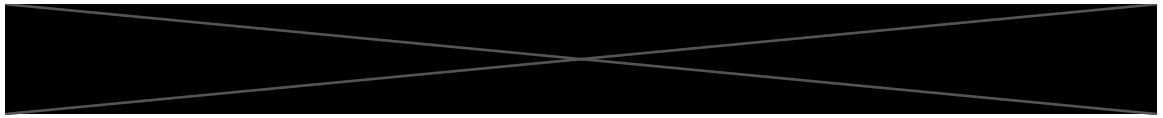
Our phishing assessments are bad .. and we should feel bad

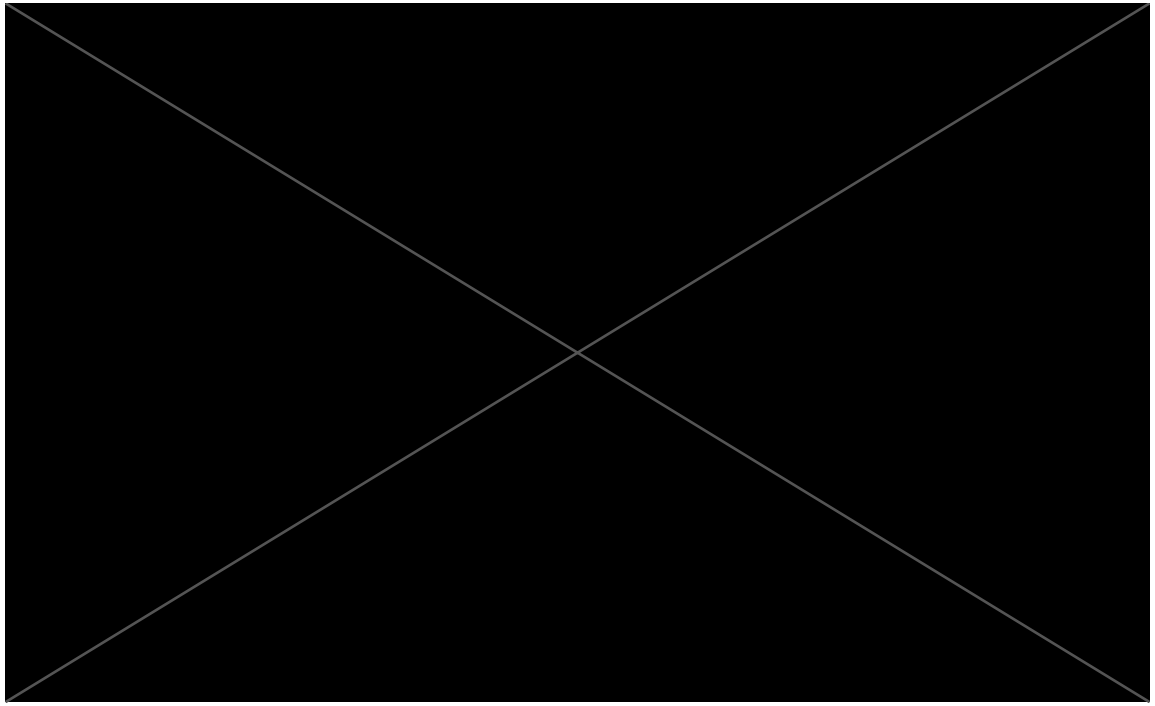


Before we start ..

- This is a non-technical talk about a very specific thing
- Please: No pictures.
- I might breathe a bit oddly at times - that's okay.

