

# I Was Tasked with Enrolling Millions of Developers in 2FA — Here's What Happened



John Swanson

<https://infosec.exchange/@swannysec>  
<https://twitter.com/swannysec>



# Story Time



# Who am I?

- You can call me **Swanny**
- Director, Security Strategy  
**@GitHub**
- Planning, leadership,  
program management.
- **Dad, nerd**



# Agenda

**Problem statement and associated challenges**

**Strategy**

**Tactics**

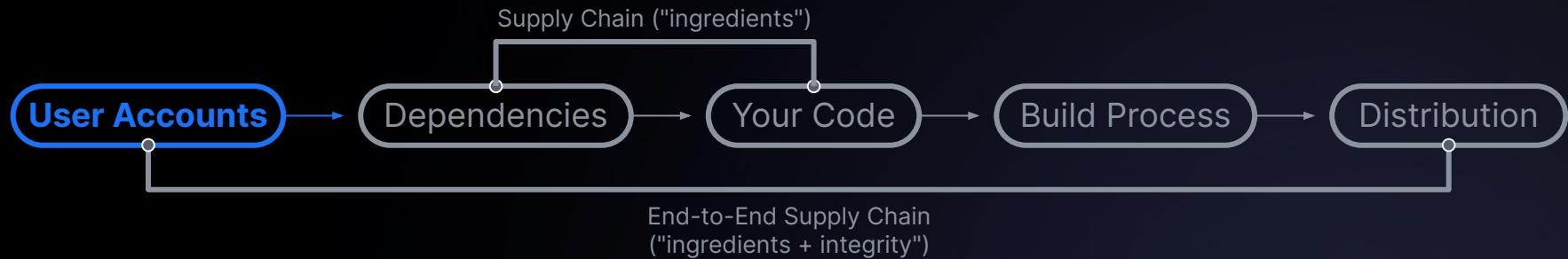
**Current state and what comes next**

**Key lessons**

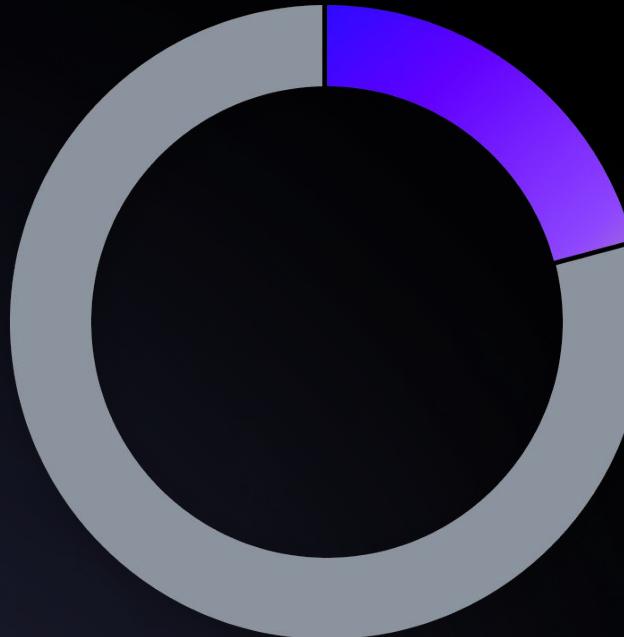
What's the  
problem?

# Protecting Developers

The software supply chain starts with the developer.  
How do we keep developers safe?



# What's missing? 2FA



~20%  
with 2FA

GitHub.com 2FA Adoption

## Our Objective

**GitHub will require all users who contribute to code on GitHub.com to enable one or more forms of two-factor authentication (2FA) by the end of 2023.**

# Two Core Issues

2FA is still hard  
to use and easy  
to lose



2FA adoption  
often conflicts  
with business  
goals

# The Classic Security Problem

- We need to introduce a new security measure which introduces cost or appears to slow users down.
- How do we get where we need to go in the face of competing priorities?
- How can you do so while limiting the downsides and maximizing the upsides?
- How do we preserve trust/buy-in and crush the “culture of no?”

# Strategy and Tactics In a Business Setting

- **Strategy pursues** the higher level business objectives and outcomes.
- **Tactics define how** individual workstreams contribute to those objectives and outcomes at the ground level.
- **Both are essential.**



*"Portrait of Carl von Clausewitz,"*  
Karl Wilhelm Wach, Public Domain.

# Strategy



# On Strategy

**Opening moves matter!**  
Set your initiative up for success by aligning with the business.

# Understand the Problem Deeply

- Research and discovery is critical **before planning or executing!**
- Involve a wide set of stakeholders **early.**



Created with Midjourney

# Research Head Start

Open Source Security

**Enrolling all npm publishers in enhanced login verification and next steps for two-factor authentication enforcement**

Today we're introducing enhanced login verification to the npm registry, and we will begin a staged rollout to maintainers beginning Dec 7.

# Establish Principles to Align Tactics with Strategy

- Figure out **how you want to work**.
- What cultural values do you want to capture?  
Is there a specific approach you want to apply?
- **Document these** and use them to make sure you're on the right course later.

