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

John Swanson

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

black hat USA 2023


Story
Time
Created with Midjourney

Who am I?

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

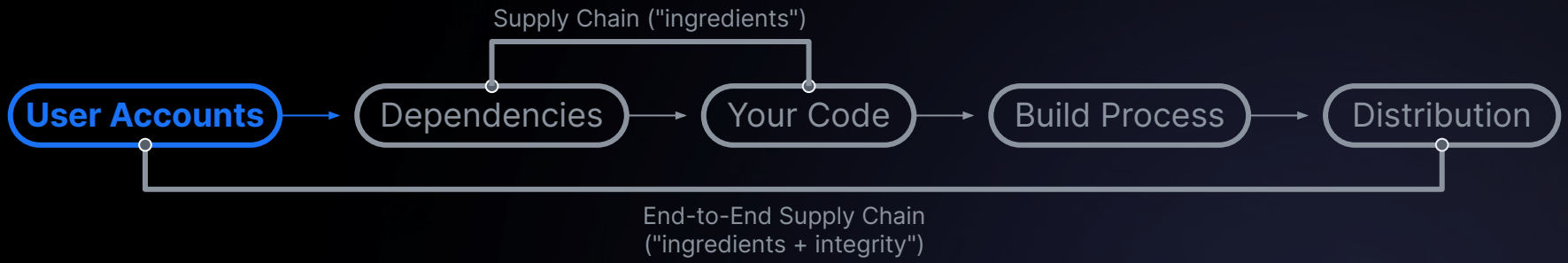
Agenda

- 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.**

Research Head Start

Open Source Security

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

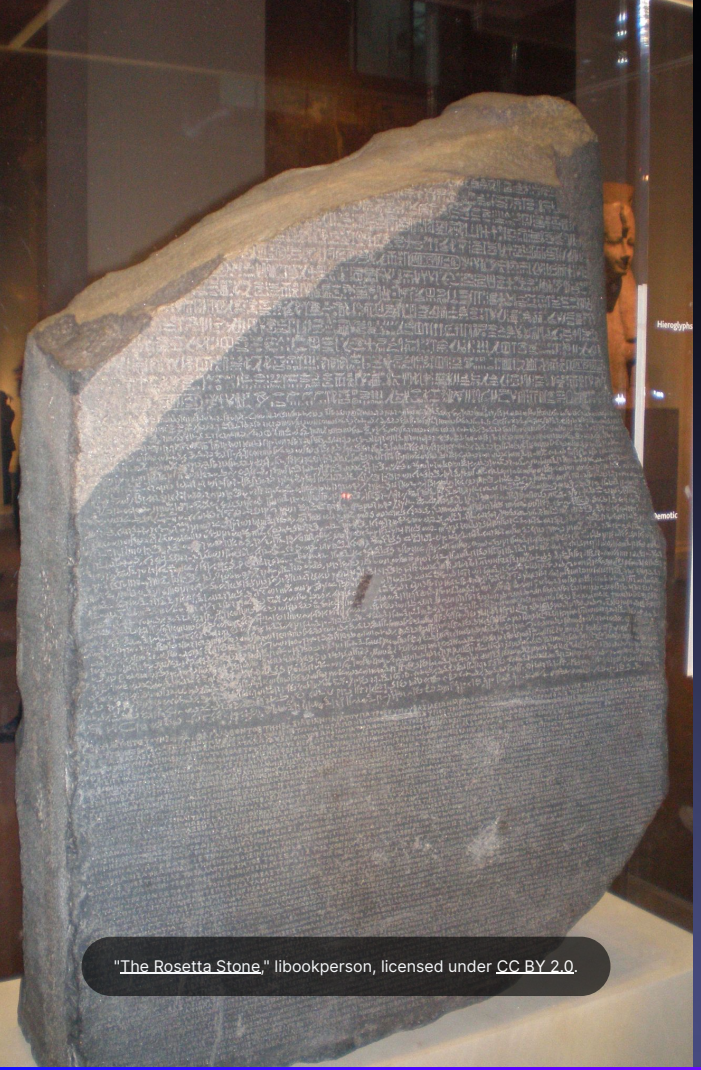
Today we're introducing enhanced login verification to the npm registry, and we will begin a staged rollout to maintainers beginning Dec 7.

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.

