SECURITY AWARENESS TRAINING AT VFS

Securing the business by securing the human.

Awareness Training Need

Data is our business. Our users are the easiest gateway to our business and our data.

- Our employees are more connected than ever before.
- We have more business partners and suppliers that can be used as attack vectors than we ever have.
- Attacking us is cheap compared to the potential return.
- There are global criminal organizations at work whose purpose is to attack companies regardless of size.

People are the largest vulnerability:

- People like to help and that helpfulness can be exploited by knowledgeable adversaries.
- There are thousands of attack vectors (phone calls, insecure Wi-Fi, e-mail, hacked iPhone apps, unsafe websites, e-mail, to name a few) and most of them involve people.
- People make mistakes that can lead to unintended consequences. Changing behaviors through training can help reduce the number of mistakes.

Phishing Training Need

Phishing e-mails are the primary entry point for hackers into organizations

- Most users are vulnerable because they do not spend enough time to discern the intention of an e-mail and have not been trained how to identify dangerous e-mails
- Phishing e-mails are much simpler and more effective than other means of hacking- our users are trained to be helpful to customers and our kindness makes us more trusting

Phishing e-mails can lead to:

- Unauthorized network access by external attackers
  - The compromised computer could be used as a “pivot point” to other internal network resources like databases or file shares
  - Attackers could install other, more persistent and undetectable data stealing malware
  - Remote Access Trojans (RAT) allow remote control of a user’s computer
  - Banking trojans look for bank account information to send to the hacker
- Installation of ransomware or other malware that could cause damage to normal operations

The occurrence of phishing e-mails has been increasing rapidly at VFS and attacks are becoming more common. Most phishing e-mails we receive now are meant to harvest user credentials for use in future attacks.

Awareness Training Structure

Phishing E-mail Simulator

- Largest threat vector
- Affects all employees
- Provides instantaneous feedback to the employee
- The training is like a game, so it's fun and therefore memorable
- Training is short and to the point
- Can be tied to incentives to improve based on results
- Simulations are in 70 local languages

"Securing the Human" General Security Awareness

- Covers broader security topics
- Very inexpensive
- Many short training modules that can be added or removed to be customized to company need
- E-learning can be interactive or not- can include quizzes with reporting capabilities
- Can include printed materials and other offline tools

Awareness Training Results

Phishing E-mail Simulator Outcomes

- Employees will be more attentive to e-mail threats and able to recognize suspicious e-mails more easily
- Reduced potential for malware or credential theft
- Provides statistics and measurable results
- Can include a mechanism for employees to report suspicious e-mails to IT

“Securing the Human” Outcomes

- Employees will have a better understanding of many security threats
- Employees will learn actions to take to counter those threats
- Quizzes can be used to reinforce the message and evaluate comprehension
- The company’s general “situational awareness” baseline is improved; employees are more aware of their digital surroundings
- The information is effective in both personal and work environments and the consistency improves results for the company

Additional Awareness Tools and Opportunities

- Monthly newsletter
- Targeted e-mails to employees when specific threats are encountered
- Violin posts about specific topics
- Printed materials in employee gathering areas
- In-person training sessions
- Video-driven messaging
- Special events (Security Day?)