PHISHING WITHOUT FAILURE AND FRUSTRATION

or “How I learned to stop worrying and love the layer 8”

Unabridged Version

Jay Beale

CTO, InGuardians

Larry Pesce

Director of Research, InGuardians

Why isn't this simple?

- As white hats, phishing should be just as easy as for black hats, right?
  - Write a crafty e-mail that directs readers to a web site.
  - Build a one-form web site to collect credentials.
  - Get client approval of the product of steps 1 and 2.
  - Send e-mail to as many people as possible at company.
  - Watch the passwords fly in.
- Sometimes you get lucky and it really is this easy. Whew!
- Expect 10–40% of employees to give their passwords.

Success Rates in Excess of 100%

- Larry once had a phishing campaign with a success rate in excess of 100%.
- The company targeted a subset of its employees.
- His "give us passwords or we cut off your access" call to action worked really well.
- They forwarded the phishing e-mail to their co-workers!
  - Oh, and tested the privilege-separated accounts.
  - All of them…

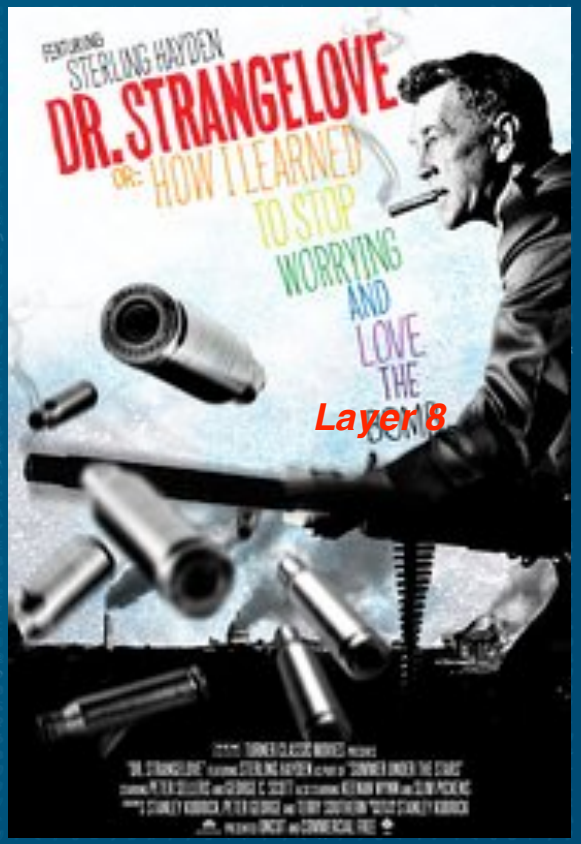
INXS

Why Phish?

- A professional phishing engagement should "harden" an organization's staff.
- More specifically:
  - increase individual resilience in every staff member.
  - train the organization in collaborative detection.
- After a couple phishing campaigns, employees will detect scams and report at higher percentages.

Why this talk?

- Most people's first few professional attempts don't go this well.
- Years ago, when we started phishing, we'd watch our consultants get so frustrated with the situation. We got better.
- The rest of this talk details ours and others' frustrating situations, teaching you how to avoid them entirely and achieve success.



TL;DR

- This isn't about red team phishing - we do that too, but it rarely involves these challenges.
- Eleven stories of failure, each with specific solutions.
- Generalizing…
- Setting up any professional phishing campaign involves:
  - Collaboration
  - Communication
  - Negotiation
- For that matter, anything in life with more than one person involves negotiation.

Penetration Test Phishing vs Red Team Phishing

- Red Team phishing is phishing solely to get initial access, not to test everyone
- Incredibly small target pool - usually 1-2 e-mails
  - Manually determine targets
  - Use open source recon: LinkedIn, Connect.com, Company website
- Low and slow - we must not get caught
  - It can help to have a pre-established persona with a LinkedIn profile
  - Pretext focused on specific job function, e.g. recruiters open resumes
  - Payload needs to be stealthy, topical and never cause suspicion
- Pro-tip: use Gmail or Office365 since many organizations whitelist these.

Eleven Stories

- We're going to tell you eleven stories from real life experience.
- Each informed the way that we run a phishing engagement.
- We give this advice as if you fill one of these roles:
  - Consultant working for multiple clients
  - Security professional inside a single organization


I can see no way in which this carefully laid plan could ever fail.
ICANHASCHEEZBURGER.COM

Story 1: Schedule Fail

- We gave our client three scenarios to choose from.
- He chose one, we got the pretext built by Wednesday, sent the URL to the client and told him we'd be sending the e-mails on Friday.
- He showed the URL to his manager on Thursday, who objected to the entire scenario.
- You've just blown your schedule to bits.