# Our 2FA Operating Principles

- **Internal metrics on user activity must not be viewed as obstacles to account security improvements** since those metrics are meaningless if we lose the overall trust of our customers through ATO and supply chain compromise.
- Conversely, **security improvements must not come at the expense of user experience (UX) or make the product inaccessible**. Security that isn't usable isn't security.
- **Good account security** is a core feature and trust preservation measure that **should not rely on additional licensing**. Security is a right, not a privilege.



# Write it Down

- **Capture** at minimum:
  - The problem and why it needs to be solved
  - Operating principles
  - The objective and relevant success criteria
- Then **socialize it widely!**

# Want a template to make this easy?



<https://github.com/swannysec/strategic-planning-template>

The screenshot shows a GitHub repository page for 'strategic-planning-template'. The repository has 70 lines of code (33 loc) and is 4.8 KB in size. The README.md file contains the following text:

*The purpose of this document is to define a high-level strategic proposal (along with any potential alternatives) to share with leadership for their approval and/or feedback and build better alignment among project teams. This document is also designed to provide a clear "north star" for subsequent tactical planning and execution. This document will help accountable leaders bring clarity to the problem they're trying to solve, the principles by which they will solve the problem, the success criteria, and a sense of the lift and critical dependencies associated with the work. Using this template helps build and maintain a sense of alignment among leaders, individual contributors, and leadership by making clear where you're going, why, and how.*

## Problem Statement

*What is the specific problem that needs to be solved? How does it impact your organization's effectiveness or values, customer outcomes, or revenue outcomes? What risk does it present? What happens if you fail to address it? This section tells the story of why you should undertake this work. Keep this section as plain and straightforward as you can so the problem is readily understood. Save the complexity for later.*

## Objectives

*What are the primary objectives for this program? Keep these short and sweet, without complexity. Use bullets, try to have no more than five total objectives, and where possible make sure the outcomes are measurable (binary objectives are ok where you simply need to establish something new!). Make sure the objectives consider all necessary business needs including customer and internal requirements, risk, sustainability, and scalability. If you intend to ship something that isn't safe or that you can't maintain, you probably need to reassess your objectives.*

## Operating Principles

*Are there already a set of existing operating principles that this program will operate under? If not, what should they be? These statements should reflect company values, business or customer requirements, and anti-goals if necessary. These help guide decision making in a consistent manner through the life of a program. Again, use simple, bulleted statements.*

A photograph of a two-story house that has been elevated on stilts and appears to be floating in the air. The house is white with a yellow roof and some missing windows. It is situated in a desert-like environment with dry grass and sand. The sky is blue with some white clouds.

# Is preparation just blocking iterative process?

**Strategy isn't optional.**  
Would you build your house  
without a foundation?

# Tactics



# On Tactics

- We built a **healthy, collaborative environment**
- We applied **no-BS pragmatism**
- **Data** drove our decisions
- We **focused on user experience (UX)**
- We invested in **communications**



# Psychological Safety =



Encourage the best work from everyone by **building** an environment which encourages **psychological safety** and open, trust-based collaboration.

# Collaboration is a Catalyst

- **Cast a wide net** to assemble the right contributors and build support for your efforts.
- **Look beyond security, engineering, and product.**



Created with Midjourney

# Who should be at the table?

- Engineering, Product, Security
- Support, Customer Success, Sales,  
Sales Engineering
- Internal Comms, PR, Marketing, Legal

# Pragmatism Beats Optimism

- **Make** hard, but **decisive choices** that lean toward ground truth over hope.
- Ensure objectives are **sustainable**.

**prag-ma-tism** noun

1. A practical approach to problems and affairs  
| tried to **strike a balance between principles and pragmatism**

"Pragmatism",  
Merriam-Webster.com Dictionary.

