

Didn't You Hear Me?

Towards More Successful Web Vulnerability Notifications

Ben Stock, Giancarlo Pellegrino, Frank Li, Michael Backes, and Christian Rossow

Berkeley
UNIVERSITY OF CALIFORNIA

Stanford
University

C | **I S P A**
Center for IT-Security, Privacy
and Accountability

Motivation and Research Questions

- Prior works in this area had limited impact
 - Low fix rates
 - Main issue: few administrators reached
- Our work: understand why notifications did not perform better and determine improvements
 - Message format/tone
 - High-effort channels

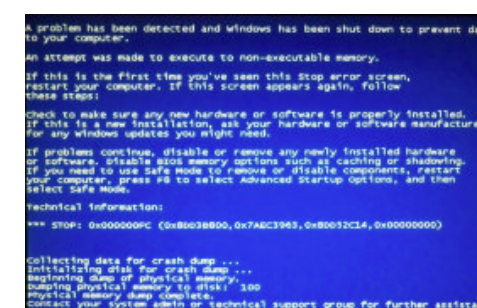




Study Setup

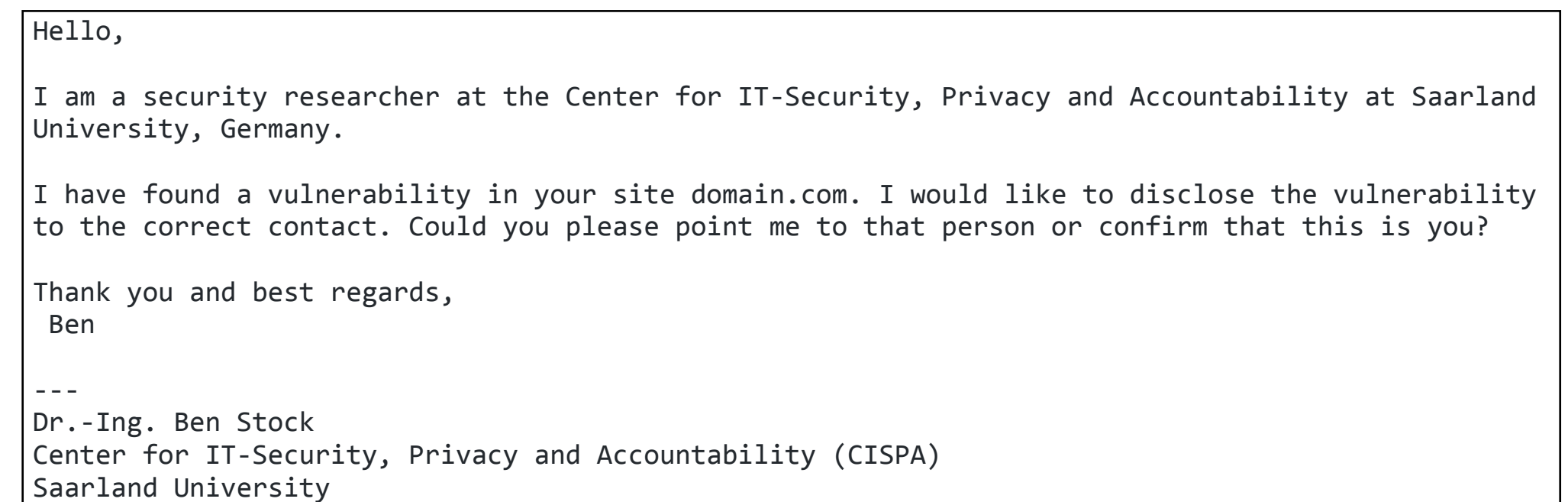
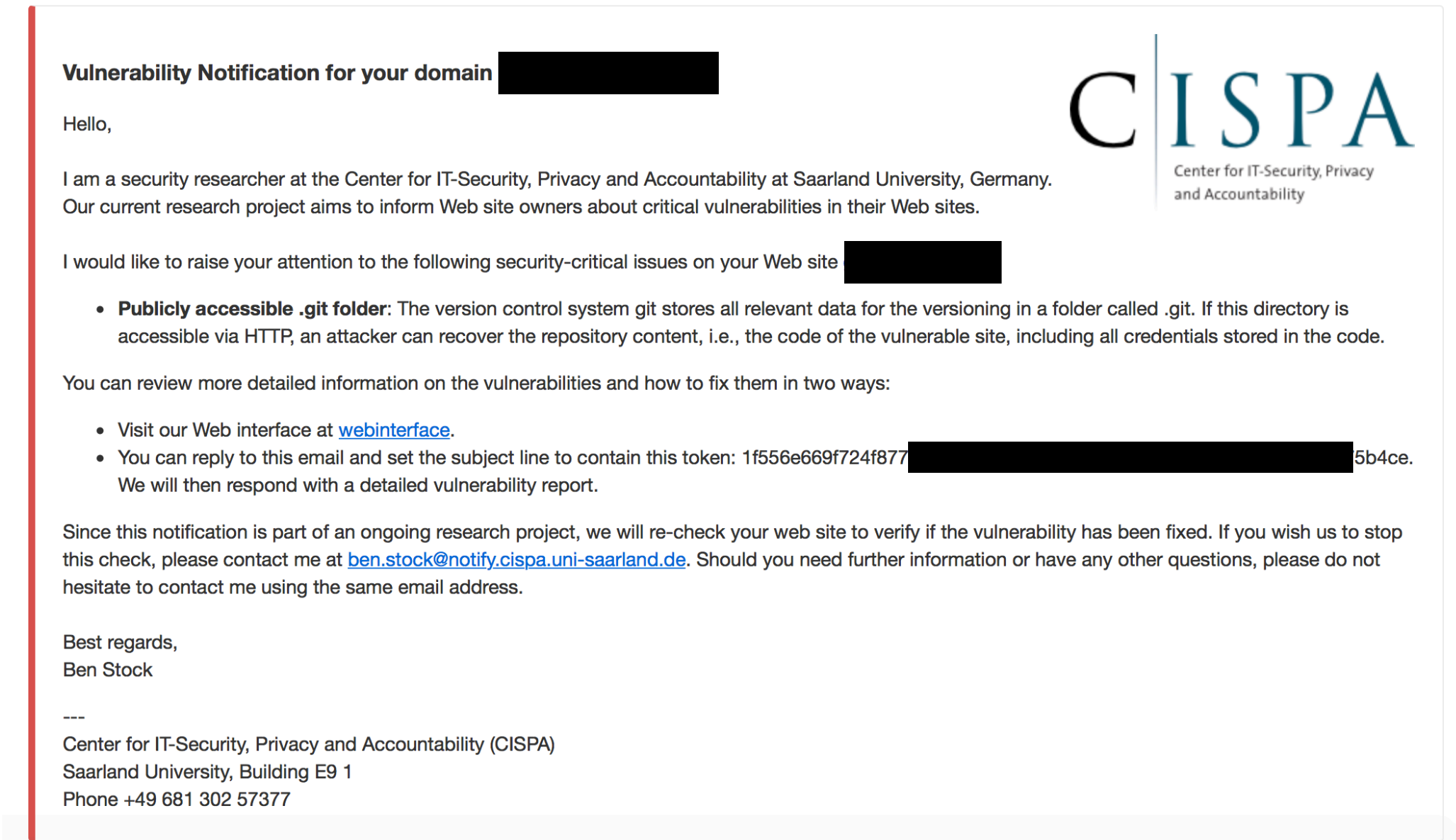
Types of Disclosed Issues

- Well-known vulnerabilities for WordPress (14,815 domains, Top 1M)
 - Two Cross-Site Scripting Flaws (CVE-2016-4566, CVE-2016-4567)
 - determined by hash values of vulnerable Flash files
- Misconfigured Git repositories (9,721 domains, Top 1M)
 - Checked presence and format of .git/config
 - Removed known public repositories (based on hash of last commit)
- Publicly accessible core dumps (790 domains, Top 1M)
 - excluded later in the experiment
 - one hoster responsible for 30% of affected sites



Different Types of Notifications

- Plain text emails
 - Real name sender (**Plain**),
"Vulnerability Notification" sender (**Mailbot**),
Signed emails (**S/MIME**)
- HTML emails
 - HTML with all information included (**HTML**),
HTML with externally linked logo (**Tracking**)
- Friendly tone
 - Merely information that some flaws was detected
 - asked for right contact to provide more info



Notification Procedure

- Used only directly available channels
 - security/abuse/webmaster/info@domain.com, WHOIS abuse contact
- Split up data set of vulnerable domains into seven groups
 - different messages and control group
- Bi-weekly emails
 - February 3rd, February 17th, March 3rd

