

Partner Use Case

AES

 Education

Starting point

Founded in 1981, AES is a multinational energy company with the mission to accelerate the future of energy, together. Powered by a global workforce of more than 8,400 people, we have more than 31 Gigawatts in operation and serve 2.6 million utility customers across 14 countries and 4 continents. AES is an industry leader in developing and growing the solutions that will enable the transition to low-carbon sources of energy and achieve the Paris Agreement’s goal of net-zero emissions by 2050.

At AES, safety is our first value and one way that our global workforce lives out that value is to put safety first in cyberspace. For many connected workers, the most important thing they can do is to recognize and report a cyber-attack. Our global cybersecurity team provides the framework and resources for awareness and training so that each local business can communicate the importance of cybersecurity.

To increase cybersecurity awareness, AES conducted phishing tests with its people. However, we recognized that our messages were not breaking through and creating the desired results. AES people did not report our phishing messages, or they clicked them. Overall, only 15-20% of the company interacted with our phishing tests. We knew we had to drive up engagement to increase awareness.

Objectives

Our goal was to increase the cybersecurity awareness of AES people by implementing a new and innovative training model that drives engagement.

Description

We decided to take a more individualized approach to phish training through a platform that creates learning paths for each individual. Like many organizations, AES relies on an external phishing simulation platform to carry out the testing. Both our old and new approaches compare as follows:

	Legacy systems	New model
Training	Annual training in separate environments	Continuous training in Outlook
Personalization	Same for everyone	Individualized
Engagement	Broadcast info to AES people	Engage AES people
Operations	Manual	Automatic
Mindset	Security awareness	Behavior change





The premise of our program is to teach each individual to be a Cyber Role Model. The idea is that we all need to take proactive steps to improve our collective digital safety and defense. Society has never been more connected, work has blended with home like never before, and protecting ourselves in the digital realm is as important as protecting ourselves physically.

To enable AES employees to be Cyber Role Models, we gave our people a set of six central recommendations – we call them the “**Cyber 6**”. These recommendations outline specific actions so our people can protect themselves, their families, and the company wherever they connect:

- 1 Secure your accounts:** Use unique, complex passphrases and enable two-factor authentication wherever possible.
- 2 Know your network:** Protect your home network by changing default passwords. Use a VPN when conducting sensitive transactions or on public WiFi.
- 3 Share data responsibly:** Use only AES-approved collaboration sites like OneDrive. Control your social media settings and be mindful when posting publicly.
- 4 Think before you click** on a link, file, or attachment on your laptop and mobile. Use the Report this email button in Outlook.
- 5 Protect your device:** Patch your devices regularly and do not connect unauthorized hardware like USB drives.
- 6 Be safe by being prepared:** Know the cyber-attack types and report anything suspicious.

Lessons learned/results

Moving to a “gamification” model for phishing training drove quantitative and qualitative engagement. It also successfully encouraged AES people to become Cyber Role Models. We paired a number of activities with the new technology to drive engagement further and accelerate the deployment of our new cyber awareness model, including:

-  Review of a monthly phish in each safety meeting
-  Communication of the leaderboard dashboard and recognition of high performers (star collectors) via monthly safety meetings and internal communication channels
-  Opportunities for behavior improvement via an increased volume of phishing simulations and one-on-one engagement
-  Utilization of communication channels to re-enforce awareness and training through micro-doses of information