# Pragmatism in Practice

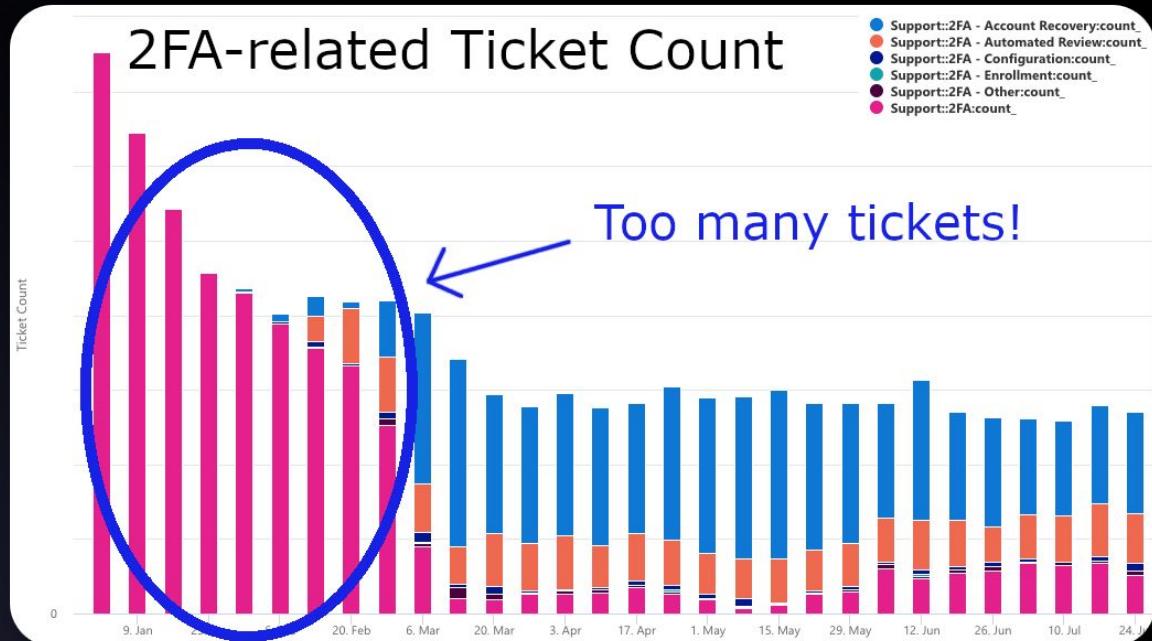
- We want **strong security outcomes**.
- We also **need to reach a diverse global audience** with different accessibility challenges.
- Decision: We chose **balanced objectives that don't exclude** developers.



"Rhodes Park School Pupils in the School Computer Lab," by IICD, licensed under CC BY 2.0.

# Let the Data Be Your Guide

- **Explore data** to figure out what the business can already tell you.
- **Measure** the effectiveness of what you build via **KPIs** and adjust as needed!



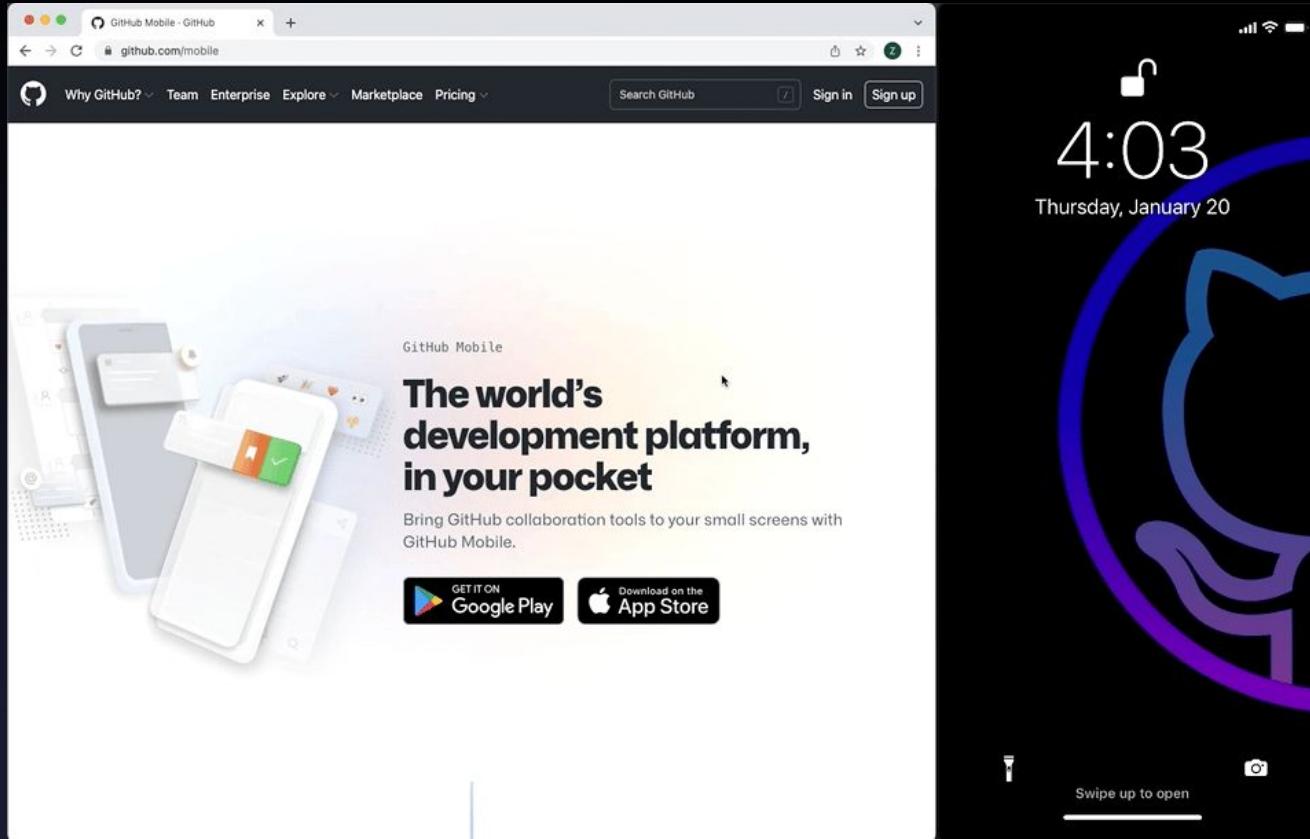


# User Experience is Everything

- If 2FA isn't **usable and durable**, can you really enroll millions of people and not make them miserable?
- Challenges:
  - Accessibility/availability of factors
  - Durability/resilience to loss
  - Ease of configuration/use

"LEGO 'Grumpy Cat' meme," Ochre Jelly, marked with Public Domain Mark 1.0.

