CYBERSECURITY ESSENTIALS FOR PHILANTHROPY

CASE STUDY: How Our Organizations Provide Security Awareness Training

Published on June 26, 2019

Calvin Lewis, Director of IT Infrastructure & Operations, Cleveland Foundation
Oleg Bell, Global Head of IT Security, Open Society Foundations

Technology Affinity Group

One North State Street, Suite 1500
Chicago, IL 60602

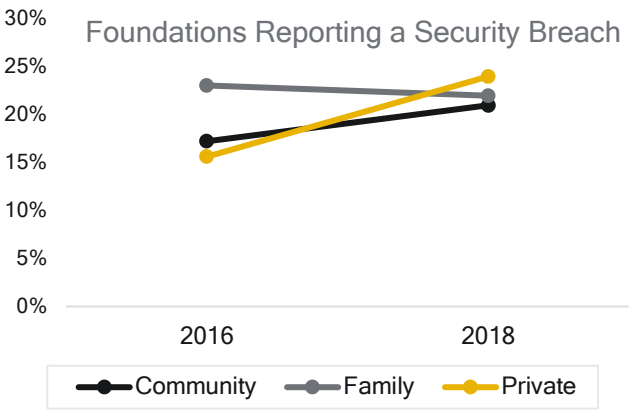
info@tagtech.org

OVERVIEW

PRAGMATIC INSIGHT FROM IT LEADERS IN PHILANTHROPY

Executives in philanthropy are increasingly concerned about cybersecurity. Phishing attacks are weekly, if not daily, and the stakes of a breach are high. In spite of our best attempts as a sector to develop robust practices, 21% of respondents to TAG's 2018 State of Philanthropy Tech survey reported experiencing a security breach in the past two years. For private independent foundations, the breach rate was even higher at 24%. No wonder there's growing concern.

Through the *CyberSecurity Essentials for Philanthropy* series, we aim to reduce your organization's risk and establish best practices throughout the sector.



Source: 2018 State of Philanthropy Tech Survey, available at http://www.tagtech.org/philanthropytech2018.

The practices and suggestions shared here are those of your peers at philanthropic organizations throughout North America. Their on-the-ground knowledge forms the basis for an invaluable set of best practices. On behalf of the members and directors of the Technology Affinity Group, we're grateful for the thought leadership generously shared by this publication's authors.

JAMES R. RUTT
Chief Information Officer, Dana Foundation
President, Board of Directors, Technology Affinity Group

CHANTAL E. FORSTER
Executive Director, Technology Affinity Group

BRINGING CYBERSECURITY AWARENESS TO PHILANTHROPY

This case study answers the question: *What does security look like at mid-sized foundations*?

> **With attacks occurring daily in our interconnected digital world, every network enabled device is vulnerable. Foundations have the same security concerns as businesses and face the same threats to sensitive information.**

Together with peers at foundations similar to yours, we've written this case study to provide pragmatic strategies and real-world tactics based on our everyday experience as IT leaders. In this case study, you'll find:

1. Data on cybersecurity threats to foundations
2. How your staff is critical to cybersecurity defense
3. Resources and examples on how to approach your cybersecurity training

Let's get started.

The Challenge

COMBATTING CYBERCRIMINALS

Philanthropic organizations are increasingly becoming targets of cybercriminals; Open Society Foundations and the Cleveland Foundation know this all too well. In our experience, email presents the largest threat and the biggest risk for our organizations.

> **In 2018 1.6 million email messages traversed the Cleveland Foundation's email system. Of those 1.6 million messages, more than 40 thousand were phishing emails.**

Technology safeguards provide adequate protection for most phishing attempts, but it is not a failsafe, and unfortunately a small number of phishing emails occasionally evade our defenses and arrive in our end-user's inbox. To combat this, both organizations have implemented cybersecurity training and awareness programs to help staff learn how to detect and report phishing attempts.

The assumption is that awareness will improve staff's ability to recognize potentially malicious emails and reduce their likelihood to fall for such attacks. Although the programs are met with positive feedback from staff, we are still presented with the challenge of consistently achieving 100% participation of staff in completing the training, reporting all phishing attempts, and continuously reducing our click rates.

The Strategy

BUILDING A HUMAN FIREWALL

As part of the cybersecurity training and awareness programs, Open Society Foundations emphasizes creating an open and positive culture of security threat reporting. By recognizing that no one is perfect and by setting up reasonable thresholds and positive reinforcement mechanisms, IT is able to both decrease risk exposure to phish attacks, as well as dramatically increase attack reporting by staff. **Positive reinforcement, coupled with education and measurement, has enabled us to build a human firewall.**

We no longer deem staff as a liability, at Open Society Foundations, but rather, we look to them as a partner in detecting cyber-attacks that our technology systems miss. The staff are our "canary in the mineshaft" and the most effective early detection and alert system.

