# An Empirical Analysis of Enterprise-Wide Mandatory Password Updates

**Ariana Mirian**, Grant Ho, Stefan Savage, Geoffrey M. Voelker

December 5, 2023

UCSDCSE
Computer Science and Engineering

# The relationship between employees and IT orgs

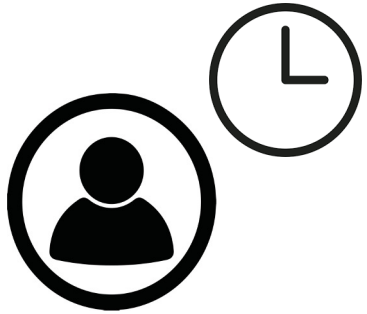
Employees are (often) protected by their IT security organization

Sometimes, they can be at odds

UC San Diego

# The relationship between employees and IT orgs

Employees are (often) protected by their IT security organization



Sometimes, they can be at odds

UC San Diego

# The relationship between employees and IT orgs

Employees are (often) protected by their IT security organization

Sometimes, they can be at odds

This is especially true during a security policy change

Friction for users can cause friction for the organization


UC San Diego

# How do we make enterprise security policy updates more efficient for all?

# The relationship between UCSD employees and IT

UCSD required all their employees to change passwords

Retroactively asked “How could we have made this more efficient?”


UC San Diego

1) What communication mechanisms are most effective at prompting user change?

2) Why do users lag in updating passwords?

3) How did the policy change affect help desk ticket workload?

# UCSD IT research details

Possible due to close collaboration with the IT Security organization

Retroactively analyzed data; not involved in design of policy change

Substantial password work; not from the perspective of the enterprise

Set out to quantify the change **as well** as potential improvement

# Available Data from IT

Logs of password updates, employee metadata, scrambled accounts

Communication messages and when they were sent

ServiceNow Help Desk Tickets, filtered by keywords and pertinent dates

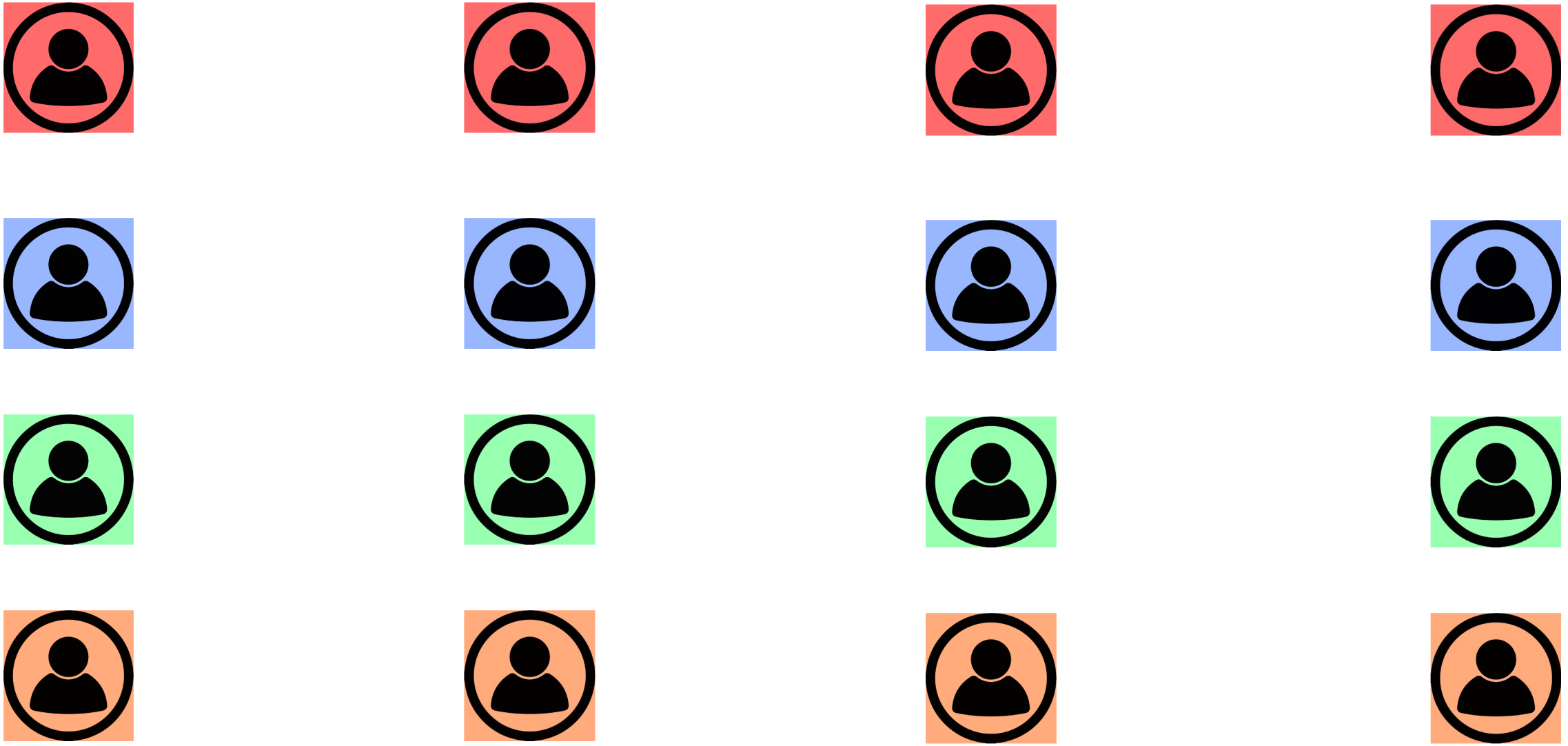
1) What communication mechanisms are most effective at prompting user change?

2) Why do users lag in updating passwords?

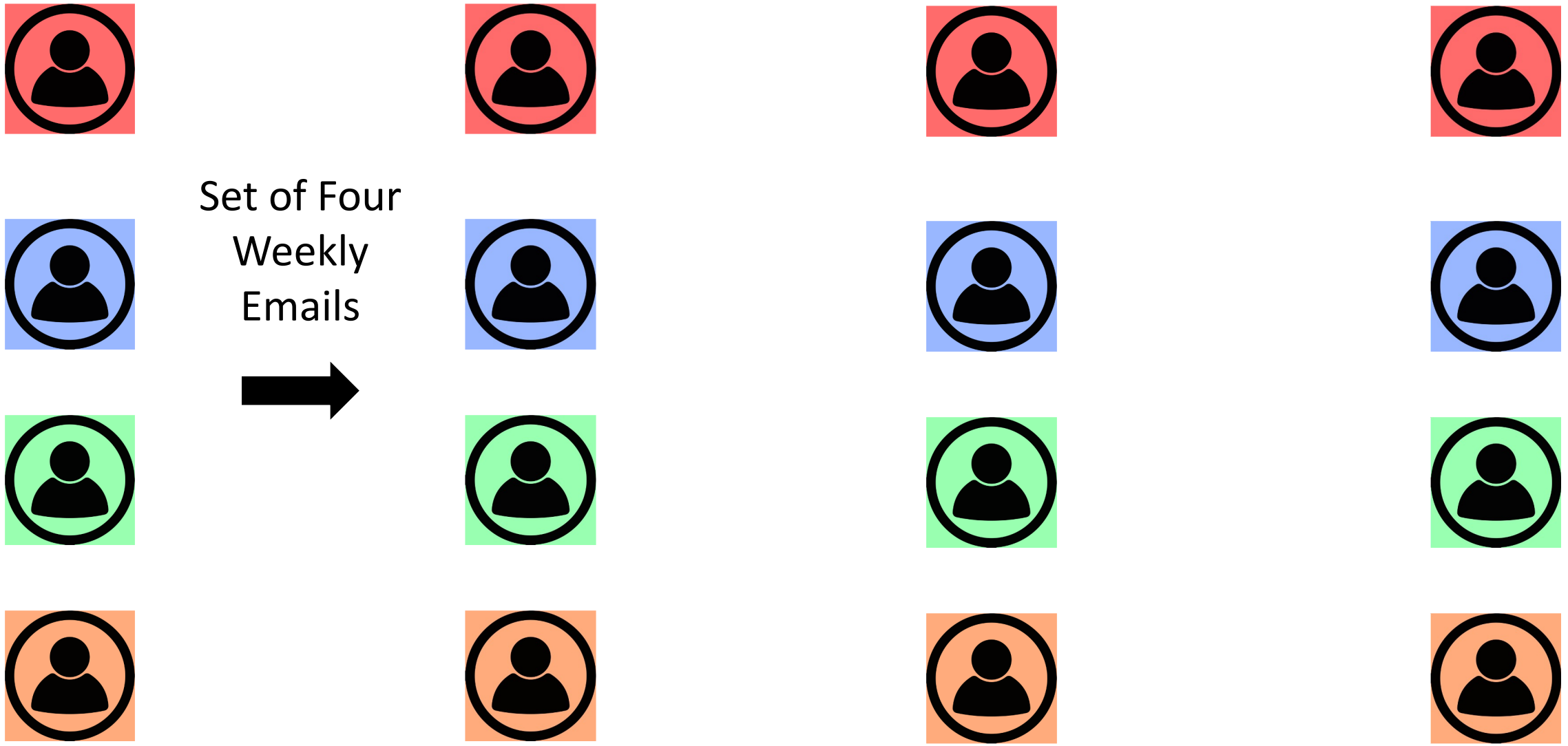
3) How did the policy change affect help desk ticket workload?

# 10K Employees

# 10K Employees



# 10K Employees



As part of our continuing effort to protect the UC San Diego community's data and systems, we are undergoing a campuswide password change action. Ensuring your passwords are strong is critical to protecting both your personal data and campus resources.

In addition to enhanced password security features, the minimum number of characters required for an AD password has been increased from 7 to 12 or more characters.

To meet the new minimum 12-character requirement, the UC San Diego Office of Information Assurance has begun requiring that all AD account holders make a one-time change of AD passwords after August 3, 2021.

## How Do I Change My AD Password?

Successfully changing your AD password depends on the devices you are using and your location. Visit How to Change Your AD Password for more information and steps to reset devices and workstations.

## Do I Have to Change My AD Password?

Yes, you are required to change your AD password, even if your current password is 12 or more characters in length.

Note that this change does not affect Business Systems SSO accounts.

## When Do I Change My AD Password?

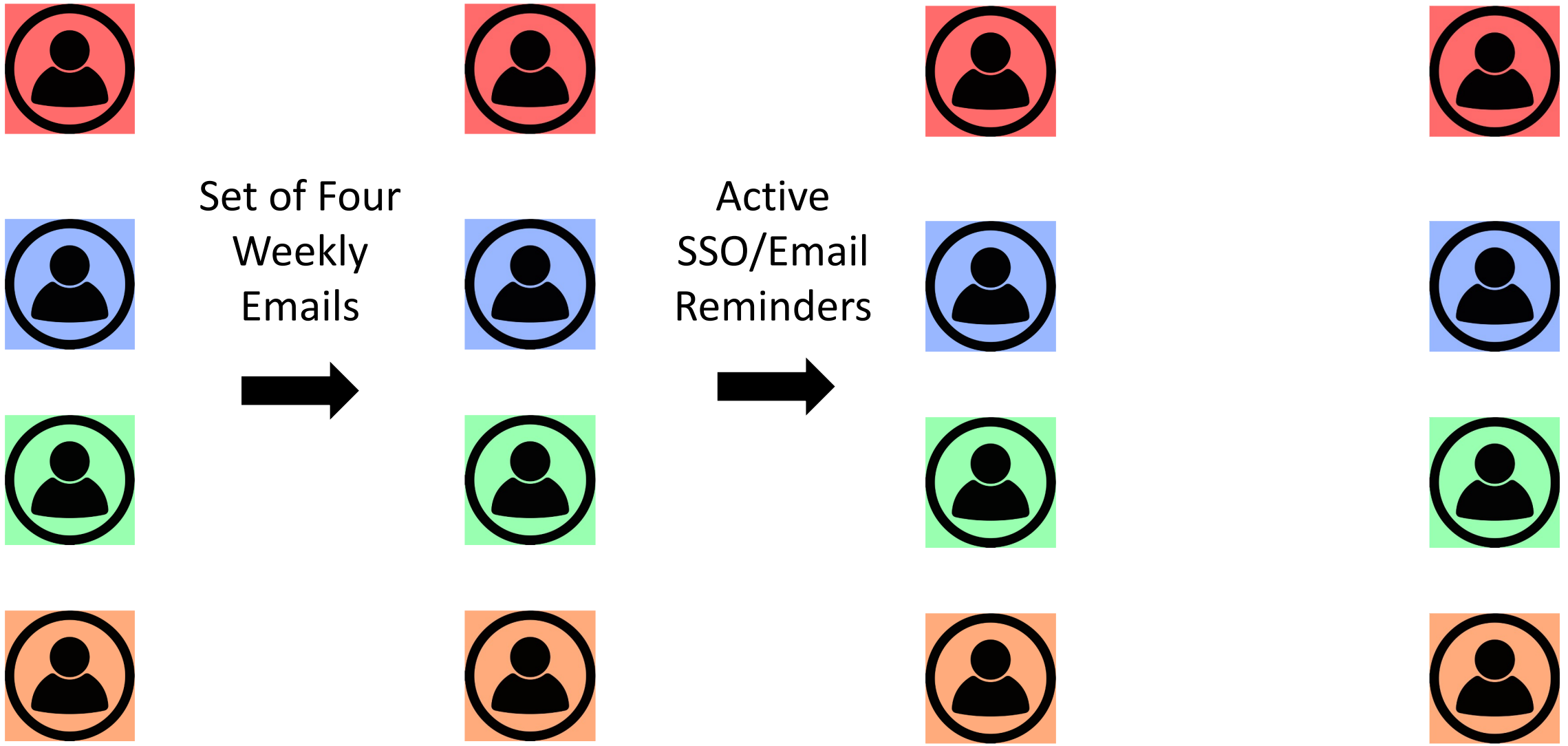
Campus academics, staff and affiliates whose **last names begin with H through N** are required to change AD passwords **any time between September 1 and September 22.**

All campus academic, staff, affiliate, Health Sciences and UC San Diego Health AD account holders have been split into groups, each group assigned dates for password changes. See the list of all groups and their assigned change dates.