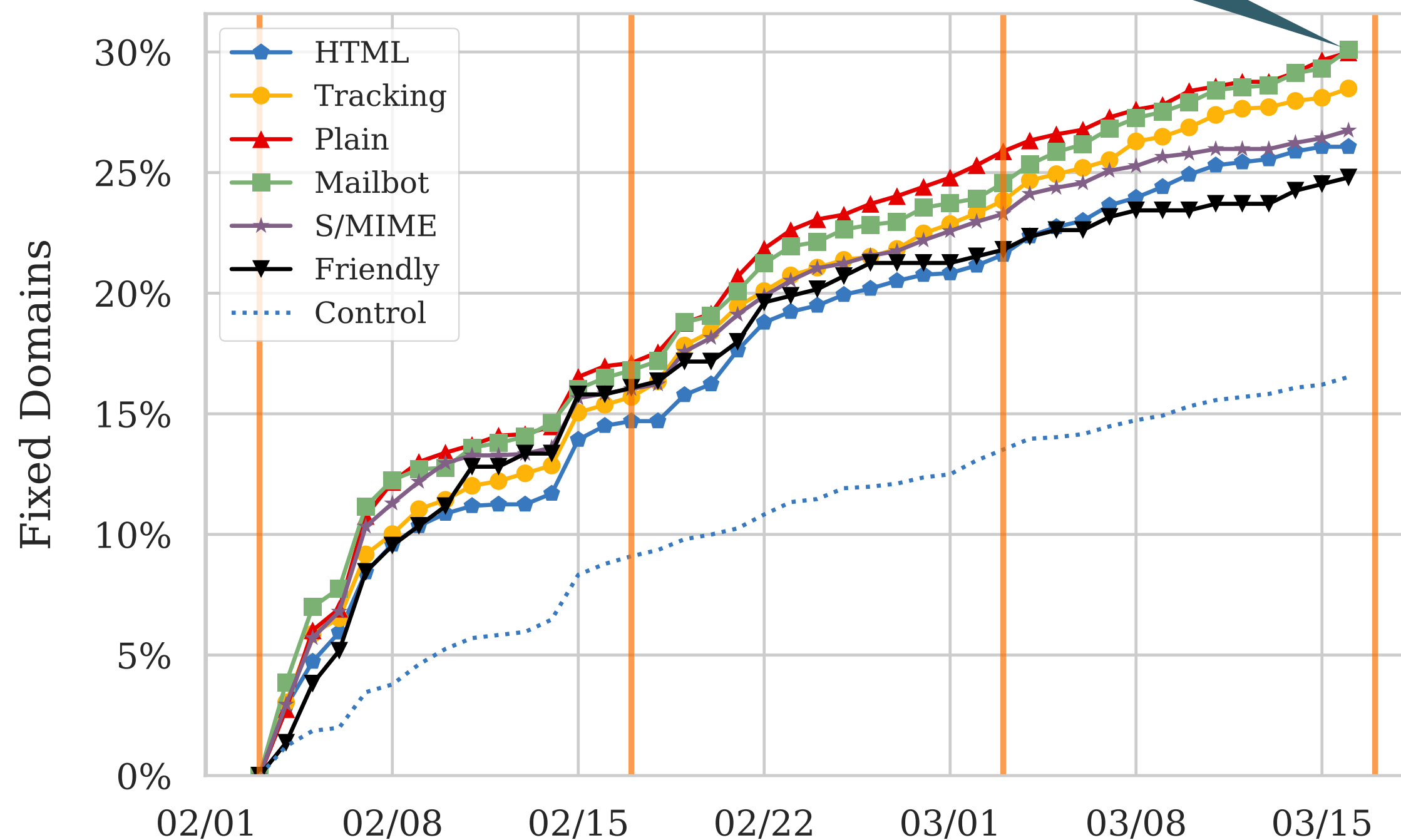




Results of our Notification

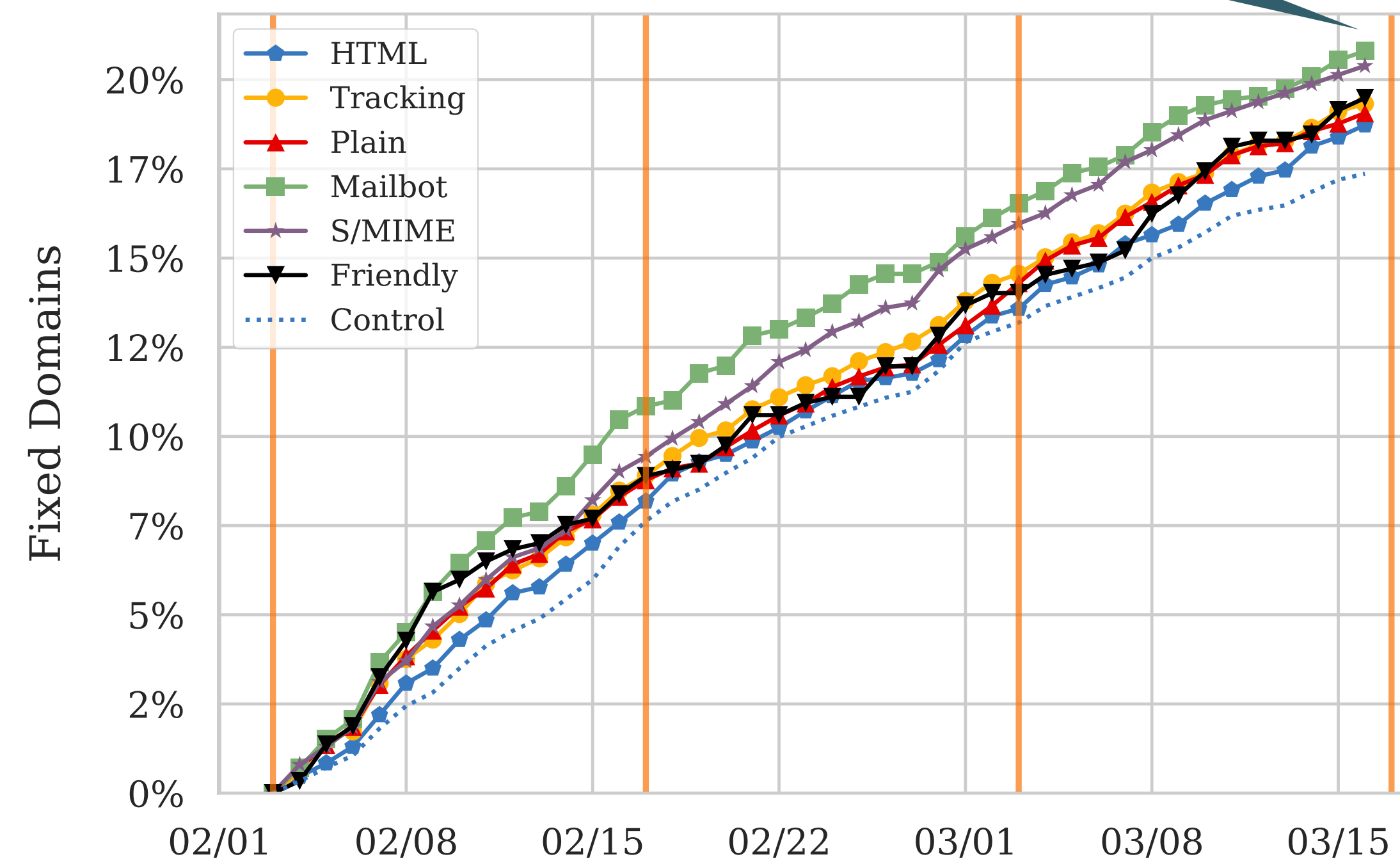
Remediation Overview

Significant improvement
for all groups



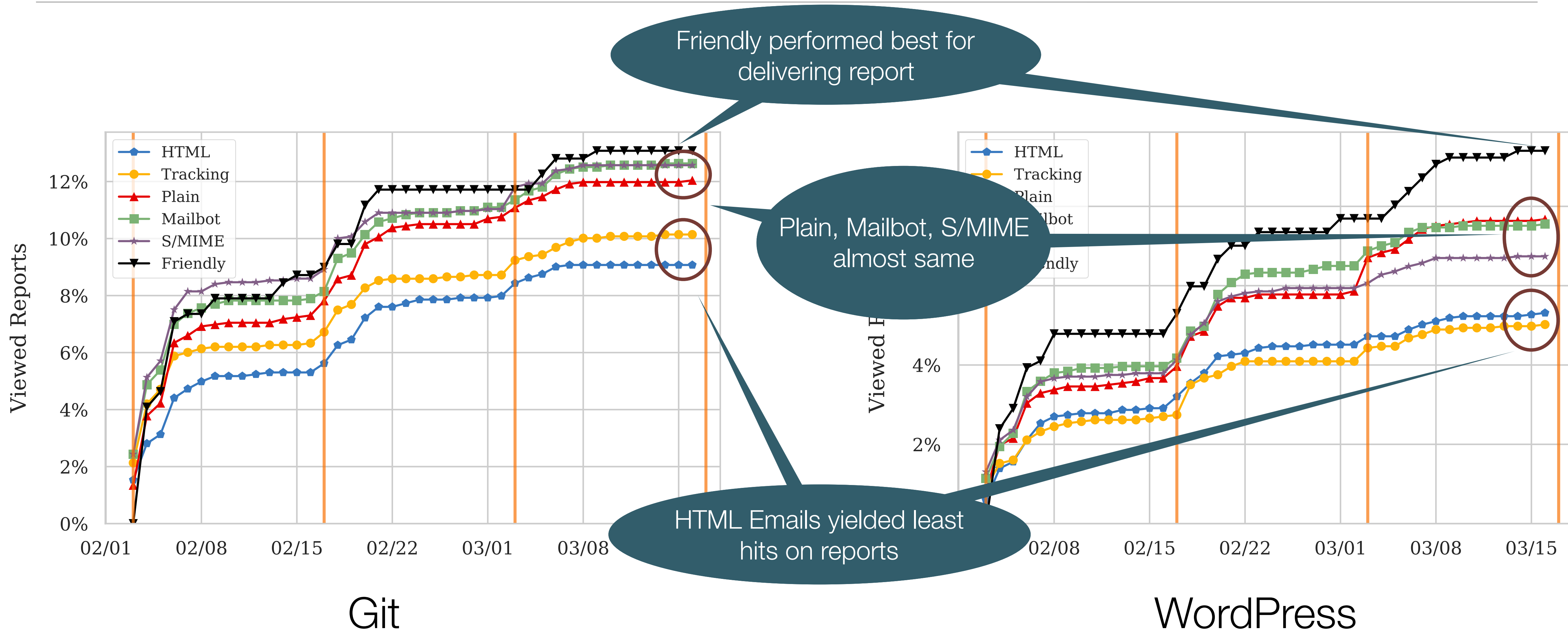
Git

Significant improvement
only for Mailbot



WordPress

