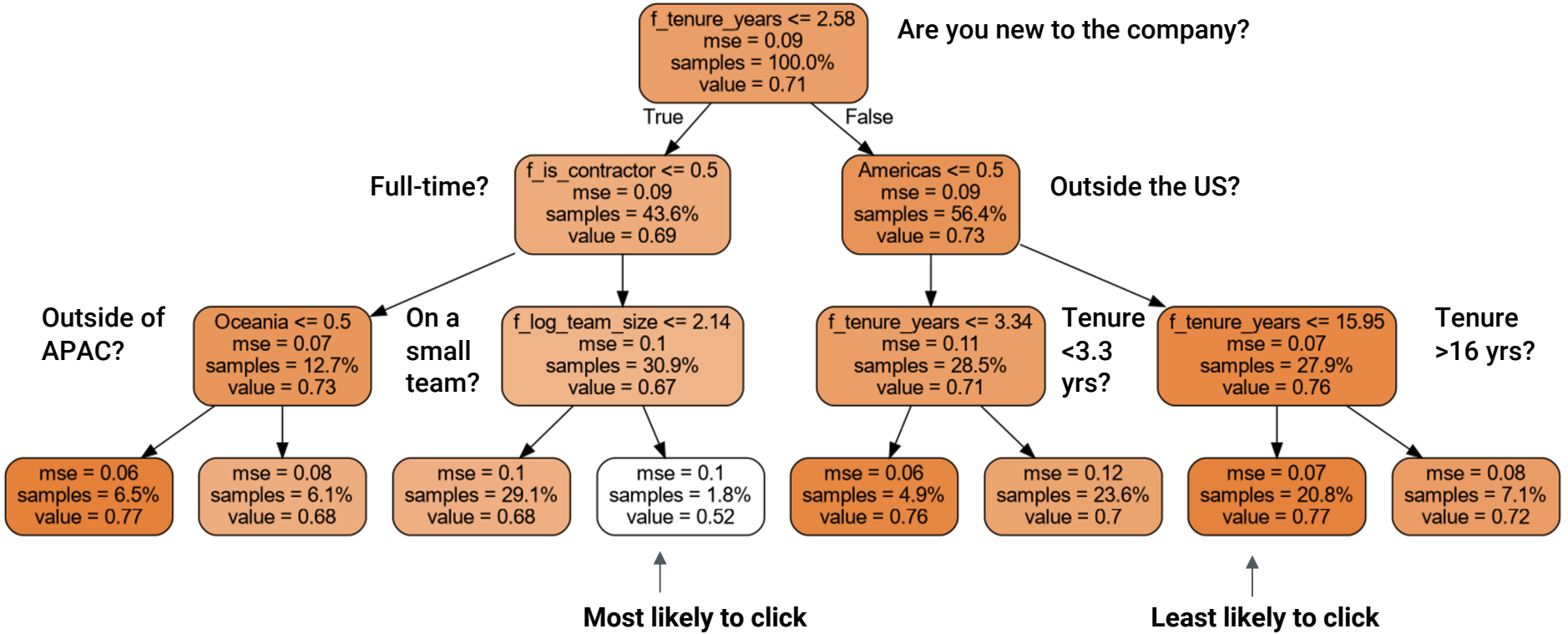
Most likely
Employees in the US, with the company longer than 1.3 years.

Geography was the strongest indicator of likelihood.

Tenure only slightly affected the predictions.

Who is most likely to fall for a phishing attack?