## The LastPass Password Management Tool

Improve password security for all of your university accounts with the UC San Diego tested and approved LastPass password management software. Visit LastPass.ucsd.edu to learn more and register.

# 10K Employees



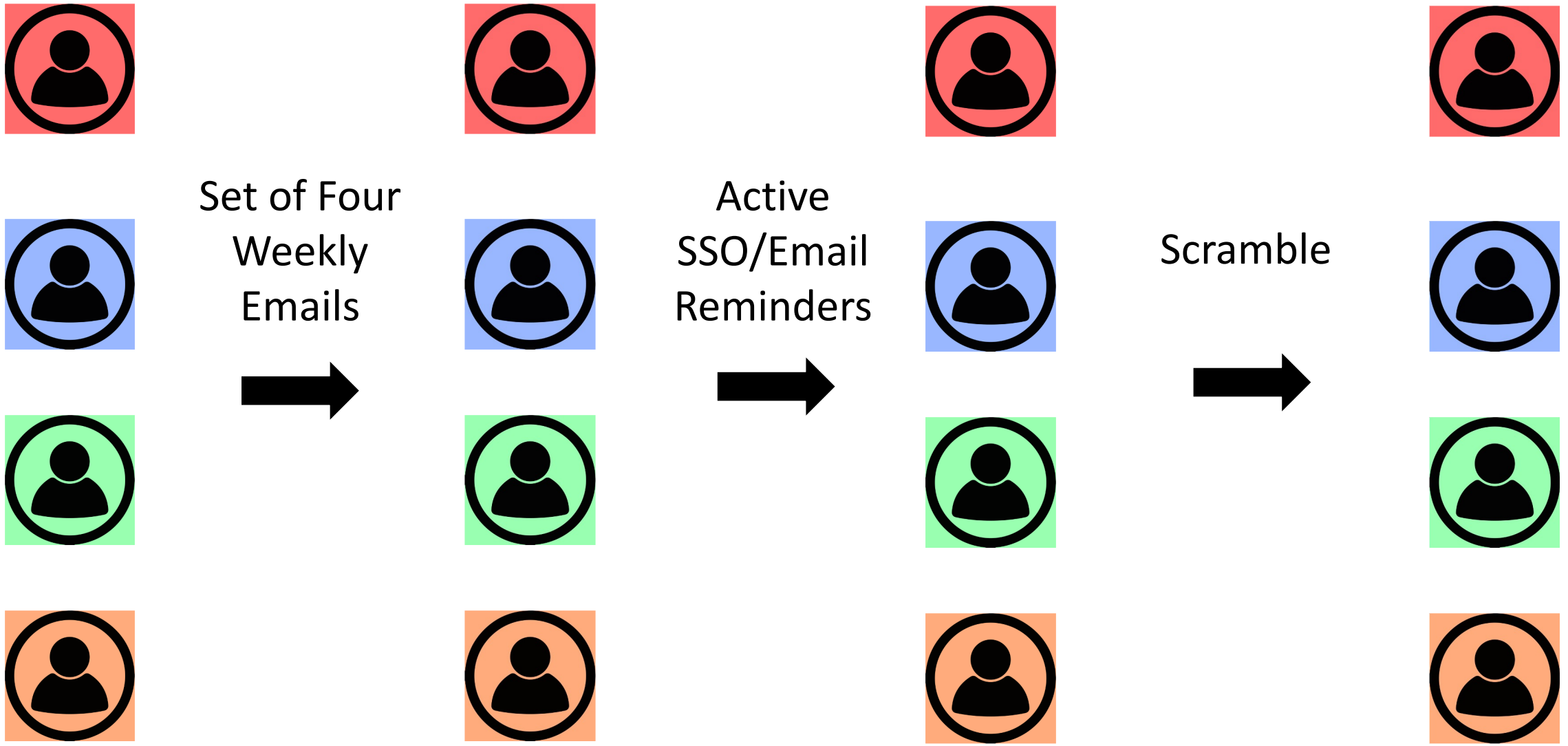
# SINGLE SIGN-ON (V3.3)

## AD Password Change Required

You are required to change your AD password by **11/17/2021**.

