Cybersecurity Awareness on a Shoestring:

Practical Steps for Small Budgets

Presented by
501Secure

501Secure.org
Cybersecurity Assistance for Nonprofits

Presenter:

Kai Dailey,
Program Manager
501Secure

kai@501secure.org

Piper Center for Nonprofit and Civic Impact

501Secure.org
Cybersecurity Assistance for Nonprofits

Ragland Institute
Igniting Potential. Transforming Lives

Contact:
kai@501secure.org

Our Mission

We're a nonprofit organization of cybersecurity professionals dedicated to helping fellow nonprofits stay safe online.

Our Work

Cybersecurity Assessment & Policy Development

Live Cyber Safety Trainings & Awareness Program Management

1:1 Technical Mentoring for Admins on Cloud Application Security

Free Community Awareness Training & Resources

Core Tenants of Our Work

Radical Vendor Neutrality

Accessible Cyber Risk Literacy

Strategic Security Planning

Community Cyber Awareness

Data Privacy Week

January 26–30

National Cybersecurity Alliance

- Data Privacy Week – January
- Cybersecurity Awareness Month – October

Sign your organization up to be a champion at

www.staysafeonline.org

501Secure is a proud
Data Privacy Week Champion
Join Us!

Upcoming Events

25 March 2026

1:00 PM Pacific Free Online Event

Navigating Google Workspace Security Checklists for Admins

29 April 2026

1:00 PM Pacific Free Online Event

Managing Cybersecurity for Older Family Members

501secure.org/schedule

Awareness as a Professional Standard

Reading your organization to get clarity

- How do we measure awareness in a way that actually changes behavior?
- How do we choose tools when every vendor is promising a fix-all solution?
- How do we build a "cyber-aware" culture that feels like an extension of our values rather than a burden on them?

A different approach for nonprofits

Integrated Approach:

Security + Awareness + Compliance =

Whole-organization initiative

A different approach for nonprofits

Security, Awareness and Compliance in a single whole-organization initiative

- Technical controls and security behaviors integrated into everyday work.
- Participation and accountability are intentionally distributed across the organization, rather than assigned to one person.
- A shared security language is adopted.
- Roles and responsibilities are named and specific.
- Accountability activities are scheduled and regularly reviewed by leadership.

Security as a standard of practice for nonprofit professionals.

Standard of Practice

- ✓ Cybersecurity Hygiene + Awareness
- ✓ Secure business processes
- ✓ Accountability
- ✓ Regular oversight

Outcome: **Resilience**

Security vs. Resilience

Security	Mission Resilience
Prevention Building a wall high enough to keep the "bad actors" out.	*Survival* Ensuring the organization can take a hit and keep serving the community.
You are either "secure" or "compromised."	You are always in a state of prepared adaptation.
Technical Firewalls, passwords, and encryption.	*Holistic* Processes, culture, leadership, and backup systems.
Brittle When the wall is breached, security loses its integrity.	*Grace Under Pressure* When a component fails, the mission continues (there's "manual" backup).
Security asks: "How do we stop them from getting in?"	*Resilience asks:* "How do we keep feeding/housing/helping people if the system is down?"

Measuring Progress

Metrics that *really* matter

(when measuring ROI and program progress)

- Resilience + Durability (active business continuity plans in place and rehearsed)
- Reduction in the Number of Security Incidents

Case Study: A Nonprofit that tried something different

Goal: stop treating security as a peripheral task and start treating it as a core institutional value

- $5M budget
- 45 employees
- a dedicated IT team
- part-time initiative leader
- urban org

Nonprofit Self-talk

The things we tell ourselves about awareness, security, and compliance

We commonly treat cybersecurity as a technical chore. It isn't. It is an essential component of the invisible scaffolding of our work. You cannot have sustained impact without resilience.

Nonprofit Self-talk

When we expand our mission perspective to encompass the digital, online safety becomes instantly relevant to our work.

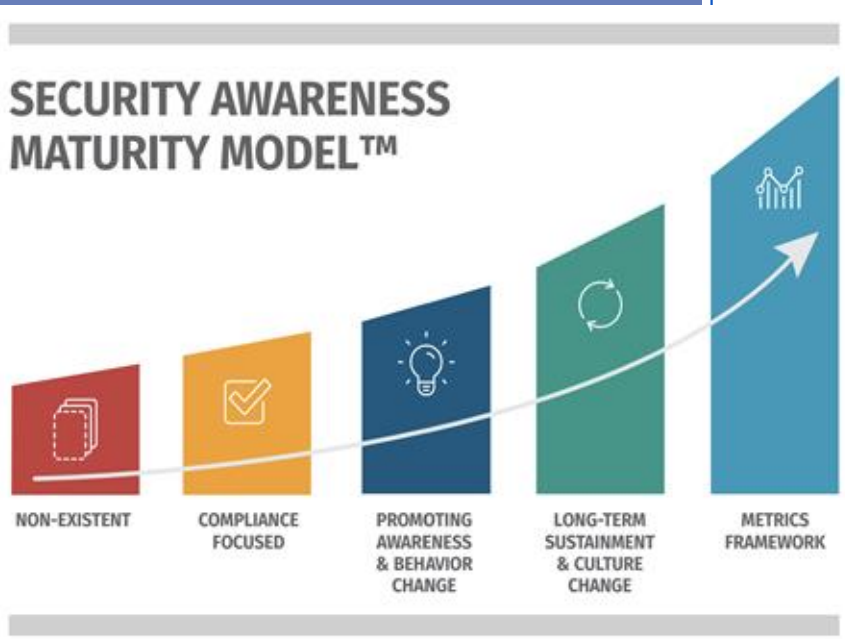
We are also stewards of the digital lives of the vulnerable.