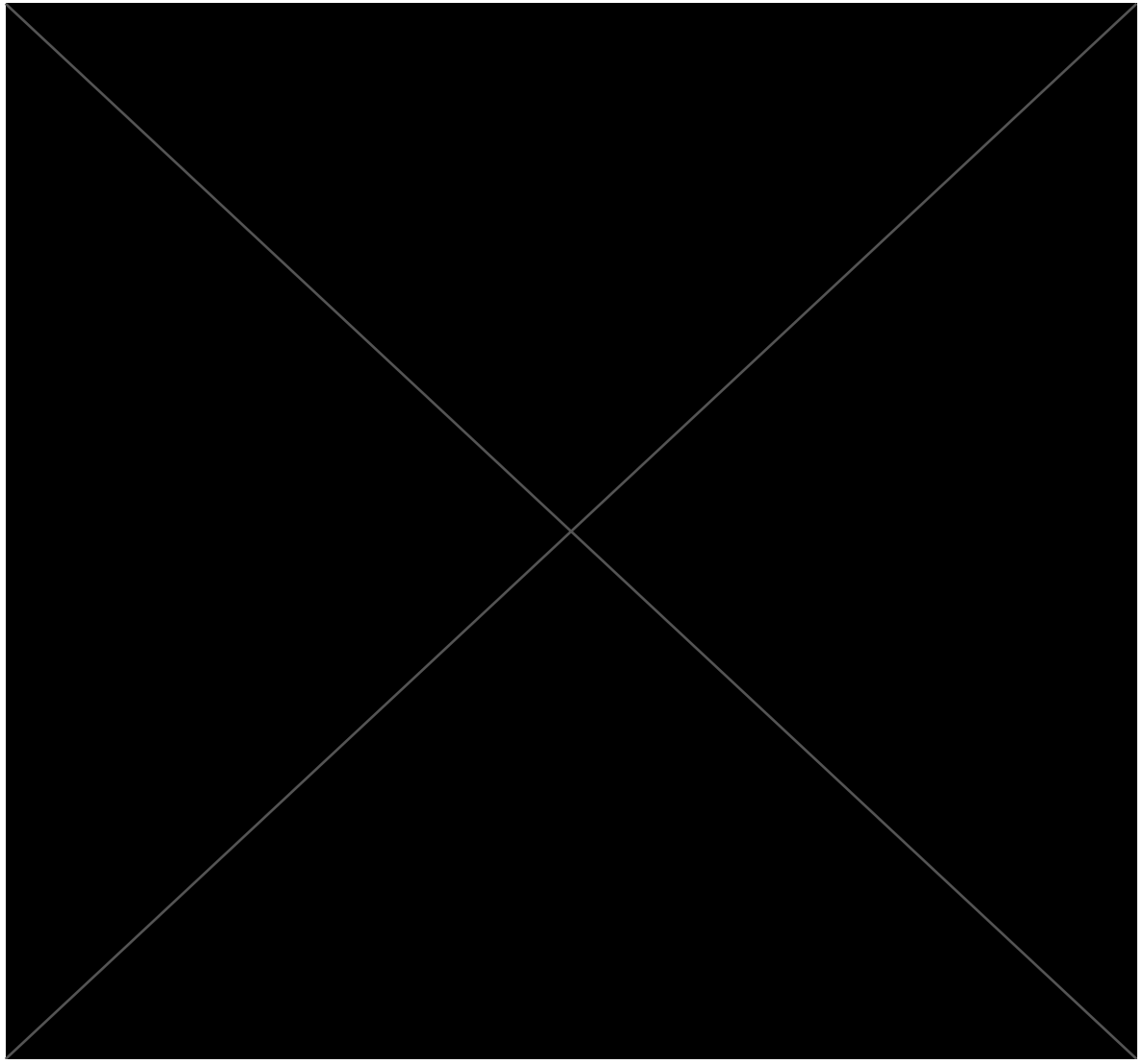
.. a bit of context ..

- Worked in IT for a decade
- Systems Engineer, Security Analyst, (Chief) Security Officer
- Seen, supported, suffered from, done quite a few phishing tests



.. a bit of context ..

- Worked in IT for a decade
- Systems Engineer, Security Analyst, (Chief) Security Officer
- Seen, supported, suffered from, done quite a few phishing tests



.. a bit of context ..