Yes ⟷ 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 that 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

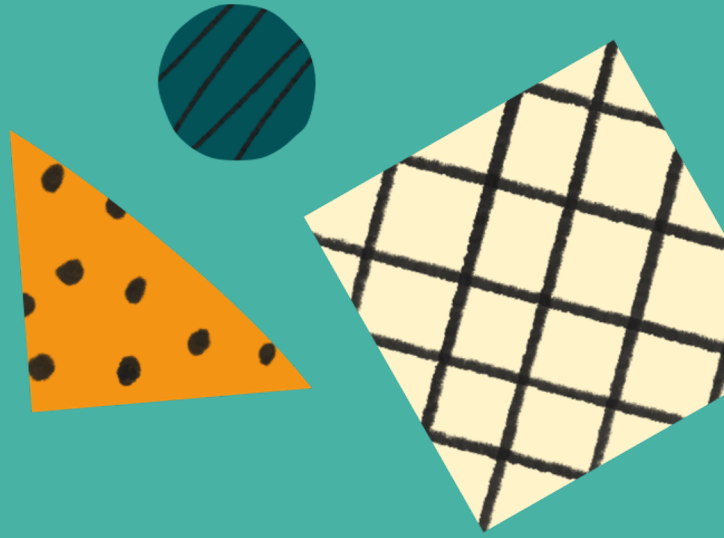
Lastpass 2017


Motivation

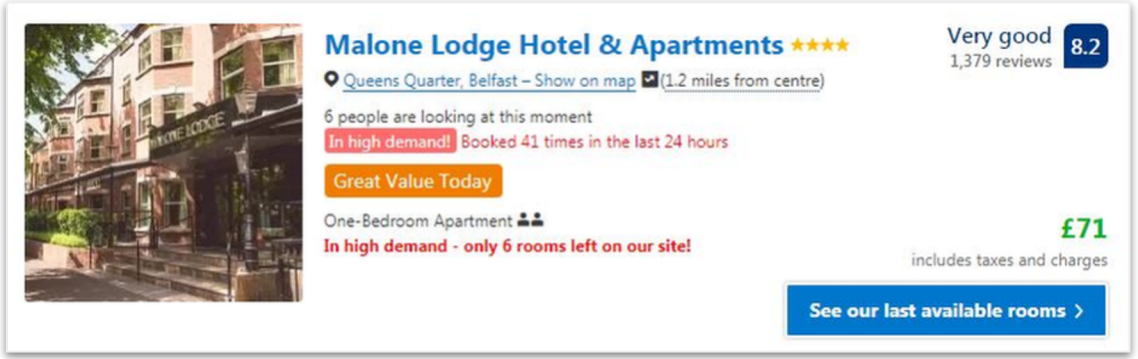
3 elements are required for behavior change