Where is your organization currently choosing convenience over resilience?

Convenience	Resilience (Security Awareness as Standard Professional Practice)
Ease of access – Quick logins | No MFA	Integrated Cyber Hygiene into work processes
Shame and blame “Who clicked the link!”	Systems Thinking “Why was that link able to cause so much damage?"
No evaluation or approval process for vendor selection or SaaS sign ups.	Process for vendor and SaaS selection. Do vendors offer the minimum security controls? What are your three non-negotiables?
Ad-hoc awareness training or security discussions when something happens	Managed integrated program of security and awareness with measurable outcomes
Designated IT person handles security.	Whole organization stewardship

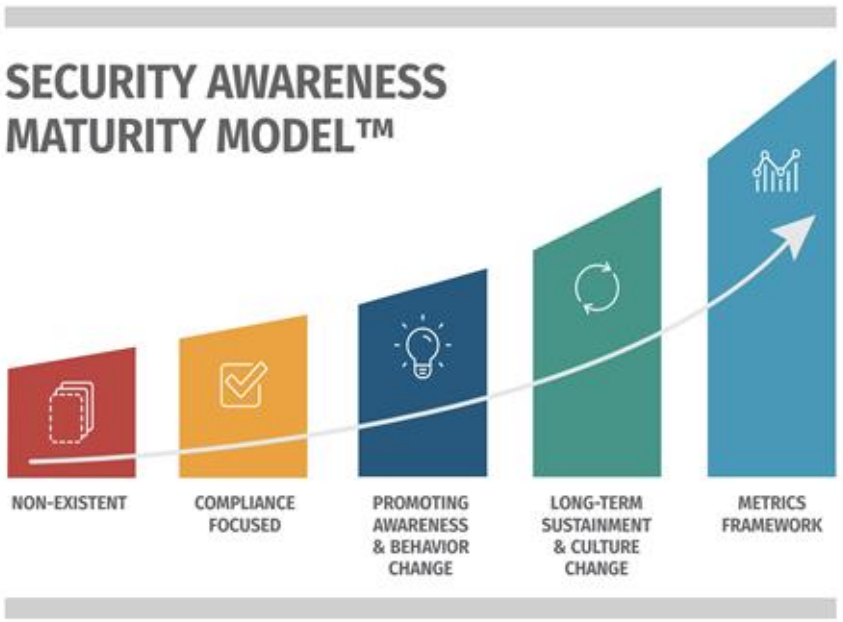
SANS Awareness Framework and Roadmap

Where does your organization currently sit on the SAMS Awareness maturity scale?



- **Non-Existent:** There is no formal awareness program. We rely on luck and hope our staff is naturally cautious.
- **Compliance Focused:** We do the annual training because a donor, grant, or insurance policy requires it. It’s viewed as a chore set apart from our real work.
- **Promoting Awareness & Change:** We go beyond the annual training videos. We send monthly tips or run phishing simulations. We’re trying to change how people think about their daily habits.
- **Long-Term Culture Change:** Security is now a shared value. It’s part of the onboarding process, it’s discussed in team meetings, and leadership models the behavior. It’s 'just how we do things here.'
- **Metrics & Framework:** We can actually prove it’s working. We track behavior change over time and use that data to refine our strategy and justify our mission-resilience budget.

Where does your organization currently sit on the Awareness maturity scale?



- **Non-Existent:** There is no formal awareness program. We rely on luck and hope our staff is naturally cautious.
- **Compliance Focused:** We do the annual training because a donor, grant, or insurance policy requires it. It's viewed as a chore set apart from our real work.
- **Promoting Awareness & Change:** We go beyond the annual training videos. We send monthly tips or run phishing simulations. We're trying to change how people think about their daily habits.
- **Long-Term Culture Change:** Security is now a shared value. It's part of the onboarding process, it's discussed in team meetings, and leadership models the behavior. It's 'just how we do things here.'
- **Metrics & Framework:** We can actually prove it's working. We track behavior change over time and use that data to refine our strategy and justify our mission-resilience budget.

