pennsylvania
OFFICE OF ADMINISTRATION

Security Awareness & Acceptable Use Training

Information Security:
SECURITY AWARENESS & ACCEPTABLE USE
This course is intended for all users of commonwealth IT resources.

Nominating Category: Cybersecurity
State: Pennsylvania

Nominator:
John MacMillan
Chief Information Officer
Commonwealth of Pennsylvania
1 Technology Park
Harrisburg, PA 17110
717-772-4240
jmacmillan@pa.gov

Initiation: June 2017
Completion: December 2017

Executive Summary

Over the years, numerous technology advances have improved the ability of organizations to prevent and respond to cyber-attacks. However, the greatest risk to most organizations continues to be their own employees. Malicious websites, phishing emails, social engineering and the loss or theft of mobile devices or credentials are just a few of the ways an employee can unwittingly allow cyber criminals to infiltrate the organization and potentially access sensitive information.

In 2017, Pennsylvania launched a brand-new security awareness and acceptable use training for its 80,000 employees and contractors.

While the previous training was effective in delivering the course content in an easy-to-understand way, the click-through format allowed them to advance through the training without necessarily paying attention to the content.

With the frequency and sophistication of cyber threats constantly growing, Pennsylvania recognized that its training needed a dramatic overhaul. Using gamification, interactive elements and other techniques, the new training is designed to more effectively engage end users and ensure that learning objectives are being achieved.

In late 2017, Pennsylvania conducted a phishing email exercise with an embedded “malicious” link that was clicked on by a percentage of recipients. A similar exercise conducted in 2018 after deployment of the new training was conducted. As a result, there was a significantly reduction in click rate from the preceding year by 38%. What makes this result even more remarkable is that the 2018 exercise was rolled out to 12,000 additional end users compared to the previous one.

Based on an estimated cost of $117 to sanitize a compromised PC, this new training has potentially saved the commonwealth over $500 thousand in efforts to re-image an infected system and in related lost productivity. The savings could be potentially much higher should the infection result in a data breach or destruction of data.

With the training having been available for only 4 months (as of this writing), we are already seeing a completion rate within 2% of last year’s overall completion rate for training.

Over the years, numerous technology advances have improved the ability of organizations to prevent and respond to cyber-attacks. However, the greatest risk to most organizations continues to be their own employees. Malicious websites, phishing emails, social engineering and the loss or theft of mobile devices or credentials are just a few of the ways an employee can unwittingly allow cyber criminals to infiltrate the organization and potentially access sensitive information.

Concept

All commonwealth employees and contractors who access to IT resources for work, including but not limited to email, the Internet, smart phones and mobile devices, are required to complete annual training on security awareness and the acceptable use policy. The training is developed in-house by the Office of Administration, Enterprise Information Security Office (EISO) in collaboration with human resources (training and development, labor relations, etc.), legal, communications and senior leadership. It is delivered in a web-based format each year through an enterprise learning management system (LMS).

Originally developed in 2009 the commonwealth's training focused on the most common threats for employees, such as phishing emails and protecting devices and credentials from loss or theft. Although the training was reviewed annually for accuracy and minor updates were made, it had remained largely the same for a number of years. Because of the click-through format of the training, users who did not understand the importance of security awareness (or who were simply bored with taking the same training year after year) were known to skip quickly through the content without taking time to comprehend it.

The EISO recognized the time had come for a major refresh of the commonwealth's security awareness and acceptable use policy training to present this critical information in new and exciting ways.

In the years since the original training was created, online trainings have become more sophisticated and effective in engaging learners through interactive features and techniques such as gamification. The EISO and the Human Resource Training Division worked together on a 6-month project to produce a new training course for 2018.

Initial planning and development of the course material took about 3 months. They identified six areas within the training where interactive modules could be used to present content in a relevant way to improve comprehension and retention. For example, the module for physical security requires the user to scan the inside of an office to identify potential security risks, such as personally identifiable information displayed on an unattended computer screen, unlocked file drawer with personnel records and an identification badge laying on the desk. Other modules present the user with a series of email messages and requires them to identify potential "red flags" that it could be a phishing attempt, while another walks the user through using the hover technique to examine a URL before clicking on it. This was not something our end users had experienced before and was the first training of its kind by the commonwealth.

After the planning and development period, the new course was reviewed by business owners (EISO and others) and other collaborators mentioned above. This feedback led to additional improvements prior to finalization of the material. The new course was completed and uploaded to our (LMS) in December. The commonwealth uses HR data from its enterprise resource planning system to enroll employees and contractors in the training and send an initial notification and reminders to complete the training in the LMS within two weeks. It also provides reporting and statistical information to track compliance with the requirement to complete the course.

Significance

The new-and-improved training keeps our users engaged every step of the way and helps to reinforce key concepts and behaviors. Effective security training is a critical piece of the commonwealth's overall cybersecurity strategy. It touches every employee and contractor that works for the commonwealth, a workforce of over 80,000 people, and represents one of the major touchpoint opportunities to reinforce cybersecurity best practices. The training also fulfills a requirement of many audits to which the commonwealth is subjected, such as PCI, SSA, and IRS. By requiring employees to acknowledge that they have read and understand the policy and the potential consequences for violations, it also provides a valuable internal compliance function.

After being available for only 4 months, with our current training completion rates being within 2% of where they were for the whole year last year we anticipate compliance for 2018 will exceed previous metrics. Commonwealth agencies recognize the importance of this training and are diligently tracking completions by their users.

Impact

In April 2018, the EISO conducted a phishing exercise to test commonwealth users and measure the effectiveness of our improved training. This exercise consisted of sending out a crafted phishing email to all 80,280 employees and contractors. The email included a hyperlink to a "malicious" site which logged information from any users who clicked on it. The results of the test showed a decline of nearly 40% from the same test conducted in 2017. Furthermore, per the instructions contained in the training, several thousand of the users forwarded the phishing email to the service account designated to accept and investigate potentially malicious messages, also a substantial improvement from 2017.

In terms of cost savings or cost avoidance, a single malware-infected PC costs an average of $117 in time spent to remediate and lost productivity of the user while their machine is unavailable. Had the phishing emails been real, the 2017 attack would have cost the commonwealth $712 thousand, compared to $519 thousand for the same type of attack in 2018. This is a very conservative estimate that assumes no data breach was experienced as a result of the malware. Given that this training was created in-house with no budget, the ROI is significant.