digitaldefense
by HelpSystems

USE CASE *(Cybersecurity)*

Security Awareness Case Study
People First Federal Credit Union

Digital Defense Helps Build a Culture of Security through Innovative Security Training

Situation Analysis:

TThe landscape of organizations across the country and the way business is conducted has changed dramatically over the last decade. New technologies have added tremendous efficiencies and methods for communicating, and corporations have benefitted from these innovations. However, there have been disturbing increases nationally in the number of attacks through criminal activities - be it cyber or onsite infiltration. People First FCU recognized that adhering to regulatory compliance does not always equate to security. In an effort to provide world-class service, as well as to ensure confidential client information remains secure, People First FCU contracted independent remote and onsite social engineering assessments.

Understanding that the modern criminal preys on the human element as a weakness, common undercover ploys were developed and executed to determine the organization's susceptibility to potential exploitation. The results identified vulnerabilities within the organization and revealed the need for corporate wide security awareness, crucial to mitigating future risks.

Testing the Security Posture of the Organization: Social Engineering Assessments

Social Engineering Assessment Methodology:

Onsite and remote social engineering engagements examined the effectiveness of the existing education and awareness programs, challenging the security posture of the institution's workforce.

AT-A-GLANCE

People First
Federal Credit Union

People First Federal Credit Union (FCUJ Background

People First FCU is a federally chartered and insured credit union offering financial services for over 60 years. As a non-profit financial cooperative, it is owned and operated by its members. With over $400 million in assets and over 51,000 members, People First Federal Credit Union's mission is to operate in a financially sound and competitive manner to ensure long-term financial stability while safeguarding member assets.

The security risk assessment methodology involved four phases, each phase conducted by a certified security analyst.

1 . Reconnaissance

2. Analysis

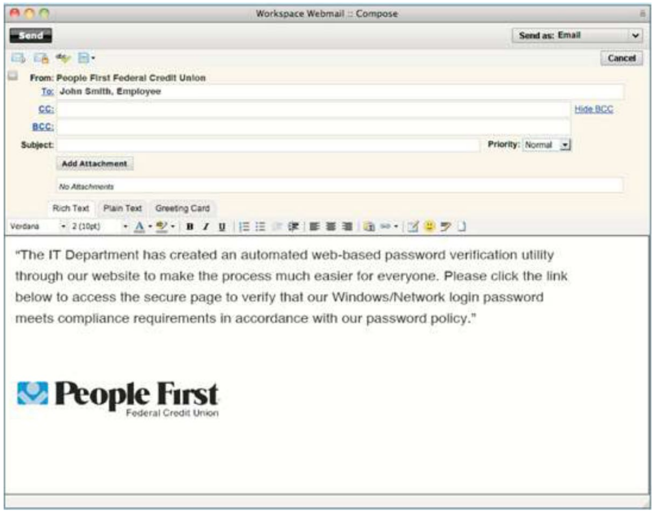
3. Penetration

4. Reporting

The engagement objective was to infiltrate the corporation and access confidential information through phishing attacks and onsite intrusions. Based on the success rate of achieving the objectives, People First FCU received a performance report for both of the social engineering risk assessments.

Remote Social Engineering Methodology

People First FCU employees were sent an email from the organization's Vice President/CID with phrasing, font and email signature to appear authentic. The pseudo email directed employees to a link and requested network login details to test the strength of the recipient's password.



Send as: Email

From: People First Federal Credit Union

To: John Smith, Employee

Priority: Normal

No Attachments

"The IT Department has created an automated web-based password verification utility through our website to make the process much easier for everyone. Please click the link below to access the secure page to verify that our Windows/Network login password meets compliance requirements in accordance with our password policy."

> ***"People First FCU employees were susceptible to the devious phishing attack. Many employees accessed the mock web page - an entry point to facilitating a larger security lapse - disclosing sensitive information upon request."***
>
> - Social Engineering Risk Assessment Analyst

"I don't get many emails from the CIO so when I received the email asking to test the strength of my password, I stopped what I was doing and quickly followed the instructions. I was so happy my password passed the test, I sent a note to management stating 'Didn't know if I had to let you know but my password passed the test, yea!' However, when I found out it was a scam, I was mortified. I felt like I was doing my job, but instead, I was giving away my password information and putting myself and my company at risk."

- D. K. Asset Recovery Clerk. Social Engineering Target

"Employees are encouraged to respect the request of senior management and to have a 'team mentality' offering help when needed . Social engineers take advantage of today's employee by creating ruses that appear to be legitimate, but in actuality are schemes to gain physical or informational access."