Making a Plan

What does integration look like?

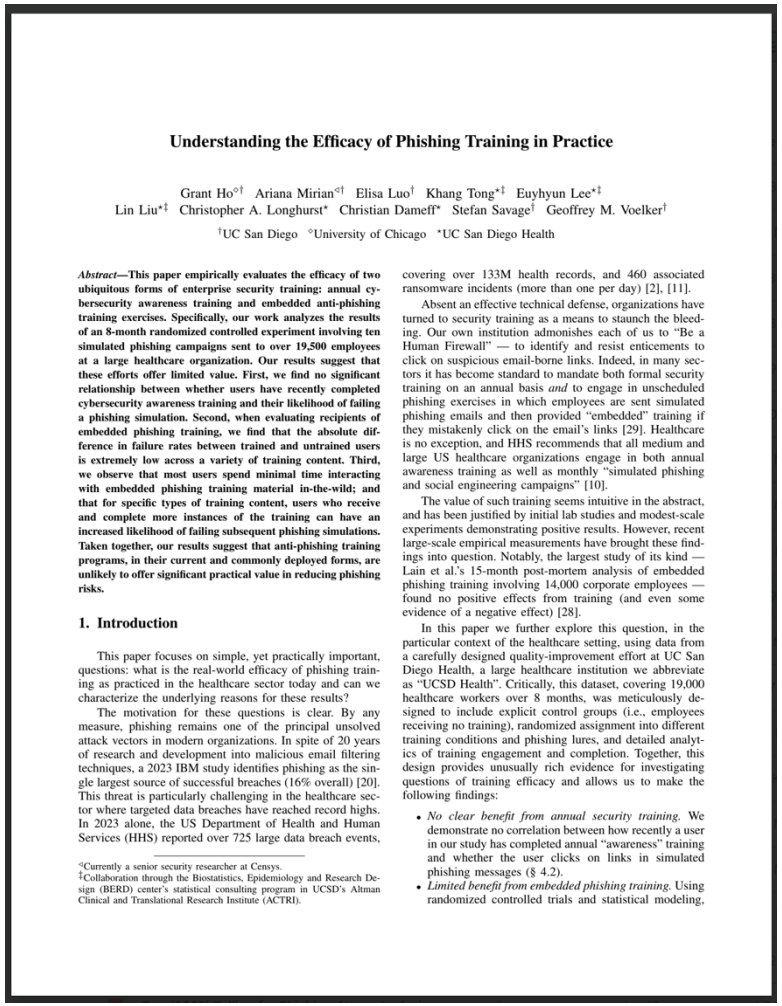
- Shared security awareness language
- Values-based “Why”
- Concrete actions of stewardship by all members of your team

Making a Plan

What does integration look like?

- Security is viewed through the lens of your organization values.
- Identify your assets, and select and prioritize what you defend
- Make a plan for defense, awareness, and compliance oversight.
- Use the process of implementing your plan and measuring its outcomes as an engine of awareness and cultural change.

Conflict in the data!



Understanding the Efficacy of Phishing Training in Practice

Grant Ho[◇†] Ariana Mirian[◇†] Elisa Luo[†] Khang Tong[⋆‡] Euyhyun Lee[⋆‡]
Lin Liu[⋆‡] Christopher A. Longhurst[⋆] Christian Dameff[⋆] Stefan Savage[†] Geoffrey M. Voelker[†]
[†]UC San Diego [◇]University of Chicago [⋆]UC San Diego Health

***Abstract*—This paper empirically evaluates the efficacy of two ubiquitous forms of enterprise security training: annual cybersecurity awareness training and embedded anti-phishing training exercises. Specifically, our work analyzes the results of an 8-month randomized controlled experiment involving ten simulated phishing campaigns sent to over 19,500 employees at a large healthcare organization. Our results suggest that these efforts offer limited value. First, we find no significant relationship between whether users have recently completed cybersecurity awareness training and their likelihood of failing a phishing simulation. Second, when evaluating recipients of embedded phishing training, we find that the absolute difference in failure rates between trained and untrained users is extremely low across a variety of training content. Third, we observe that most users spend minimal time interacting with embedded phishing training material in-the-wild; and that for specific types of training content, users who receive and complete more instances of the training can have an increased likelihood of failing subsequent phishing simulations. Taken together, our results suggest that anti-phishing training programs, in their current and commonly deployed forms, are unlikely to offer significant practical value in reducing phishing risks.**

1. Introduction

This paper focuses on simple, yet practically important, questions: what is the real-world efficacy of phishing training as practiced in the healthcare sector today and can we characterize the underlying reasons for these results?