Access Reports over Time

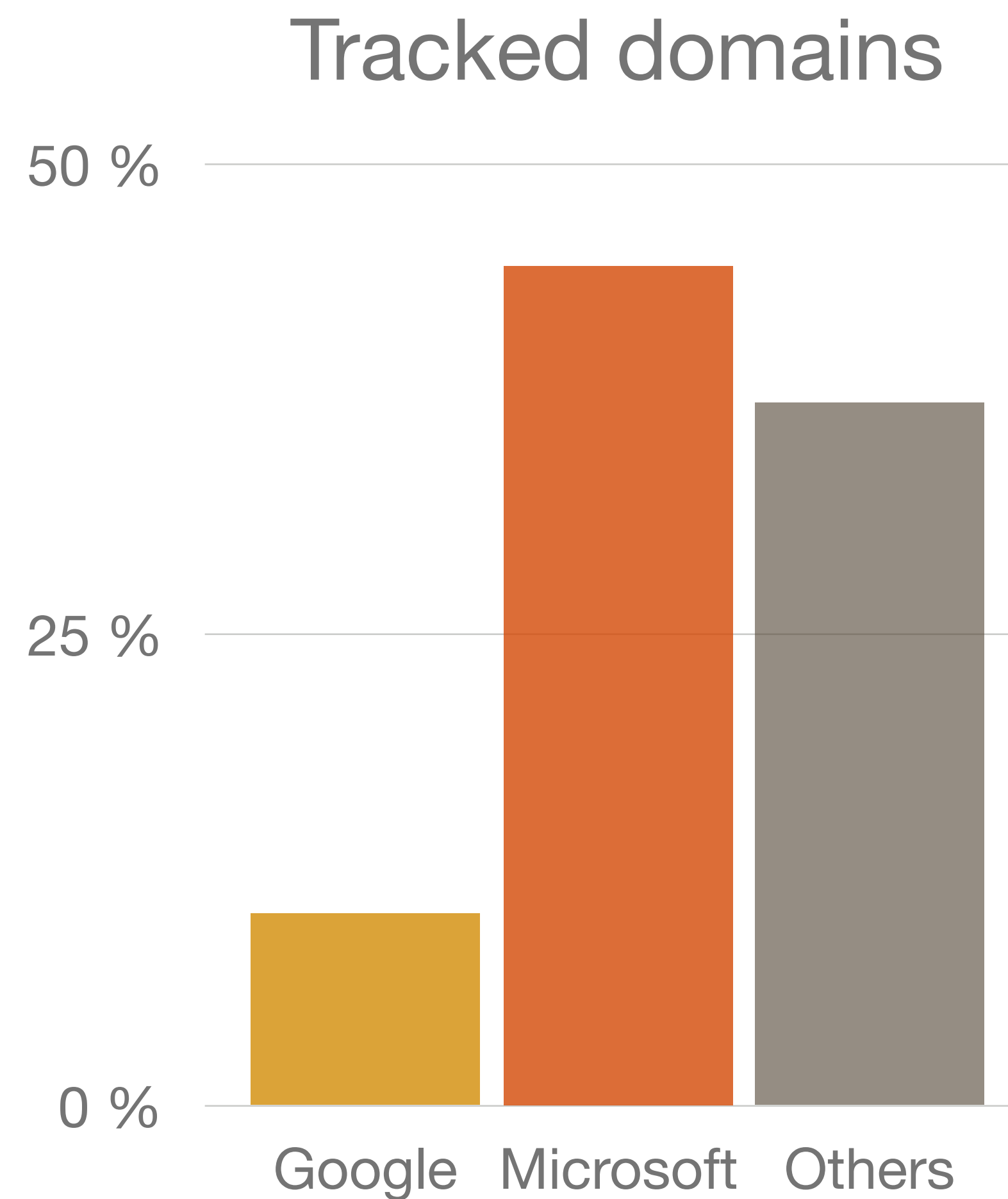




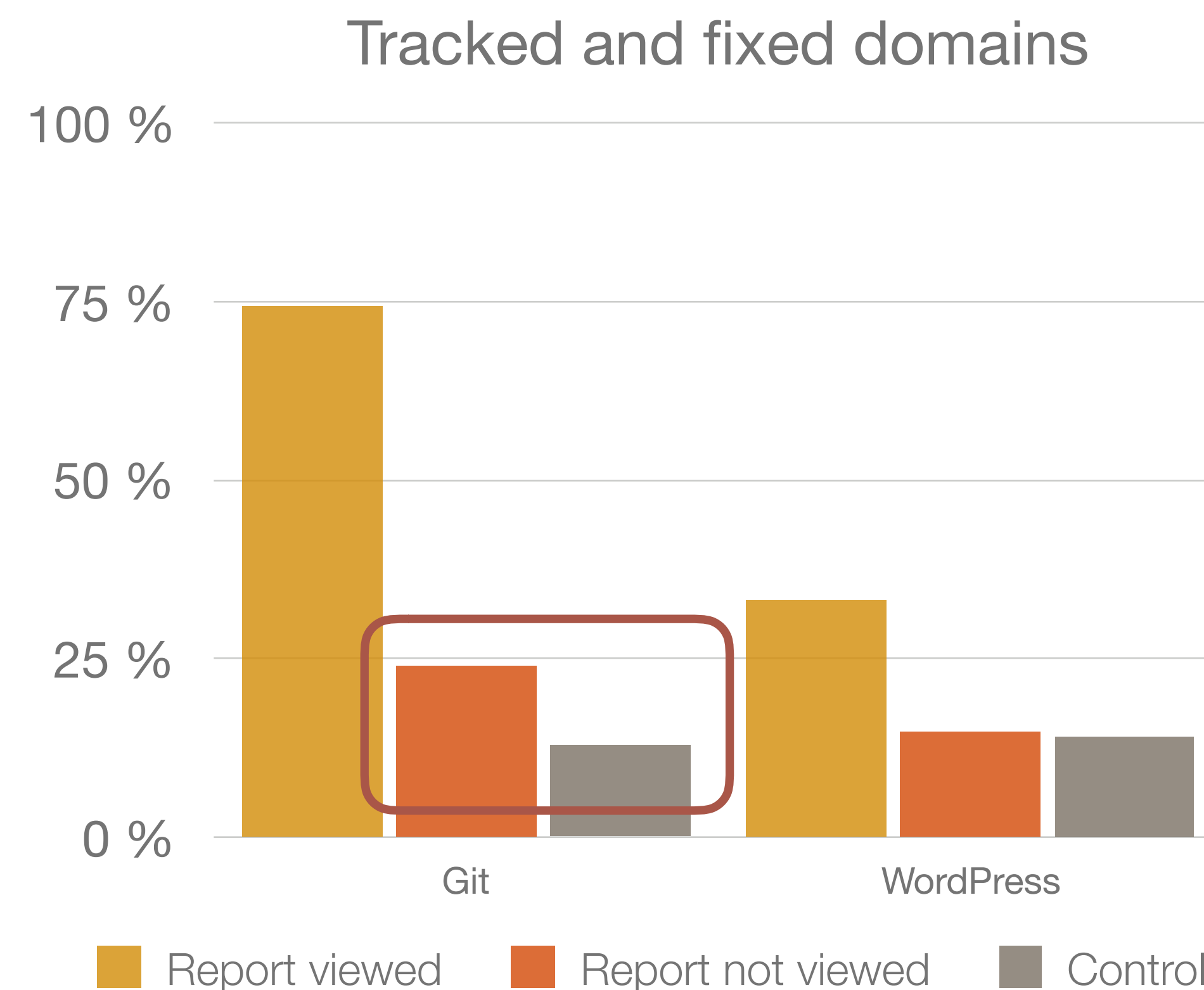
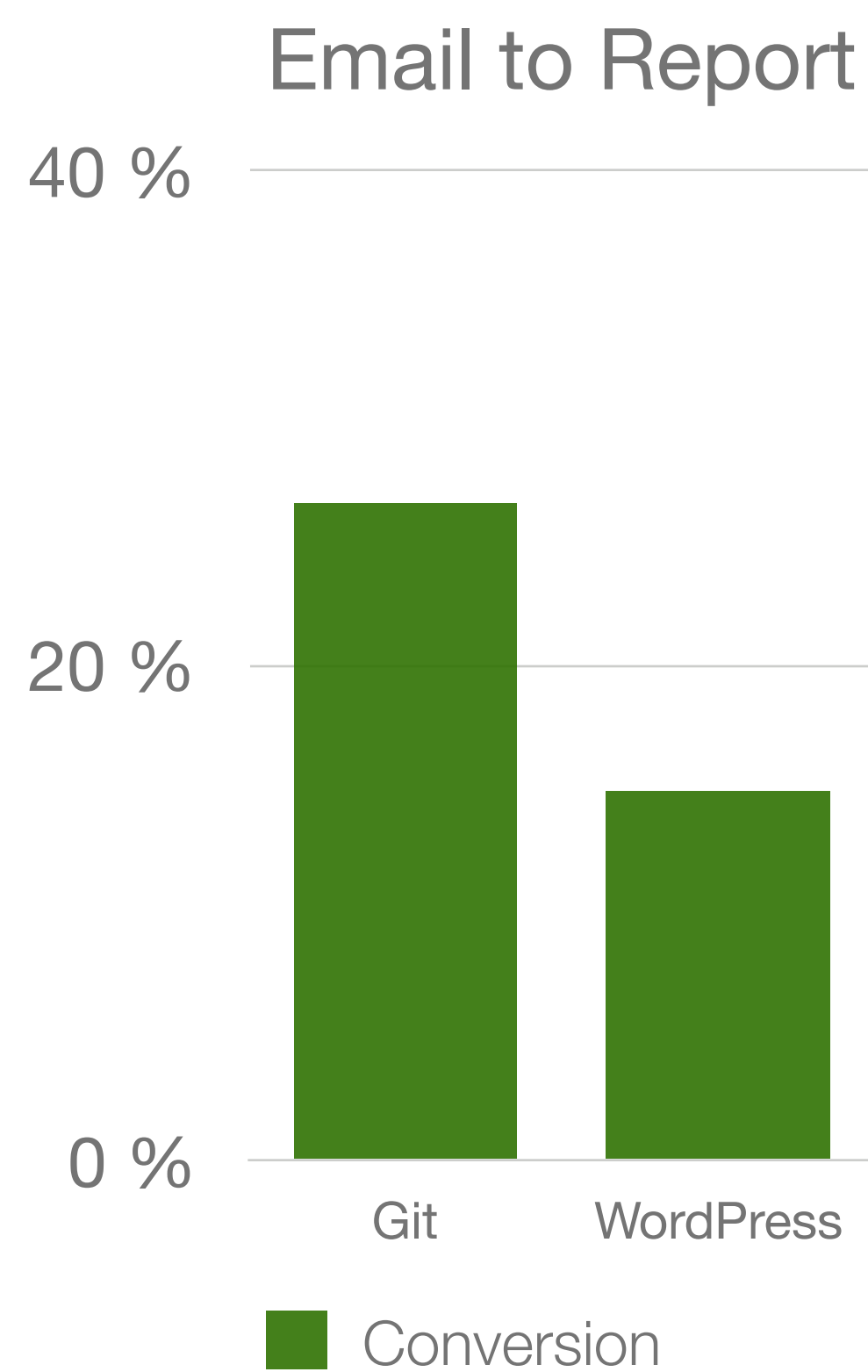
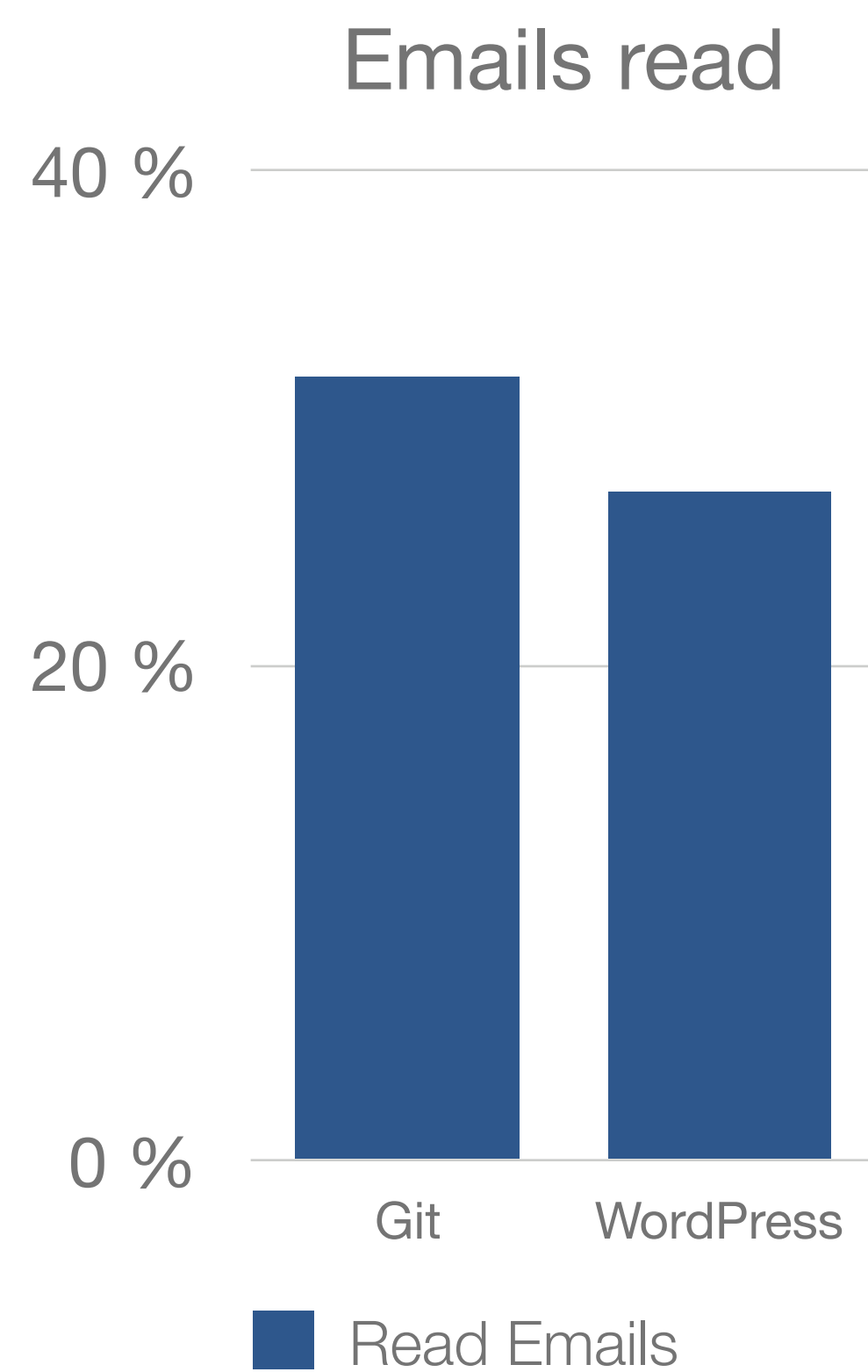
Insights from Tracking Analysis

Spam Filtering

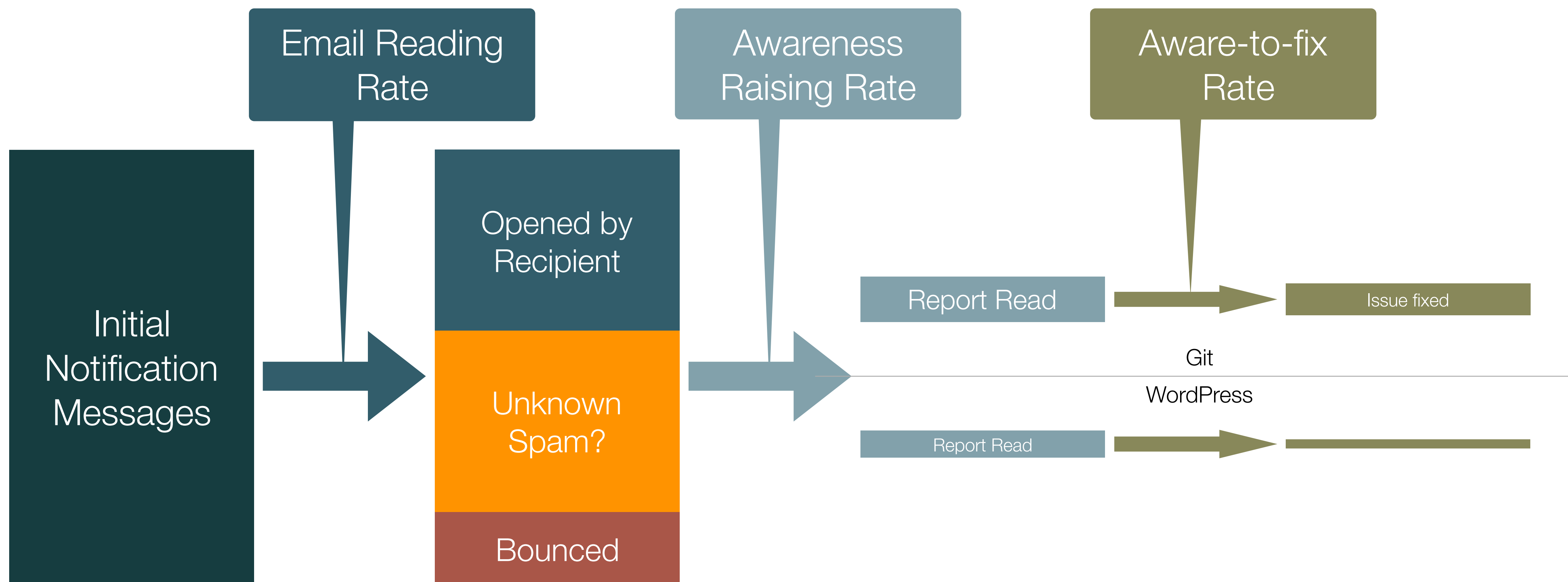
- Analyzed fraction of tracked emails per provider
 - Removed bounces first
 - Google, Microsoft-hosted (business), all other providers
- Assumption: inherent email access levels do not vary
- Drastic difference between providers
 - likely due to Google's spam filters