# More Factor Options



# New 2FA Configuration Flow

Enable two-factor authentication (2FA)

1    2    3

**Setup authenticator app**

Use a phone app like [1Password](#), [Authy](#), [LastPass Authenticator](#), or [Microsoft Authenticator](#), etc. to get 2FA codes when prompted during sign-in.

[Re-scan the QR code](#)

Use an authenticator app from your phone to scan. If you are unable to scan, [enter this text code instead](#). [Learn more](#).



**Verify the code from the app**

[Cancel](#) [Continue](#)

**Alternative 2FA option:**

[SMS authentication](#) [Select](#)

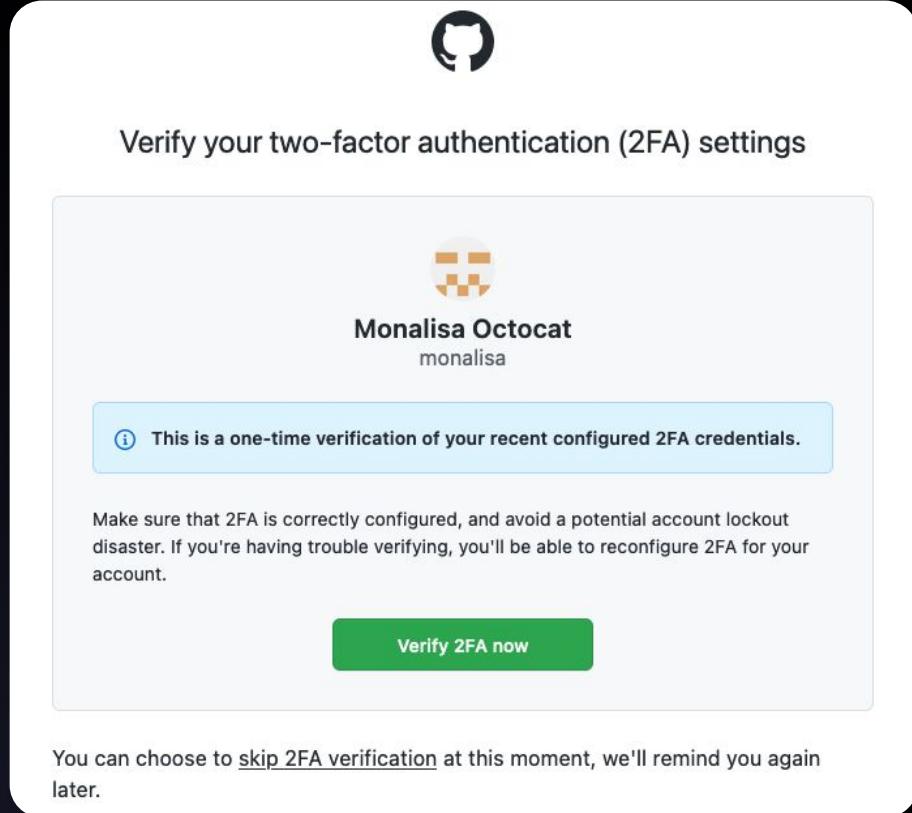
Get one-time codes sent to your phone via SMS to complete authentication requests.

**23%**  
reduction in SMS  
2FA registration 

# Scheduled 2FA Verification

25%

of users safely  
re-configure 2FA  
without lockout 😊



The image shows a screenshot of a GitHub two-factor authentication (2FA) verification interface. At the top, there is a GitHub logo. Below it, the text "Verify your two-factor authentication (2FA) settings". In the center, there is a profile picture of a cat named "Monalisa Octocat" with the handle "monalisa". A blue callout box contains the text: "ⓘ This is a one-time verification of your recent configured 2FA credentials." Below this, there is a message: "Make sure that 2FA is correctly configured, and avoid a potential account lockout disaster. If you're having trouble verifying, you'll be able to reconfigure 2FA for your account." At the bottom, there is a green button labeled "Verify 2FA now". At the very bottom of the interface, there is a note: "You can choose to skip 2FA verification at this moment, we'll remind you again later."

Verify your two-factor authentication (2FA) settings

Monalisa Octocat  
monalisa

ⓘ This is a one-time verification of your recent configured 2FA credentials.

Make sure that 2FA is correctly configured, and avoid a potential account lockout disaster. If you're having trouble verifying, you'll be able to reconfigure 2FA for your account.