The motivation for these questions is clear. By any measure, phishing remains one of the principal unsolved attack vectors in modern organizations. In spite of 20 years of research and development into malicious email filtering techniques, a 2023 IBM study identifies phishing as the single largest source of successful breaches (16% overall) [20]. This threat is particularly challenging in the healthcare sector where targeted data breaches have reached record highs. In 2023 alone, the US Department of Health and Human Services (HHS) reported over 725 large data breach events, covering over 133M health records, and 460 associated ransomware incidents (more than one per day) [2], [11].

Absent an effective technical defense, organizations have turned to security training as a means to staunch the bleeding. Our own institution admonishes each of us to "Be a Human Firewall" — to identify and resist enticements to click on suspicious email-borne links. Indeed, in many sectors it has become standard to mandate both formal security training on an annual basis *and* to engage in unscheduled phishing exercises in which employees are sent simulated phishing emails and then provided "embedded" training if they mistakenly click on the email's links [29]. Healthcare is no exception, and HHS recommends that all medium and large US healthcare organizations engage in both annual awareness training as well as monthly "simulated phishing and social engineering campaigns" [10].

The value of such training seems intuitive in the abstract, and has been justified by initial lab studies and modest-scale experiments demonstrating positive results. However, recent large-scale empirical measurements have brought these findings into question. Notably, the largest study of its kind — Lain et al.'s 15-month post-mortem analysis of embedded phishing training involving 14,000 corporate employees — found no positive effects from training (and even some evidence of a negative effect) [28].

In this paper we further explore this question, in the particular context of the healthcare setting, using data from a carefully designed quality-improvement effort at UC San Diego Health, a large healthcare institution we abbreviate as "UCSD Health". Critically, this dataset, covering 19,000 healthcare workers over 8 months, was meticulously designed to include explicit control groups (i.e., employees receiving no training), randomized assignment into different training conditions and phishing lures, and detailed analytics of training engagement and completion. Together, this design provides unusually rich evidence for investigating questions of training efficacy and allows us to make the following findings:

- *No clear benefit from annual security training.* We demonstrate no correlation between how recently a user in our study has completed annual "awareness" training and whether the user clicks on links in simulated phishing messages (§ 4.2).
- *Limited benefit from embedded phishing training.* Using randomized controlled trials and statistical modeling,

[◇]Currently a senior security researcher at Censys.
[‡]Collaboration through the Biostatistics, Epidemiology and Research Design (BERD) center's statistical consulting program in UCSD's Altman Clinical and Translational Research Institute (ACTRI).

Source:

G Ho, A Mirian, E Luo, K Tong, E Lee, L Liu… - 2025 IEEE Symposium on Security and Privacy (SP), 2025

An 8-month, large-scale analysis of 19,500 employees evaluating the efficacy of annual awareness and embedded phishing training.

- No significant relationship between completed cybersecurity awareness training likelihood of failing a phishing simulation.
- Whether or not phishing training was taken had little impact on future phishing test failure rates.
- Most users spend minimal time interacting with embedded phishing training material and for specific users more training increases likelihood of future phishing failures.
- Anti-phishing training programs, in their current and commonly deployed forms, don't reduce phishing risks.

Conflict in the data!

Bridging Cybersecurity Research Gaps through Meta-Analysis: State of the Art and Future Directions

Chola Chhetri
Northern Virginia Community College
Annandale, VA, USA
cchhetri@nvcc.edu

Abstract

Meta-analysis is a rigorous statistical technique that integrates findings from multiple independent studies addressing the same research question to produce more accurate, comprehensive, and generalizable results. It has been extensively applied in fields such as medicine, psychology, education, and environmental science to resolve inconsistencies, advance evidence-based practice, and guide policy and research. Despite its potential to synthesize diverse outcomes, clarify human factors such as cognitive biases that affect security behavior, and assess training effectiveness, meta-analyses remain scarce in cybersecurity and cybersecurity education. Increasing adoption of meta-analytical methods in cybersecurity could yield stronger, data-driven insights to improve risk management, enhance training outcomes, and strengthen the resilience and readiness of cybersecurity professionals.

CCS Concepts

• **Social and professional topics** → **Computational thinking**; • **Security and privacy**;

Keywords

Meta-analysis, Meta-analyses, Cybersecurity, Cybersecurity Education, Systematic, Analysis, Cyber Security, Education.

ACM Reference Format:

Chola Chhetri. 2025. Bridging Cybersecurity Research Gaps through Meta-Analysis: State of the Art and Future Directions. In *26th Annual ACM Conference on Cybersecurity and Information Technology Education (ACM SIGCITE 2025), November 06–08, 2025, Sacramento, CA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3769694.3771152

1 Introduction to Meta-Analysis

Meta-analysis is the study of studies. It is a quantitative research method that systematically integrates findings from multiple independent studies investigating a common research question. By statistically combining results, it improves statistical power, yields more precise estimates of effect size, and helps to resolve heterogeneity or conflicting findings among primary studies [10]. It improves the generalizability of conclusions, identifies broader trends or gaps in the literature, and supports evidence-based decision-making in both research and policy [3]. It provides objective and transparent evaluation of existing research, reducing bias and conserving resources by obviating the need for new large-scale studies.[7].