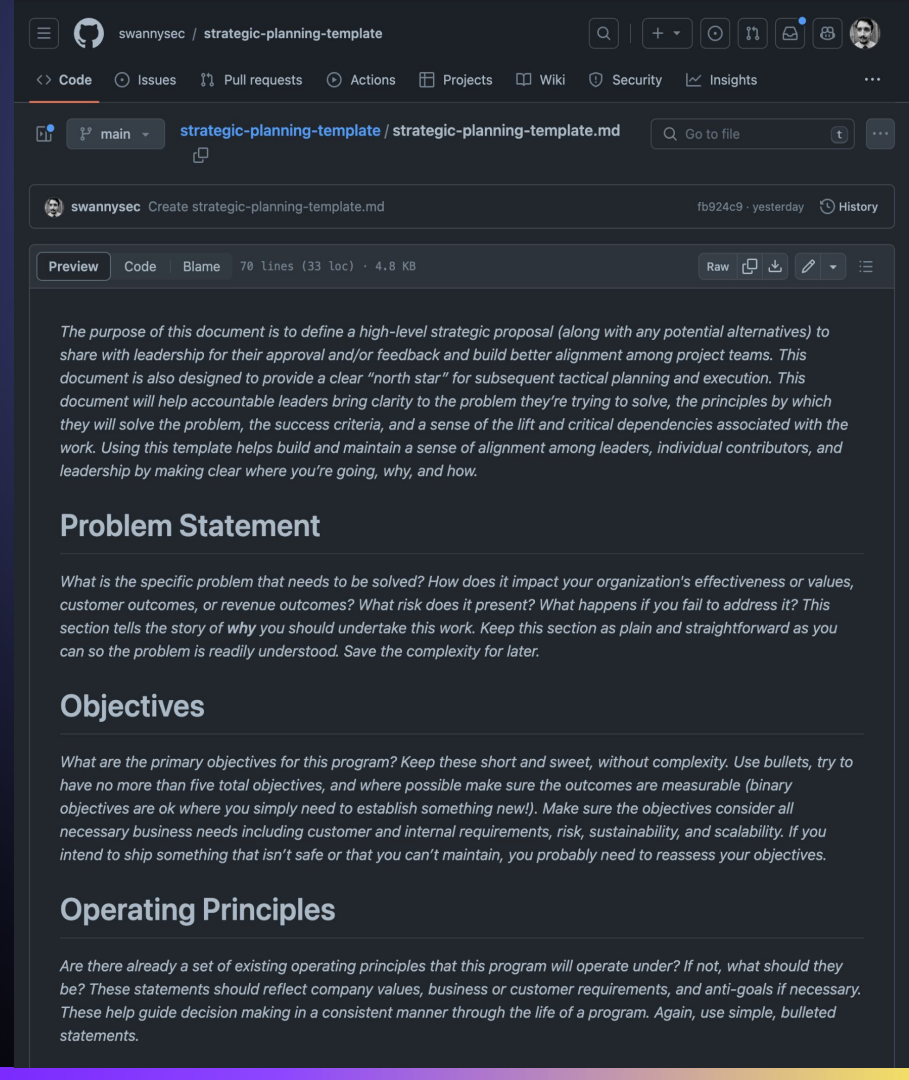


Write it Down

- **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



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.

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**

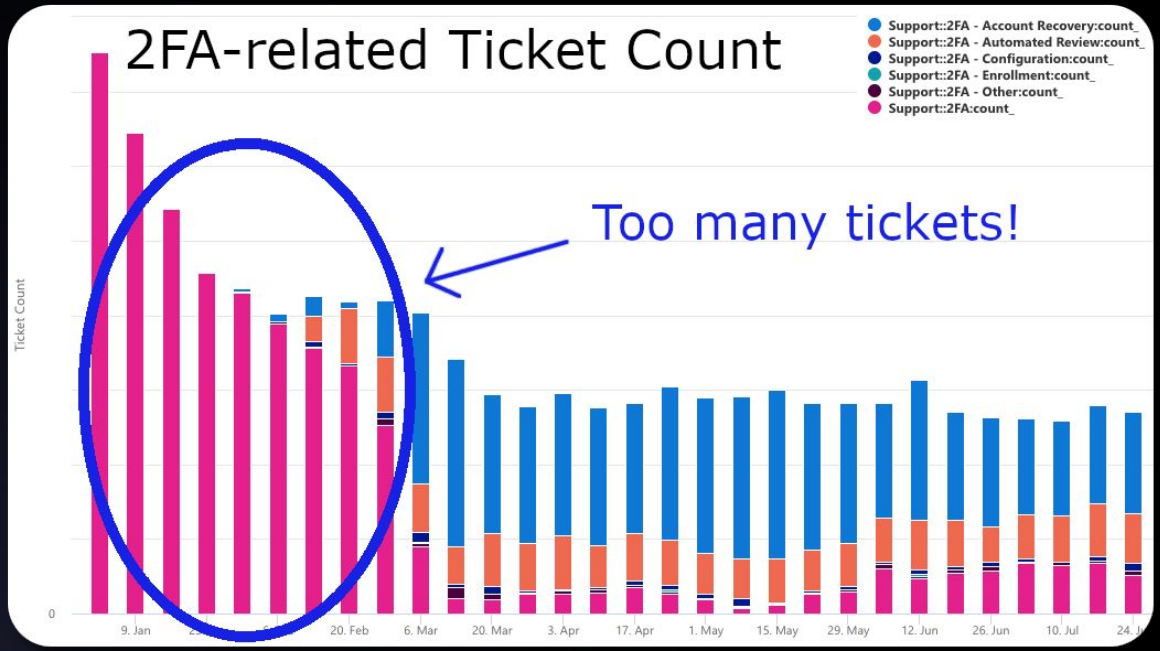
"Pragmatism",
Merriam-Webster.com Dictionary.