Change AD Password  Continue Log In

# 10K Employees

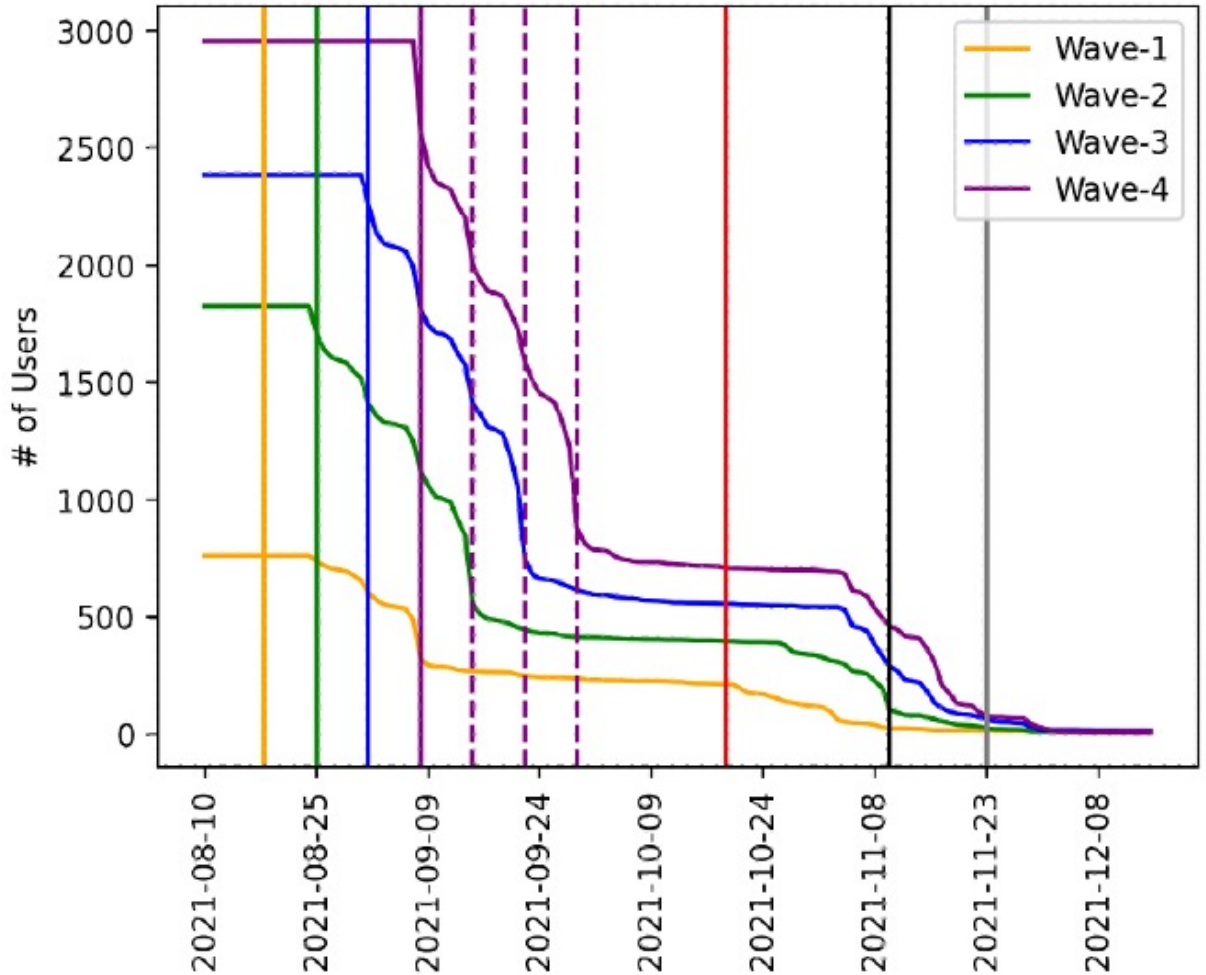


# Proportion of Change Modalities

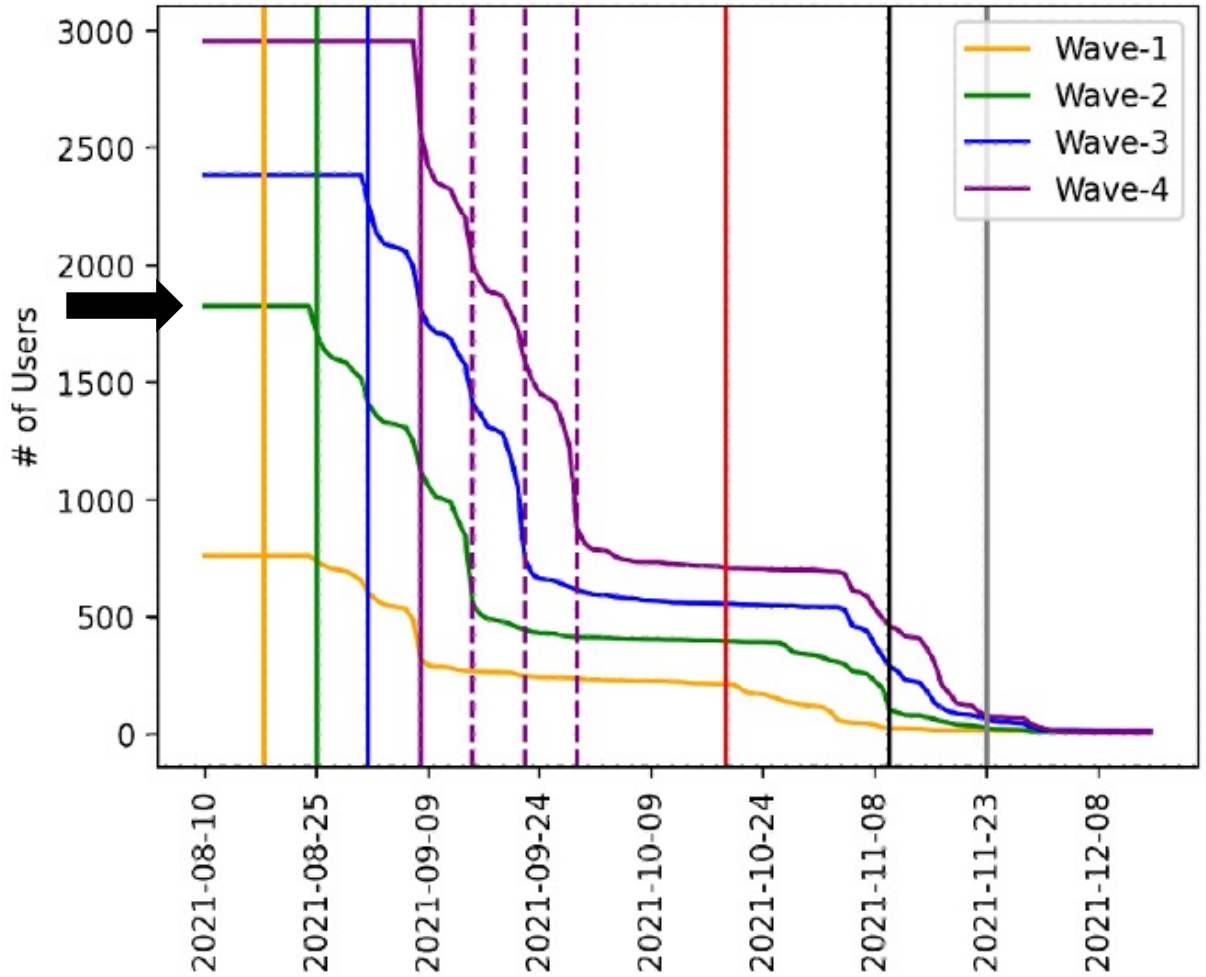
81.3% are single change users

12.2% are multiple change users

5.42% are scrambled users

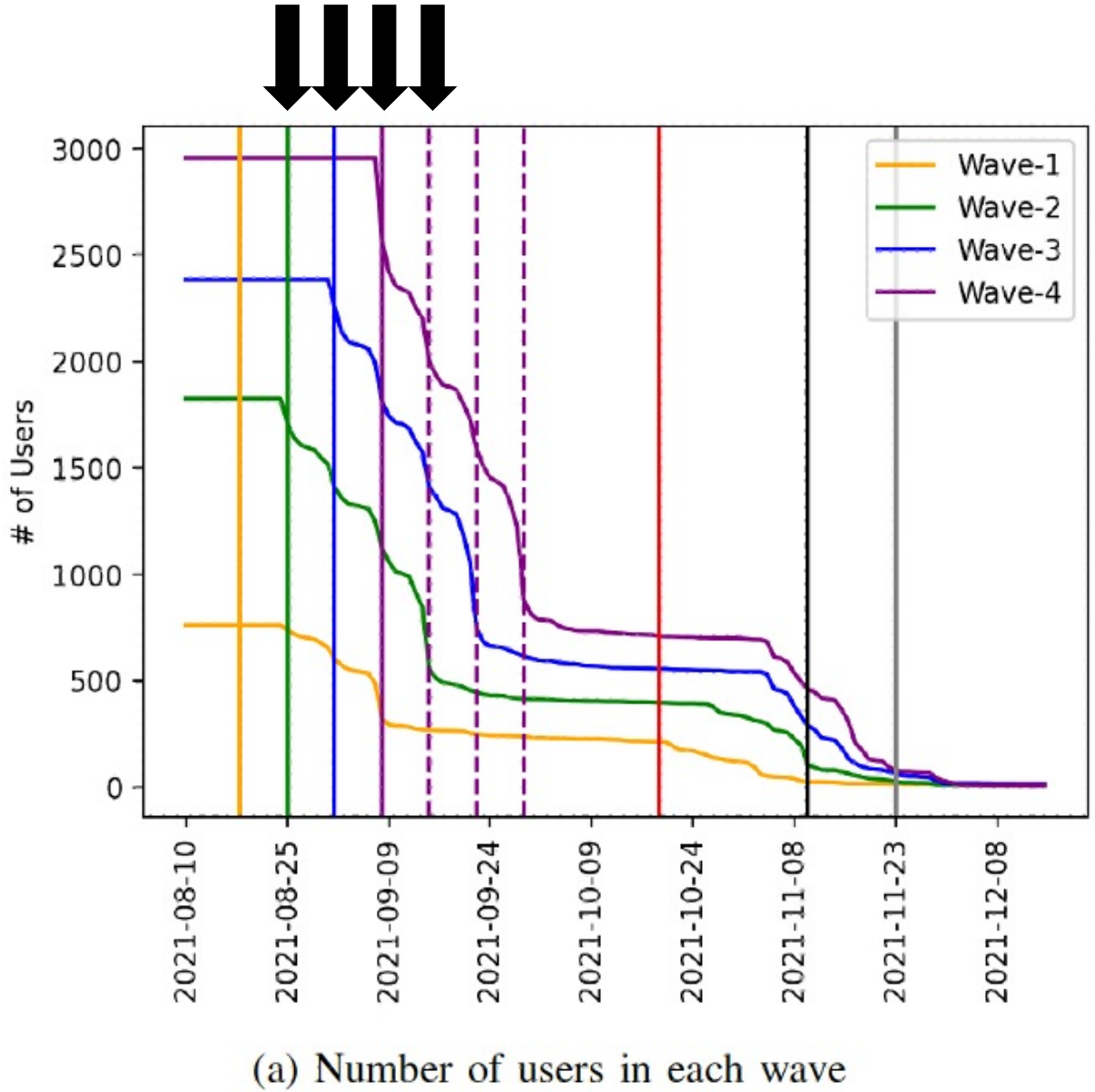



(a) Number of users in each wave




(a) Number of users in each wave

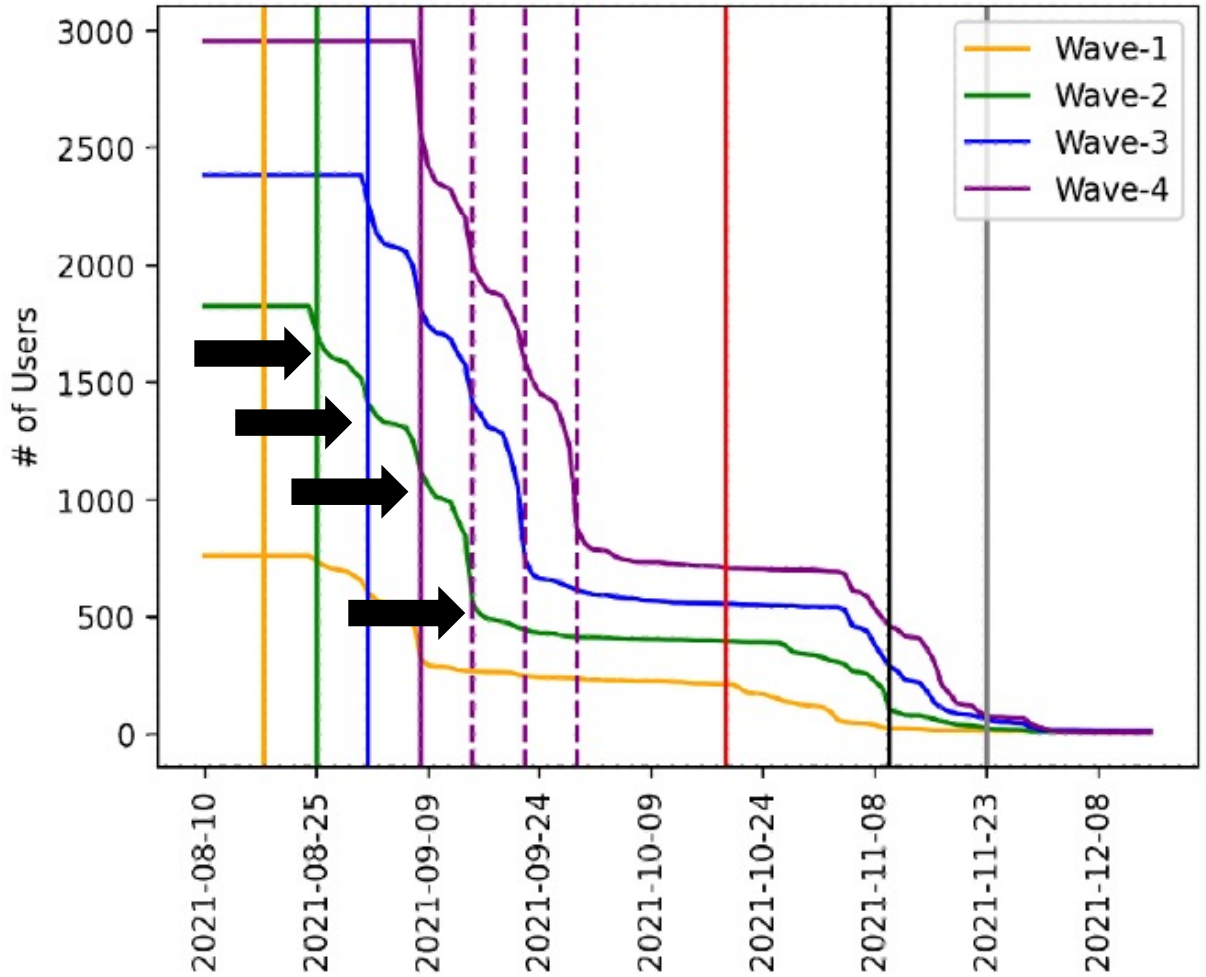
Each color represents a wave and the number of users who have not changed their password




(a) Number of users in each wave

Each color represents a wave and the number of users who have not changed their password

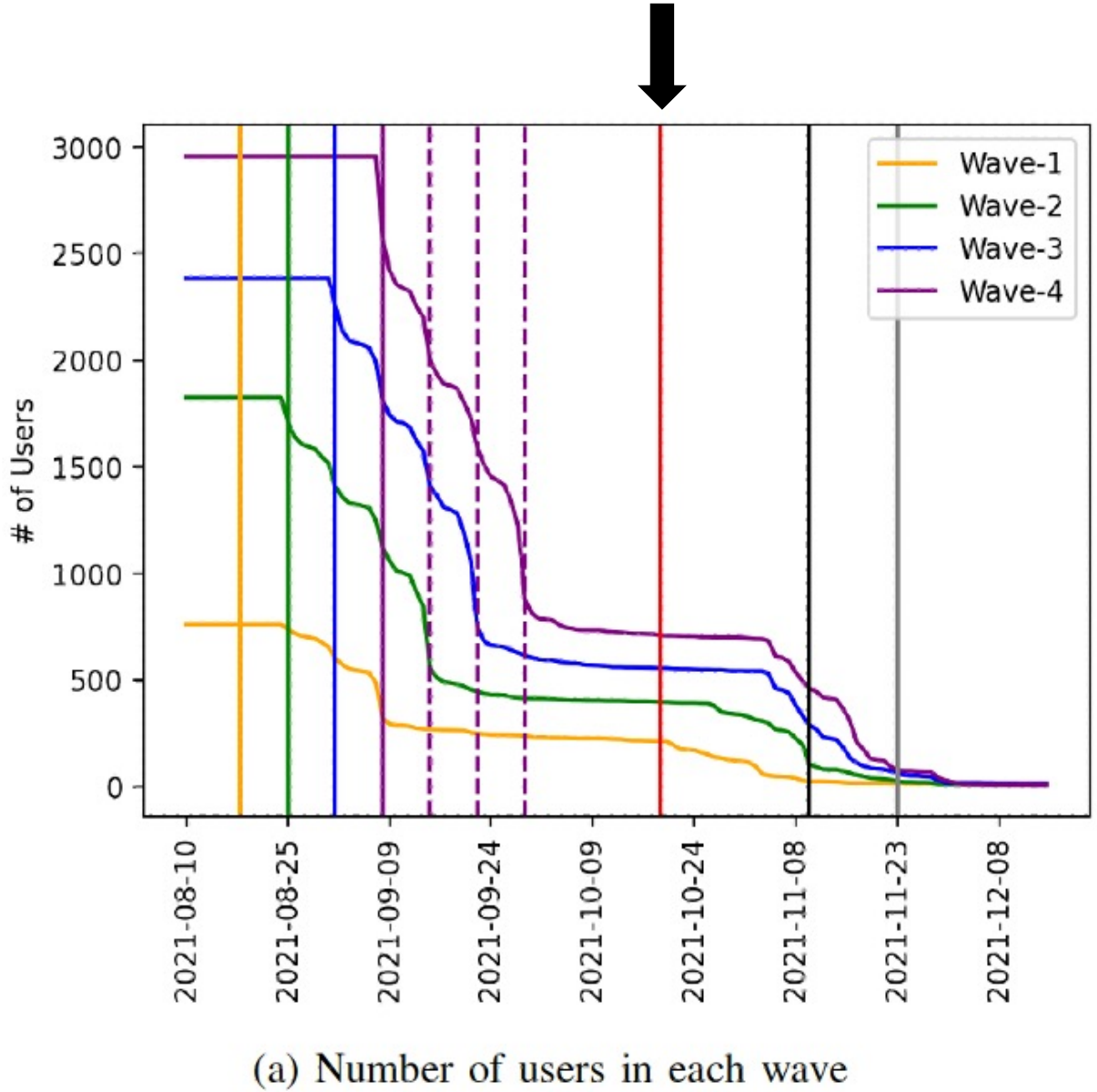
Solid vertical lines matching color of waves represent initial email communication




(a) Number of users in each wave

Each color represents a wave and the number of users who have not changed their password

Solid vertical lines matching color of waves represent initial email communication

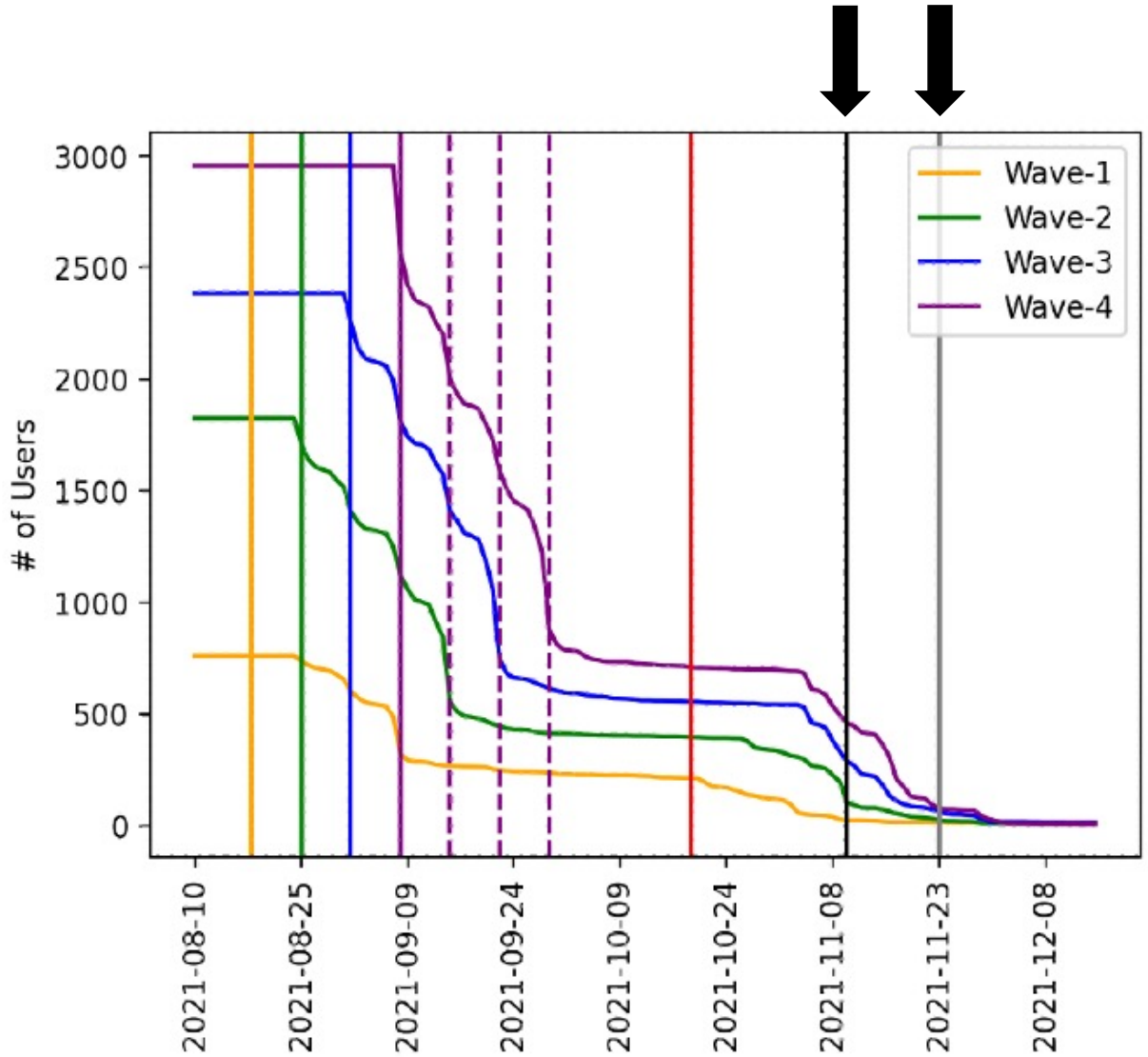



(a) Number of users in each wave

Each color represents a wave and the number of users who have not changed their password