The roots of meta-analysis trace back to Karl Pearson's 1904 quantitative synthesis of clinical data on typhoid inoculation, which influenced public health policies [8]. It was formally established in 1978 by Smith and Glass in their study on psychotherapy effectiveness and recognized as a rigorous statistical tool to synthesize empirical evidence [12]. Since then, it has been widely adopted across disciplines such as medicine, psychology, and social sciences, shaping policy and guiding evidence-based practice.

However, in cybersecurity, the systematic use of meta-analysis remains emergent. This paper explores how meta-analysis can strengthen the field by consolidating fragmented and diverse studies, thereby building a stronger scientific foundation. By reviewing a selection of existing cybersecurity meta-analyses, it highlights contributions to evidence-based practice, examines current challenges and research gaps, and outlines directions for future studies. Ultimately, meta-analysis holds significant potential to advance cybersecurity by informing more effective practices and policies in response to an increasingly complex and rapidly evolving threat landscape.

2 Meta-Analyses in Cybersecurity

This section describes several meta-analyses that have been conducted in the field of cybersecurity to synthesize empirical evidence about human factors and interventions in cybersecurity.

2.1 The Impact of Training on Cybersecurity Attitudes, Knowledge, and Behavior

A meta-analysis of 55 articles reveals that training interventions generally have a strong positive impact on end-users, as reflected by a moderate to large effect size (d = 0.75, 95% CI [0.58, 0.92]). This positive effect is even more pronounced when the measured outcomes are *predictors* or *precursors* of end-user behavior, such as attitudes or knowledge, where the effect size is large (d = 1.02, 95% CI [0.58, 1.46]), indicating that training is particularly effective in improving what users know and how they feel about cybersecurity. However, when it comes to actual *behavior* change, the effect is much smaller and statistically inconclusive (d = 0.36, 95% CI [−0.09, 0.80]), suggesting that improvements in knowledge and attitudes do not necessarily translate into safer or more secure behaviors. This discrepancy reveals a significant weakness in current training programs: while they successfully enhance users' perceptions, they do not result in robust, empirically verified changes in cybersecurity-related behaviors [9].

ACM SIGCITE 2025, Sacramento, CA, USA

ACM ISBN 979-8-4007-2240-0/25/11
https://doi.org/10.1145/3769694.3771152

Source:

Chhetri, C. (2025, November). Bridging Cybersecurity Research Gaps through Meta-Analysis: State of the Art and Future Directions. In *Proceedings of the 26th ACM Annual Conference on Cybersecurity & Information Technology Education* (pp. 301-302)..

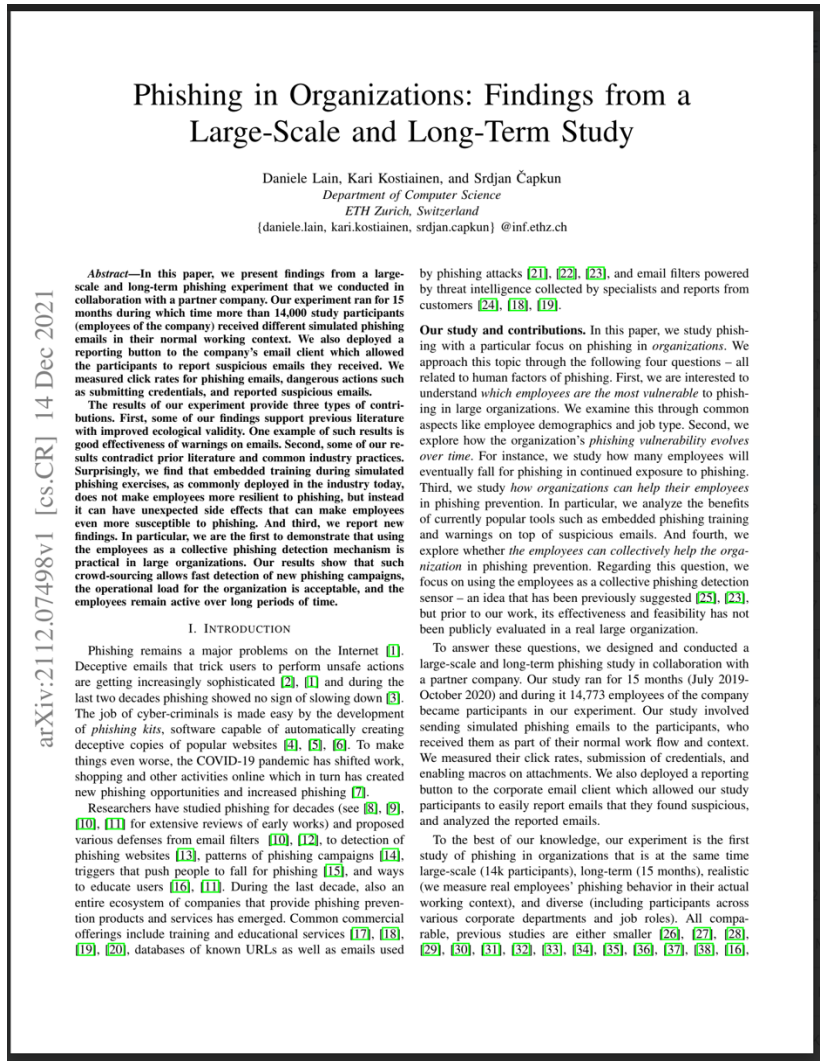
Question: What is the Impact of Training on Cybersecurity Attitudes, Knowledge, and Behavior