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.

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!

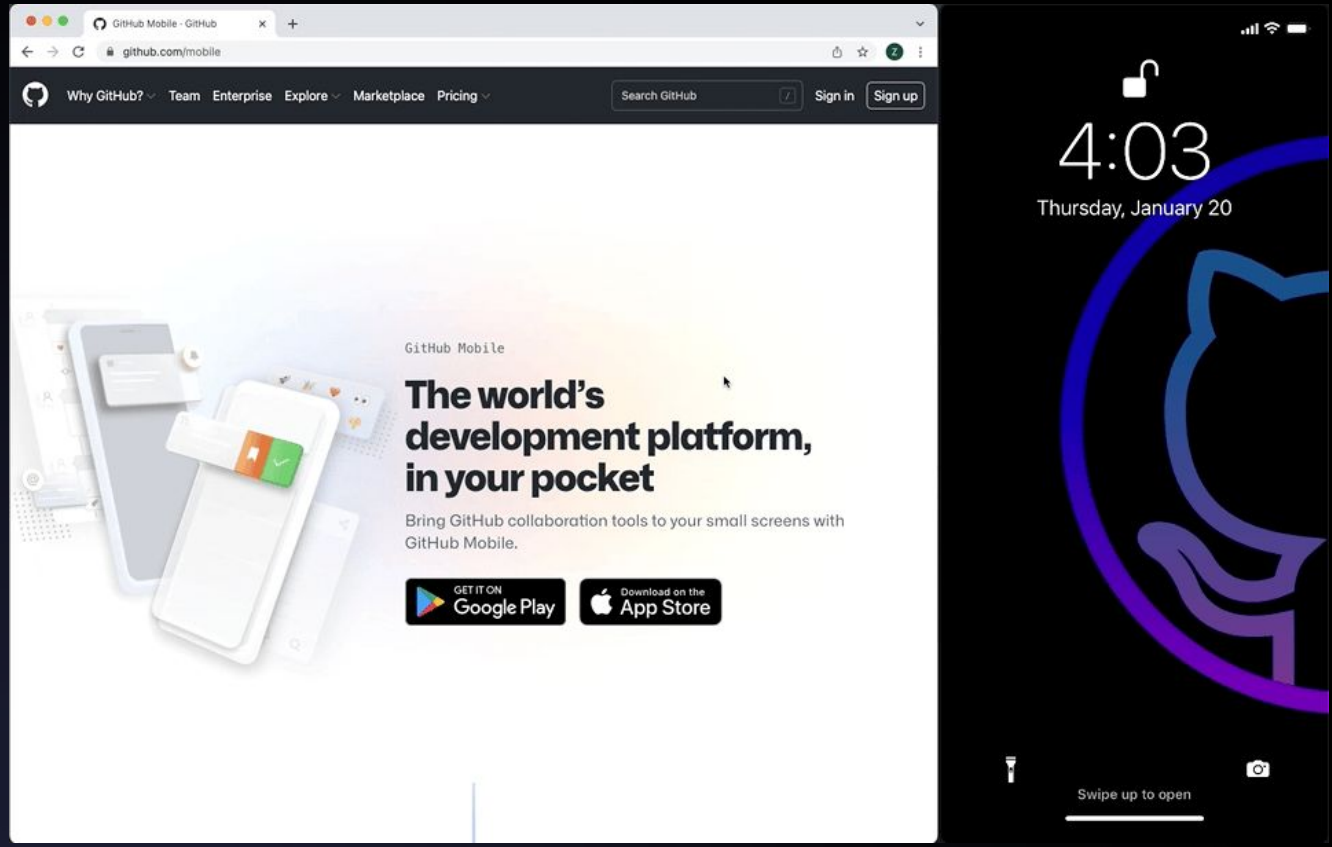


"LEGO 'Grumpy Cat' meme," Ochre Jelly, marked with Public Domain Mark 1.0.