Solid vertical lines matching color of waves represent initial email communication

Solid vertical red line represents the start of the SSO Active Directory intercept



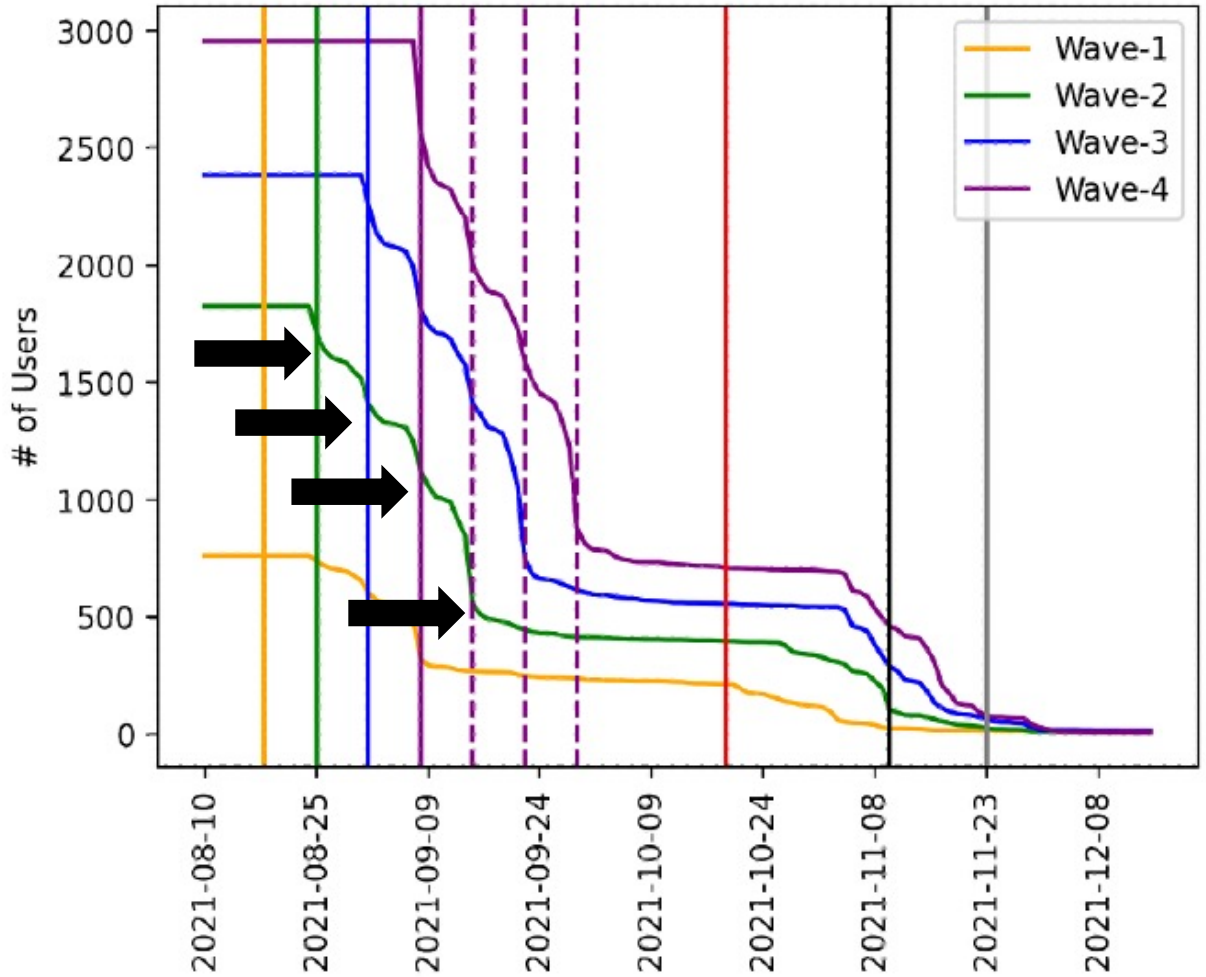

(a) Number of users in each wave

Each color represents a wave and the number of users who have not changed their password

Solid vertical lines matching color of waves represent initial email communication

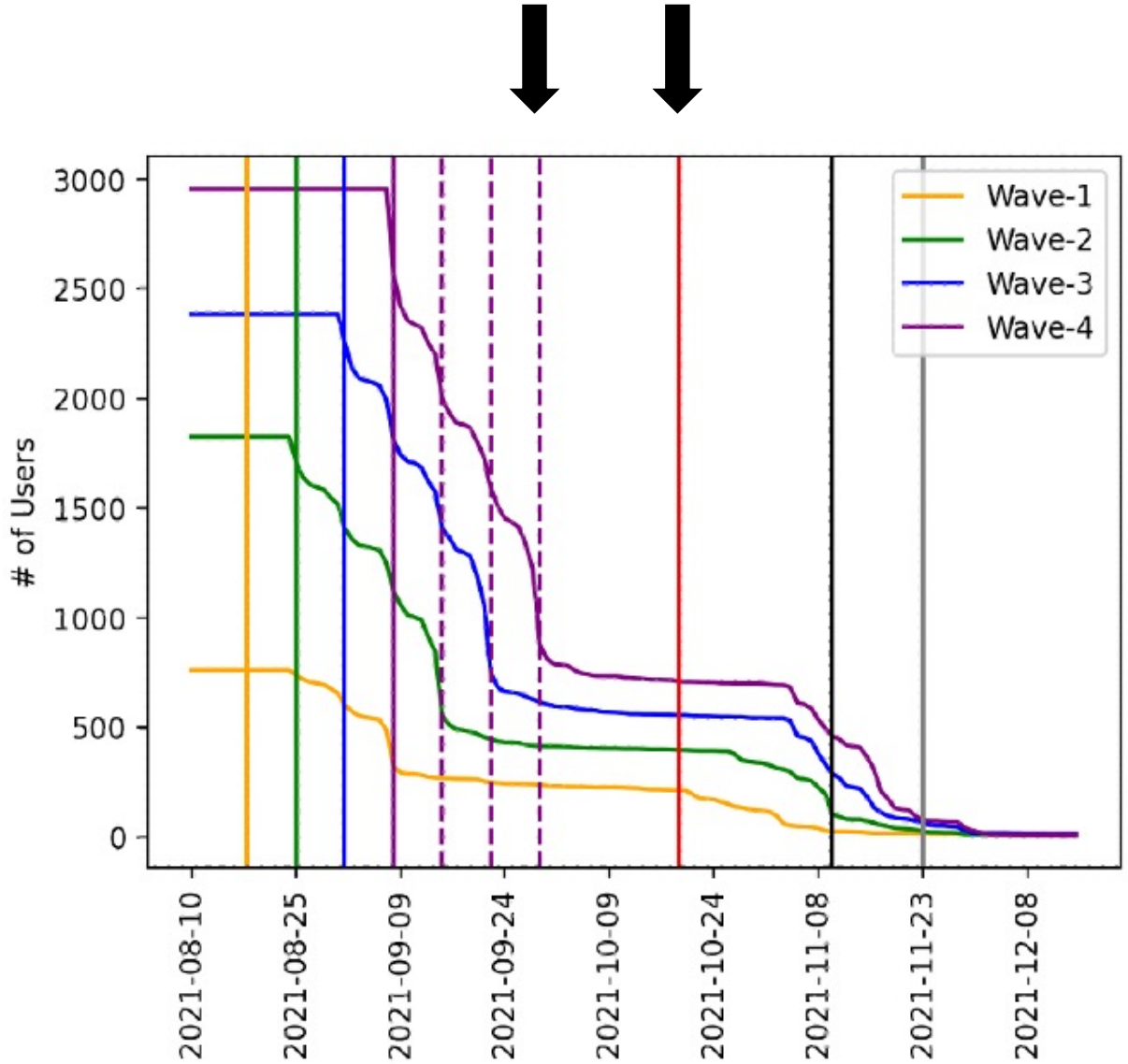
Solid vertical red line represents the start of the SSO Active Directory intercept

Solid black/grey lines represent the start of final email communications (SSO intercept active)




(a) Number of users in each wave

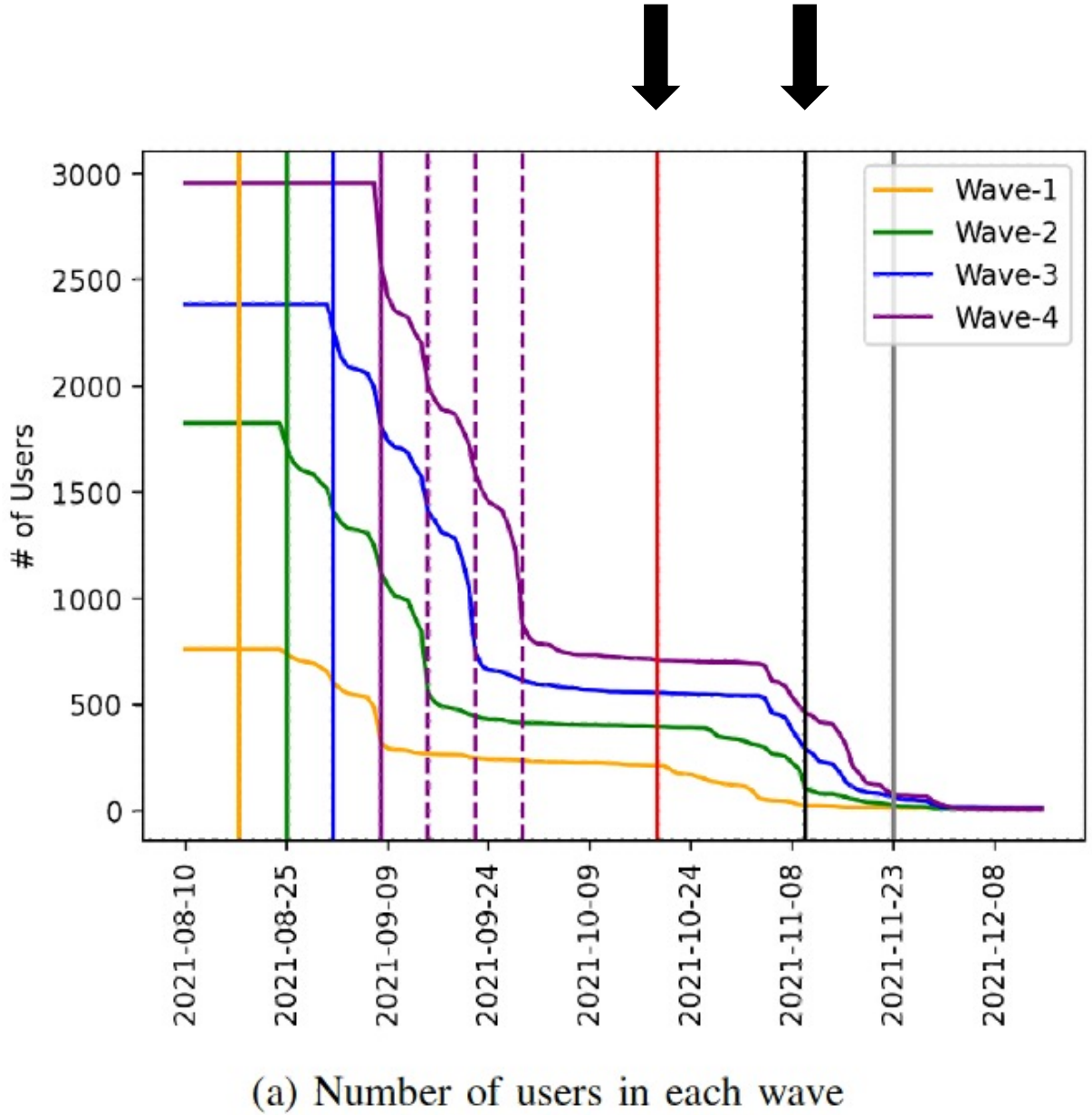
Repetitive emails are useful but have potential diminishing effectiveness