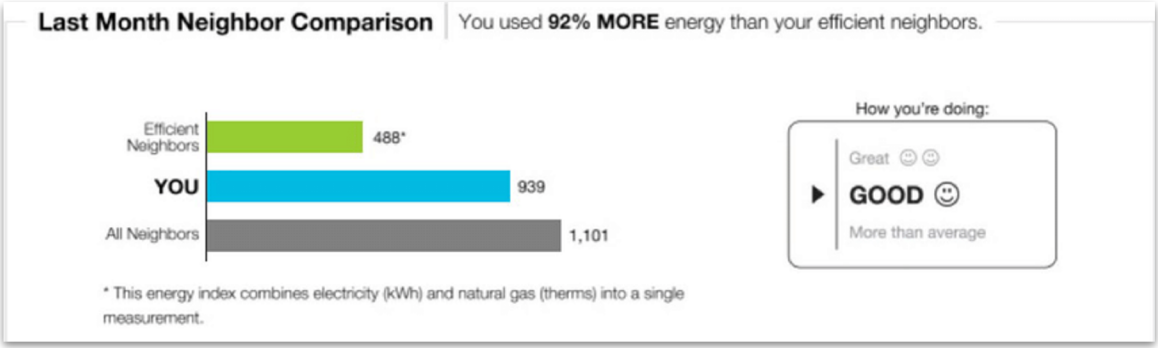
Motivation Hack #1

Social Proof

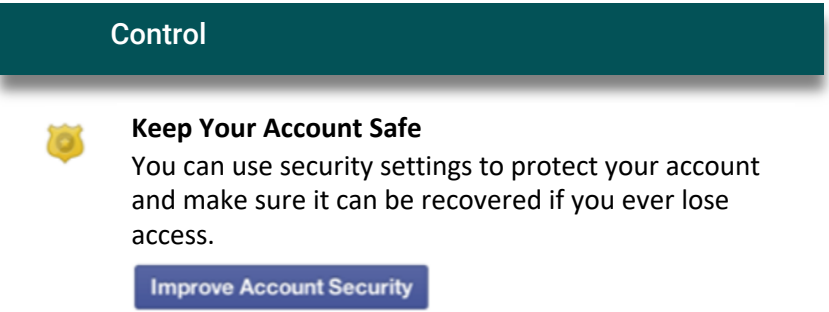


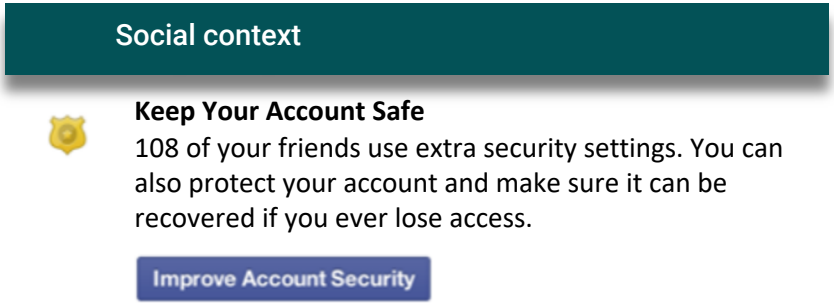
The power of social proof





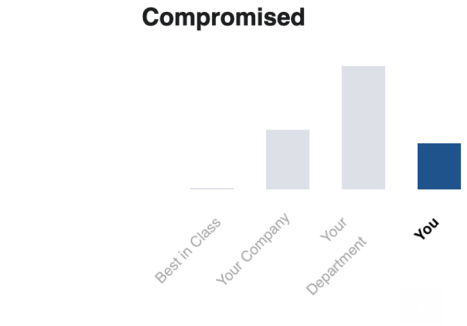
Social proof in security





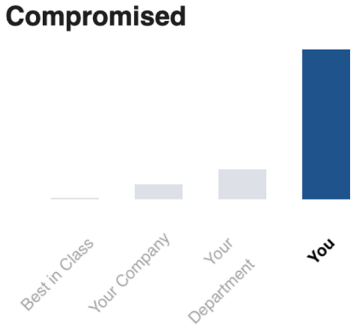
1.36x more successful when using social proof

Using social proof



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!



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!

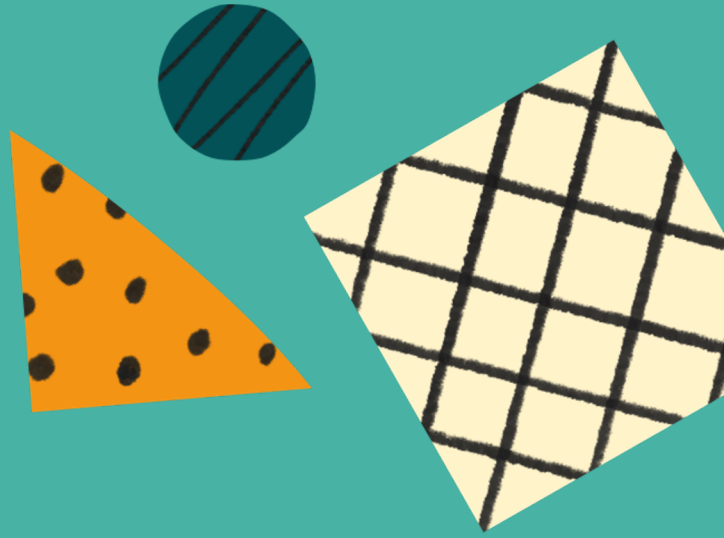
50% of your department has installed Lastpass.