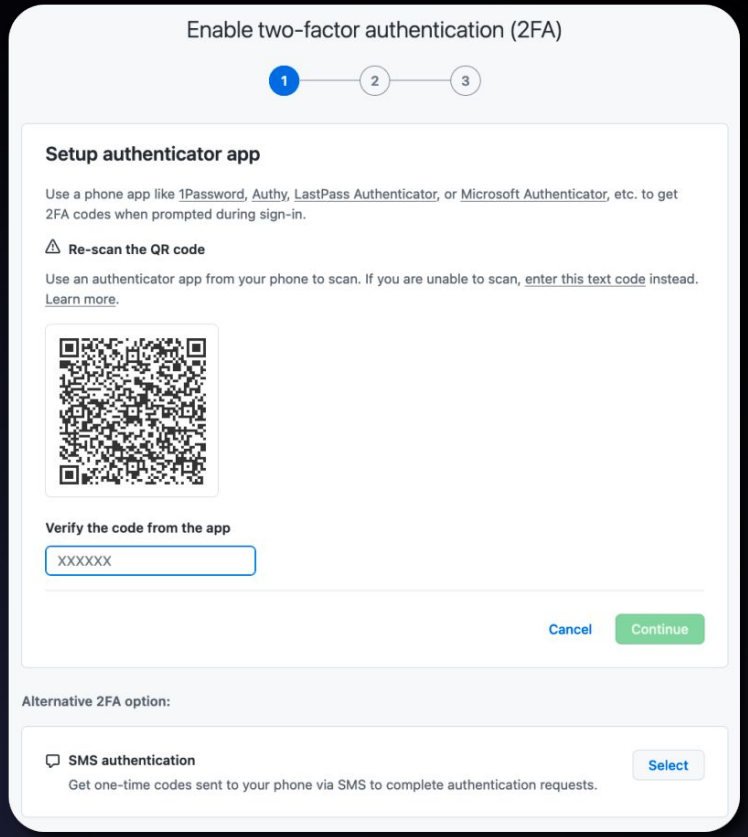
User Experience is Everything

- 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

More Factor Options



New 2FA Configuration Flow



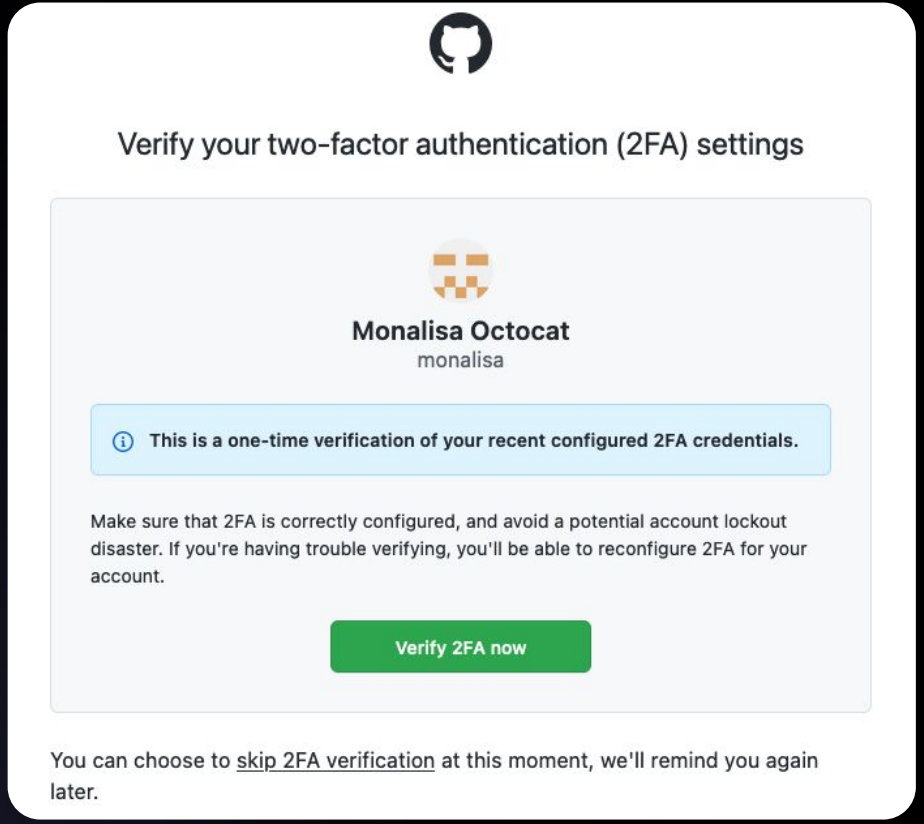
23%

reduction in SMS 2FA registration 🎉

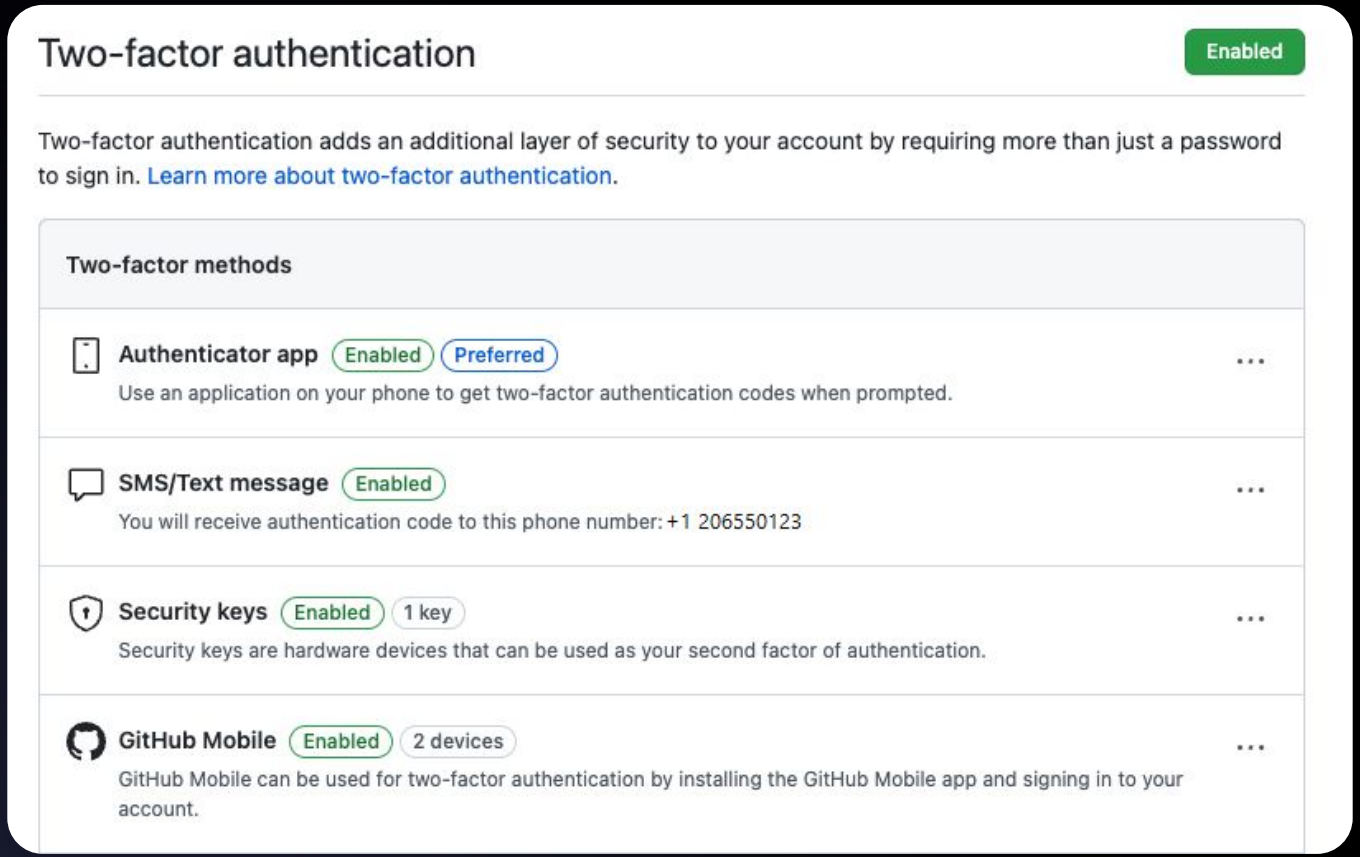
Scheduled 2FA Verification