(a) Number of users in each wave

Repetitive emails are useful but have potential diminishing effectiveness

“Idle” period produces little change in users

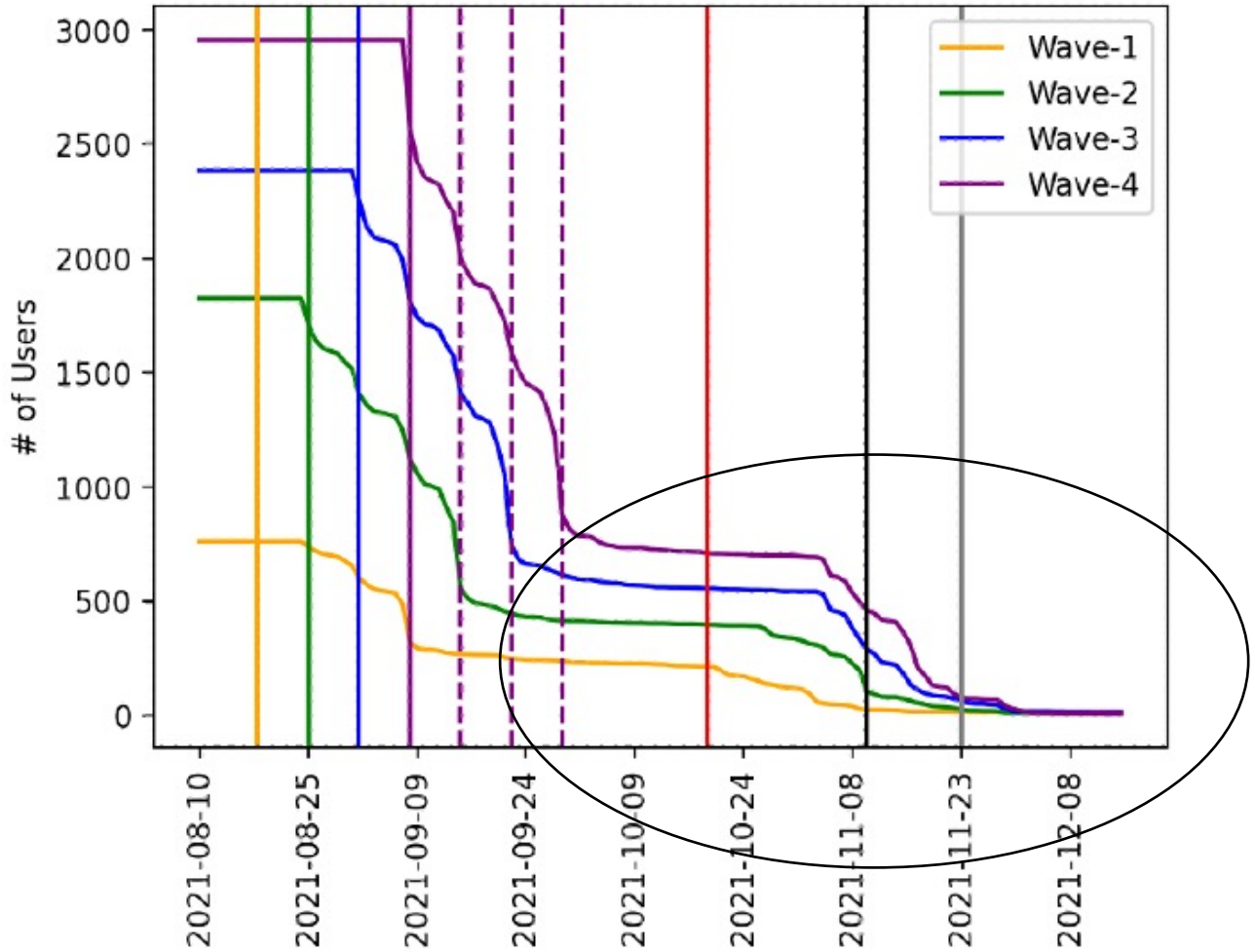



(a) Number of users in each wave

Repetitive emails are useful but have potential diminishing effectiveness

“Idle” period produces little change in user

SSO is most effective communication with ~80% user change rate in isolated period




(a) Number of users in each wave

1) What communication mechanisms are most effective at prompting user change?

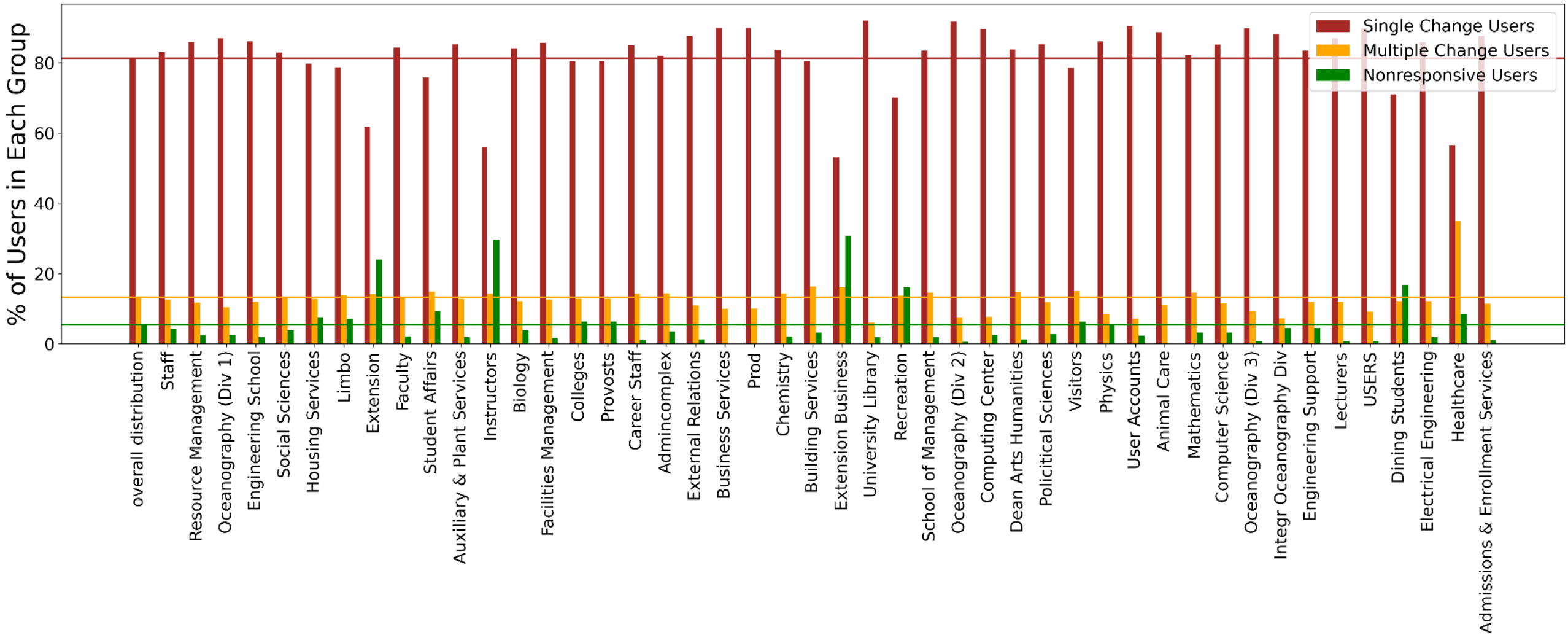
2) Why do users lag in updating passwords?

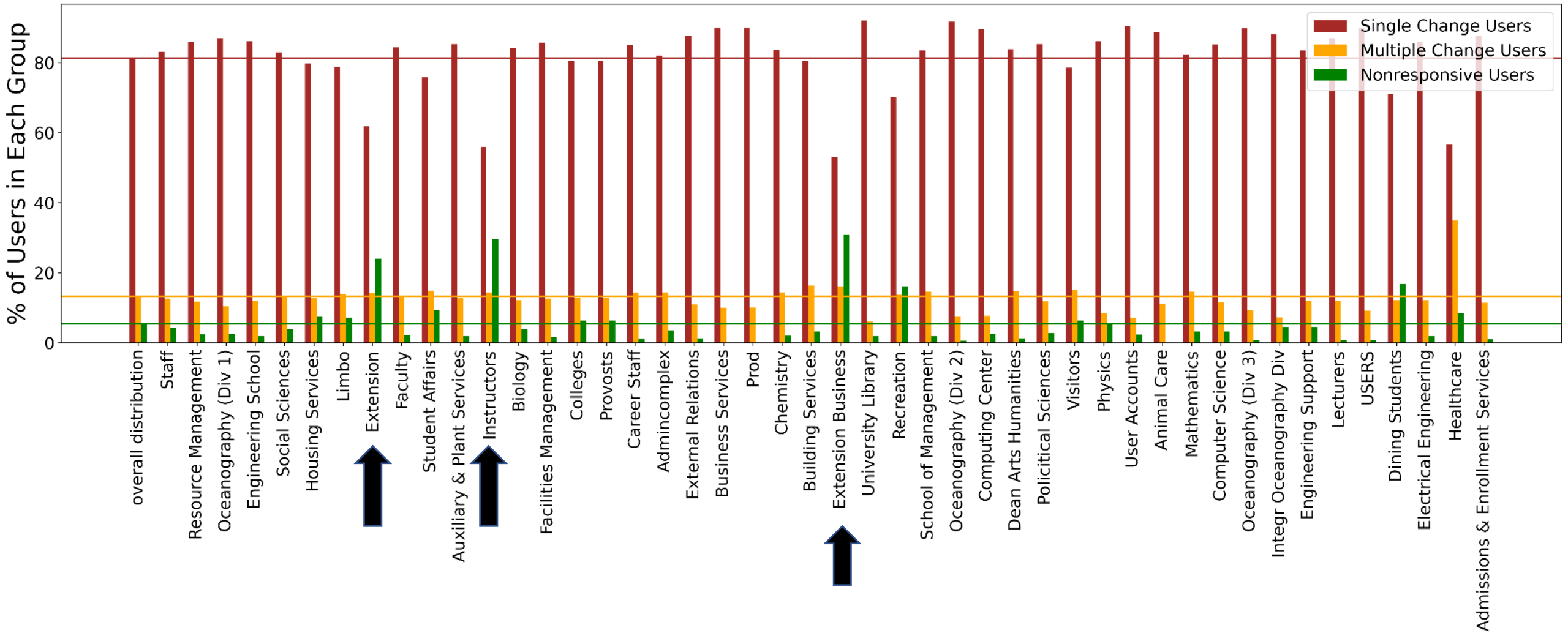
3) How did the policy change affect help desk ticket workload?

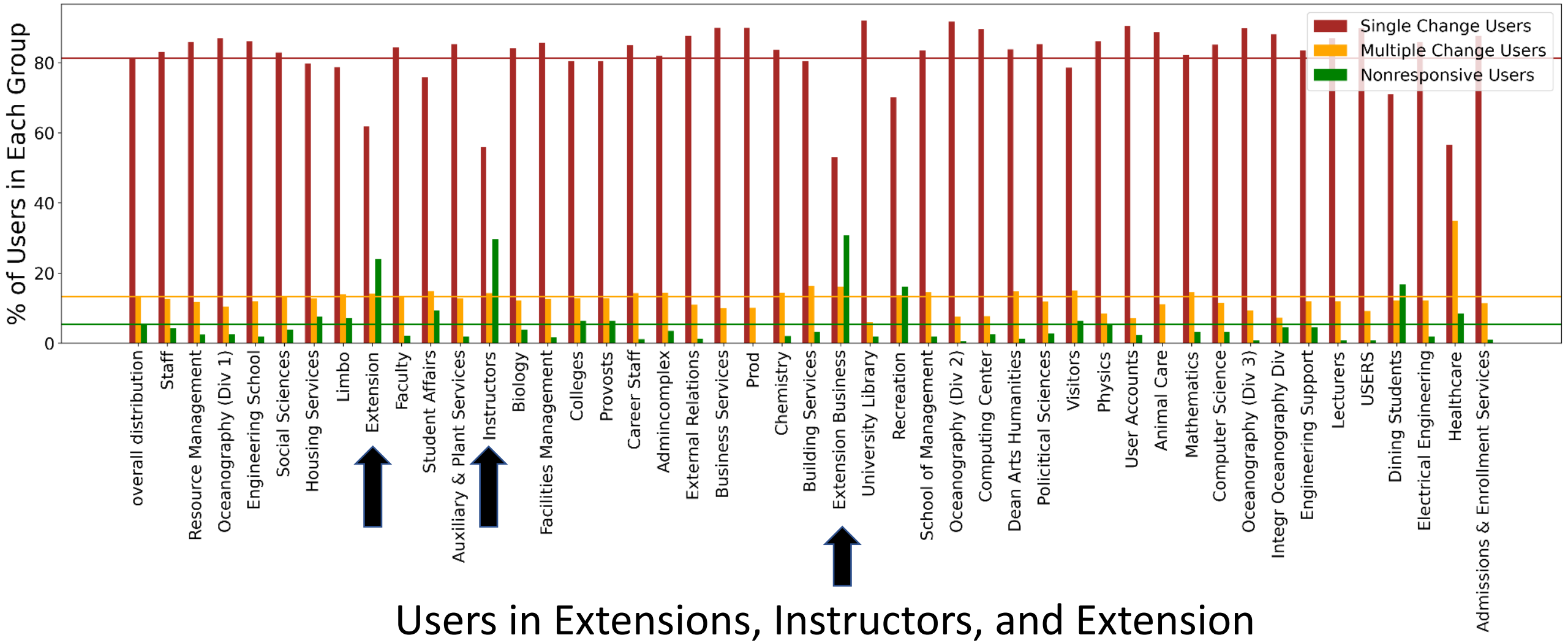
# Why do users lag in their update behavior?

Examine a user’s organizational unit and relate it to their change status

Organizational unit is a proxy for someone’s department on campus


% of Users in Each Group
0
20
40
60
80
Single Change Users
Multiple Change Users
Nonresponsive Users
overall distribution
Staff
Resource Management
Oceanography (Div 1)
Engineering School
Social Sciences
Housing Services
Limbo
Extension
Faculty
Student Affairs
Auxiliary & Plant Services
Instructors
Biology
Facilities Management
Colleges
Provosts
Career Staff
Admincomplex
External Relations
Business Services
Prod
Chemistry
Building Services
Extension Business
University Library
Recreation
School of Management
Oceanography (Div 2)
Computing Center
Dean Arts Humanities
Policitical Sciences
Visitors
Physics
User Accounts
Animal Care
Mathematics
Computer Science
Oceanography (Div 3)
Integr Oceanography Div
Engineering Support
Lecturers
USERS
Dining Students
Electrical Engineering
Healthcare
Admissions & Enrollment Services


% of Users in Each Group
0
20
40
60
80
Single Change Users
Multiple Change Users
Nonresponsive Users
overall distribution
Staff
Resource Management
Oceanography (Div 1)
Engineering School
Social Sciences
Housing Services
Limbo
Extension
Faculty
Student Affairs
Auxiliary & Plant Services
Instructors
Biology
Facilities Management
Colleges
Provosts
Career Staff
Admincomplex
External Relations
Business Services
Prod
Chemistry
Building Services
Extension Business
University Library
Recreation
School of Management
Oceanography (Div 2)
Computing Center
Dean Arts Humanities
Policitical Sciences
Visitors
Physics
User Accounts
Animal Care
Mathematics
Computer Science
Oceanography (Div 3)
Integr Oceanography Div
Engineering Support
Lecturers
USERS
Dining Students
Electrical Engineering
Healthcare
Admissions & Enrollment Services




Users in Extensions, Instructors, and Extension Business are significantly overrepresented in the non-responsive user population

# Why do users lag in their update behavior?

Repeated same analysis for single change users

Examined relation between organizational unit and when user changed

# Why do users lag in their update behavior?

Repeated same analysis for single change users

Examined relation between organizational unit and when user changed

Building services, Recreation, and Dining services are over-represented in the Active SSO (intervention) period

Users in peripheral organizations take more time to respond

1) What communication mechanisms are most effective at prompting user change?

