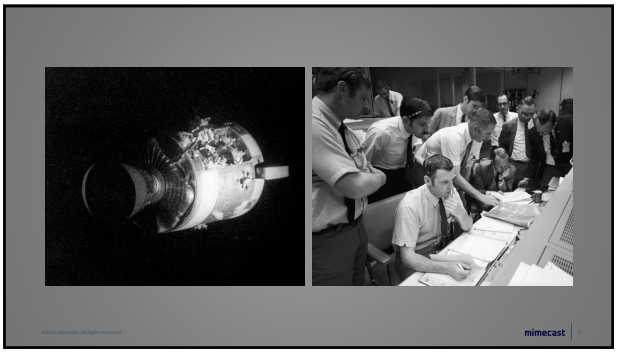
mimecast

High Risk Users & Where to Find Them

Rethinking Security Awareness and Controls

1



2

3

4

Today's approach to securing the "human element"

1. Mandatory awareness training
2. Ongoing simulated phishing tests w/ remedial training

mimecast

5

Why does the current approach have limited impact?

mimecast

6

Simulated Risk ≠ Real Risk

Who is riskier to the business?

Employee A

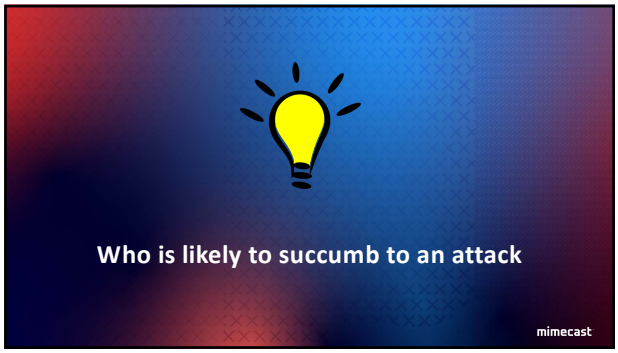
VS

Employee B

	Employee A	Employee B
Security Awareness:	• Completes all assigned training • Has never failed a simulated phish	• Rarely completes assigned training • Has failed 2 heavily crafted simulated phish
Email Security:	• Downloads attachments from unknown senders. • Susceptible to urgent language • Clicks suspicious links	• Reports suspicious emails using the "report phish" button • Carefully examines emails with urgent language • Avoids clicking suspicious links

mimecast | 7

7



8

Too Much to Think About Leads to Security Errors

Cognitive loads statistically impact security mistakes

- Workload[1]
- Workplace distractions (deadlines) [1]
- High total email quantity[2]
- Low phishing prevalence[2]

Sources:
1: Yeng et. al, 2022, Chowdhury, 2019
2: Sarno et al., 2021

mimecast | 9

9

Many Policy Violations Are Driven by Stress, Not Desire to Harm

% of study participants who knowingly circumvented cybersecurity policies at least once in a 10-day period.

Why?

- Family demands that conflict with work
- Job security fears
- To enable productivity hindered by security policies

"to better accomplish tasks for my job,"
"to get something I needed,"
"to help others get their work done."

Only 3% of cases were out of a desire to cause harm

Why Employees Violate Cybersecurity Policies
HBR, January 05, 2022

mimecast | 10

10

Neutralization Techniques

Why some employees disregard security rules

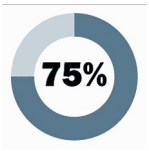
Denial of Injury	Justifying policy breaches with the belief that no harm is done, making rule-breaking acceptable.
Appeal to Higher Loyalties	Prioritizing loyalty to projects or managers over security guidelines, treating loyalty as more important than compliance.
Denial of Responsibility	Refusing responsibility for actions by blaming external factors, such as unawareness or insufficient training.
Metaphor of the Ledger	Balancing positive actions against negative behaviors to justify occasional rule violations without guilt.
Defense of Necessity	Justifying violations as unavoidable due to extenuating circumstances, like urgent deadlines necessitating prohibited actions.
Condemnation of the Condemners	Discrediting enforcers or policies to justify ignoring rules, viewing the security team or their policies as unreasonable or out of touch.