Verify 2FA now

You can choose to skip 2FA verification at this moment, we'll remind you again later.

# Preferred Factors

## Two-factor authentication

Enabled

Two-factor authentication adds an additional layer of security to your account by requiring more than just a password to sign in. [Learn more about two-factor authentication.](#)

### Two-factor methods



Authenticator app

Enabled

Preferred

...

Use an application on your phone to get two-factor authentication codes when prompted.



SMS/Text message

Enabled

...

You will receive authentication code to this phone number: +1 206550123



Security keys

Enabled

1 key

...

Security keys are hardware devices that can be used as your second factor of authentication.



GitHub Mobile

Enabled

2 devices

...

Github Mobile can be used for two-factor authentication by installing the Github Mobile app and signing in to your account.

# Slow and Steady Wins the Race



## 45 days before

Regular in-product reminders,  
occasional email reminders



## On 2FA deadline

Prompt to enable 2FA once a  
day when accessing GitHub



## After 7 days

Blocked from accessing GitHub  
features until you enable 2FA



## 2FA check-up after 28 days

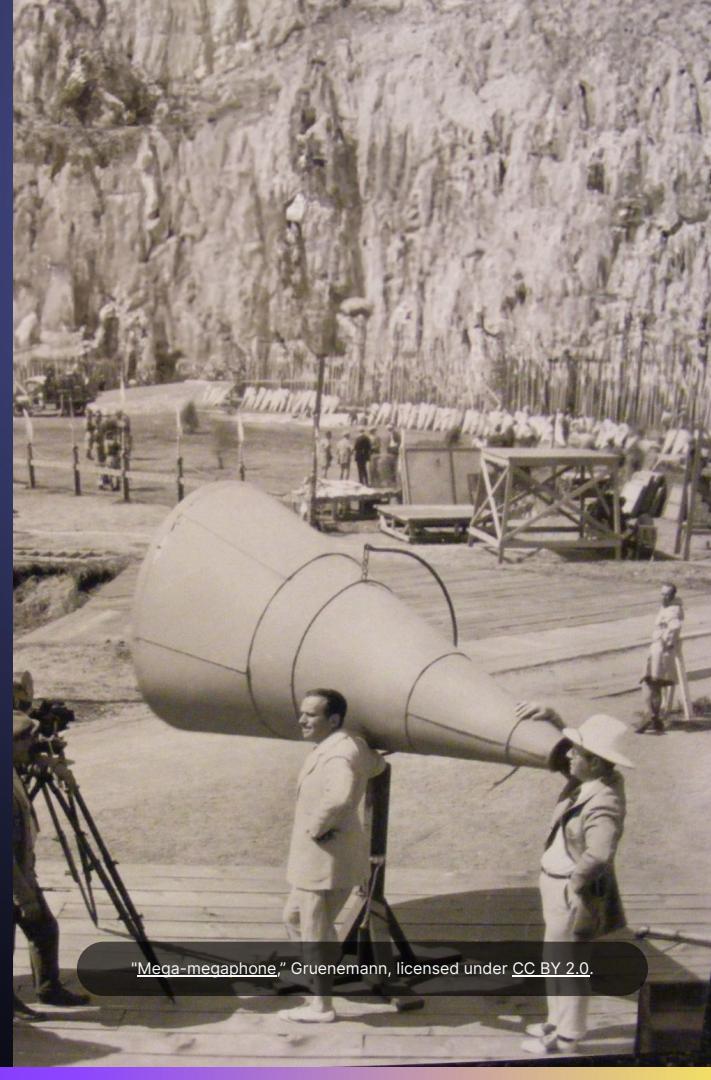
Validate that your 2FA setup is working correctly

Speed kills.

It's tempting to be  
bold and ship fast.  
It's also a good way  
to end your 2FA  
project before it  
gets off the ground!

# Customer-facing Roles are Amplifiers

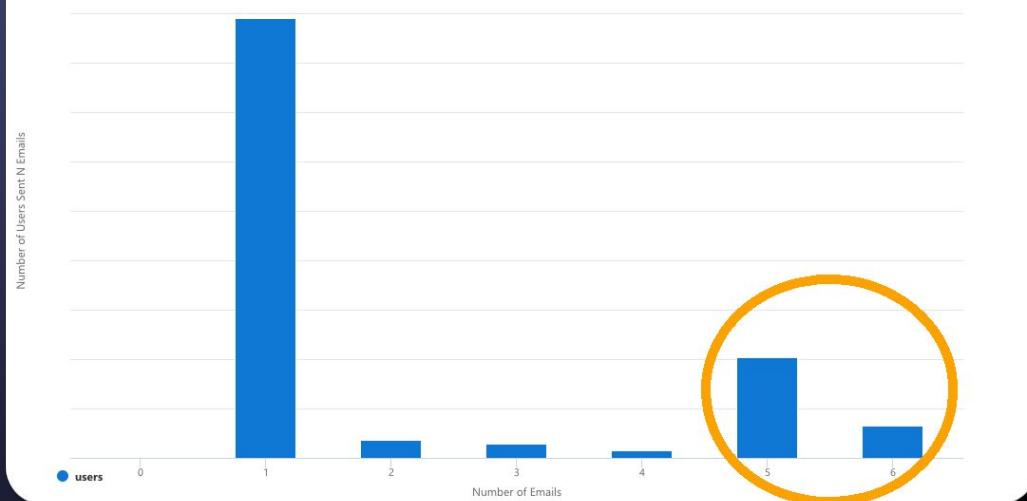
- Support, Customer Success, and Sales preparation isn't a "nice to have." It's **essential**.
- Consider:
  - Business process
  - Policy
  - Awareness