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

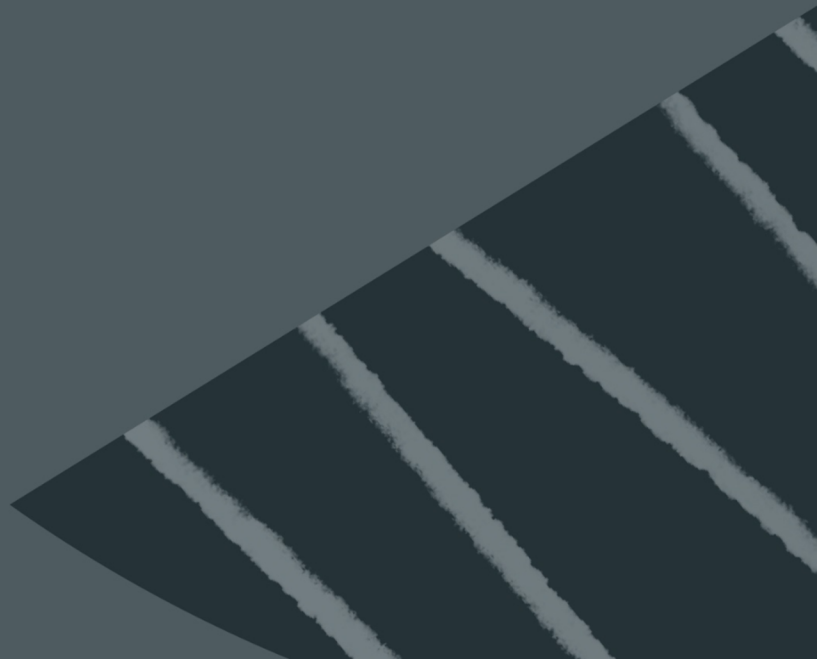
AUTONOMY | We Like Having Choices

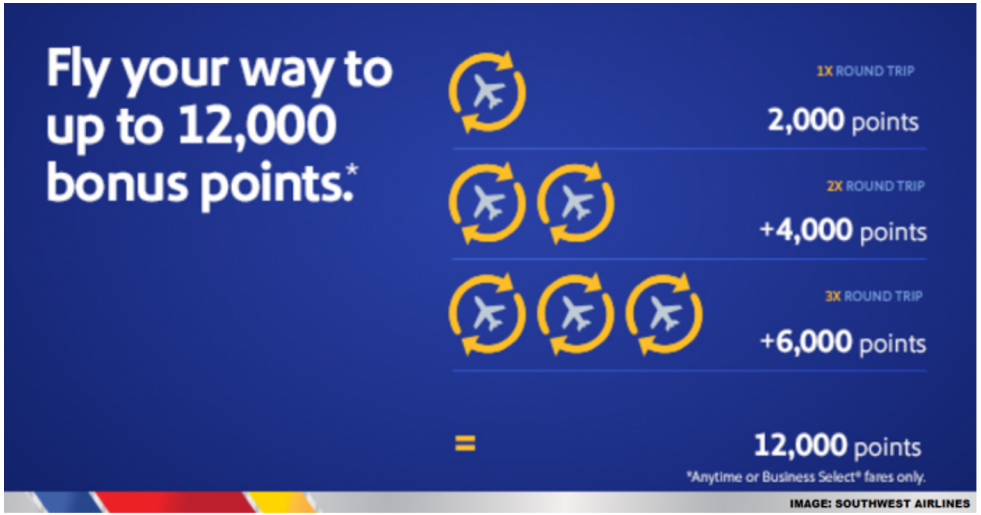
MASTERY | We Like to Get Better at What We Do