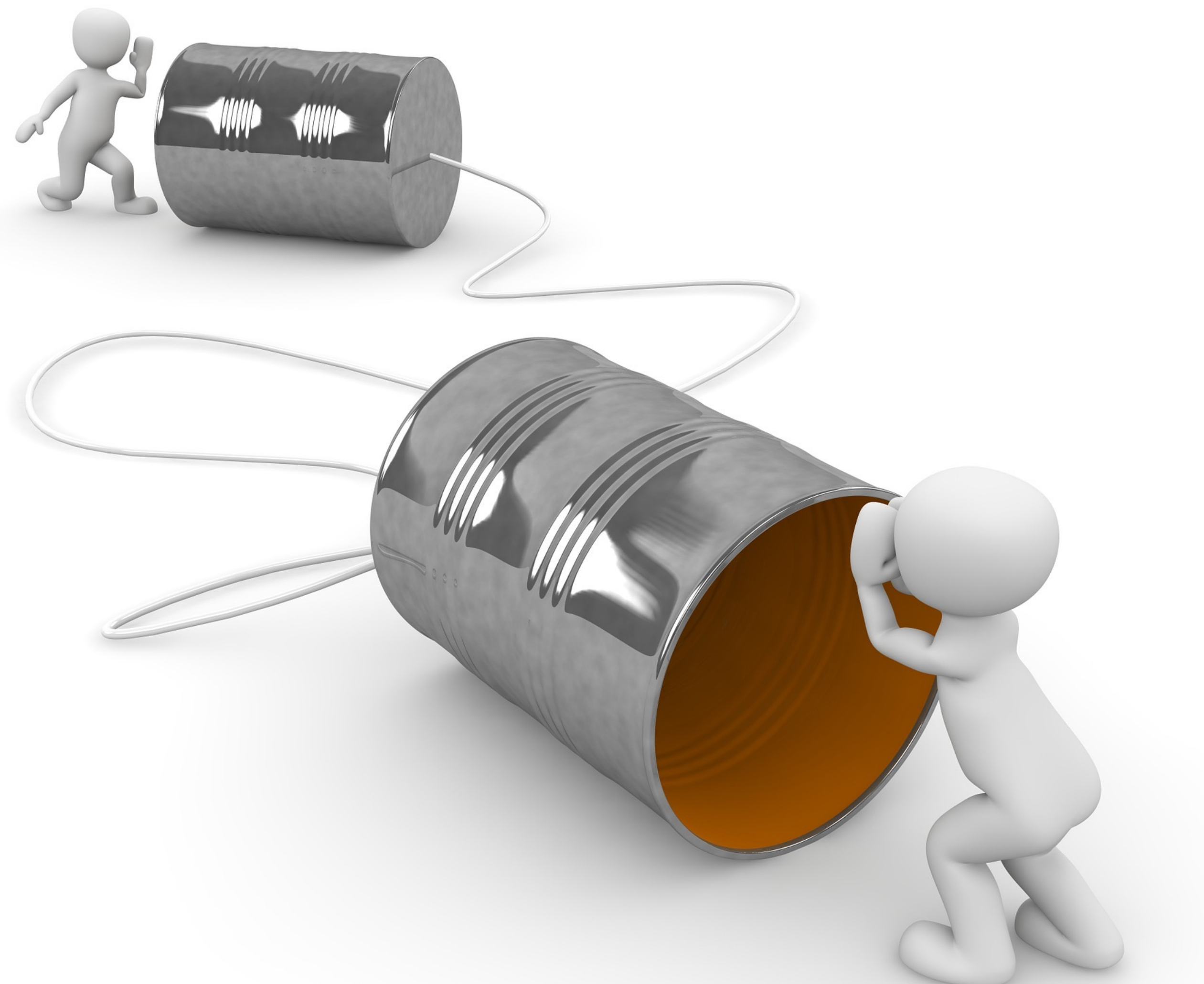


Read emails to viewed report to fixed issues



Parameters to the Success of a Notification Campaign

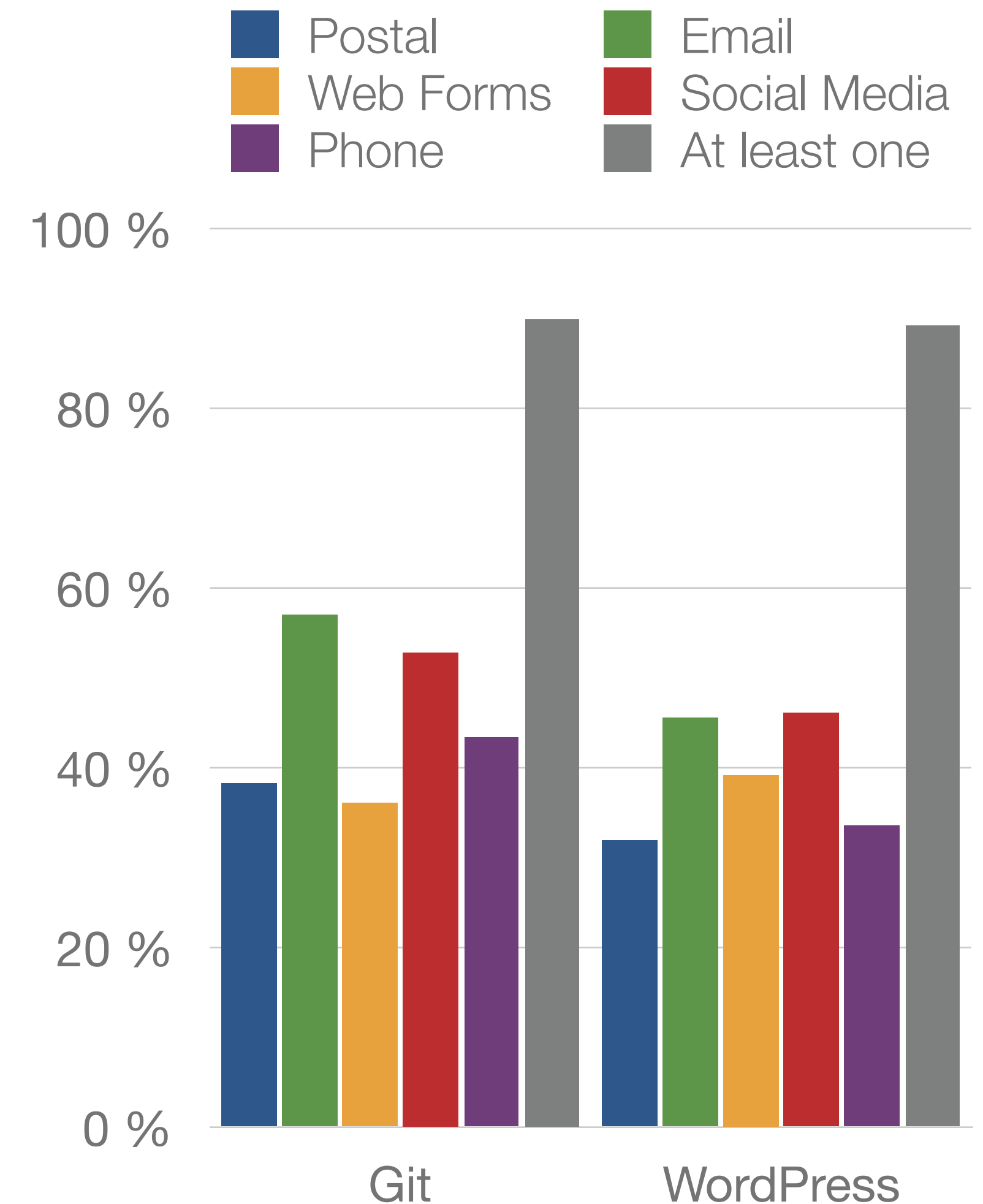




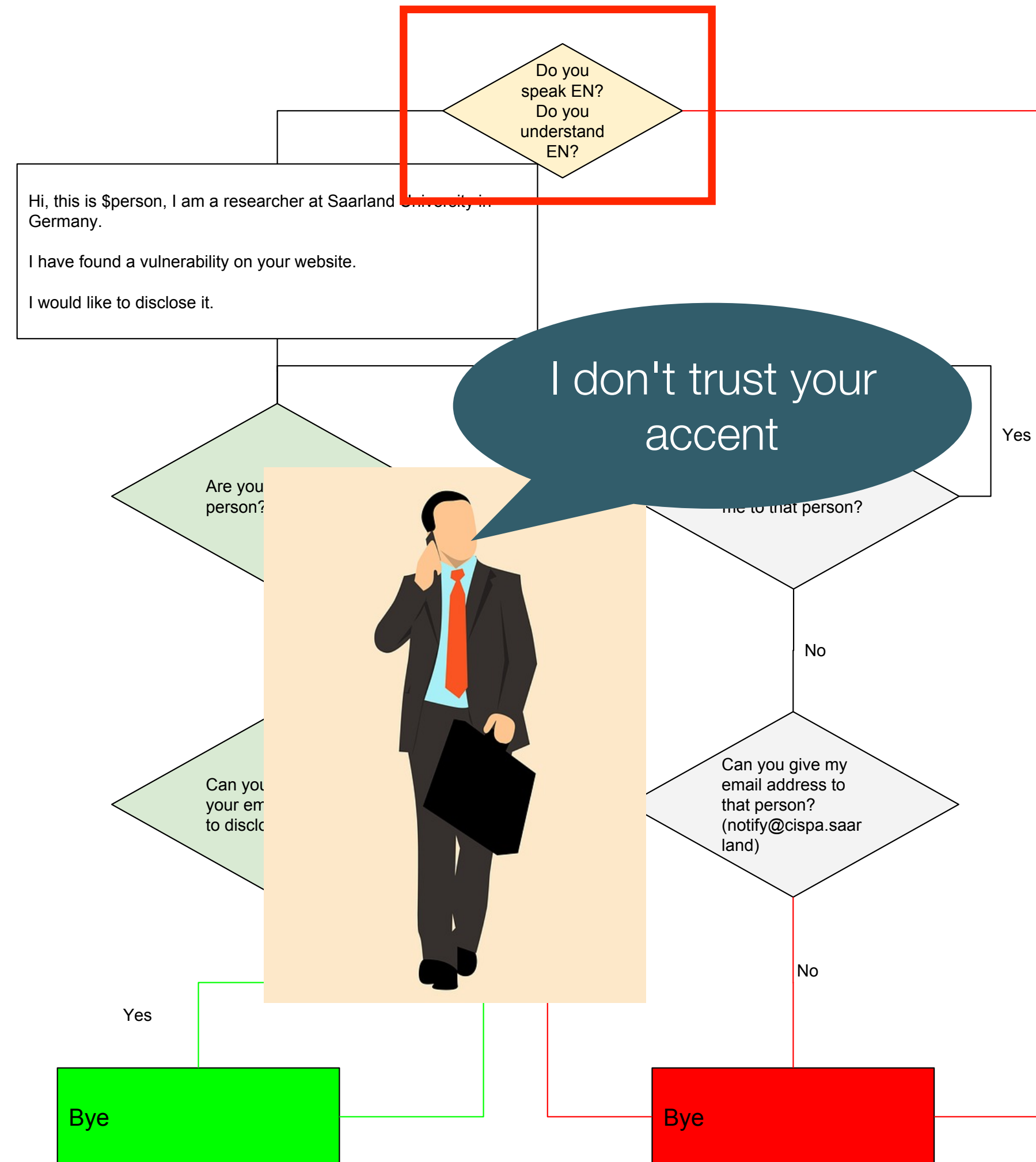
Manual Notification















Manual Notification - Channels and Availability

- Randomly sampled 970 unfixed domains
 - only domains without previous viewed reports
- Manually checked each site for contact info
 - considered postal, email, forms, social media, and phone
 - ~90% had at least one
- Randomly assigned channel to each domain
 - to avoid bias, availability of channel not considered
 - only 364/970 domains could be contacted



Manual Notification - Roadblocks

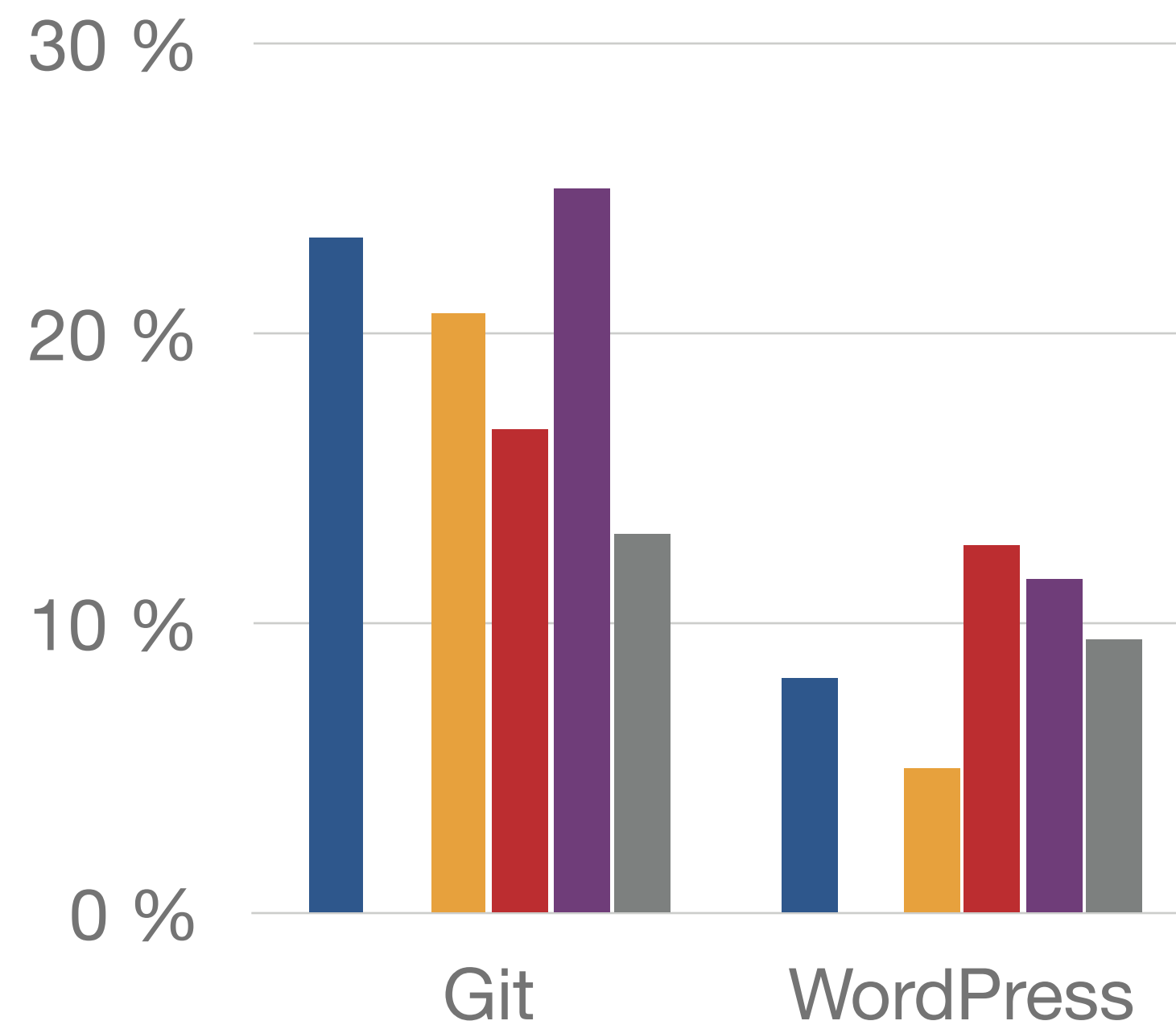


-  **A.Y. NOT DEAD** 11/04/2017
Dear Sir or Madam, I am a security researcher at th...
-  **SDIS 17** 11/04/2017
You: Dear Sir or Madam, I am a security researcher ...
-  **Midtown Lunch** 11/04/2017
You: Dear Sir or Madam, I am a security researcher ...
-  **Patriot** 11/04/2017
Dear Sir or Madam, I am a security researcher at th...
-  **Jornal do Consórcio** 11/04/2017
Dear Sir or Madam, I am a security researcher at th...
-  **الطبية نت** 11/04/2017
You: Dear Sir or Madam, I am a security researcher ...
-  **Trè Magazine** 11/04/2017
Dear Sir or Madam, I am a security researcher at th...
-  **Facebook User** 11/04/2017
Dear Sir or Madam, I am a security researcher at th...
-  **Snow Leopard Conservancy** 11/04/2017
Dear Sir or Madam, I am a security researcher at th...
-  **BeelMG** 11/04/2017
Dear Sir or Madam, I am a security researcher at th...
-  **Bestfreebies** 11/04/2017
You: Dear Sir or Madam, I am a security researcher ...
-  **PlaneteBain** 11/04/2017
Dear Sir or Madam, I am a security researcher at th...
-  **ElectroPortal - ElectroYou** 11/04/2017
You: Dear Sir or Madam, I am a security researcher ...
-  **Ezo-Világ** 11/04/2017
You: Dear Sir or Madam, I am a security researcher ...