Sykes & Matza, 1950

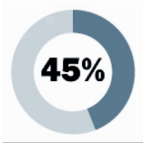
mimecast

11

What percentage of employees get phished at least once a month?



of managers get attacked monthly



of individual contributors (IC) get attacked monthly

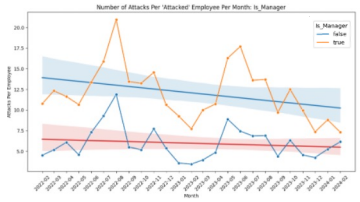
mimecast | 12

12

For those employees who are attacked, how many phishing emails do they get monthly?

Median phishing amount for **Managers: 13 emails**

Median phishing amount for **ICs: 6 emails**



13

Why?

- Managers have more access & sensitive information.
- Manager are doing more context switching
- Managers have a wider pool of contacts internally and externally (vendors).

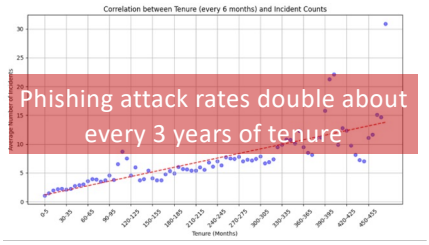

Microsoft Executives' Emails Hacked by Group Tied to Russian Intelligence

The hackers appeared to be trying to learn what the company knew about them, a regulatory filing said.

14

Are new hires or tenured employees get attacked more?

Phishing attack rates double about every 3 years of tenure



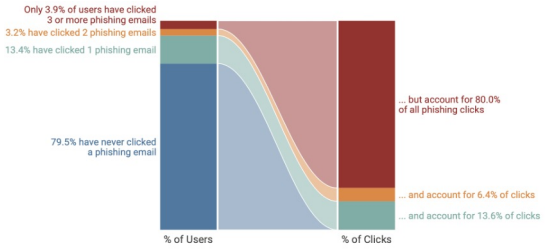
Phishing attack rates double about every 3 years of tenure

15

A few employees cause the majority of incidents

16

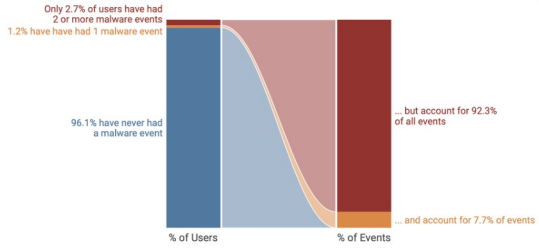
Phishing Emails Clicked



Source: High Risks Users and Where to Find Them, Cyentia Institute, 2023

17

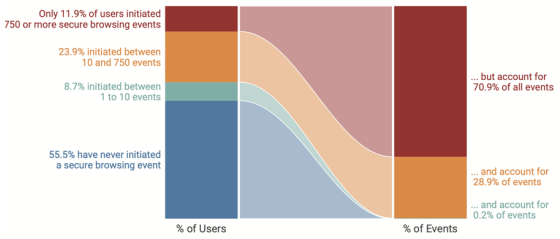
Malware Downloaded/Executed



Source: High Risks Users and Where to Find Them, Cyentia Institute, 2023

18

Browsing Policy Violations

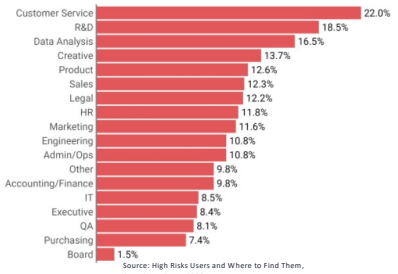


Source: High Risks Users and Where to Find Them, Cyentia Institute, 2023

mimecast | 19

19

Percentage of High Risk Users per Dept



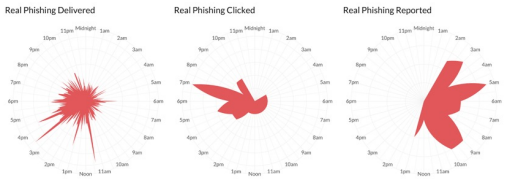
Source: High Risks Users and Where to Find Them, Cyentia Institute, 2023

mimecast | 20

20

Timing Matters

Phishing behaviors have time-based patterns



Source: Cyentia & Elevate report, Human Attack Surface, 2022

mimecast | 21

21

22

How does training impact phishing resilience?