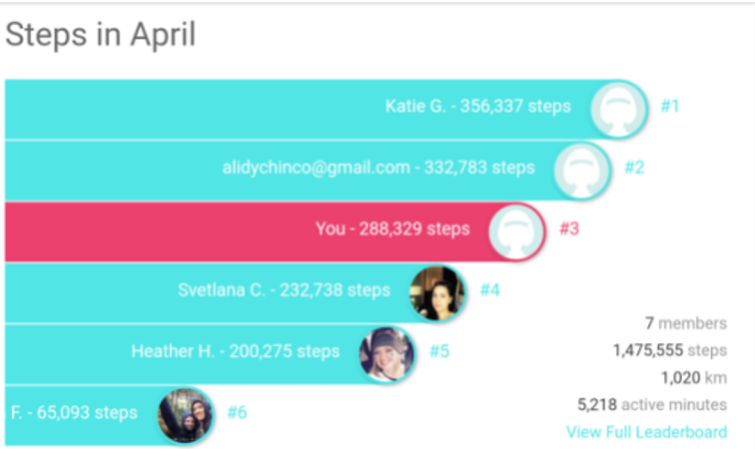
FEEDBACK | We Like Getting Feedback on our Progress

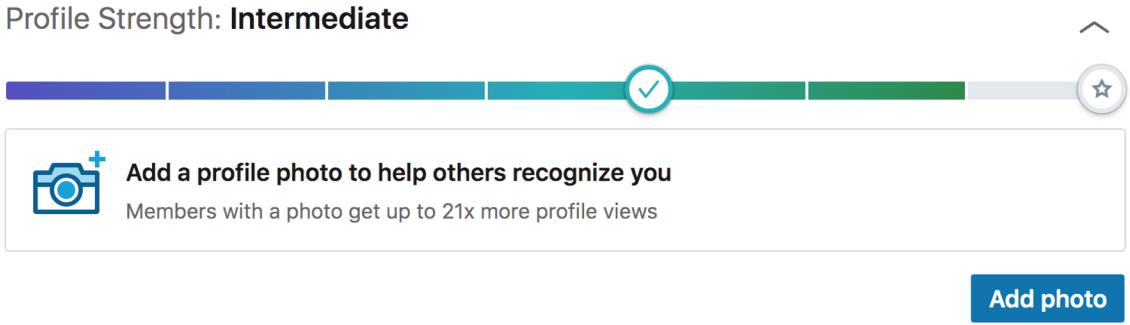
PURPOSE | Meaning Amplifies What We Do

SOCIAL | All This Means More With Others



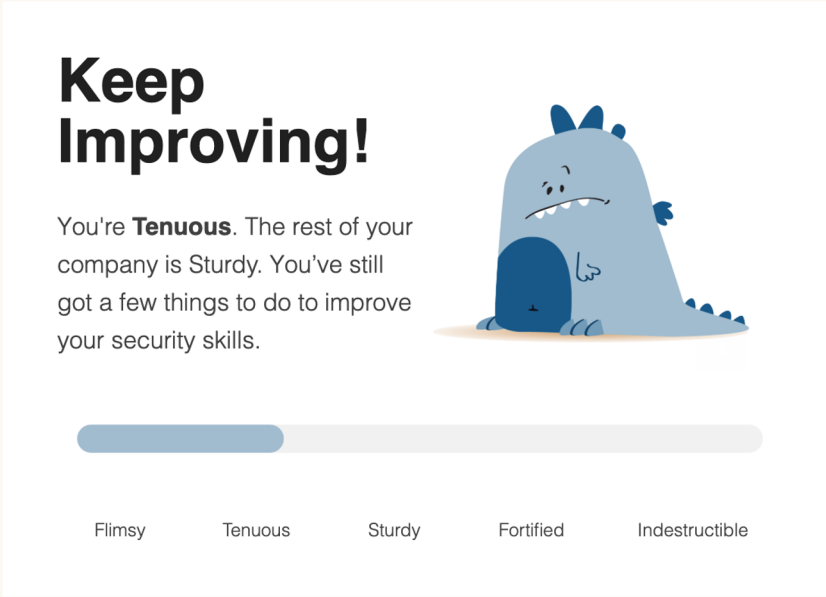

Fly your way to up to 12,000 bonus points.*
1X ROUND TRIP
2,000 points
2X ROUND TRIP
+4,000 points
3X ROUND TRIP
+6,000 points
=
12,000 points
*Anytime or Business Select® fares only.
IMAGE: SOUTHWEST AIRLINES