The Approach

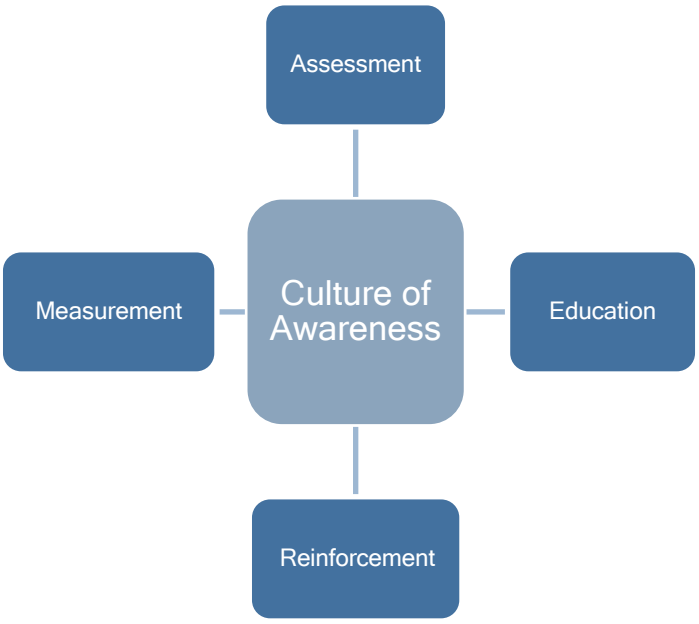
CONTINUOUS TRAINING

Training is key in building our "human firewall." Both Open Society Foundations and Cleveland Foundation prioritize a wide variety of training and simulation programs.

Training Approach at Cleveland Foundation

At the Cleveland Foundation, we assessed various phishing simulation and training service providers on the market, and selected Wombat Security, a division of Proofpoint. Cleveland Foundation chose Wombat for three reasons:

1. Innovation put them ahead of anything else on the market.
2. Their approach aligned with the culture of the organization.
3. Their continuous training methodology, which consists of assessment (via phish simulations), education (via training modules), reinforcement (via library of images, articles and posters on security awareness), and measurement (via reporting on strengths and weakness) helps to increase learning and creates a culture of awareness.



In terms of specific products, Cleveland Foundation uses Wombat's "Anti-Phishing Training Suite", which combines customizable "Threat Sim Phishing Simulations", interactive training modules, and significant business intelligence and reporting tools.

Cleveland Foundation assigns training every other month and conducts phishing simulations continuously throughout the year.

Training Approach at Open Society Foundations

In contrast, Open Society Foundations (OSF) uses both in-house and subscription materials. As a baseline, Open Society Foundations uses in-house created training materials that are short, easy to digest, and that are frequently assigned to users. Additionally, we utilize simulation training via "PhishMe" which emphasizes "showing" rather than "telling" about social engineering risks. **Industry data suggests that such behavioral awareness programs can reduce the organization's risk by 3X, by reducing click rates from 40 percent to between 10-15 percent.** While by no means a total mitigation of the risk, this decrease is considerable and significant. It's also worth noting that this training is accessible to most mid-sized foundations as PhishMe offers its basic product for free for up to 100 users.

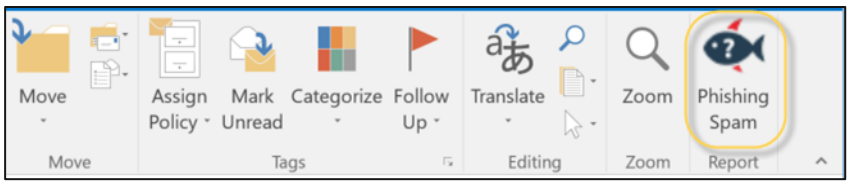
Open Society Foundations conducts on average between 12 and 15 training simulations per year.

Most of our training simulations at OSF focus on the entire organization across the board, while a few focus on high risk departments and groups such as accounts payable or payroll and benefits teams.

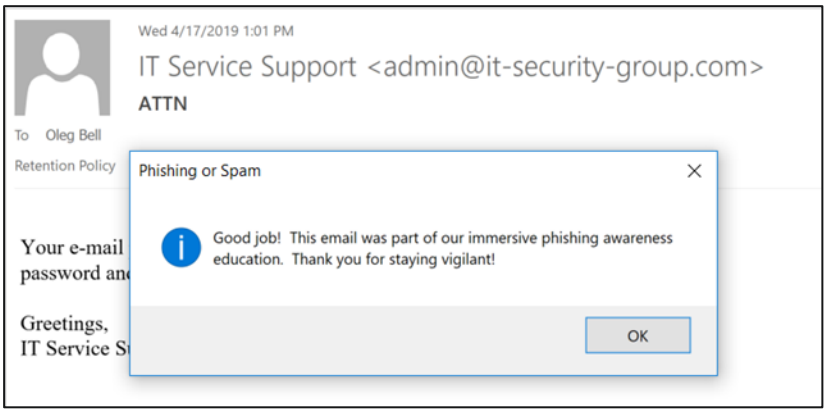
MAKE REPORTING EASY & FUN

Over the years at OSF, we have conducted over 150 phishing email simulations, and yet 5-10 percent of our users continue to fall for the phishing tests. However, **both Cleveland Foundation and OSF have experienced a significant increase in staff reporting phishing attempts.** We believe this is due, not only to continuous training, but also because we focus on making reporting easy and fun.