The study[1]: 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

1: "Going Spear Phishing: Exploring Embedded Training and Awareness," Feb 2014

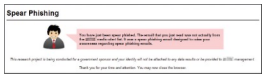
mimecast | 23

23

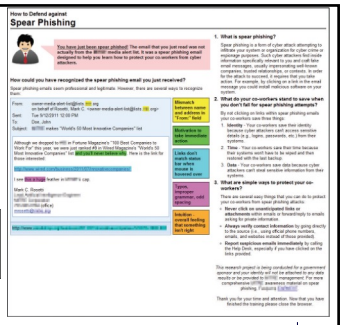
Post-compromise training

The control group just got a notification that they were spear phishing.

The test group received a training (seen on the right) that explained how they could detect the attack.



Control group notification



Post-compromise training

mimecast | 24

24

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.

These results have been reinforced in the study:
Phishing for Long Tails: Examining Organizational Repeat Clickers and Protective Stewards.
https://doi.org/10.1177/21582440231908056

mimecast | 25

25

Training has a very limited impact

One-time or Narrow Focus	Continuous process
Password creation	Password management
Downloading/install of antimalware software	Sharing of personal information
Updating systems	Ability to identify a phish in real world
Ability to identify phish in a lab	

mimecast | 26

26

Adapting Interventions To Individual Risk

mimecast

27

For phishing threats, how would you define an employee who is:

- High Risk
- Medium Risk
- Low Risk

mimecast

28

Sample Risk Thresholds:

High	Medium	Low
Click regularly. Rarely/never report. Top 10% of attacked individuals.	Click infrequently, rarely/never report. Course-correct quickly.	Click rarely/never. Report often.

29
mimecast | 29

29

Interventions options for low/medium risk users

For low risk users:
- Enrolling in champion program
- Give kudos & unlock perks

More medium risk users:
- Provide feedback with social proof
- Assign training on phishing
- Mandate use of password manager
- Increase frequency of phishing tests for additional practice

mimecast | 30

30

"Bubble Wrapping" High-Risk Phishing Users

Example of adaptive controls and policies

Preventing Phishing/Cred Stealing

- Phishing-resistant MFA
- Reduce MFA timeout
- Enroll in data deletion service (ie. DeleteMe)
- Security buddy

Reducing Access

- Review access more frequently
- Encourage surrendering unneeded access

Mitigation/Recovery

- VPN usage
- Enhance monitoring
- Retain logs longer
- Alert help desk to use enhanced auth when user calls in

mimecast | 31

31

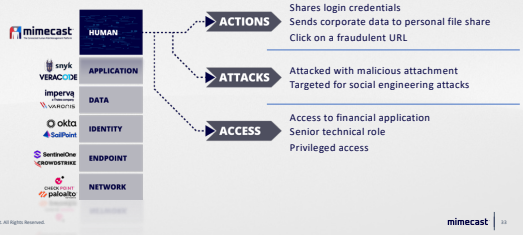
Our vision of Human Risk Management

mimecast

32

THE CATEGORY

Securing Human Risk



mimecast | 33

33

OUR SOLUTION

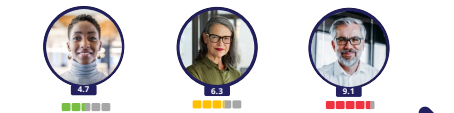
The Connected Human Risk Management Platform

mimecast | 34

34

Adapt response based on risk and context

Targeted response minimizes risk without impacting productivity



Low intervention

- Training opt-out
- Recognition for good security performance
- Baseline security controls

High intervention

- Tailored feedback on how to improve
- Increase email security controls

mimecast | 35

35

mimecast

The Connected Human Risk Management Platform

36