2) Why do users lag in updating passwords?

3) How did the policy change affect help desk ticket workload?

# Did ticket volume change with the policy change?

# Did ticket volume change with the policy change?

Filtered ServiceNow tickets by: user, date, password related keywords

Examined ticket volume for these users during the policy change and a year prior

# Did ticket volume change with the policy change?

Filtere
date, p

Examir
users c
a year

| Password Update Campaign | | | Prior Year | |
|---|---|---|---|---|
| All Waves | 7.82% | (762 / 9,744) | 2.21% | (215 / 9,744) |
| Wave 1 | 7.94% | (78 / 983) | 2.24% | (22 / 983) |
| Wave 2 | 7.66% | (174 / 2,272) | 2.60% | (59 / 2,272) |
| Wave 3 | 8.04% | (237 / 2,948) | 2.37% | (70 / 2,948) |
| Wave 4 | 7.71% | (273 / 3,541) | 1.81% | (64 / 3,541) |

# Did ticket volume change with the policy change?

Filtere
date, p

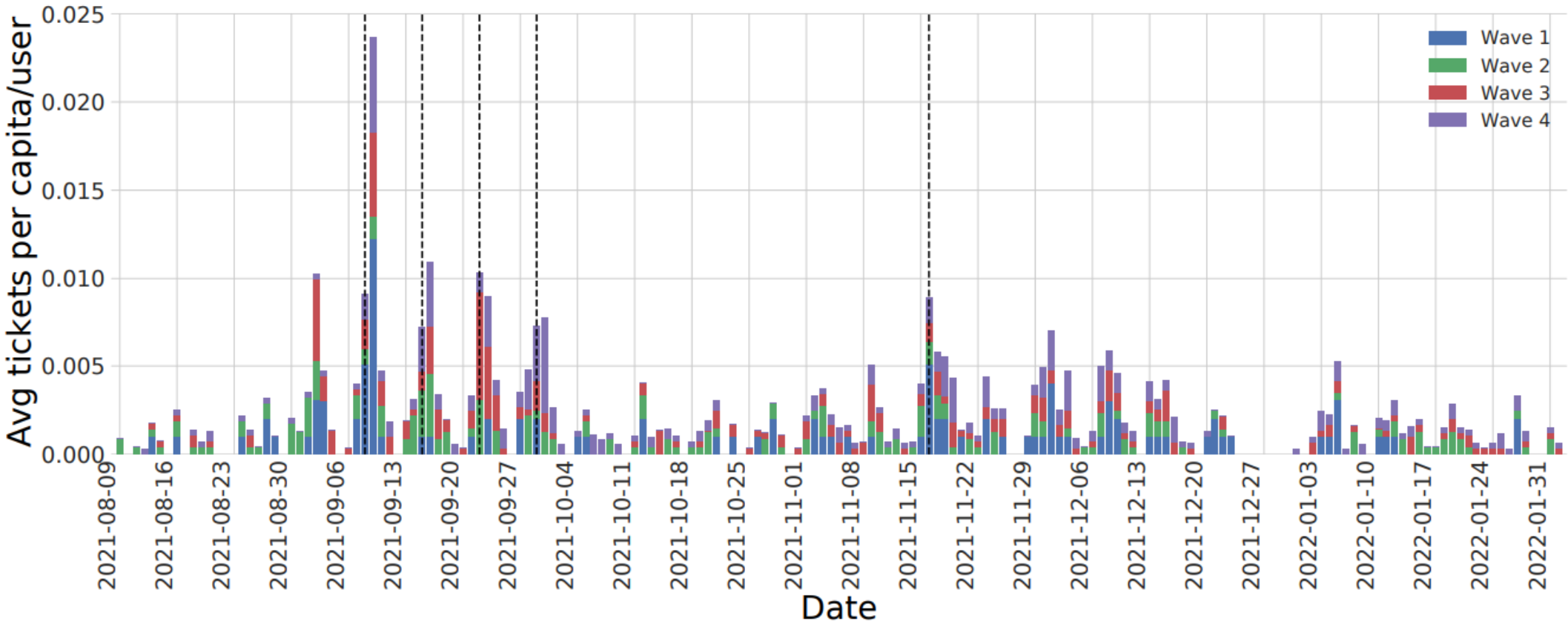
Examir
users c
a year

| Password Update Campaign | | | Prior Year | |
|---|---|---|---|---|
| All Waves | 7.82% | (762 / 9,744) | 2.21% | (215 / 9,744) |
| Wave 1 | 7.94% | (78 / 983) | 2.24% | (22 / 983) |
| Wave 2 | 7.66% | (174 / 2,272) | 2.60% | (59 / 2,272) |
| Wave 3 | 8.04% | (237 / 2,948) | 2.37% | (70 / 2,948) |
| Wave 4 | 7.71% | (273 / 3,541) | 1.81% | (64 / 3,541) |

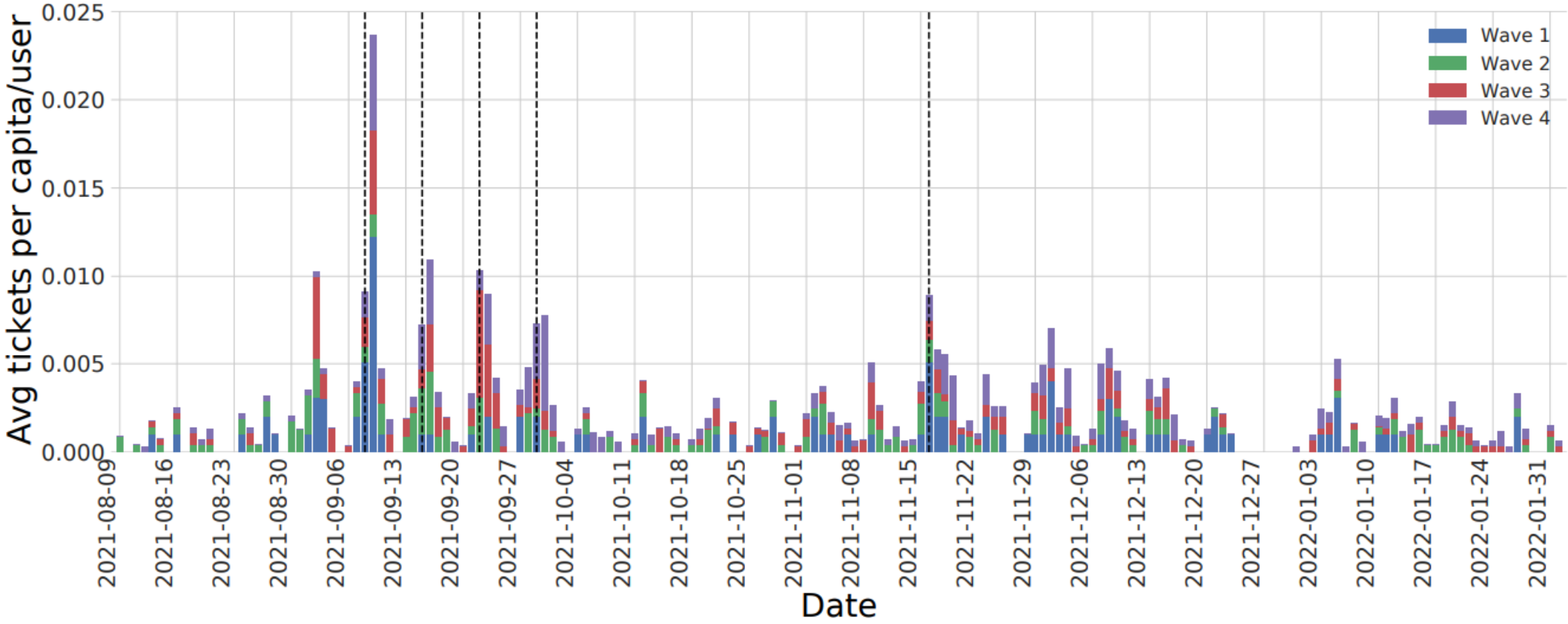
Ticket volume increases 3-4x during the policy change

# Was ticket volume uniform during the policy change?

# Was ticket volume uniform during the policy change?

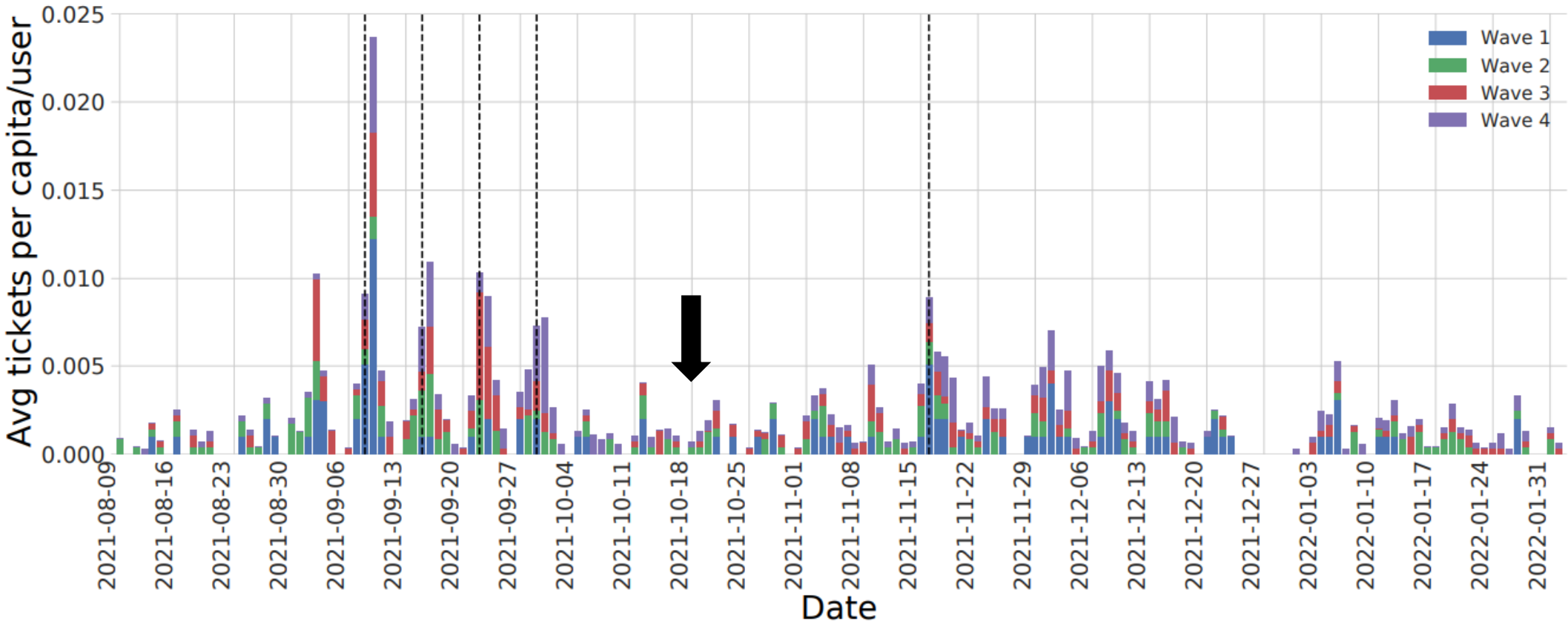


# Was ticket volume uniform during the policy change?

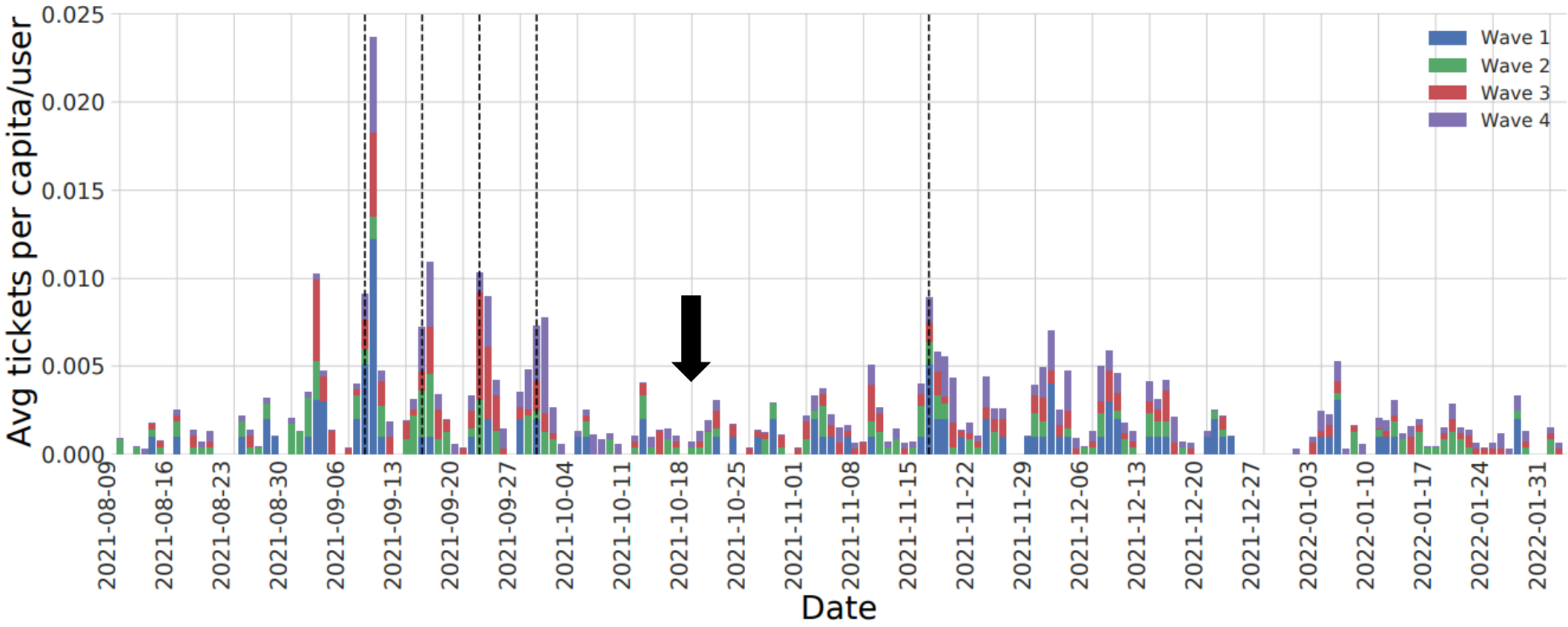



Ticket volume was more heavily concentrated during the initial email campaign, especially after the last email

# Was ticket volume uniform during the policy change?



# Was ticket volume uniform during the policy change?




Ticket volume is lowest during the active SSO time period

1) What communication mechanisms are most effective at prompting user change?