- Worked in IT for a decade (which feels odd at 30)
- Systems Engineer, Security Analyst, (Chief) Security Officer
- Seen, supported, suffered from, done quite a few phishing tests

.. and a brief introduction on the issue

> the fraudulent practice of sending messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

It's a big thing .. I know, duh!

- Mostly based around Email, but messenger-based phishing increases
  - Medium depends heavily on where the victim is located
- Been around since ~1995, will be around for a while
- DKIM, DMARC, SPF, Sandboxes, Blocklists, mAcHiNe LeArNiNg, ..

We learned!

- We can't secure our systems with technology alone
- It's the people!
- Awareness for the necessity of awareness

Phishing tests, simulations, assessments, ..

> Phishing assessments are programs that organizations can use to send realistic phishing email to employees in order to gauge their awareness of attacks and what to do with phishing emails when they receive them.

They're now *everywhere*

- Wide variety of software and services available
- Commercial providers *love* those - low cost, high billable
- Quite often: Compliance-driven

Just another magic phish-ing *sing*

- Someone (tm) orders an assessment
- A phishing message is composed, often enough utilizing internal information
- The message is sent out to some or all employees
- Most people will ignore it, few will fall for it, next to none report it
- The people who fell for it are, at best, shamed quietly
    - At worst: Repercussions

There are problems with that .. like, a lot

- Not necessarily the right motivation behind it
- Chances are there are issues with ethics
- Most malicious mails originate from elsewhere
- Completely ignoring what happens "afterwards"
- The users are treated as a problem, not an asset

The wrong people tend to be involved

- Rarely coming from security people directly
- Preparations without IT, Operations, Security, ..
- Result: Mixed understanding of goals
    - Plus: Misunderstood threat model - what about BEC?

It might be legal, but ..

- Especially since the pandemic, I've seen / heard about horrible ideas
  - Alleged bonus payments, cluster outbreaks, vaccine spots, ..
- Service providers are usually the worst offenders
  - Bonus points for: Consultant fresh out of school who drank the "Intelligence World"-juice

But the bad guys!

- Yes, the bad guys don't care about your feelings
- The bad guys are also more clever than this
    - They'll ask you to unsubscribe from an adult newsletter
- It's a fine line, don't tread it too hard

You shall (unfortunately) pass!

- Most phishing attacks originate from outside your perimeter
    - Talked to Red Teamers, DFIR people, even threat actors - yes, they do.
- Internal messages often circumvent protection mechanisms
    - Yes, there are issues with that.

Spotlight: My monster peeve

- We often tend to look at users the wrong way
- The elitism is crushing sometimes
- There's way too much smugness involved - unless for management

One more!

- If someone actually fell prey, this would be a security incident
- Incident response procedures, not security awareness procedures

So .. what have you actually achieved?

- Some statistics that aren't really useful in comparison to actual attack statistics
  - Plus: By themselves, those are snapshots
- Probably resentment, likely annoyance - future cooperation? Questionable.

Statistics you say?

- Disclaimer: This is based on (somewhat significant) anecdotal data
- ~20% of users gave up their credentials
- <10% of users reported, little overlap

y u no improve?

- More training, rewards, punitive measures, gamification
- Some short-term improvements, but no improvements where it mattered
- Yes, occasional improvements where made - but were they really caused by phishing tests?

existential crisis

- Changes everywhere *much* more helpful
  - Blocking hosts without rDNS helped wonders
  - Same goes for greylisting
  - Simplifying reporting was surprisingly effective as well
- Training didn't really, relatively consistent numbers
- Issues not just with execution, but principally?

No step forward, one step back

> "A phishing assessment is supposed to be a test for employees!"

...

> the means by which the presence, quality, or genuineness of anything is determined; a means of trial.

What are you testing for?