25%

of users **safely re-configure 2FA without lockout** 😌



Preferred Factors



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

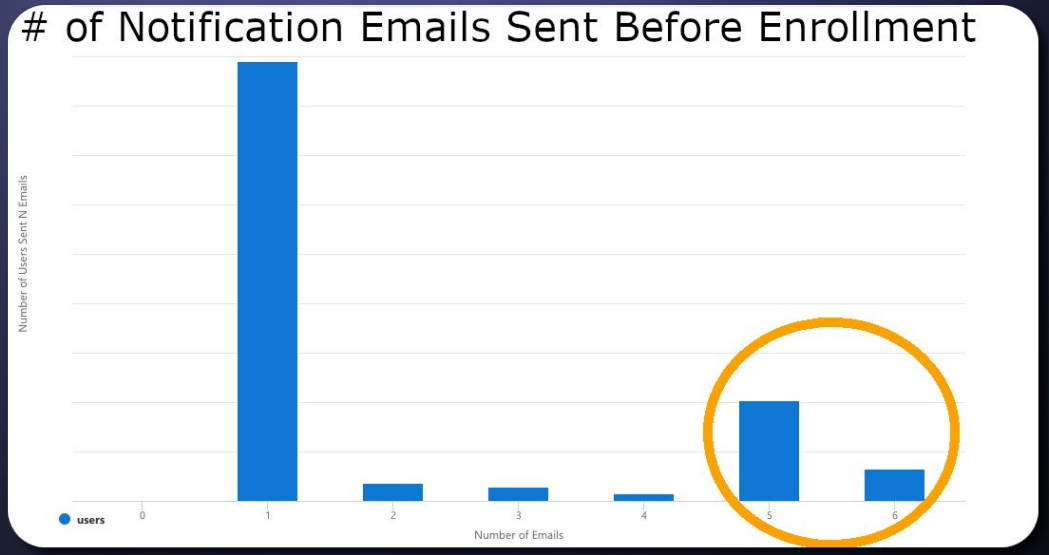
Speed kills.
It's tempting to be bold and ship fast. It's also a good way to end your 2FA project before it gets off the ground!