Looked at the findings from 55 independent studies completed over the last five years addressing the same research question regarding cybersecurity education.

☑ Effective at improving cybersecurity attitudes and knowledge

☒ Ineffective at changing risky behaviors

Conflict in the data!



Phishing in Organizations: Findings from a Large-Scale and Long-Term Study

Daniele Lain, Kari Kostiainen, and Srdjan Čapkun
Department of Computer Science
ETH Zurich, Switzerland
{daniele.lain, kari.kostiainen, srdjan.capkun} @inf.ethz.ch

***Abstract*—In this paper, we present findings from a large-scale and long-term phishing experiment that we conducted in collaboration with a partner company. Our experiment ran for 15 months during which time more than 14,000 study participants (employees of the company) received different simulated phishing emails in their normal working context. We also deployed a reporting button to the company's email client which allowed the participants to report suspicious emails they received. We measured click rates for phishing emails, dangerous actions such as submitting credentials, and reported suspicious emails.**

The results of our experiment provide three types of contributions. First, some of our findings support previous literature with improved ecological validity. One example of such results is good effectiveness of warnings on emails. Second, some of our results contradict prior literature and common industry practices. Surprisingly, we find that embedded training during simulated phishing exercises, as commonly deployed in the industry today, does not make employees more resilient to phishing, but instead it can have unexpected side effects that can make employees even more susceptible to phishing. And third, we report new findings. In particular, we are the first to demonstrate that using the employees as a collective phishing detection mechanism is practical in large organizations. Our results show that such crowd-sourcing allows fast detection of new phishing campaigns, the operational load for the organization is acceptable, and the employees remain active over long periods of time.

I. Introduction

Phishing remains a major problems on the Internet [1]. Deceptive emails that trick users to perform unsafe actions are getting increasingly sophisticated [2], [1] and during the last two decades phishing showed no sign of slowing down [3]. The job of cyber-criminals is made easy by the development of *phishing kits*, software capable of automatically creating deceptive copies of popular websites [4], [5], [6]. To make things even worse, the COVID-19 pandemic has shifted work, shopping and other activities online which in turn has created new phishing opportunities and increased phishing [7].

Researchers have studied phishing for decades (see [8], [9], [10], [11] for extensive reviews of early works) and proposed various defenses from email filters [10], [12], to detection of phishing websites [13], patterns of phishing campaigns [14], triggers that push people to fall for phishing [15], and ways to educate users [16], [11]. During the last decade, also an entire ecosystem of companies that provide phishing prevention products and services has emerged. Common commercial offerings include training and educational services [17], [18], [19], [20], databases of known URLs as well as emails used by phishing attacks [21], [22], [23], and email filters powered by threat intelligence collected by specialists and reports from customers [24], [18], [19].

Our study and contributions. In this paper, we study phishing with a particular focus on phishing in *organizations*. We approach this topic through the following four questions – all related to human factors of phishing. First, we are interested to understand *which employees are the most vulnerable* to phishing in large organizations. We examine this through common aspects like employee demographics and job type. Second, we explore how the organization's *phishing vulnerability evolves over time*. For instance, we study how many employees will eventually fall for phishing in continued exposure to phishing. Third, we study *how organizations can help their employees* in phishing prevention. In particular, we analyze the benefits of currently popular tools such as embedded phishing training and warnings on top of suspicious emails. And fourth, we explore whether *the employees can collectively help the organization* in phishing prevention. Regarding this question, we focus on using the employees as a collective phishing detection sensor – an idea that has been previously suggested [25], [23], but prior to our work, its effectiveness and feasibility has not been publicly evaluated in a real large organization.

To answer these questions, we designed and conducted a large-scale and long-term phishing study in collaboration with a partner company. Our study ran for 15 months (July 2019-October 2020) and during it 14,773 employees of the company became participants in our experiment. Our study involved sending simulated phishing emails to the participants, who received them as part of their normal work flow and context. We measured their click rates, submission of credentials, and enabling macros on attachments. We also deployed a reporting button to the corporate email client which allowed our study participants to easily report emails that they found suspicious, and analyzed the reported emails.