COMMUNICATION FAIL

Story 1: Fix It

- Guide the client/organization through the process strongly from the beginning.
- Tell the org what you're going to need before you even start brainstorming pretexts.
- Find out on Day 0 who can veto a pretext. Explain the risk of a late-stage veto.
- Set and remind org of deadlines for pretext acceptance.
- Prototype pretexts: don't build a site until final agreement on pretext.
- Involve the org contact in developing pretexts.
- Realize that you're in a multi-party negotiation and rock it accordingly.

Introvert Pro-tip

- Communicate more in the beginning

- Far less time spent later on:
  - talking about frustrations
  - assigning blame
  - lamenting failure


WHAT DO YOU MEAN YOU DIDN'T GET MY FATHER'S DAY CARD?
DID YOU CHECK YOUR SPAM FOLDER???

Story 2: SPAM Filters

- You spend substantial time developing a pretext e-mail and landing page, but then none of your e-mails make it through the organization's spam filters.
- Spam filters trigger because:
  - your domain is too new
  - your domain lacks or has broken SPF/DKIM/MTA configs
  - they get lucky
- Back to the drawing board! The schedule suffers and the org contact is annoyed.


YO DAWG USER TESTING
SO I'VE TESTED THE TEST WITH USER TESTING
memegenerator.net

Fix 2: Technical and Human

- On the technical side, configure:
  - SPF
    - make sure to include your IPv6 address
  - DKIM
  - MTA with a domain that has existed for at least a week.

- An even better solution is to explain to your contact that you're testing the humans, not the technology, and ask for a spam filter whitelist.
- Make sure to budget time and test the whitelist!

Show all work for the questions in this section. Circle all of you

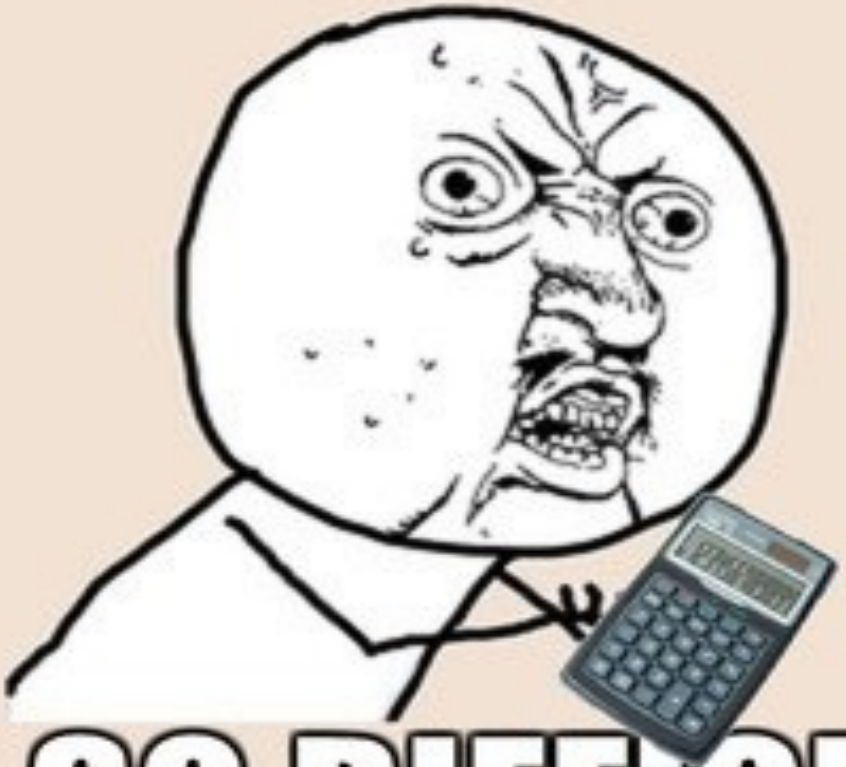
51. Find the volume and surface area of the right cylinder.

SUSHI

Story 3: Numbers Game Fail

- You use all the best tools (including Maltego) and get only 15 e-mail addresses.
- If you want to test the organization as a whole, you need a heck of a lot of e-mail addresses.
- Black Hats get to:
  - brute force mail servers to find valid e-mail addresses
  - buy mailing lists

MATH.