"Mega-megaphone," Gruenemann, licensed under CC BY 2.0.

# Communicate Early and Often

# of Notification Emails Sent Before Enrollment



- Engage your PR, marketing, and internal communications teams.
- Be **clear, consistent, and transparent** in your comms. Explain why.
- Include a **straightforward call to action**.
- **Use multiple forms** of communication!

# Results and Next Steps

# Initial Feedback = ❤️

 **Paul Razvan Berg @ EthCC**   
@PaulRBerg

Major props to [@github](#) for making 2FA mandatory for all code contributors.

This is an important step towards enhancing the security of the Internet.

[GitHub 2FA] Your GitHub account, PaulRBerg, will require 2FA

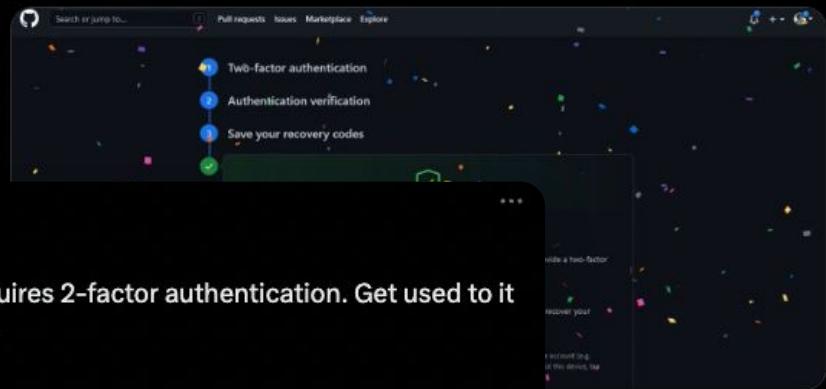
GitHub  
Hey PaulRBerg!  
We're reaching out to let you know that as [announced last year](#), we will officially require two-factor authentication (2FA) for certain contributors on [GitHub.com](#). You are required to enable 2FA by May 4th, 2023 at 00:00 (UTC). If you disable 2FA, your access to GitHub.com will be restricted until you re-enable 2FA. This email, along with notifications in the [GitHub.com](#) UI, will be the only notifications about this change.  
  
You don't need to do anything in response to this email, but please do not disable 2FA before May 4th, 2023 at 00:00 (UTC). If you disable 2FA, your access to GitHub.com will be restricted until you re-enable 2FA. This email, along with notifications in the [GitHub.com](#) UI, will be the only notifications about this change.  
  
Making the software supply chain more secure is a team effort, and we could not have done it without you! Enrolling in 2FA is an impactful step in keeping the world's software secure.  
  
**What to know about the required 2FA initiative**  
  
We are enrolling GitHub users who manage or contribute to code that others depend on. You are one of the first users to receive this notification.

 **Andres Pineda**  
@ajpinedam

Folks at [@github](#) care so much about your security that they get very happy when we turn on 2FA on our accounts.

If you haven't done it yet, go and bring them some happiness 

#Security #MFA



 **Stephen Shankland**  
@stshank

Microsoft's [@github](#) now requires 2-factor authentication. Get used to it — it's the wave of the future.

With all the open-source projects at GitHub 2FA makes it harder for bad actors get access and insert malware that'd distributed to other projects.

[github.blog/2022-05-04-sof...](https://github.blog/2022-05-04-sof...)

