VERSION 2.0

MAY 26, 2018

COFENSE

EMAIL SECURITY INTIATIVE SUMMARY PLAN

PRESENTED BY:

STANISLAUS STATE, OFFICE OF INFORMATION TECHNOLOGY (OIT)

VISION AND MISSION OF STANISLAUS STATE

VISION

Stanislaus State strives to become a major center of learning, intellectual pursuit, artistic excellence and cultural engagement for California's Greater Central Valley and beyond. We will serve our diverse student body, communities and state by creating programs, partnerships and leaders that respond effectively to an evolving and interconnected world.

MISSION

The faculty, staff, administrators, and students of Stanislaus State are committed to creating a learning environment which encourages all members of the campus community to expand their intellectual, creative, and social horizons. We challenge one another to realize our potential, to appreciate and contribute to the enrichment of our diverse community, and to develop a passion for lifelong learning. To facilitate this mission, we promote academic excellence in the teaching and scholarly activities of our faculty, encourage personalized student learning, foster interactions and partnerships with our surrounding communities, and provide opportunities for the intellectual, cultural, and artistic enrichment of the region.

OFFICE OF INFORMATION TECHNOLOGY

The faculty, staff, administrators, and students of Stanislaus State are committed to creating a learning environment which encourages all members of the campus community to expand their intellectual, creative, and social horizons. We challenge one another to realize our potential, to appreciate and contribute to the enrichment of our diverse community, and to develop a passion for lifelong learning. To facilitate this mission, we promote academic excellence in the teaching and scholarly activities of our faculty, encourage personalized student learning, foster interactions and partnerships with our surrounding communities, and provide opportunities for the intellectual, cultural, and artistic enrichment of the region.

COFENSE REPORTER IMPLEMENTATION

Roll out in computer replacement program via imaging, 2018.

STAN STATE PHISHING AWARENESS PROGRAM

Social engineering via email to steal login credentials or install malicious software is a quick, low cost way for attackers to gain access to an organizations digital infrastructure and data. Stan State addressed this risk with technology, process, training, and awareness.

TECHNOLOGY

Stan State employs mail-filtering resources to identify spam and malicious email traffic. Identity detection/protection services block traffic to known sources of malicious software.

PROCESS

When targeted phishing messages do make it through the technical controls listed above the Support Center crafts and distributes awareness emails to warn the campus community. The messages include details of how to spot the offending message.

TRAINING & AWARENESS

Stan State has access to Cofense, (formerly PhishMe), a service that provides testing and training related to email threats. Stan State periodically tests the employee population's ability to spot and avoid phishing and other malicious unsolicited email threats. The tool provides in the moment training for those who do not recognize the risk associated with a message. This allows us to test the whole population but only deliver training to those in need and demonstrate a reduction in risk. In-depth training content from Cofense is available in SkillSoft and for assignment to individuals or groups.

TESTING PROCESS VIA COFENSE

Phishing campaigns are conducted quarterly using the following process:

1. T-14 days – pick campaign templates
2. T-7 days – send pre-campaign reminder with tips for spotting malicious email
3. T-0 – send the phishing campaign
4. T+7 days – collect campaign stats, craft post-campaign results and how the message could have been spotted based on live campaign
5. T+10 days send post-campaign update