- Tom DeSot, DOI - EVP /Chief Information Officer

The overwhelming response to the well-crafted, staged email identified a weakness that, if leveraged by a social engineer. could result in damage to both the institution's reputation and bottom line.

Results of Remote Social Engineering Analysis:

FAIR

Information security controls were vulnerable to skilled penetration.

Onsite Social Engineering Methodology

During the engagement, the security analyst attempted to gain unauthorized entry to secure areas of People First FCU offices and network equipment. Posing as an employee of a large telecom provider, with badges easily created with basic office tools, the analyst attempted admittance. Prepared for potential questions the analyst was ready to explain the he was there as a contractor for technical system upgrades.

The analyst easily gained entrance into the building and was able to confiscate a 'Visitor' badge. The ruse, including an imitation telecommunications vendor badge, coupled with the People First FCU Visitor badge, elicited credibility for the analyst. This credibility was leveraged to infiltrate the organization's multiple financial branches in the region. Preying upon the inherent human 'trust' factor, at many of the locations, the analyst was greeted warmly and escorted to secure communication areas, then left alone to complete his tasks.

In one scenario, however, a suspicious employee followed company policy only to be misled with incorrect internal authentication:

"Our normal procedure is for the branches to receive a call or an email providing advance notice when a contracted technician may be coming onsite. I hadn't received notification prior to the telecommunications imposter approaching me. I reached out to our IT team to confirm his legitimacy, and when I confirmed he had a People First visitor's badge, I was given the approval to allow the man to conduct his work. I led him to the back room and left him there to complete his tasks."

- L. S., Branch Manger

Results of Onsite Social Engineering Analysis:

POOR

Security controls were affected by easily exploitable vulnerabilities and required minimal or no in-depth skills to exploit a weakness. The analyst was able to gain access to restricted areas through piggybacking techniques at the initial corporate location.

"Piggybacking describes the act of an unauthorized person who follows someone to a restricted area without the consent of the authorized person. "

Over 85% of the employees fall victim to this staged social engineering attack.

Security Awarness Training: A Smart Solution

Solution:

With disconcerting results, Susan Phillips, Vice President/CID, understood the need for improved security awareness. In an effort to build a culture of security, Phillips evaluated the existing corporate security training program. Confronted with proof that regulatory compliance and annual security training programs were insufficient, she began researching security training programs in the marketplace. Following a review of multiple programs, Phillips was concerned the vast majority would be perceived by employees as tedious or boring and essentially be ineffective. When Phillips was introduced to SecurED™ , she was intrigued by the unique approach.

> ***"Everyone was shocked at the results of the social engineering testing. We knew we had to do something! We understand the importance of education based on performance and were excited about SecurED because of the DD expert analysis on the training topics as well as the unique ."***
>
> twist - comic relief

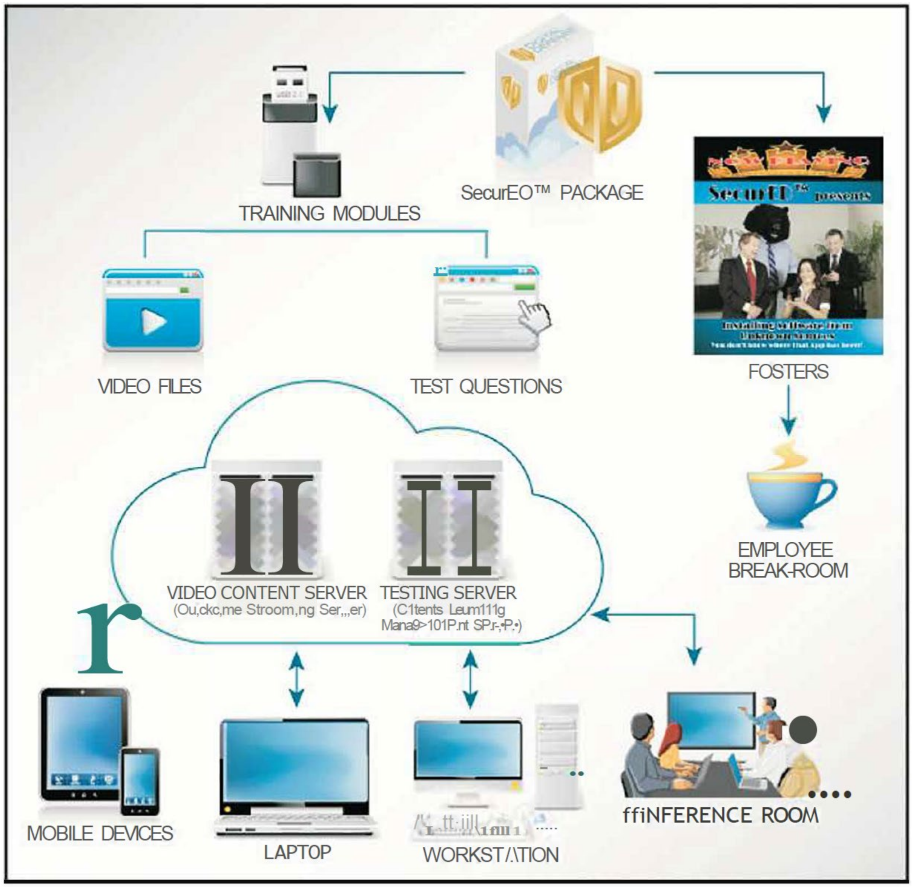
Employee Feedback of SecurED Training:

> ***"Absolutely excellent!"***
>
> ***"Very informative."***
>
> ***"I found myself taking notes not just for work but also for my personal use."***
>
> ***"The training was on basic topics but seemed to be more in-depth than what we have seen in the past."***

> ***"Quite interesting"***
>
> ***"I like to learn and this made learning fun!"***
>
> ***"I thought the bear was funny. Very out of the ordinary."***
>
> ***"Helpful and entertaining"***

SecurED ™

SecurED is a new, innovative security awareness education program developed by Digital Defense in collaboration with an Emmy® award winning comedy sketch writer. The training videos feature fun, engaging characters to leverage the "stickiness factor" required to optimize employee retention of serious security intelligence and best practices.



Implementation

The first step in the corporate security campaign was to create excitement. Anticipation was generated by posting SecurEO posters in the corporate training room. These posters effectively attracted attention generating questions prior to the scheduled training.

Training was introduced company-wide with required participation. Seven of the 12 available modules were selected based on the findings uncovered in the Social Engineering assessments:

- Acceptable Use of Computer Systems
- Onsite Social Engineering
- Password Development
- & Security
- Preventing Virus & Malware Outbreaks
- Remote Social Engineering
- Safe Web-Browsing Habits
- Social Media Dangers

The security training videos were viewed and test questions were distributed with the expectation of a mandatory pass rate.

SecurED: Success from a Smart Investment

Measuring Success

After completion of the security training, an onsite and remote social engineering assessment was conducted for the second time. The objective of the test was to measure the effectiveness of the training and take the pulse of the organization's security posture.

Investing in security training to address potential compromises and raise employee awareness proved to be valuable.

Excellent - No weaknesses were found in the employee information security awareness controls, and employees appear to be following information security best practices. An attacker would find it difficult to socially engineer employees into disclosing sensitive information.

> ***"Our team found it extremely difficult to infiltrate the organization even with our most advanced techniques engaged."***
>
> \- Social Engineering Analyst

	Fall 2012 Results	SecurED Training	Spring 2013 Results
Onsite Social Engineering Assessment	**POOR**	✓	**Excellent**
Remote Social Engineering Assessment	**FAIR**	✓	**Excellent**

SecurED Proves to be a Sound Investment

Return on Investment (ROI)

The ROI of a security education program designed to increase awareness and mitigate risk is measured by reducing the possibility of a data breach. The investment in ODI's SecurED training program proved to be a wise investment. The cost analysis below illustrates this value by comparing the cost of the program to the savings realized by avoiding a single breach.

Cyber crime continues to be costly. The average annualized cost of cyber crime is $8. 9 million per year, with a range of $1 .4 million to $46 million*.

The ROI is based on the following assumptions:

- People First FCU services 50,000+ members
- One data breach could potentially compromise the personal and protected information of all 50,000+ members
- Average cost of U.S. data breach is $188 per capita*
- Average cost of SecurED training program based on less then 250 employees

Customer Records Potentially at Risk	50,000
Potential Cost of a Single Breach	$9,400,000
Cost of SecurED Program (based on less than 250 employees)	$3,000
% Return on Investment	313,000% More Than 3000x

*2013 Cost of A Data Breach: Global Analysis - Ponemon Institute© Sponsored by Symantec

Security Awareness has never been more important.

Reduce Your Risk.

Build a Culture of Security.

digitaldefense
by HelpSystems

www.digitaldefense.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.