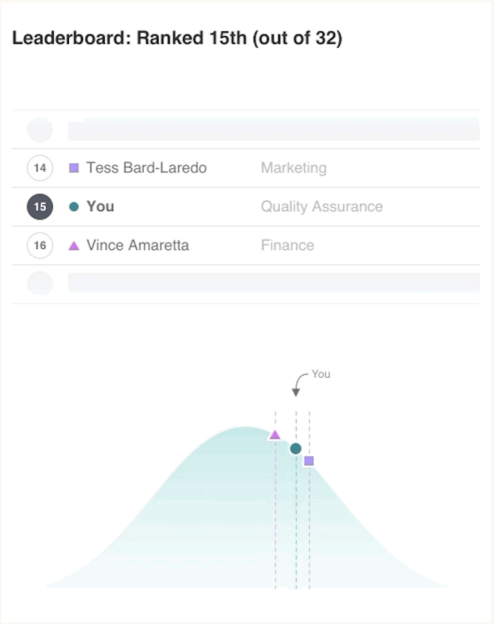

Steps in April
Katie G. - 356,337 steps #1
alidychinco@gmail.com - 332,783 steps #2
You - 288,329 steps #3
Svetlana C. - 232,738 steps #4
Heather H. - 200,275 steps #5
F. - 65,093 steps #6
7 members
1,475,555 steps
1,020 km
5,218 active minutes
View Full Leaderboard


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


STARBUCKS
Frequency Card
Purchase 10 grande or larger espresso, blended or coffee drinks, and be entered into a raffle to win your choice of Starbucks Merchandise*
*Raffles take place once a month. Prize selected must be equal to or less than $50.