2) Why do users lag in updating passwords?

3) How did the policy change affect help desk ticket workload?

# Improving Policy Update Effectiveness

1) SSO is the most effective communication mechanism, email still useful

2) Peripheral users might not use same communication mechanisms as other units on campus, and thus lag in their update behavior

3) Ticket load does increase non-uniformly, with active SSO creating the least amount of tickets

# Improving Policy Update Effectiveness

1) SSO is the most effective communication mechanism, email still useful

2) Peripheral users might not use same communication mechanisms as other units on campus, and thus lag in their update behavior

3) Ticket load does increase non-uniformly, with active SSO creating the least amount of tickets

Lessons can and have been used for future policy changes

# Thank you

Grant Ho, Stefan Savage, Geoffrey M. Voelker for collaborator support

Elaine Fleming, James Dotson, Edward Wade for IT data/policy support

Phillip Lopo and Mike Corn for collaboration advocacy

# Questions?

arianamirian.com

arianamirian28@gmail.com

@arimirian

@amirian@infosec.exchange

# Extra Slides

# Overview slide

Behind every employee is an IT organization that works to keep it safe, but sometimes, the individual and the employee can be at odds. The employee wants to finish their job function, whatever it is, and the organization might impose limitations that make this difficult for them to do so. An employee and organization may especially be at odds during a security policy change, where an organization tries to increase it's security posture, but disrupts employee's workflows in order to do so. This is not to say that security changes are bad, but they can cause a lot of friction for users, which then trickles to friction for the organization. There is a very practical question of how do we make these security policy changes more "efficient" for both the organization and the user?

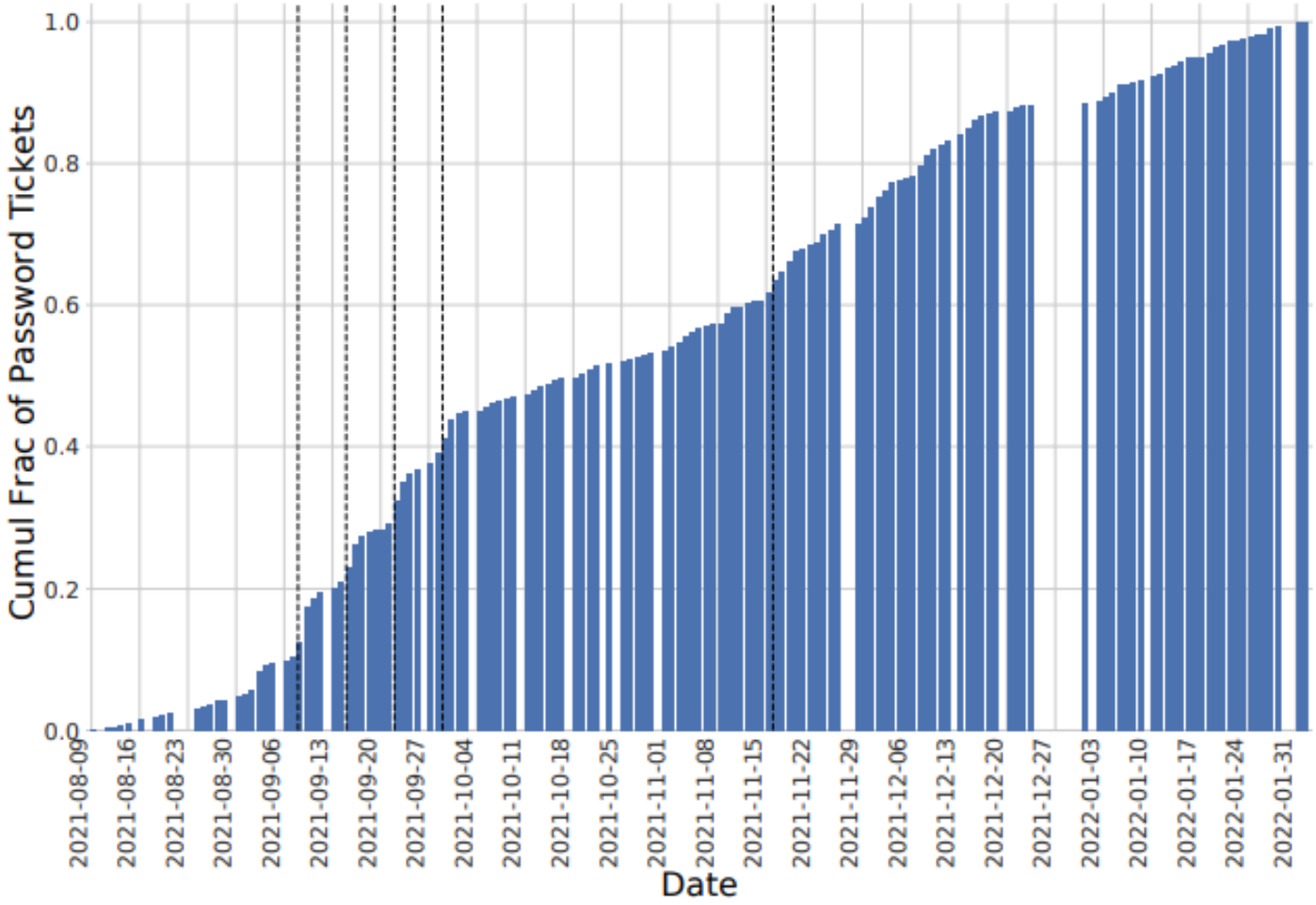
It is not ironic that this is exactly the position our large academic institution found themselves in. they asked all of their employees to change their password to increase the security posture of the organization as a whole, but after the fact came to us and asked "how could this have gone more smoothly?" Given the lack of recent research in this, our group of empiricists set out to answer three main questions

1) What communication mechanisms are most effective at prompting user change?
2) Why did some users lag in their update behavior?
3) How did help desk support ticket load change in lieu of this policy change?

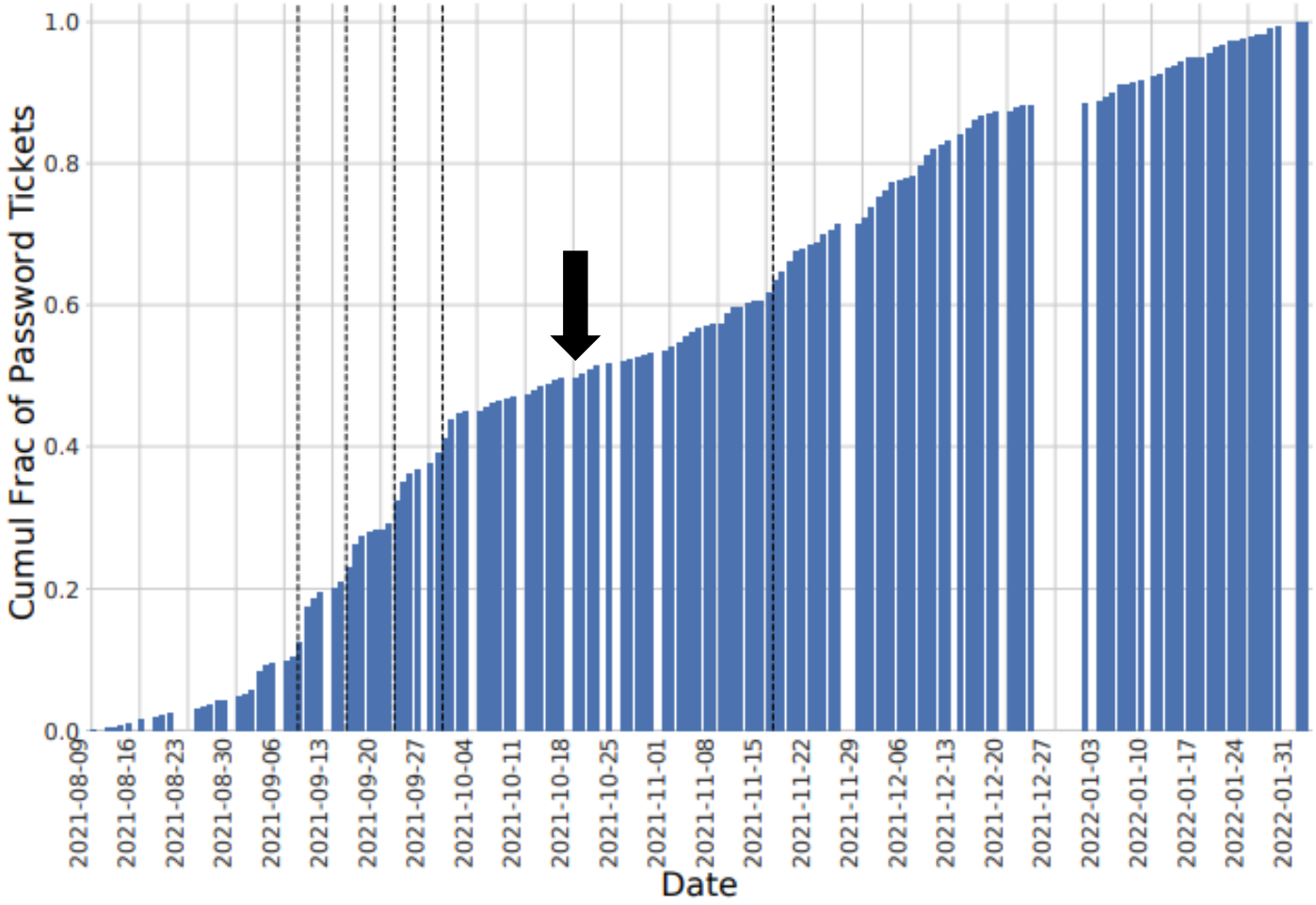
To concretize, we set out to quantify this change, but also figure out room for improvement for future policy changes, and other organizations.

We were in a unique position where we were granted access to within the IT organization, which is in large part due to advocates we had at the IT office within UCSD.

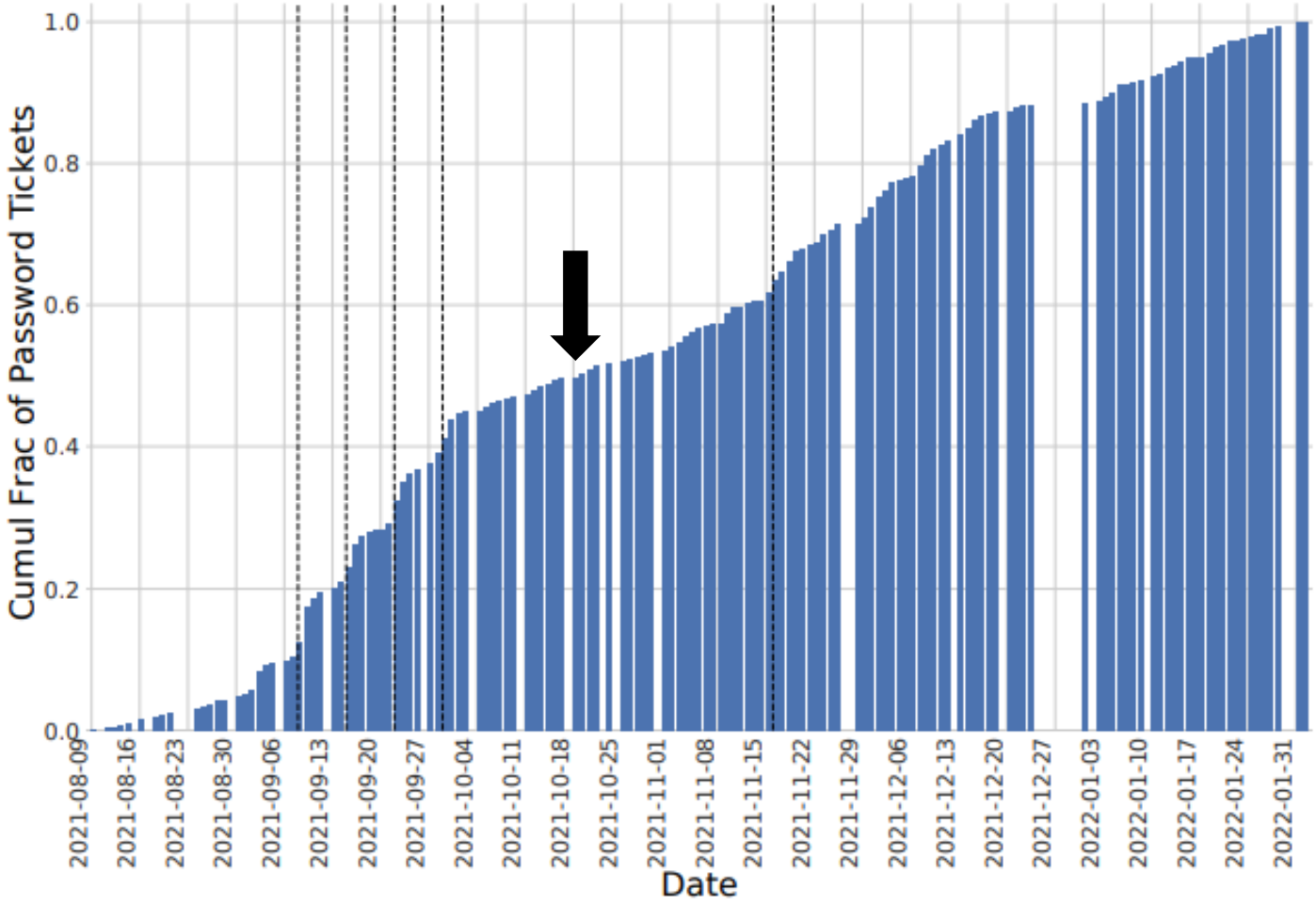
# Was ticket volume uniform during the policy change?