Y U SO DIFFICULT

MathMemes.com

Fix 3: Numbers Game Fail

- Let's stipulate that an attacker could get a very comprehensive list of e-mail addresses.
- RED TEAM TACTICS: White Card event
- Present options to the client:
  - We'll find addresses, include them in the report, but then client gives us a comprehensive list of e-mail addresses.
  - We can brute force your mail server with spam.
  - Just give us a complete set of e-mail addresses.


BRACE YOURSELF
OPEN FLOOR PLAN IS COMING
memegenerator.net

Story 4: The Open Floor Plan

- Your e-mail says it's from Robert Smith, the Director of Information Technology.
- Your target organization all sits in a one story open floor plan.
- People start walking over to Robert’s desk, and he quickly alerts everyone.
- Your success rate plummets!

Having an open-office floor plan has helped me bond with coworkers who also despise having an open-office floor plan.

someecards

Fix 4: The Open Floor Plan

- Know your target.
- If you are a third party, ask your client contact about:
  - Where everyone sits
  - How they communicate
  - Their escalation procedure
    - Do they call compliance, help desk, or HR?
- Better still, make your client/boss contact and at least one level of management above her part of the pretext brainstorm. Catch pretext problems early.


NOT SURE IF SLOW
INTERNET
OR A PIXELATED
IMAGE
memecenter.com
MemeCenter

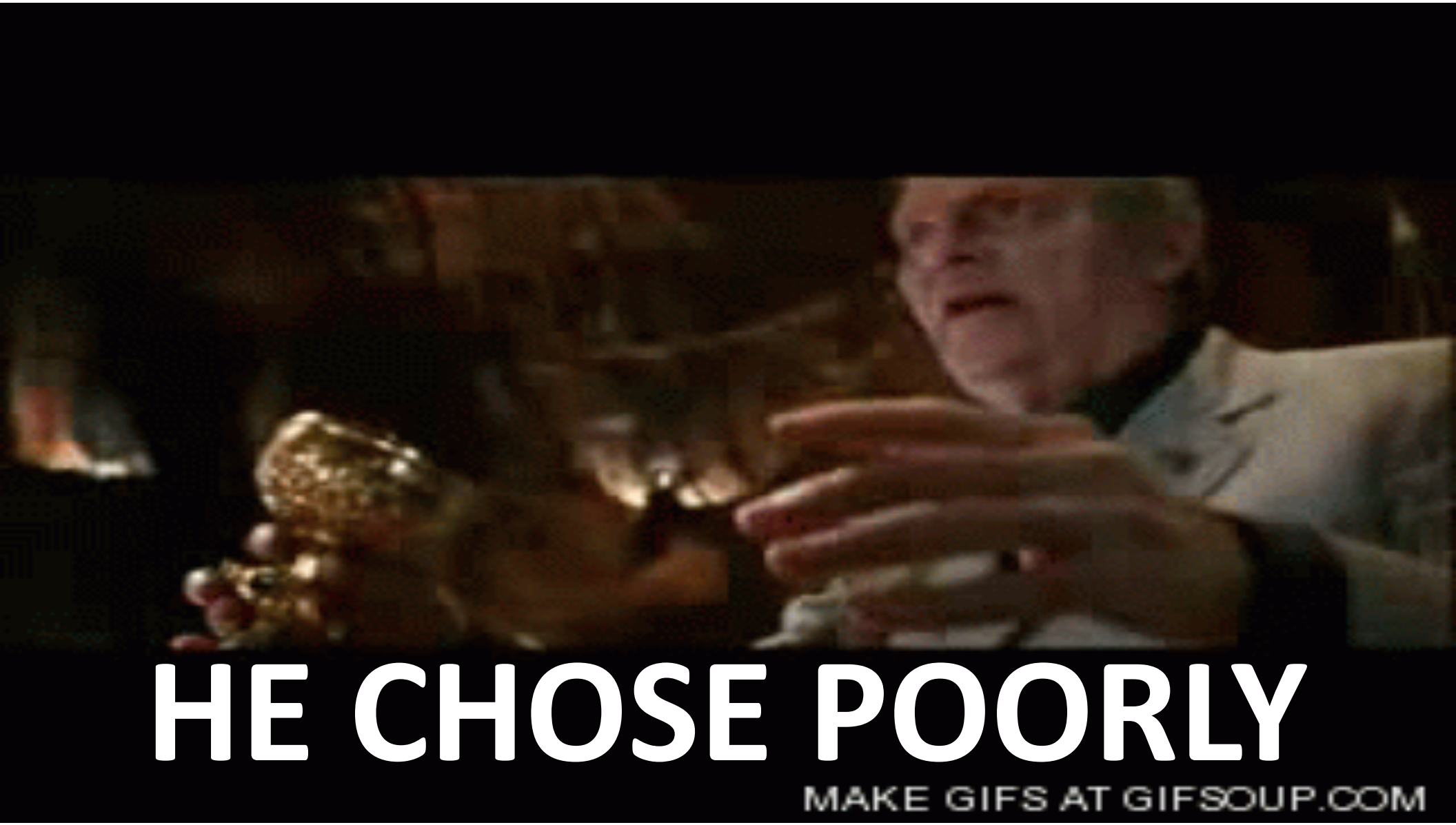
Story 5: Low and Slow

- Your client asks you to send the phishing e-mails slowly, to avoid detection.
- Your victims start to talk. By the time you've got ten e-mails out, someone has alerted the security folks, compliance or the help desk, who send out a mass e-mail.
- The jig is up!


MOVE LOW AND SLOW SON. LOW AND SLOW.
WHY DAD?
BARBECUE, CARL. BARBECUE!
FML!
BLOCK
imgflip.com

Fix 5: Speed (racer meme)

- Phishing truly is about speed. You must rush.
- You're racing an organization's ability to communicate and collaborate.
- Make sure your e-mail gives so short a deadline that people rush to take your desired action, before:
  - Someone warns them
  - They get a chance to think about whether this is a good idea.


HE CHOSE POORLY
MAKE GIFS AT GIFSOUP.COM

Story 6: Poor Domain Choice

- You choose a domain where a single letter is changed or one where you leave out a letter.
- Bonus: you can register a TLS certificate!
- Examples:
  - elilily.com
  - elilil1y.com
- Outcome: The employees are trained to catch this. None of them are fooled.