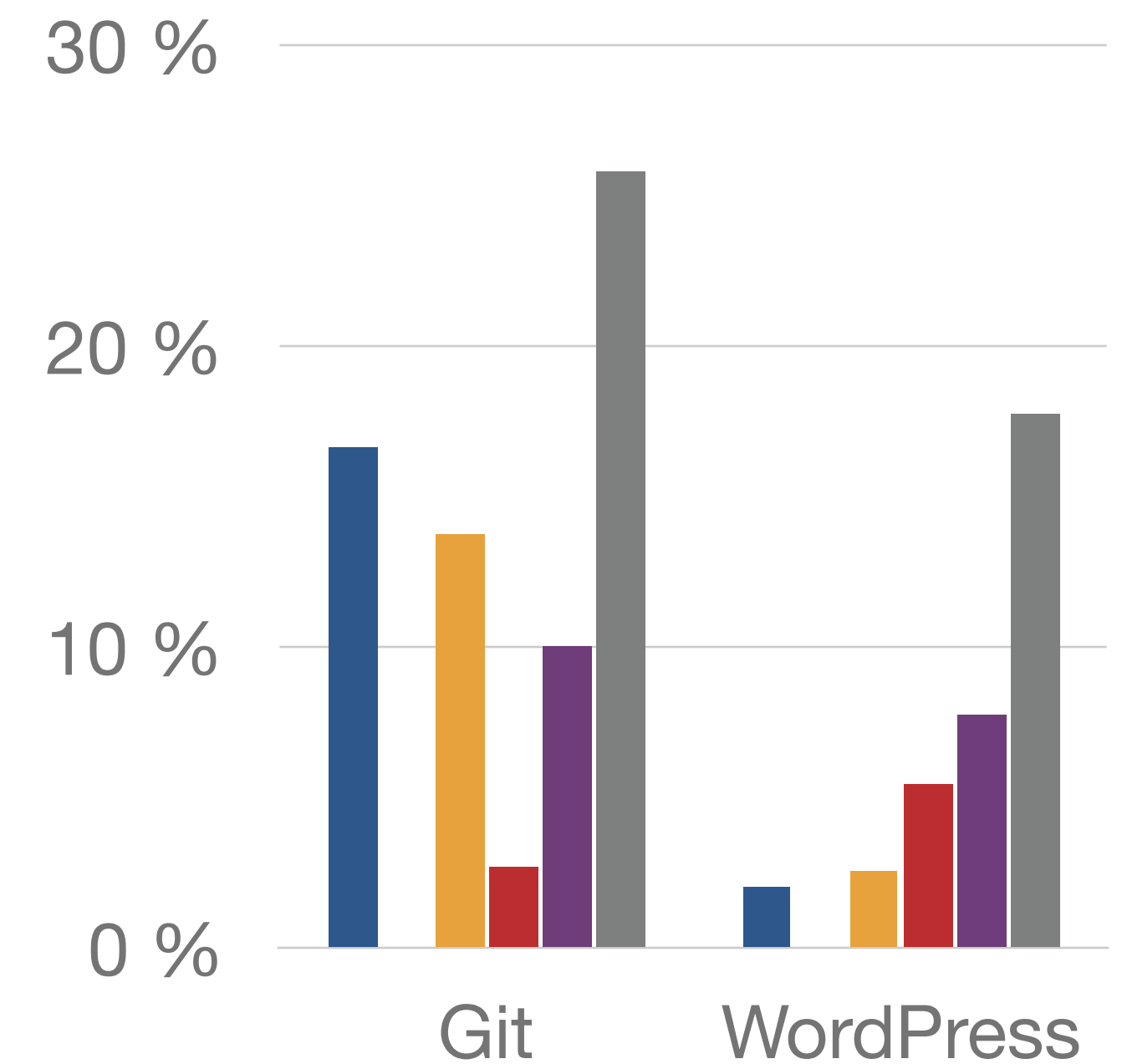
Manual Notification - Results

- 60 hours of manual work
 - 40 hours for contact lookup
 - 20 hours for notifications
- Reaching
 - Notable improvement for Git
 - small improvement for WordPress
- Fix: no improvements
- Bias needs to be considered

Viewed Reports



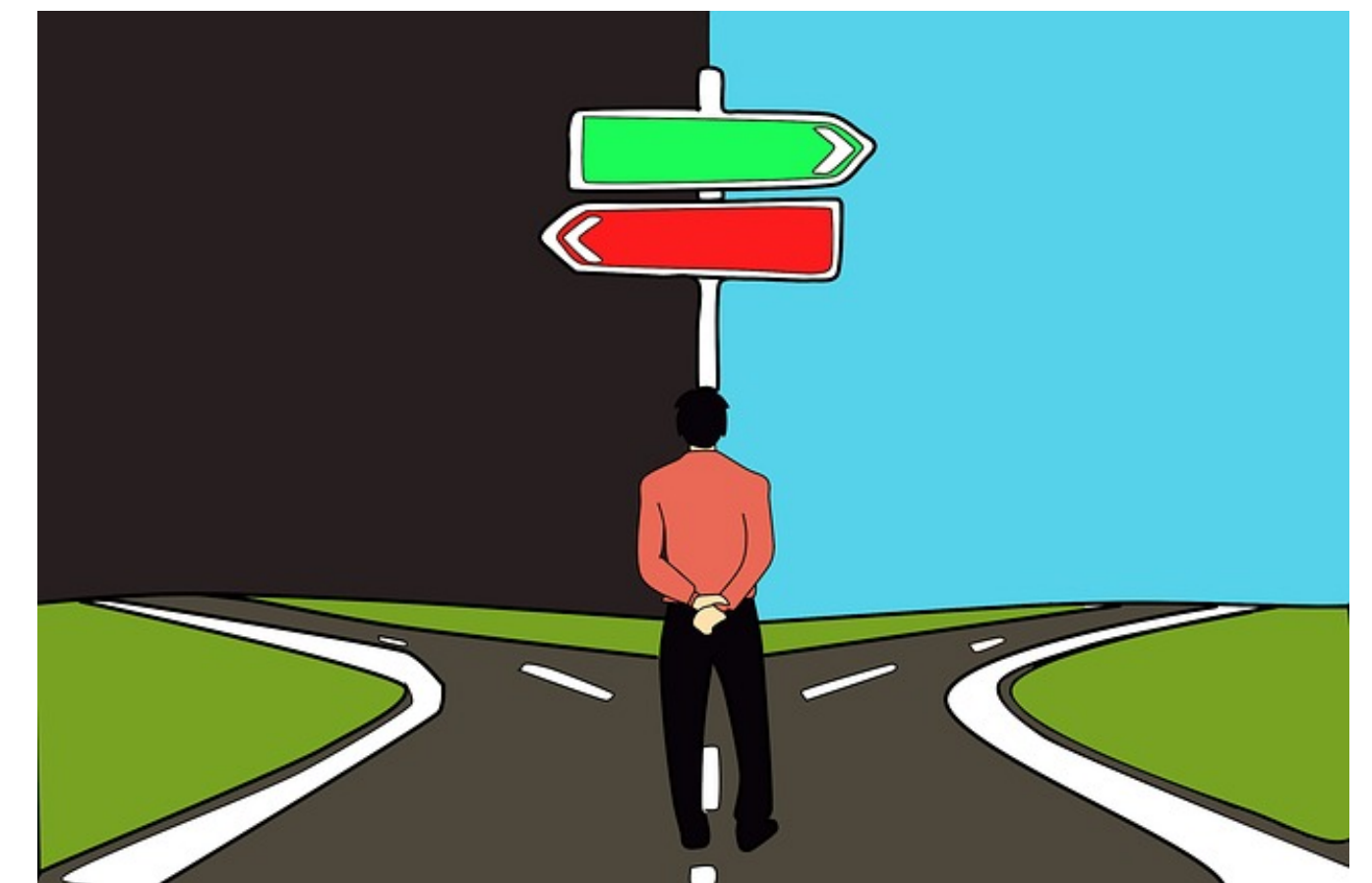
Fixed Domains



Postal Email Web forms Social Media Phone Best Automated

Quo Vadis Vulnerability Notifications

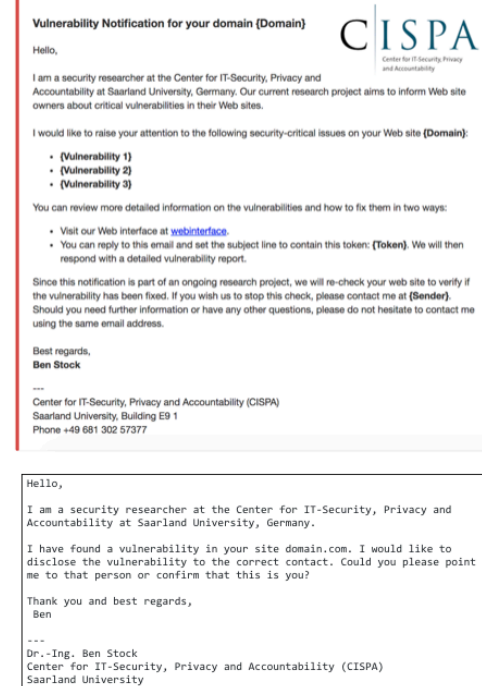
- Better Delivery Mechanisms
 - security@ bounced for 85% of all domains
 - Google's spam filter likely had significant impact on success
- Increasing Trust in Notifications
 - only between 1/6 and 1/4 followed up on our information
 - prior work with Search Console yielded 80% reactions
- Tailored Notifications
 - low fix rates for WordPress indicate lack of proper understanding