- If people detect bad mails? They won't, mostly.
    - If it were that easy, computers would do it.
- If people click on mails? Oh, they will.
    - Your own marketing department sees to that
- If people learned something from awareness training?
    - They have. And you'll still send them for more.

No matter how hard you try, you'll fail

No matter how hard you try, you'll fail

- Even *if* there are some improvements, there's still a gap
  - That "if" is a very big one
- The return on investment is small to begin with and decreases rapidly
- The investment is bigger than we think!

~~Money, money, money~~ Time, time, time (and money)

- 1+ meetings involved, including follow-up communication
  - If not done yourself: You will be dragged into more meetings
- Setting up the infrastructure, coming up with a lure, bugfixing
- Following up with users, preparing a report, winding down things
  - Guess what .. it smells like meetings!
  - Also people loathe you know.

Invest smartly

- <Insert a joke about Elon Musk here>
- Security will cost you - time, money, energy
- Why not invest it smartly? For example ..

You know what (generally) doesn't fail? 2FA

- Rolling out hardware-based 2FA is 🔥
  - But literally, every form of 2FA is better than nothing
  - Yes, even SMS-based 2FA
  - I'm willing to throw hands here
- It might be more costly than phishing tests, yes.
  - But the ROI is *actually* good
- This is just an example; a lot depends on your org

Is that a no to phishing assessments?

- In general: Yes. Staunchly so.
- Exception: Getting to know the situation
    - If you're tremendously successful, you have more than one issue
- The reality: They are likely here to stay, sadly.

If you have to do them, remember:

- Design them to teach, not to trick
- Encourage, don't embarass - less shaming, more reporting!
- Be creative
  - Let users create their own phishing mails
  - Use defanged phishing mails
  - Challenge your Red Teams
- If feasible: Push back against them!
  - No, they are not mandatory.

No, seriously

- No compliance framework mandates those!
    - PCI DSS, HIPAA, SOC2, ISO27001, ..
- Specific, typical example:

> “All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.”

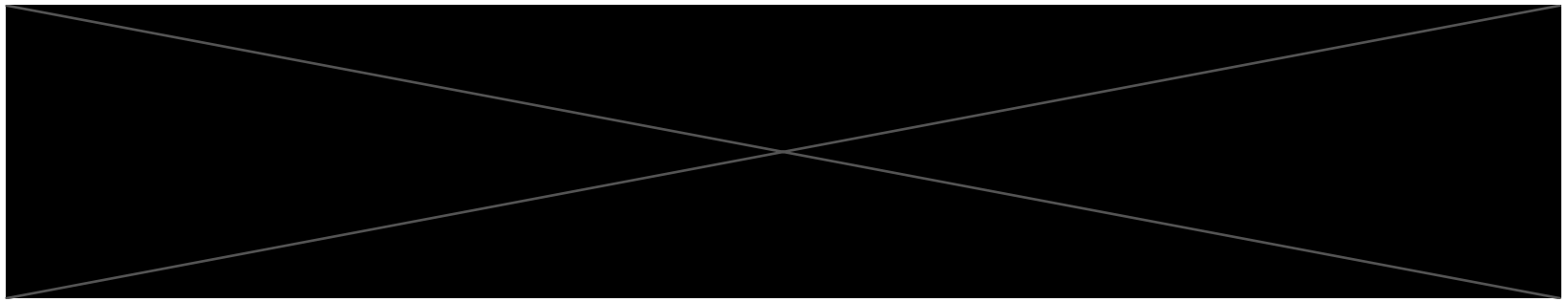
Smarter people are working on this!

- There is ongoing academic research, especially since 2020
- Very few broad studies, but preliminary results point in a similar direction
- Focus on US, Asia so far - anyone in need of a thesis topic?

Too long, waiting for beer

- Phishing assessments are generally not worth it
- There are better things to invest in (first)
- Stop shaming users. Right. fucking. now.

Thank you for your attention!



Questions?

&

Obligatory dog: