CSU CCC UC

THE CALIFORNIA STATE UNIVERSITY

CSU SYSTEMWIDE ANTI-PHISHING CAMPAIGN

FOCUS ON EFFICIENCY

Phishing exposes the higher education community to malware, risk and liability. It targets executives and staff members alike. By reducing susceptibility to these attacks we reduce costs, raise awareness and enhance our information security.

Targeted of 'spear' phishing has been on the rise in higher education. In the CSU, these attacks have targeted campus and system executives, and staff members in critical roles such as HR, benefits and finance. By raising awareness through educational campaigns and including positive reinforcement, we have reduced risk, lowered the costs associated with the loss of system availability and productivity, and increased overall information security.

OPPORTUNITIES AND SOLUTIONS

Success at the Chancellor's Office (CO) has led to increased participation systemwide, reduced susceptibility and increased reporting. Campuses are targeting efforts to business units and job titles that are at higher risk or demonstrate increased susceptibility. We are increasing the complexity of attack simulations as our constituents are becoming more savvy.

QUANTIFICATION AND RESULTS

In the February 2016 Valentine's Day Campaign, 27 percent of Chancellor's Office users clicked or were susceptible; 11 users reported the Phishing attempt; and 45 percent of users in a critical CO business unit were susceptible.

In the April 2016 Scanner Phish Campaign, 24 percent of the CO clicked or were susceptible; 70 users reported the phishing attempt; and 36 percent of users in a critical CO business unit were susceptible, for a nine percent reduction. Participation increased from 7 to 18 of the CSU campuses.

PhishFood Ice Cream and Goldfish crackers were used as rewards and recognition for business units reducing their overall susceptibility ratings.

IMPACT AND BENEFIT

Increasing awareness and resistance to these attacks reduces cost and lost time and productivity due to responding to attacks. We are expanding the PhishMe effort to include more than twice the number of CSU campuses.

MILESTONES

Jul 2016	• Purchase by 18 campuses.
May 2016	• Compromise of 10 HR systems at CSU campuses.
Apr 2016	• Ransomware at CSU Campus via phishing.
Feb 2016	• Valentine's Day Campaign.
May 2015	• Original purchase of PhishMe by Chancellor's Office and 7 campuses .
Jan 2015	• Identification of issues and receipt of notices.

QUALITY, COST OR DELIVERY

Reduced costs in responding to compromised systems by reducing the number of successful phishing attacks. An example is the successful phishing attack at one campus, which comprised ten systems that processed payroll. Systems were down for three days.

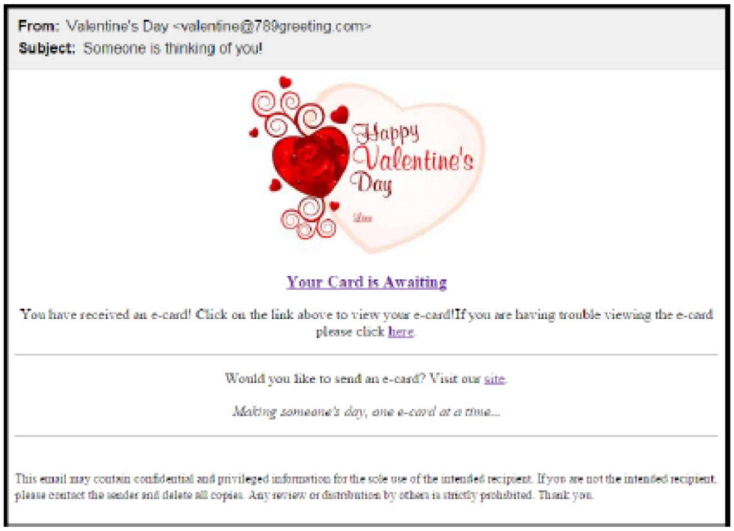
Ten systems down for three days equals 80 staff hours lost. Cost for outside incident management was $15,000; staff time to re-image systems at 70 systems times three equals 210 tech hours necessary to re-image infected systems. Secondary stand-alone systems purchased included 20 trusted connections for the State Controller's Office. Ten Ironkey secure drives were issued at a cost of $200 each, for a total of $2,000.

PROJECT TEAM

William Perry
Chief Information Security Officer

Edward Hudson
director of Systemwide
Information Security

Campus Information Security Officers



From: Valentine's Day <valentine@789greeting.com>
Subject: Someone is thinking of you!

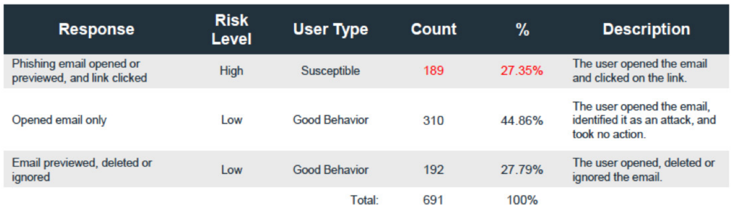
Your Card is Awaiting

You have received an e-card! Click on the link above to view your e-card!If you are having trouble viewing the e-card please click here.

Would you like to send an e-card? Visit our site.

Making someone's day, one e-card at a time...

This email may contain confidential and privileged information for the sole use of the intended recipient. If you are not the intended recipient, please contact the sender and delete all copies. Any review or distribution by others is strictly prohibited. Thank you.



Response	Risk Level	User Type	Count	%	Description
Phishing email opened or previewed, and link clicked	High	Susceptible	189	27.35%	The user opened the email and clicked on the link.
Opened email only	Low	Good Behavior	310	44.86%	The user opened the email, identified it as an attack, and took no action.
Email previewed, deleted or ignored	Low	Good Behavior	192	27.79%	The user opened, deleted or ignored the email.
		Total:	691	100%	