11:39 AM · May 4, 2022

# 2FA Adoption vs. Ticket Volume

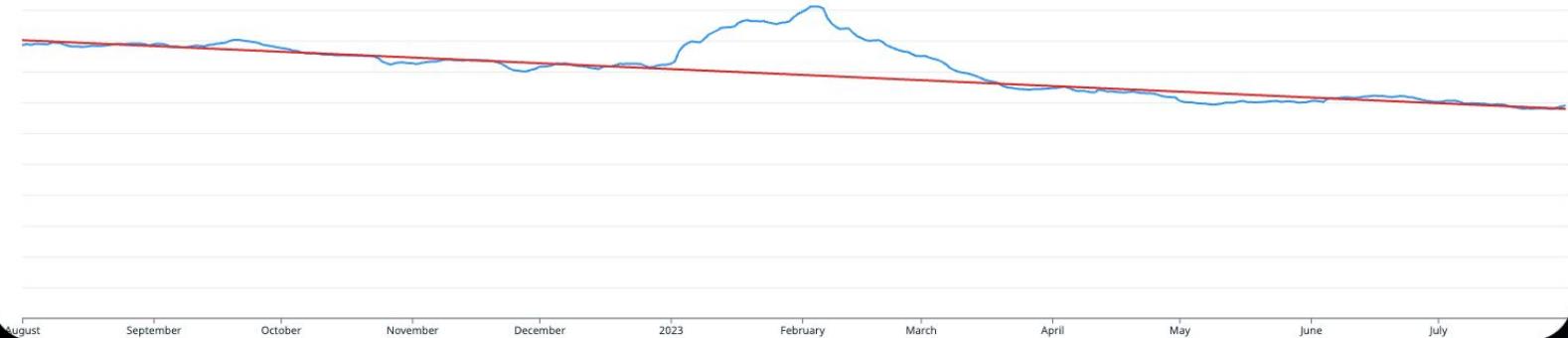


42%

reduction in 2FA-related  
support tickets per 100k  
users

# Account Lockouts

## Daily Account Recovery Attempts

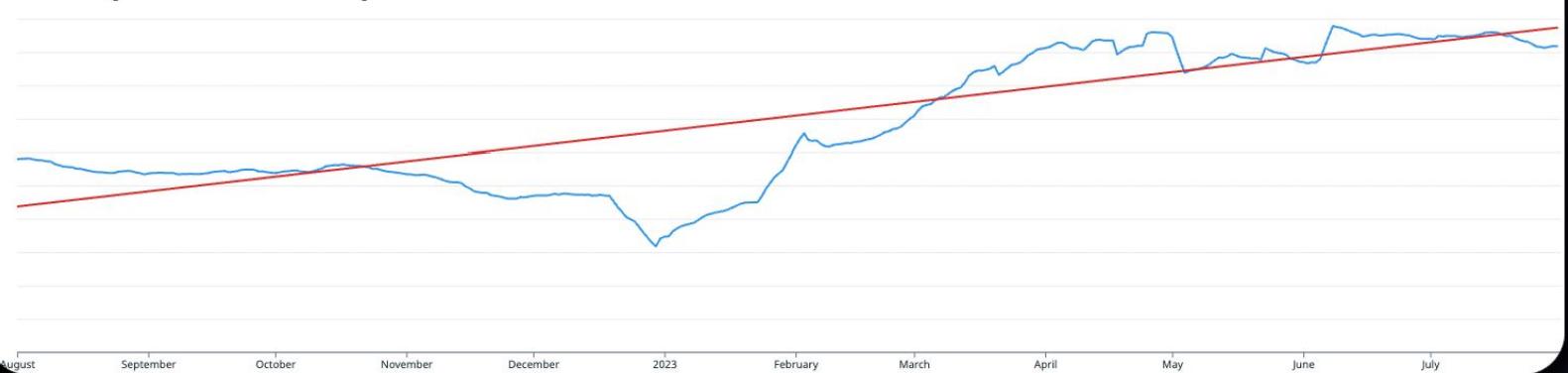


33%

reduction in account lockout  
recovery attempts per 100k  
users

# Recovery Code Interaction

## Daily Recovery Code Retrievals



38%

increase in recovery code  
downloads or prints per 100k  
users 🎉

# Positive Ecosystem Impact

15 Aug 2022

## Requiring MFA on popular gem maintainers

by Jenny Shen



Two months ago, we outlined our [commitment](#) to making Ruby's supply chain more secure. To combat account takeovers — the second most common software supply chain attack — we announced a policy to require multi-factor authentication (MFA) on at least the top-100 RubyGems packages.

["Requiring MFA on popular gem maintainers."](#) Jenny Shen.

## Securing PyPI accounts via Two-Factor Authentication

by: Donald Stufft · 2023-05-25

#security #2fa

One of the key security promises that PyPI makes is that when you're downloading something, that only the people associated with that project are going to be able to upload, delete, or otherwise modify a project. That when you look at that project and see that it is owned by someone that you trust, that you can be assured that nobody else is making changes to that package on PyPI.

This promise is predicated on the security of each and every individual account on PyPI used to create and maintain a Python project. In the past we've taken steps to safeguard these accounts by [blocking compromised passwords](#), strong 2FA support using [TOTP](#) and [WebAuthN](#), [support for API tokens with offline attenuation](#), [enrolling the most downloaded projects into mandatory 2FA](#), and [enabling short lived tokens for upload](#).

Today, as part of that long term effort to secure the Python ecosystem, we are announcing that every account that maintains any project or organization on PyPI will be required to enable 2FA on their account by the end of 2023.

["Securing PyPI accounts via Two-Factor Authentication."](#) Donald Stufft.

# What's Next?

- Lots of users left to enroll!
- Passkey support
- 2024+

Security

## Introducing passwordless authentication on GitHub.com

Passkeys are now available in public beta. Opting in lets you upgrade security keys to passkeys, and use those in place of both your password and your 2FA method.