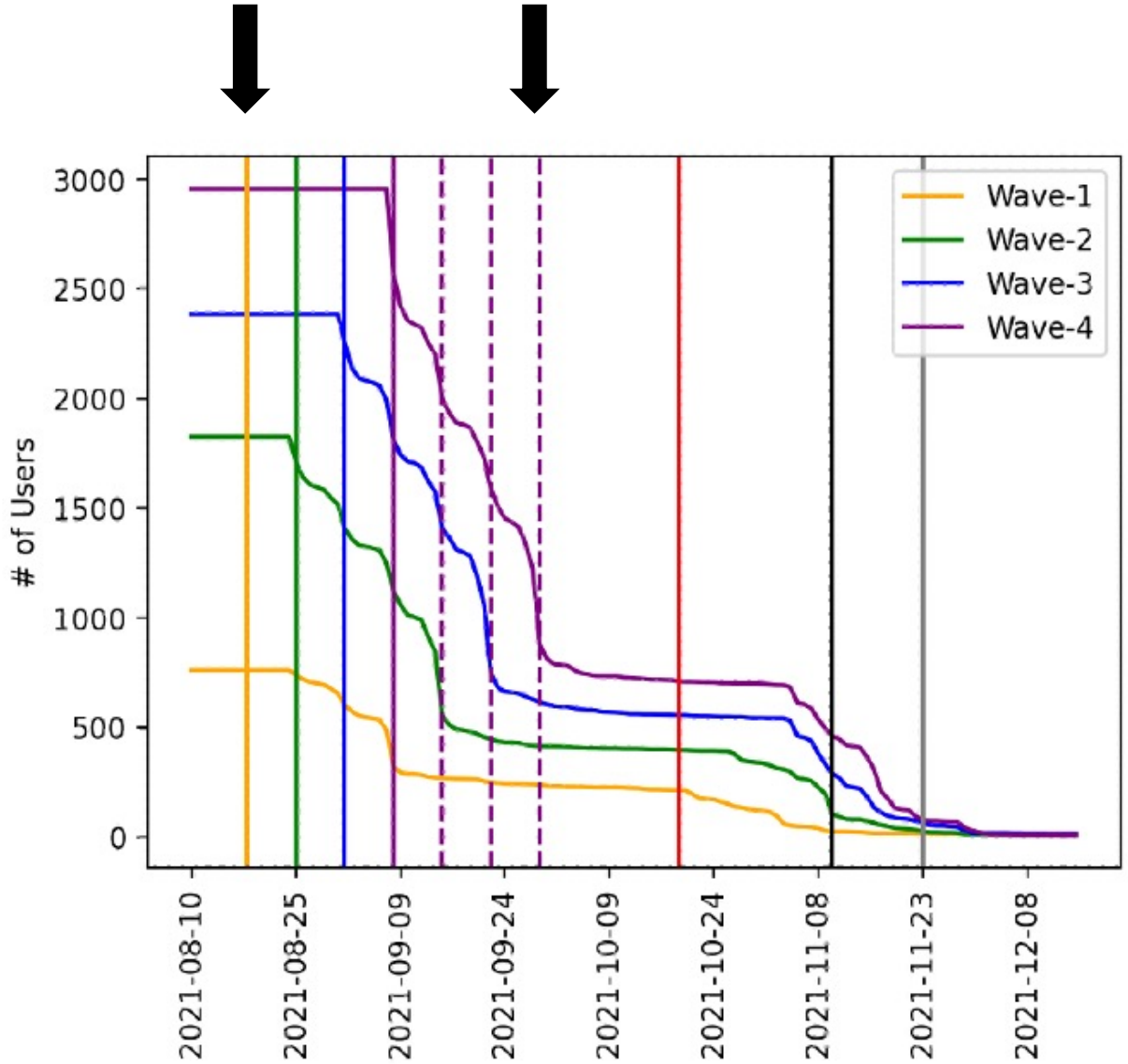
# Was ticket volume uniform during the policy change?



# Was ticket volume uniform during the policy change?

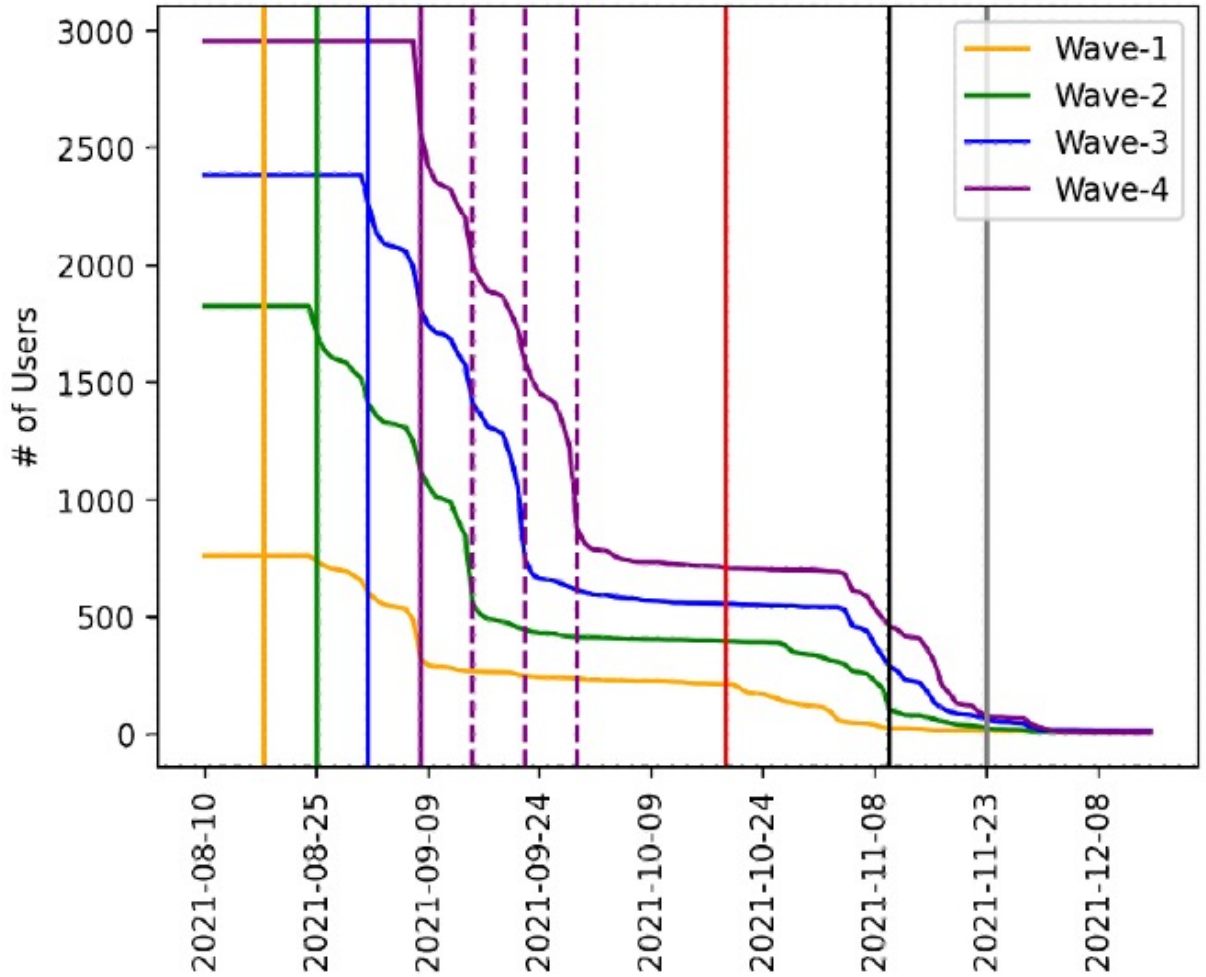



Ticket volume is lowest during the active SSO time period




(a) Number of users in each wave

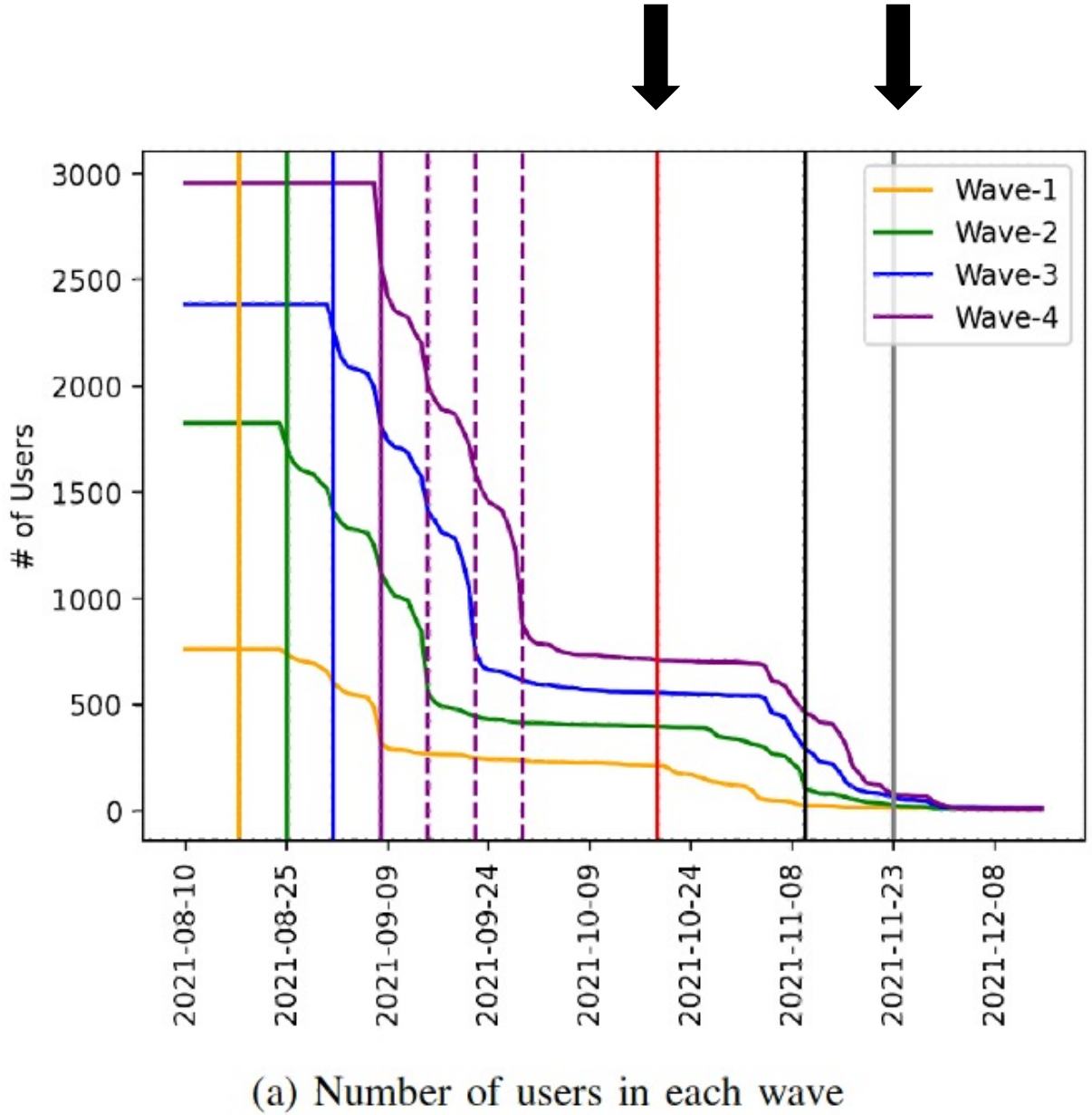
Period during initial email waves is categorized as “responsive period”




(a) Number of users in each wave

Period during initial email waves is categorized as “responsive period”

Period in between communications is categorized as “idle” period




(a) Number of users in each wave

Period during initial email waves is categorized as “responsive period”

Period in between communications is categorized as “idle” period

Period during SSO intercept/final email communications is the “interventional” period