Applying Gamification

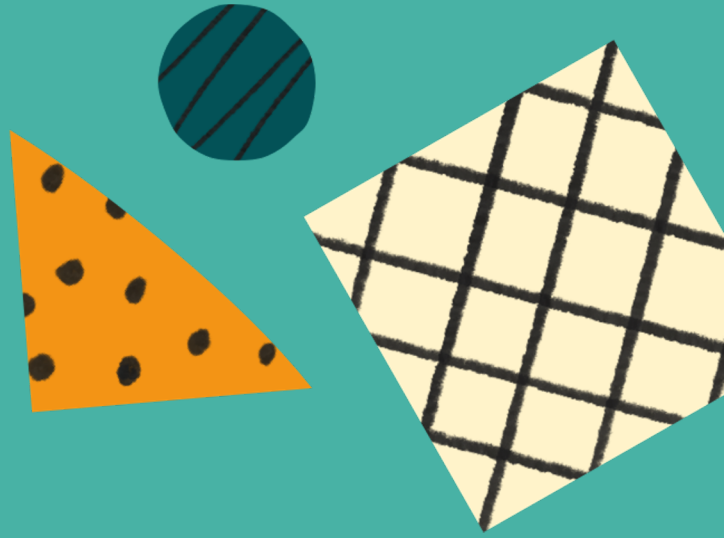




Motivation Hack #3

Positive

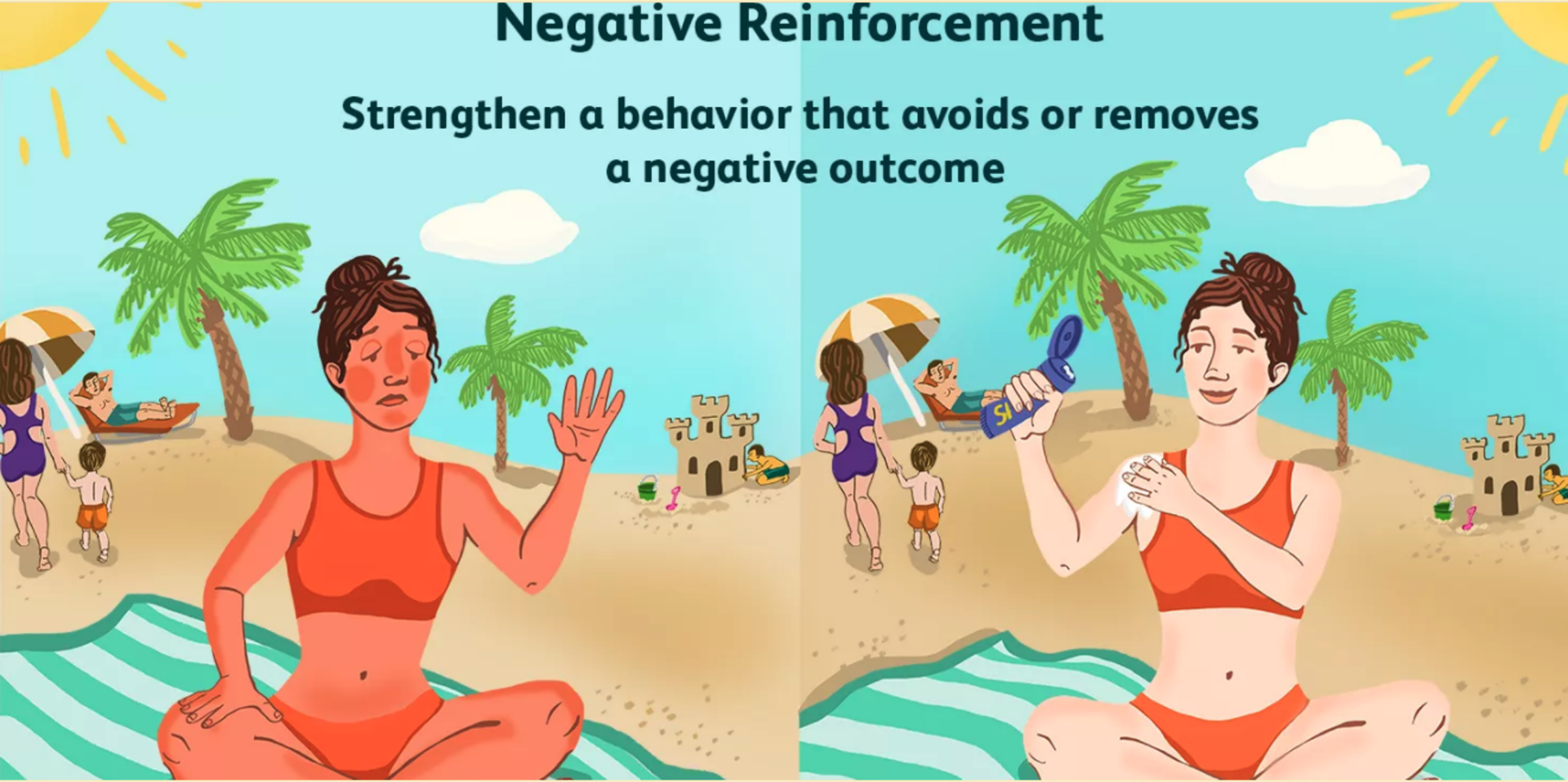
Reinforcement



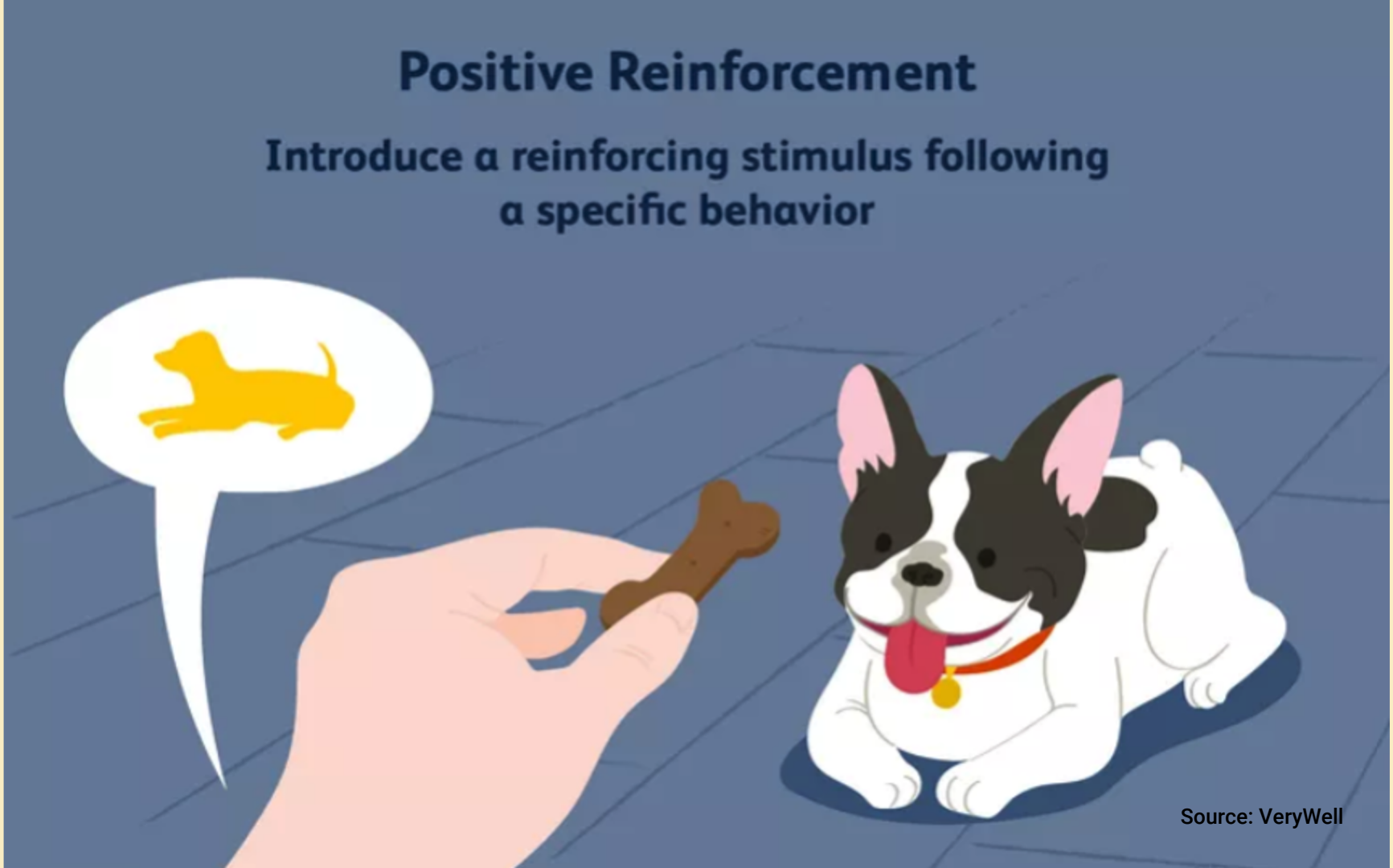
vs.

Negative Reinforcement

Strengthen a behavior that avoids or removes a negative outcome



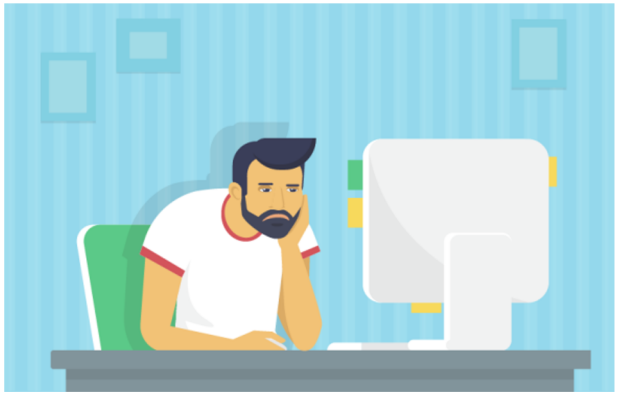
Source: VeryWell


Positive Reinforcement
Introduce a reinforcing stimulus following a specific behavior
Source: VeryWell

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