PhishMe and Wombat, for example, make it easy to report suspicious emails with an Outlook add-in that enables a simple one-click reporting mechanism. Staff reports any spam/phishing message by clicking a button on their Outlook ribbon. The reported messages are automatically removed from the user's mailbox and forwarded to IT Security for analysis.



The user receives instant feedback by using the Outlook button, and IT staff are committed to rapid follow-up for any messages that the staff are reporting.



The Outlook "phishing" button also enables us to collect backend statistics on how fast and how frequently each staff member reports phishing simulation exercises as well as whether they click on the phishing link, report it, or both. OSF gathers these metrics on a quarterly basis and we publish them across the organization as part of the challenge we call "King of Phish".

Each quarter, the department with highest phish reporting rate becomes the "King of Phish" and is publicly recognized.

In addition to the recognition, the IT Security team spends time with each "King of Phish" to celebrate their challenge victory and arranges refreshments for team members while running through the performance metrics for their team, pointing out their team MVPs and fastest reports. The grand prize for the winning team is the ability to skip next year's mandatory IT Security training. Making such an exception for our best and fastest reporters is the best recognition of their efforts and positive reinforcement that everyone appreciates. It is highly motivating for our staff to receive special treatment from the IT security team.

Such recognition and teambuilding also builds trust and a positive relationship between staff and the IT Security team. **Establishing this open and trustworthy relationship is what enables our staff to engage without the fear of being penalized if they miss reporting a cyber-attack or fall for one.** Such willingness to come forward and report attacks is crucial for OSF to leverage; the "human firewall" is the next line of defense against cyberattacks that slip through our email filters and firewalls.

> **Our staff is the best firewall we can ask for as well as our last line of defense that can never be replaced by technology. We appreciate their efforts and willingness to partner with IT Security and treat them as such.**

Even with a culture of positive reinforcement, both OSF and Cleveland Foundation feel that our security awareness training is never over. When 90% of incidences and breaches included a phishing element[1], security training is a simply a service we will offer for the foreseeable future and beyond.

RESOURCES

Below are links to the tools and resources referenced in this document:

- Request a free trial of Cofense for under 100 users: https://cofense.com/cbfree/
- Wombat Security
- PhishMe
- [1] https://www.phishingbox.com/resources/phishing-facts

ABOUT THE AUTHORS

CALVIN LEWIS

Director of IT Infrastructure & Operations
Cleveland Foundation

https://www.linkedin.com/in/calvin-lewis-1264894b/

Calvin brings more than 20 years of IT experience, including security, communications, infrastructure, and operating systems. Prior to joining the Cleveland Foundation, Calvin worked as an IT Manager, Enterprise Network Services for Forest City Enterprises, were he was responsible for leading a team tasked with resource planning, technical leadership, management, cost center ownership and the complete operation of a network consisting of approximately 165 sites distributed across the US, including their corporate headquarters.

Calvin earned his Bachelor of Arts in psychology, graduating Magna Cum Laude, from Ursuline College in Pepper Pike, Ohio.

OLEG BELL

Global Head of IT Security
Open Society Foundations

https://www.linkedin.com/in/oleg-bell-23b03a1/

For the past seven years, Oleg has been busy building the security program at OSF from scratch, all while navigating constant attention from APT actors. Honed by daily exposure to malware and regular incident response working shoulder to shoulder with leading forensic and threat intelligence vendors, Oleg knows the cybercriminal perspective well. Prior to leading the security team, Oleg has spent ten years with OSF IT Operations and Infrastructure teams, working to expand the global network spanning over a dozen countries and time zones and serving two thousand staff.

Oleg also serves as a Vice President and is a founding board member of NGO-ISAC, an intelligence sharing community that enables the NGO sector to communicate cyber-attack information coordinate incident response and promote cyber security best practices. He holds a BS in Computer Science and an MBA in Strategic Management from the Lubin School of Business in NY.

ABOUT THIS SERIES

The *CyberSecurity Essentials for Philanthropy* series launched in 2019 is provided by the Technology Affinity Group (TAG) in partnership with member organizations and private sector advisors.

View the full curriculum available for the series at: tagtech.org/cybersecurity

This is an educational publication and is not intended as legal advice. You should contact your attorney for legal advice. The opinions expressed here are the opinions of the individual authors and may not represent the opinions of their employers or of TAG.

TAG CYBERSECURITY WORKING GROUP

This work is led on a volunteer basis by the TAG Cybersecurity Working Group whose members include the following:

Jim Rutt (Chair), Dana Foundation
John Mohr, The MacArthur Foundation
Oleg Bell, Open Society Foundations
Karen Graham, Idealware
Darlene Ott, The Winnipeg Foundation
Dan Callahan, CGNET
Calvin Lewis, Cleveland Foundation
Christopher Jean-Pierre, Wellspring Philanthropic Fund
Steve Jarboe, Accenture
Anthony Putignano, Wizehive
Charles Boname, Vancouver Foundation

FUNDING PROVIDED BY

This series is funded in part through an award from the Robert Wood Johnson Foundation President's Grant Fund at the Princeton Area Community Foundation.