More info (including survey) can be found in our paper

Different Types of Notifications

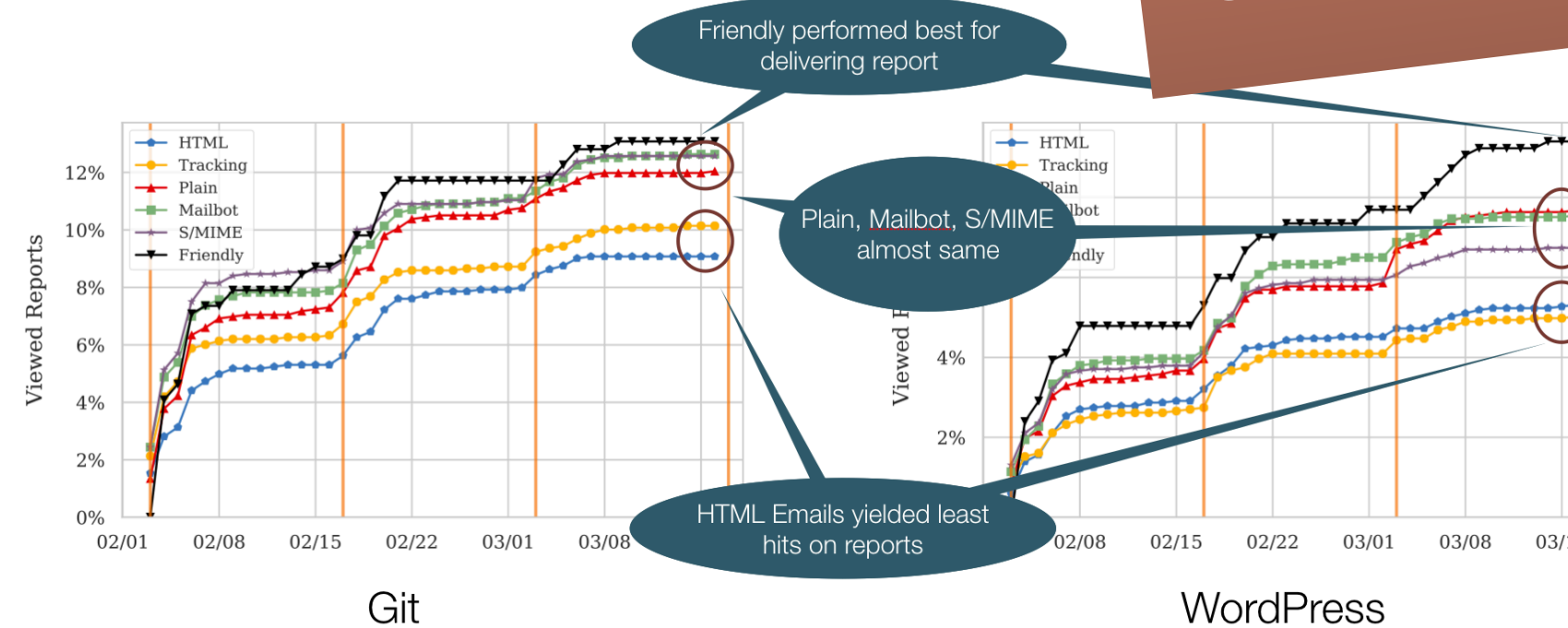
- Plain text emails
 - Real name sender (**Plain**), "Vulnerability Notification" sender (**Mailbot**), Signed emails (**S/MIME**)
- HTML emails
 - HTML with all information included (**HTML**), HTML with externally linked logo (**Tracking**)
- Friendly tone
 - Merely information that some flaws was detected
 - asked for right contact to provide more info



Ben Stock - NDSS 2018 - Didn't You Hear Me? Towards More Successful Web Vulnerability Notifications

4

Access Reports over Time

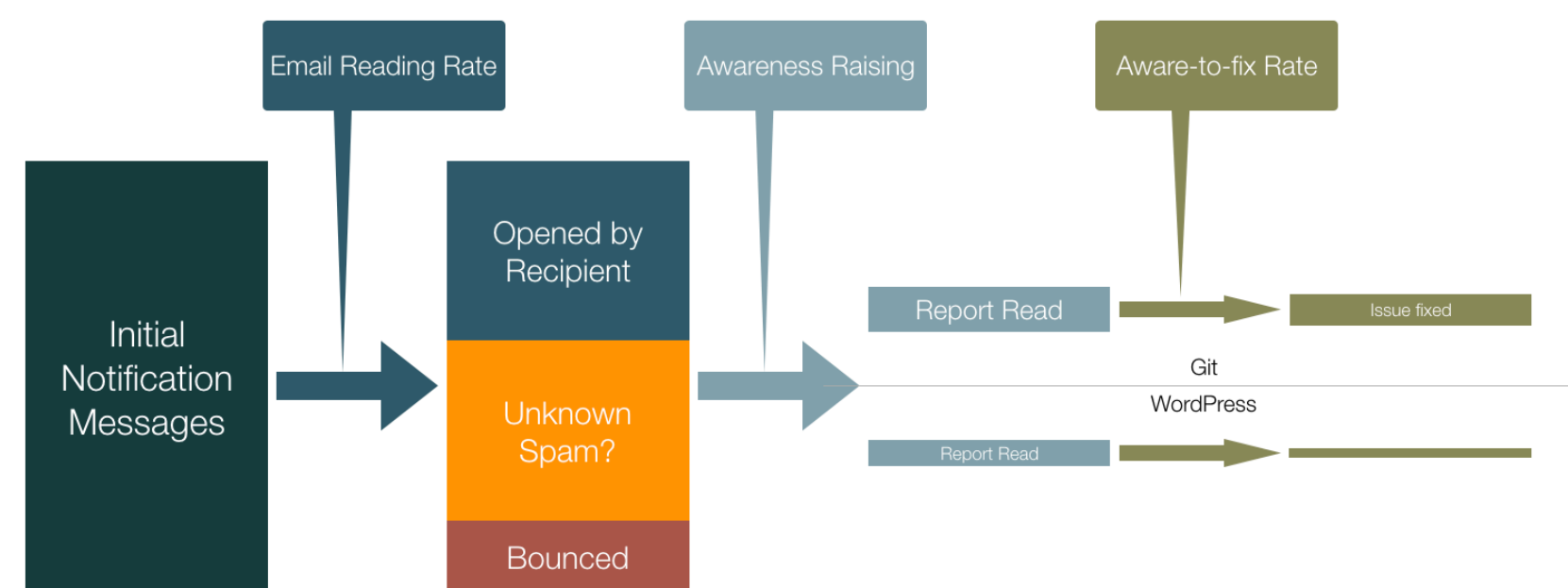


Ben Stock - NDSS 2018 - Didn't You Hear Me? Towards More Successful Web Vulnerability Notifications

9

Thanks!

Parameters to the Success of a Notification Campaign

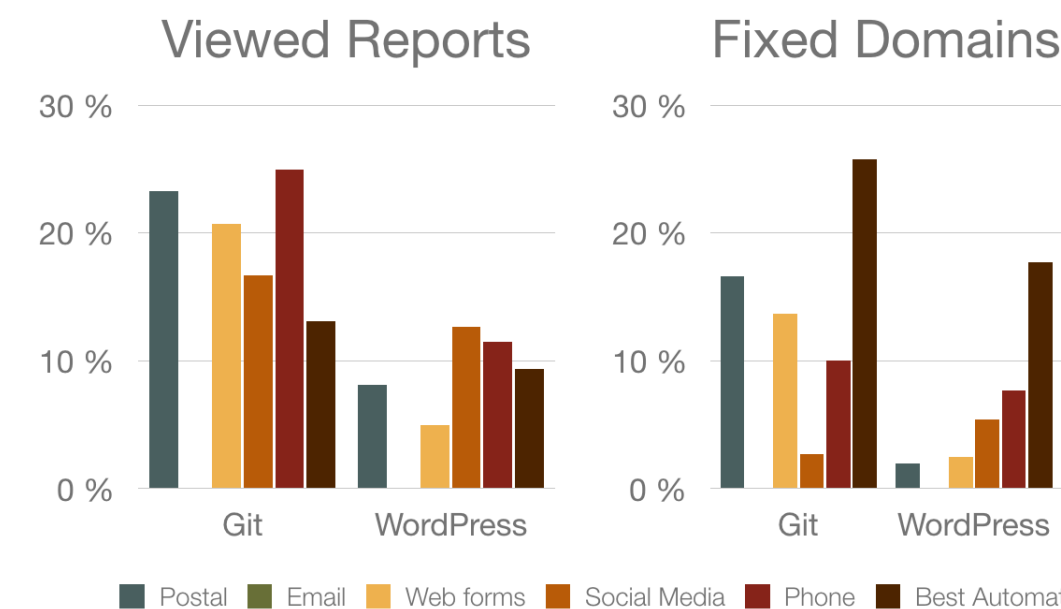


Ben Stock - NDSS 2018 - Didn't You Hear Me? Towards More Successful Web Vulnerability Notifications

11

Manual Notification - Results

- 60 hours of manual work
 - 40 hours for contact lookup
 - 10 hours for calls
 - 5 hours letters
 - 5 hours forms/social media
- Reaching: Notable improvement for Git, small improvement for WordPress
- Fix: no improvements



Ben Stock - NDSS 2018 - Didn't You Hear Me? Towards More Successful Web Vulnerability Notifications

17

CISPA
Center for IT-Security, Privacy and Accountability

Stanford University

Berkeley UNIVERSITY OF CALIFORNIA