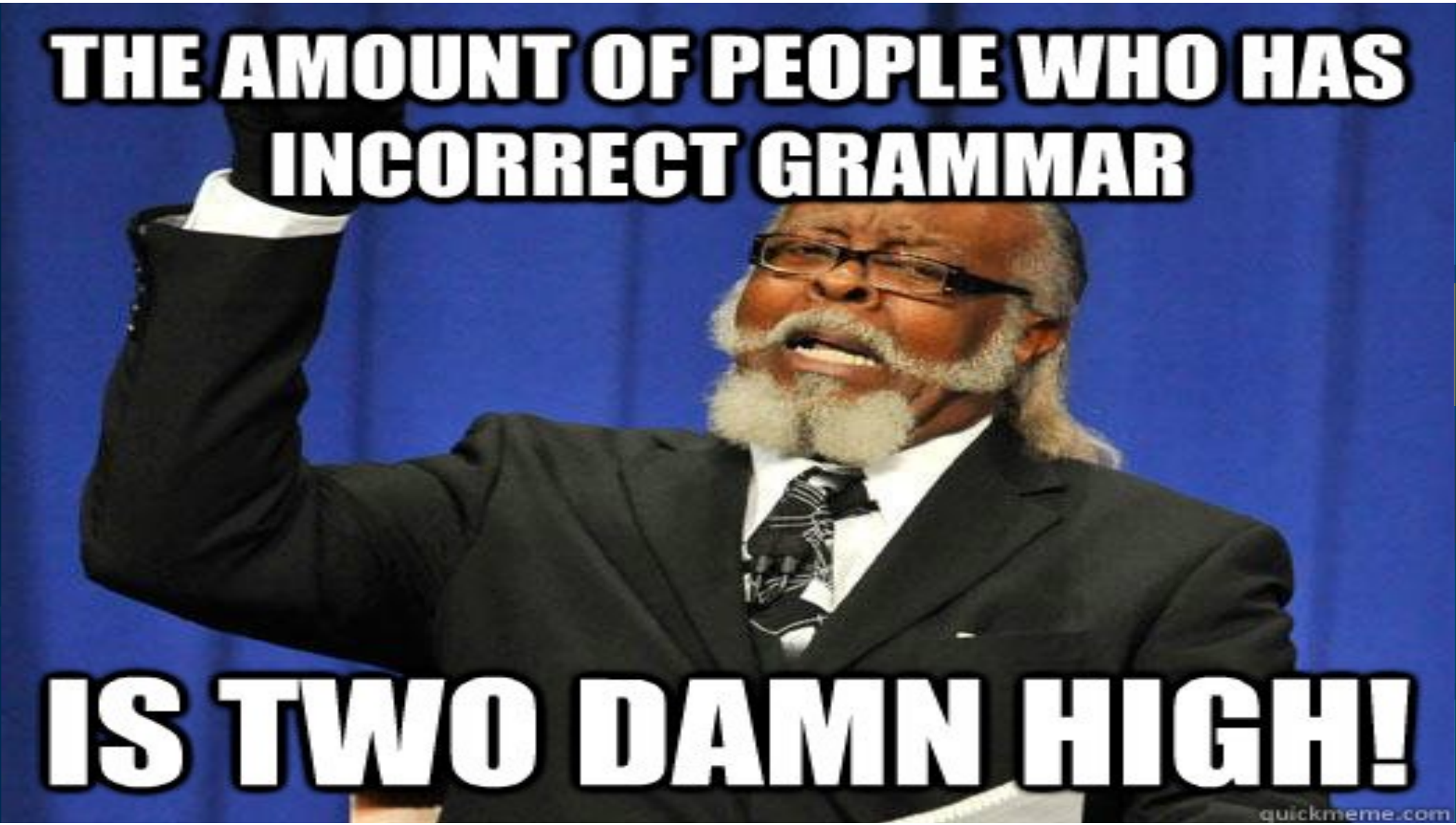

YOU HAVE CHOSEN
WISELY.
memegenerator.net

Fix 6: Good Domain Choice

- We've had very, very good results with domain names that include the company's true name:
  - elililly-benefits.com
  - elilllilly.myhealthbenefits.com
- Figure out what will work.
- Check it with the org and your colleagues.

Negotiation

- What if your client asks for the L-changed-to-1 domain?
- Phishing is all about:
  - Collaboration
  - Communication
  - Negotiation
- The easiest and most common way to lose in a negotiation is to not realize you're in one.
- Can you agree to brainstorm domains as a larger group?


THE AMOUNT OF PEOPLE WHO HAS INCORRECT GRAMMAR
IS TWO DAMN HIGH!
quickmeme.com

Story 7: Broken Grammar

- Your org contact asks you to use broken grammar and spelling to simulate the weakest phishes they get.
- This lowers your success rate, leaving you feeling frustrated.
- Your client has given his company a false sense of security.
- By winning his negotiation, the client just lost.
- Rule of Negotiation: if anyone loses, everyone loses.


GRAMMAR NAZIS BE LIKE
*ARE LIKE
imgflip.com

Fix 7: Communication

- Share with the org about how broken grammar fails to harden the staff against phishers who write well.
- Find a phishing e-mail you've received with perfect grammar and share it.
- Negotiation: offer to do a round without the broken grammar, then a round with broken grammar/spelling

S.C.A.J.

Some Cops are Jedi

Story 8: the SEC Investigation

- The org doesn't involve their HR, Legal or Compliance folks, who call in the SEC to investigate.
- Story of a recent client's compliance department calling the SEC and the investigation.


TRUST ME
WE ARE INVISBLE

Fix 8: YOU Have to Lead

- You have to lead the phishing project. Make involving HR, Legal and/or Compliance a mandatory part of the test.
- Humans most easily learn and persuade through story. Make this story part of the conversation early on.
- Know your org. Talk about what the escalation paths are and understand where to place your debugger breakpoints.


