

**UC Tech Awards 2023 Candidate**

**Category:** IT SECURITY
**Name:** Phishing Simulation Initiative (8)
**Number of people:** (8)
**Location:** UC San Diego Health

1. **Person submitting the application/nomination**
	1. Christian Dameff MD, MS, FACEP**,** Assistant Professor of Emergency Medicine, Biomedical Informatics, and Computer Science (Faculty)
	2. **Email address:** cdameff@health.ucsd.edu
	3. **The name of your organization:** UC San Diego Health
2. **Award category**

IT Security

1. **Name of person, name of the team, or name of the project to receive the award**

Phishing Simulation Initiative

1. **All project team members - if applicable**

Faculty:

* Christopher Longhurst MD, MS, Chief Medical Officer, Chief Digital Officer, UC San Diego Health, Associate Dean, UC San Diego School of Medicine, clonghurst@health.ucsd.edu
* Christian Dameff MD, MS, FACEP**,** Assistant Professor of Emergency Medicine, Biomedical Informatics, and Computer Science, UC San Diego Health, cdameff@health.ucsd.edu
* Stefan Savage, PhD, Professor, Department of Computer Science and Engineering, UC San Diego, ssavage@ucsd.edu
* Geoffrey Voelker PhD, Professor, Department of Computer Science and Engineering, UC San Diego, voelker@cs.ucsd.edu

Staff:

* Scott Currie, Chief Information Security Officer, UC San Diego Health, gscurrie@health.ucsd.edu
* Ken Wottge, Information Security Director, UC San Diego Health, kwottge@health.ucsd.edu
* Ariana Mirian PhD, ITS Security Researcher, UC San Diego
* Grant Ho PhD, Postdoctoral Fellow, UC San Diego, grho@ucsd.edu
1. **Which location was affected by the work?** (the name(s) of the organization affected)

UC San Diego Health

1. **Summary:** Healthcare cyber-attacks can be costly, disruptive, and dangerous to organizations and patients. Increasing the resilience of employees to phishing attacks using never before collected data can greatly increase the defenses of hospitals and make everyone more cyber safe. UC San Diego Health’s innovative approach to evaluating the effectiveness of phishing training will help to develop the most effective phishing simulation and training program for staff awareness.
2. **Narrative**

Cyber-attacks on healthcare systems have been increasing in frequency and severity over the last 20 years. E-mail phishing poses unique threats to healthcare because every employee of the health system needs to be vigilant and trained to identify, isolate, and report phishing attacks. Success of just one phishing attack can lead to breaches of protected health information and/or devastating attacks like ransomware which can devastate important clinical care of patients. Currently there is not much data on how best to train, monitor, and remediate employees who fail phishing exercises or fall victim to actual attacks.

UC San Diego Health (UCSDH) faces hundreds of phishing attacks daily directed at our enterprise. Some of these have resulted in official breach notifications to university leadership, patients, and federal government agencies. The reputational damage as well as monetary fines on hospital systems nationwide are significant and annually cost millions of dollars.

UCSDH developed a unique phishing simulation initiative that aims to identify characteristics common with staff members who repeatedly fail our test exercises and/or fall victim to actual phishing attacks. In order to evaluate the effectiveness of training techniques UCSDH randomized staff into groups who were given phishes of varying difficulty. Within each group, different training was delivered to allow us to assess over time the most effective approach to cybersecurity awareness training. The overall goal of this program is to test phishing mitigation strategies to identify the most effective tools, training, and remediation efforts that will result in long term success at reducing the risks associated with phishing attacks.

One measurable goal we established is the reduction in the failure rate of our monthly “mock” phishing exercises. We proposed a goal of reducing the click through rate to below 8%. To accomplish this, we are trying to better understand the commonalities among staff who fall victim develop and implement mitigations and measure the effectiveness. This builds an evidence base to make informed decisions and establish best practices around mitigating healthcare phishing attack risk reduction. The failure rate is measured and monitored using an existing tool already in deployment at UCSDH. This tool allows us to see who, when, and how employees interact with simulated phishing tests.

This work was started in the fall of 2022 (October) with our first monthly simulated phishing campaign starting in January 2023. The work is expected to conclude by the end of 2023.

The work on this project was incredibly complex and spanned several disciplines including psychology, engineering, and healthcare delivery. The impact this work has on increasing healthcare’s resilience to phishing and other cyber-attacks is significant. Beyond the monetary losses, risks to patient safety due to delayed or degraded care are present anytime you disrupt time sensitive complex clinical care, which has been increasingly dependent on technology over the last thirty years.