# Key Lessons

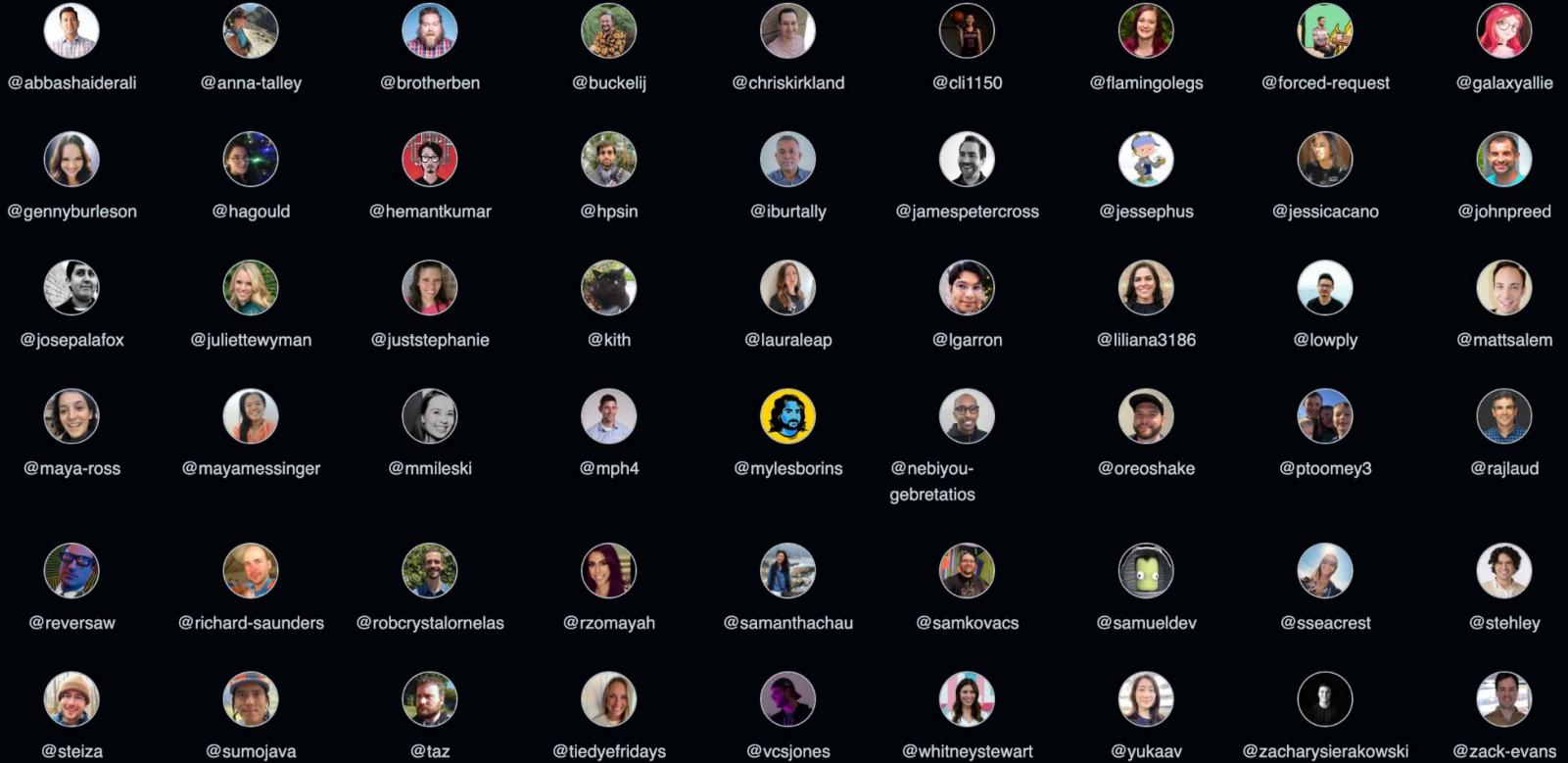
# Lessons for 2FA

- Trust by design: optimize user experience and internal preparation before raising requirements!
- Think hard about whether 2FA is feasible for everyone. Consider alternatives or adjust your objectives to add flexibility.
- Invest effort in solid communication (internal and external). Lean into comms specialists.
- Moderate the pace of enrollment to allow improvements!

# Lessons Useful Beyond 2FA

- Prepare thoroughly and write these down, then share broadly:
  - Problem statement and relevant **data from research**
  - Operating **principles**
  - Clear and **sustainable objectives**
- Leadership and culture matter.
  - Maintain a **psychologically safe**, positive team environment
  - **Collaborate** with teams **across the whole organization**

# Acknowledgments



# Questions?

Need more info on GitHub's 2FA efforts?

<https://github.blog/tag/2fa/>



## Want to follow-up?

swannysec@github.com

or

swanson.john.d@gmail.com

<https://swannysec.net>

<https://twitter.com/swannysec>

<https://infosec.exchange/@swannysec>



Planning Template