IF AT FIRST YOU DON'T SUCCEED
WILL KITTY PLAY WITH IT?
FAIL, FAIL AGAIN

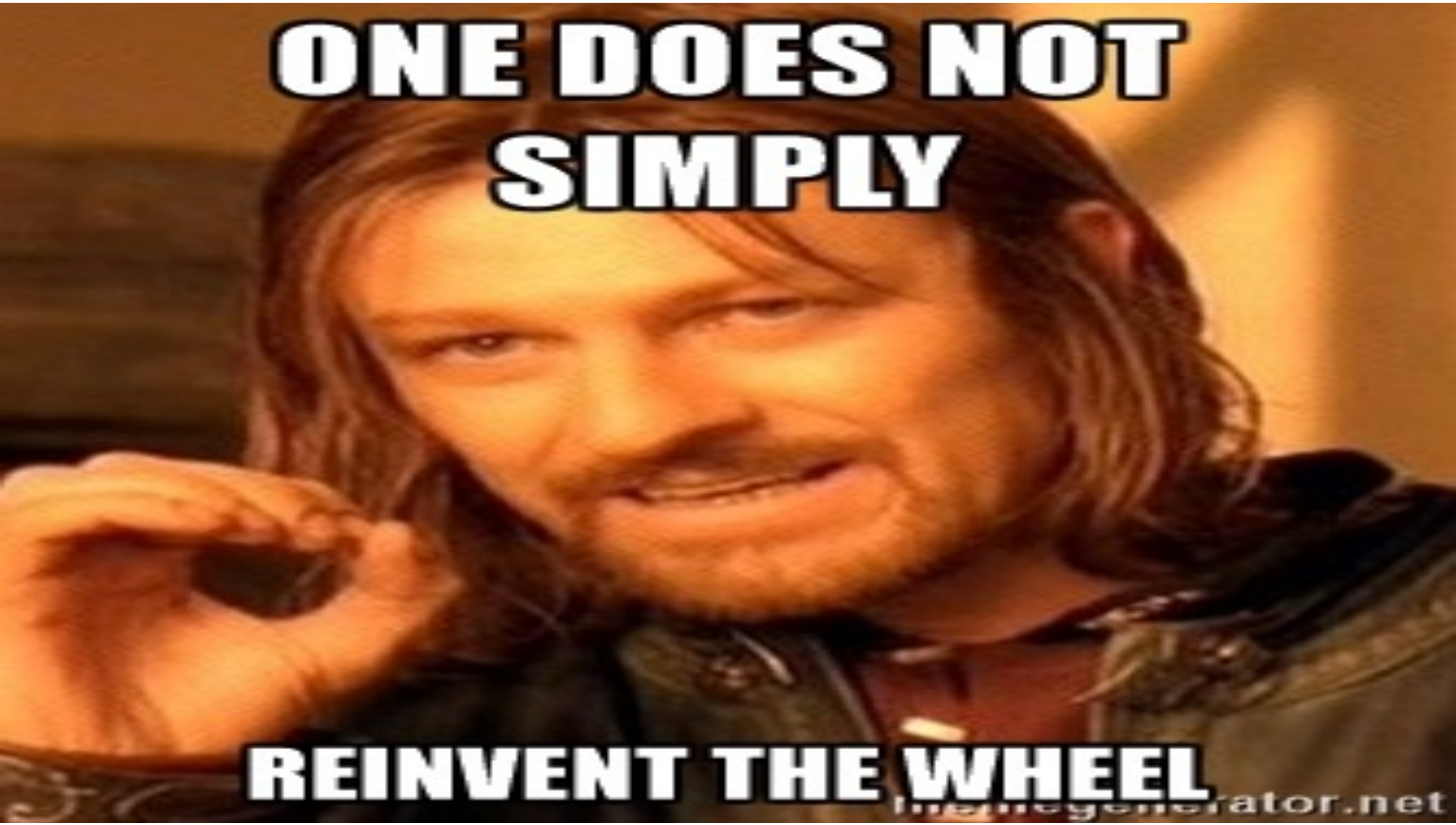
Story 9: Success and an Unhappy Client

- Your campaign is successful, but the client feels like you didn't communicate enough.
- OR
- The client calls you hourly for results.


CYCLEJERK.COM

Fix 9: Success and a Happy Client

- Make client feel loved by giving them stats even more often during first day.
- Remember client contact (security people) has been rooting for this kind of thing for a long time .
- Pro-Tip: Expectations Management
- Keep your level of effort under control by telling them in advance how often you'll be giving stats.