To the best of our knowledge, our experiment is the first study of phishing in organizations that is at the same time large-scale (14k participants), long-term (15 months), realistic (we measure real employees' phishing behavior in their actual working context), and diverse (including participants across various corporate departments and job roles). All comparable, previous studies are either smaller [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [16],

Source:

Lain, D., Kostiainen, K., & Čapkun, S. (2022, May). Phishing in organizations: Findings from a large-scale and long-term study. In 2022 IEEE Symposium on Security and Privacy (SP) (pp. 842-859). IEEE.

A 15-month large-scale study investigating employee vulnerability, warnings, and collective detection mechanisms at company with 14,000 employees.

- Warning labels on emails reduce risk.
- Embedded training during simulated phishing exercises don't make employees more resilient to phishing.
- Employee crowd-sourcing of phishing using a reporting button facilitates fast detection of new phishing campaigns and employees remain engaged over a long period of time.

Conflict in the data!

Conclusions:

1) Reporting a phishing simulation is **not** a reliable proxy for preventing security incidents.

2) Standard automated approaches to awareness training **do not** prevent security incidents.

What is the benefit of security awareness?

Resilience

- Shortening the time between “the click” and the response
- Risk reduction
- Limiting the severity of incidents
- Staff trained and ready to respond when an incident occurs

Case Study: A Nonprofit that tried something different

Awareness Journey First Steps:

- All team members completed Cybersecurity 101 training to learn the basics of cyber hygiene and cyber risk
- Crowdsourced an inventory of data, devices, processes, and compliance responsibilities
- Asked “How will a compromise impact us?”
- Organically raised awareness at all levels of the organization

What are assets?

WHAT TO INCLUDE IN YOUR DATA INVENTORY

Knowledge

Documents
Databases
Media files
Knowledge Base

Tools

Software
Hardware
Cloud accounts
Social media accounts

Include your compliance responsibilities for state, regulatory agencies, contracts, and government partners.

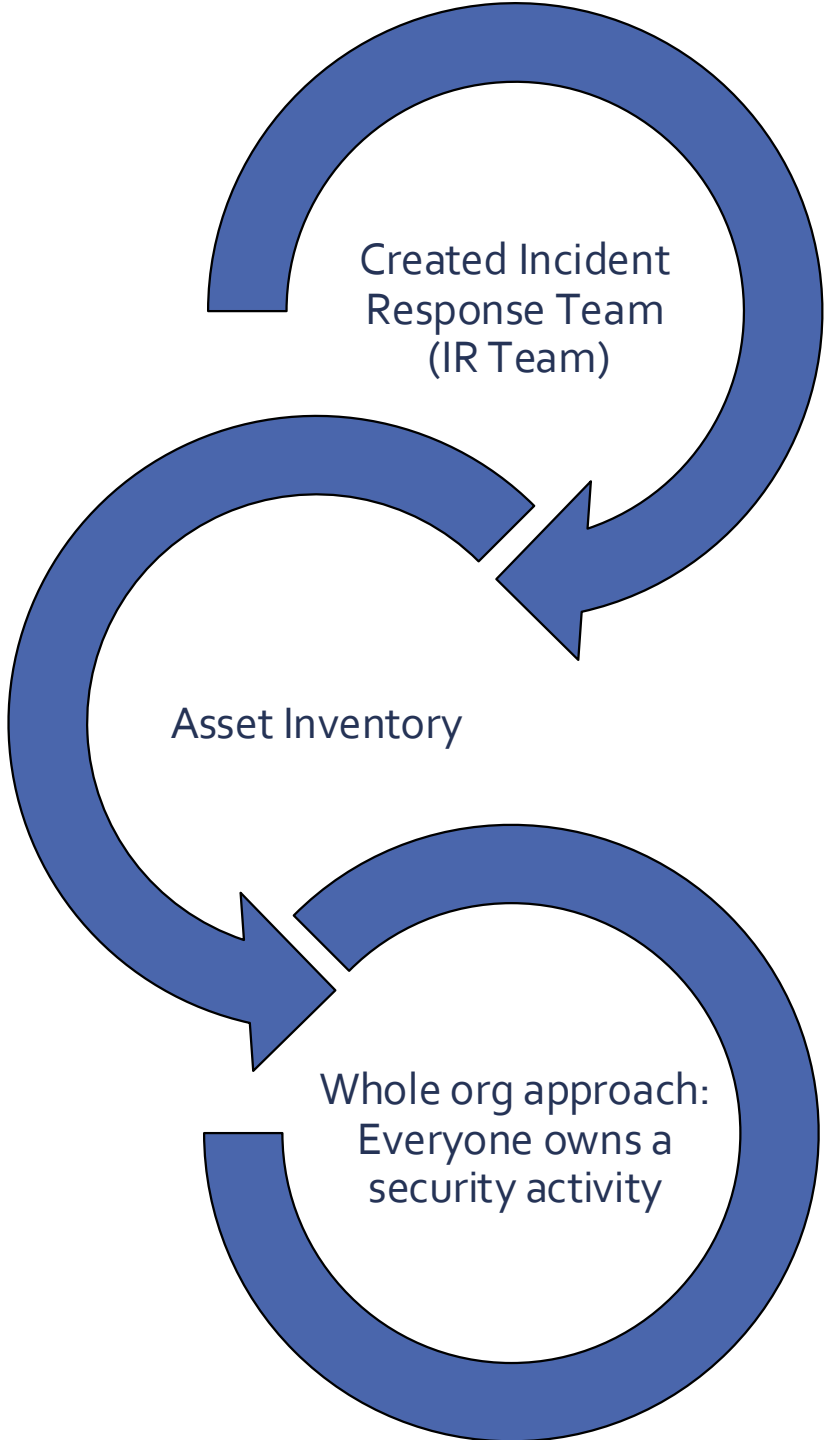
Processes critical to providing essential functions