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



- 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

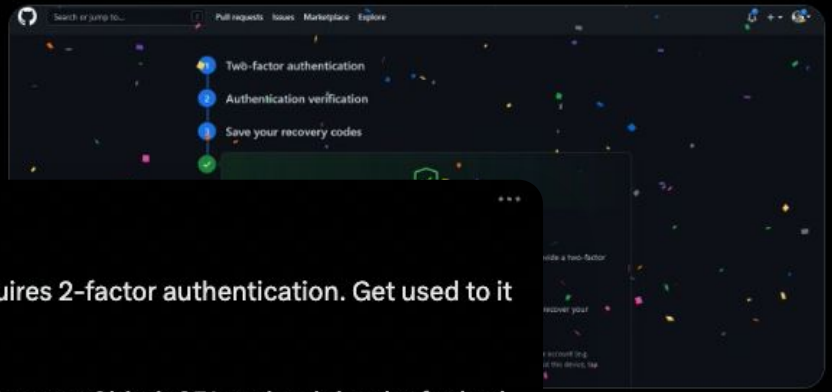
Initial Feedback = 💖

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



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 offic... factor authentication (2FA) for certain contributors on GitHub.com. You are ... because your account meets the criteria for the current enrollment group - t... already!

You don't need to do anything in response to this email, **but please do not di...** and May 4th, 2023 at 00:00 (UTC). If you disable 2FA, your access to GitHub.c... day enrollment period will be restricted until you re-enable 2FA. This email, a... 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 coul... enrollment 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

Stephen Shankland
@stshank

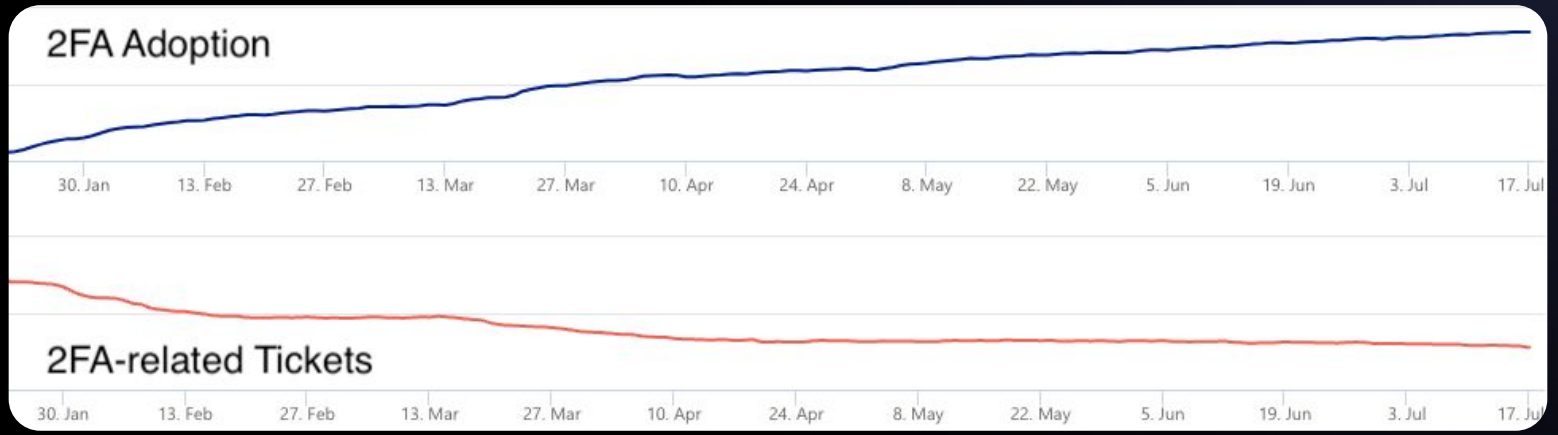
Microsoft's @github now requires 2-factor authentication. Get used to it — it's the wave of the future.

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...

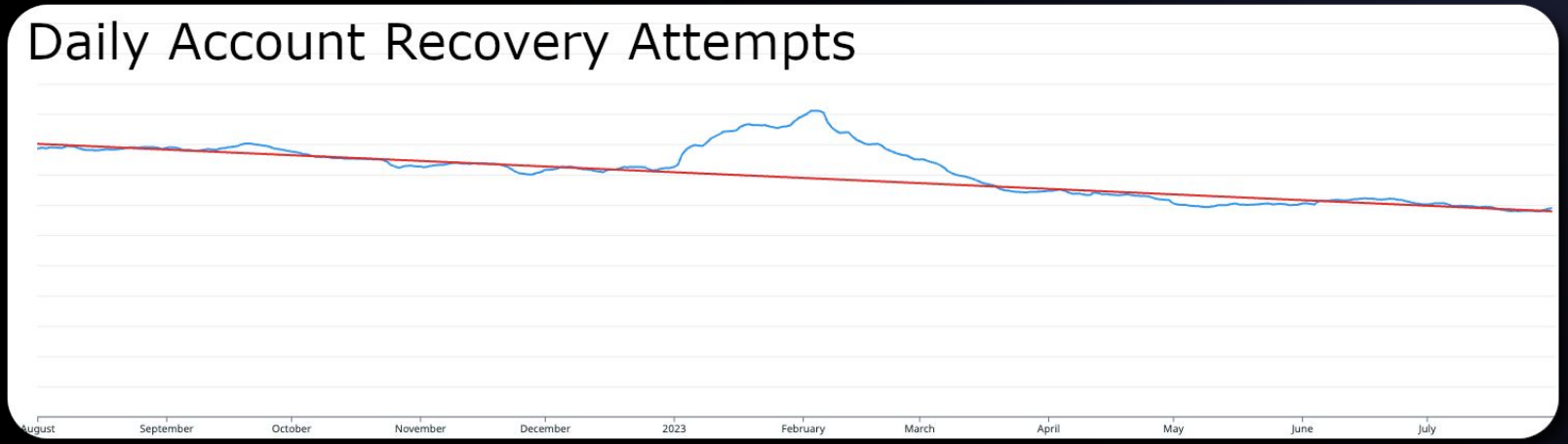
11:39 AM · May 4, 2022

2FA Adoption vs. Ticket Volume



42% **reduction** in 2FA-related support tickets per 100k users 🎉

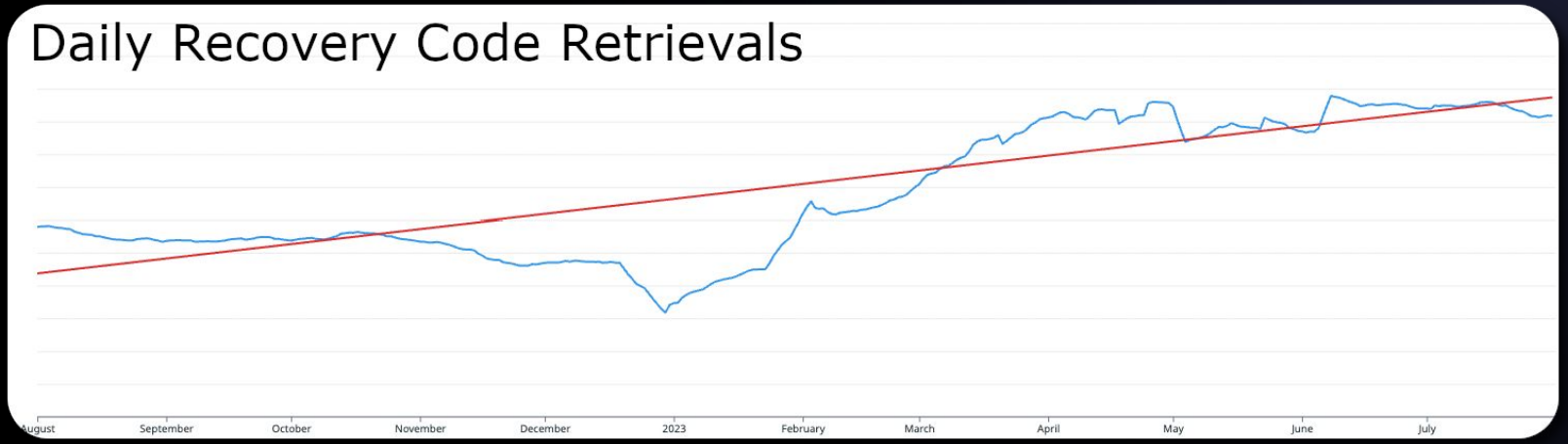
Account Lockouts



33%

reduction in account lockout recovery attempts per 100k users 🎉

Recovery Code Interaction



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.

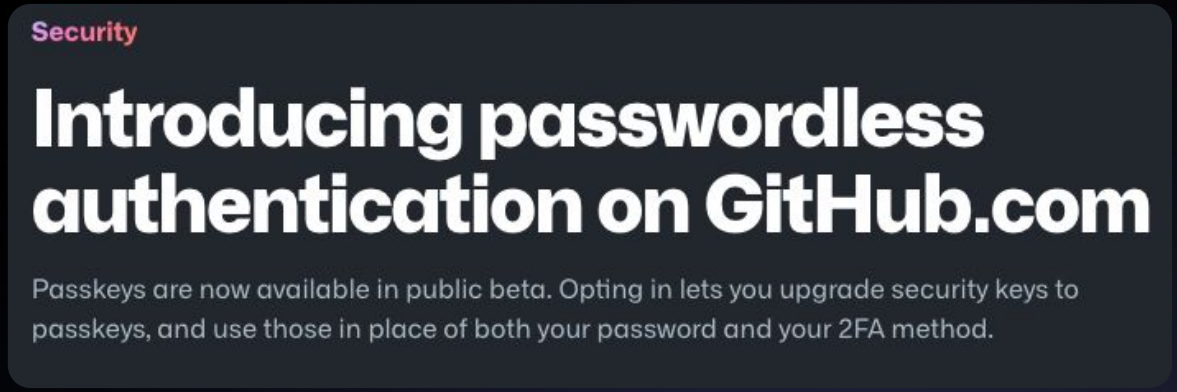
This promise is predicated on the security of each and every individual account on PyPI used to create and maintain a Python project. In the past we've taken steps to safeguard these accounts by blocking compromised passwords, strong 2FA support using TOTP and WebAuthN, support for API tokens with offline 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+



Key Lessons

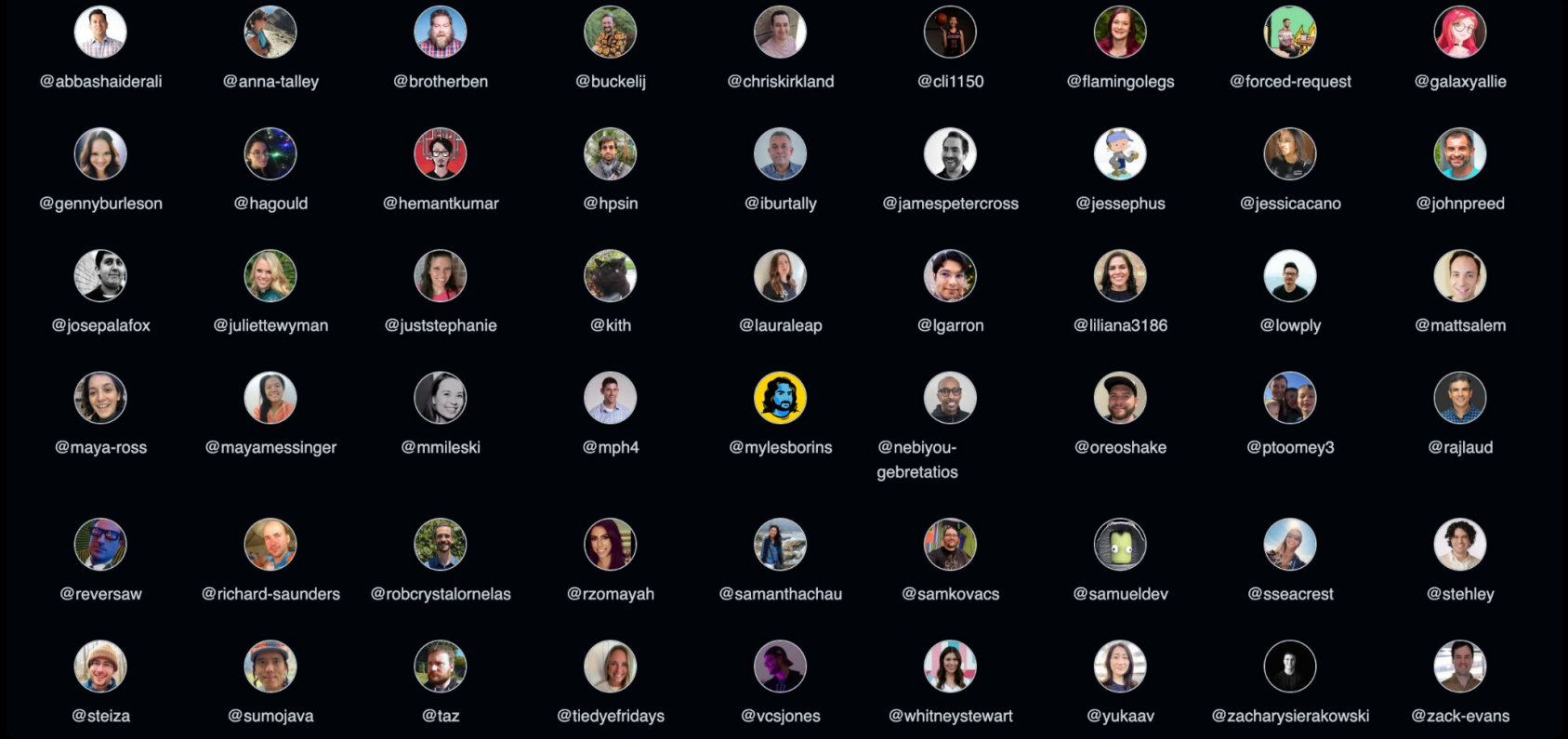
Lessons for 2FA

- **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/

black hat USA 2023

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