ONE DOES NOT
SIMPLY
REINVENT THE WHEEL
memegenerator.net

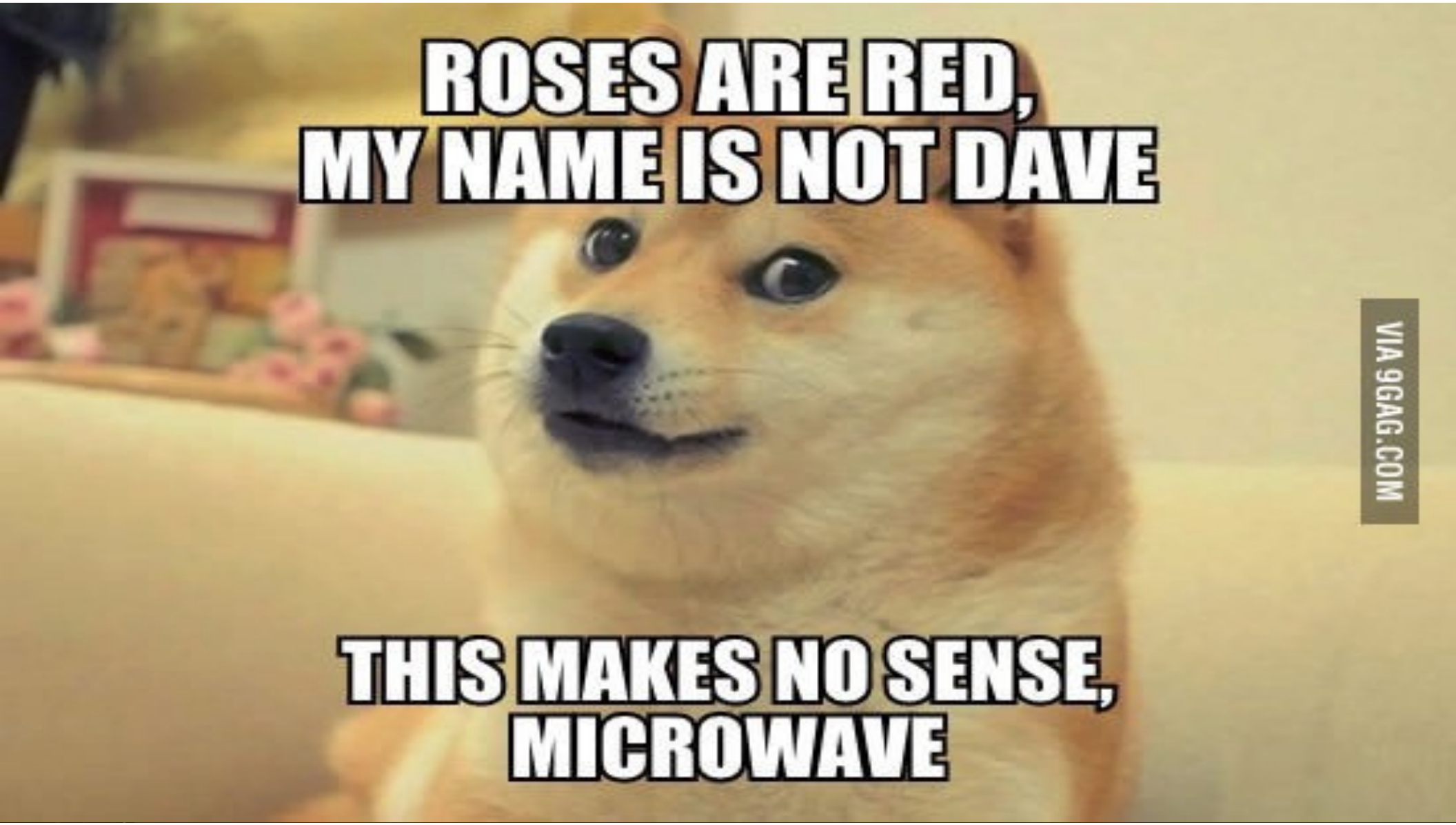
Story 10: Re-inventing the Wheel

- You re-invent the wheel every time your group does a phishing campaign, so you don't innovate enough.
- Story: every person in our company who phished created new infrastructure from scratch.
- You don't move forward, you spend too much time building and debugging infrastructure.


Did you hear the news? My boss wants me to...
Fail More!
Wow!
You guys are so innovative!