Reporting
Email
Newsletters

Payroll
Invoicing
Donation Processing

Data Inventory Template

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
									STEP 1								
											DATA						
Asset Owner (Program or Individual)	**Description of Data Asset**	**Data Elements Y/N**															
		Personally Identifiable Information							**System Logs**		**Legally Protected Data**						
		Personal Name	Tel #	Address	SSN	DOB	DL	Other	Is system log reviewed and/or stored?	List application managed by Program for which system usage is stored. Who has access?	PHI	FERPA	HIPPA	Financial	HR / Payroll	Other	Sensitive data - professional history, religious beliefs, ethnicity, political opinions or organization memberships (trade union, political, etc.), sexual life & orientation, genetic or biometric information
								Describe		Describe							Describe
EXAMPLE IN ROW: Volunteer applications	Volunteer application form is shared as PDF via email. Volunteer fills out the form and attaches to return email. Applications from prospective volunteers contain PII. We store all applications regardless of current volunteer status. Do we need to revisit our retention policy for this data?	Y	Y	Y	N	Y	N	Email address, family contact information. Work and volunteer history.	Y	Google Workspace. Workspace admin.	N	N	N	N	N		Volunteers often share personal narratives in their applications which may reveal sensitive details about them.
Additional Data Assets																	


Created Incident Response Team (IR Team)
Asset Inventory
Whole org approach: Everyone owns a security activity

Every staff member owns a security activity.

The Role of Executive Leadership

Visible support for the security program

Establishing security roles and teams

- Resource Owner
- Data Steward
- Incident Response Team
  - Communication Plan
  - Legal Obligations
  - Business Continuity
  - Lead incident response

Case Study:
A Nonprofit that tried something different

Resource Owner

- Anyone who has admin access to online platforms and SaaS
- Add users and adjust access privileges
- Regularly monitor logins and account activity (e.g., downloads or user permission changes)
- Stay current on security best practices
- Use security features available to security accounts and data

Case Study:
A Nonprofit that tried something different

Data Steward (or digital steward)

- Everyone in an organization, including volunteers, contractors, board members, and leadership
- Anyone with access to your organization's systems, accounts, or data
- Consistently practice Cyber Hygiene
- Ensure device safety
- Adhere to data entry practices
- Complete assigned safety trainings by deadline

Case Study:
A Nonprofit that tried something different

Incident Response Team (IR Team)

- A cross-functional team with representatives for IT, HR, operations, leadership, communications, legal, outside vendors and partners
- Maintain a holistic view of institutional survival
- Resilience planning + leads incident response:
  - communication
  - legal
  - business continuity
  - incident response playbooks
- Initially met monthly
- Served informally as awareness and security champions

An
Asset Inventory is an Essential Resource!

Uses for an asset inventory

- Reference and a working document
- Training and awareness opportunity
- Basis for creating policies
- Tool for adapting an industry recognized cybersecurity framework
- Communication tool for vendors, regulators, funders
- Assists with succession planning
- Guides security incident recovery
- It’s a living document

Making the most of what you have

Cyber Hygiene

Low cost. Built into most of the commercial platforms and SaaS subscriptions.

- MFA
- Unique, long passphrases
- Identity management
- Conditional access for devices
- Limiting access to sensitive data and platforms
- Anti-malware on devices
- Using security settings available on the platforms in use
- Protocols for requesting and approving financial transactions
- Backups and recovery testing
- Regularly log out of accounts and clear browser cache
- Keep software updated

Your mission is too important to leave its security to chance.

Q&A

Contact Kai Dailey, Program Manager

kai@501Secure.org

Thank you for attending!

501Secure.org

Cybersecurity Assistance for Nonprofits