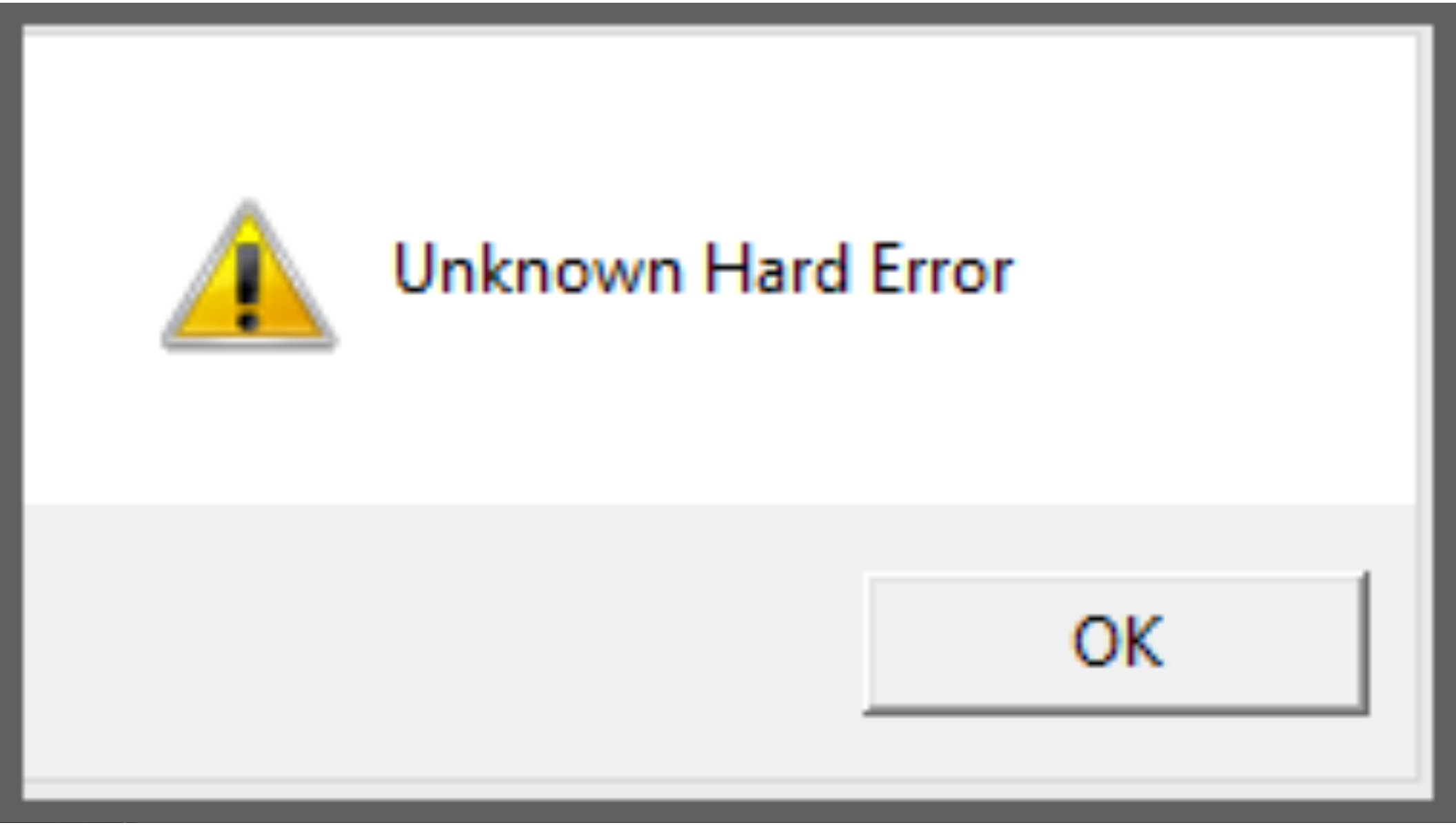
Fix 10: Create, Maintain, Publicize

- Pro-tip: use existing good free tools (Phishing Frenzy or dev your own), then teach everyone how to use it.
- Every phishing test (or at least every other) should make you better at phishing. Get better or stagnate.
- Spin up a few mail servers (MTA's) then write scripts/processes to change the domain names around.
- Enlightened Laziness (automate anything you can) means you reduce errors and spend your time truly creating.


ROSES ARE RED,
MY NAME IS NOT DAVE
THIS MAKES NO SENSE,
MICROWAVE
VIA 9GAG.COM

Story 11: Unknown Impact

- You don't follow up with the right people afterward and learn what effect you're having, and what they did after the campaign.


Unknown Hard Error
OK

Fix 11: Unknown Impact

- Plan how to tell the staff who fell victim about it, focussing on producing better results proactively, not through shame.
- Watch to see how reporting rates, escalation and alerting improves.
- If you're a third party, recommend that the org phish itself at least quarterly.


HAIR
I USED TO HAZ IT
made on imgur

Overall Lesson

- Phishing is all about collaboration, communication and negotiation.
  - If there are 2 people talking, it's a negotiation.
- Most of the failures we've described are failures to think ahead and communicate, collaborate and lead with the org.
- Use and spread these stories to persuade, plan and win.
  - If anyone loses a negotiation here, everyone loses.