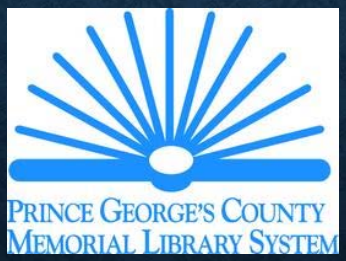
Implementing a Security Awareness Program – Creating Security Conscious Employees

DECEMBER 8, 2017

PREPARED BY CARLA MOORE, DIRECTOR OF INFORMATION TECHNOLOGY
PRINCE GEORGE'S COUNTY MEMORIAL LIBRARY SYSTEM



SECURITY AWARENESS PROGRAM

What is a Security Awareness Program?

A program to train employees to make smarter security decisions within an organization and it helps to improve the organization's security posture and mitigate risk.

- Establishing and maintaining security awareness through a security awareness program is vital to an organization's progress and success.
- The program assists the organization with the education, monitoring, and ongoing maintenance of security awareness within the organization.

Why Implement a Security Awareness Program?

- Employees need to be aware of the importance of protecting the internal network and data and how to handle all securely and understand the risks.

Why Implement a Security Awareness Program?

- IT security is often not the weakest link in the technology environment. It is the behavior, actions or inactions by employees and staff that lead to a security incident.

Examples:

1. Sharing of information that can be used for social engineering.
2. Ignoring or not reporting unusual activity.
3. Not following proper procedures and protocol.

PROBLEMS ENCOUNTERED AT PGCMLS

- Major Security Incident
- Phishing
- Spear Phishing
- Staff Actions

KNOWN FACTS

- Growing cyber threats has changed IT security.
  - 57% of businesses now assume their IT security will become compromised.
  - Businesses are also waking up to the fact that one of the biggest weaknesses against cyberattacks is their own employees.
- End-users are a known source of all kinds problems, including viruses and malware.
  - 52% of businesses admit that employees are their biggest weakness in IT security, due to careless actions putting business IT security strategy at risk.
- Small organizations with limited resources and staff need a security awareness program that can be deployed quickly, protects your network, and actually start saving your IT Department time.
- Your users are your last line of defense.

SOME BEST PRACTICES

- Security Awareness must be ongoing to ensure that training and knowledge is delivered regularly. It is used to maintain a high level of security awareness on a daily basis.

SOME BEST PRACTICES

- Support and buy-in needed from management and leaders.
- Educate leadership and management so they understand the risk factors to the organizations information.
- Leadership and managers need to understand security requirements so they can discuss with staff and reinforce them.

SOME BEST PRACTICES

- Establish your team, roles and responsibilities.
- Determine training content and audience for delivery of content and courses.
- Establish multiple ways to communicate the program information.
- Require all employees to participate.

PGCMLS GOALS

- Protect the network and organization
- Easy access
- Continuous training
- Measure effectiveness of program
- Regular reporting with benchmarking
- Build human firewalls
- Reduce insider threats from employees
- Continue to find ways to communicate security awareness

Who is KnowBe4?

KnowBe4 is the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing attacks and enterprise strength reporting, to build a more resilient organization with security top of mind.

Website: www.KnowBe4.com

FEATURES OF KNOWBE4

- Cloud- based application
- Reports and benchmarking
- Continuous phishing with testing
- Easily identify employees who are struggling with the course content and testing
- Free phishing security test
- Free email exposure check
- Free domain spoof test
- Free phishing alert button for staff
- Ransomeware simulator
- Ability to share courses with friends and family for free
- Scam of the week and other alerts

LESSONS LEARNED OVER 6 MONTHS

- Mandatory continuous learning and testing is key
- Continue to communicate program information
- Make time to plan regularly for security
- **Establish rules and guidelines for training**
- Find ways to keeping employees engaged
  - Communicate program and purpose – newsletter, posters and intranet
  - Train new hires immediately
  - Provide regular reminders to employees

RESULTS

reports#.pdf - Adobe Acrobat Pro

File Edit View Window Help

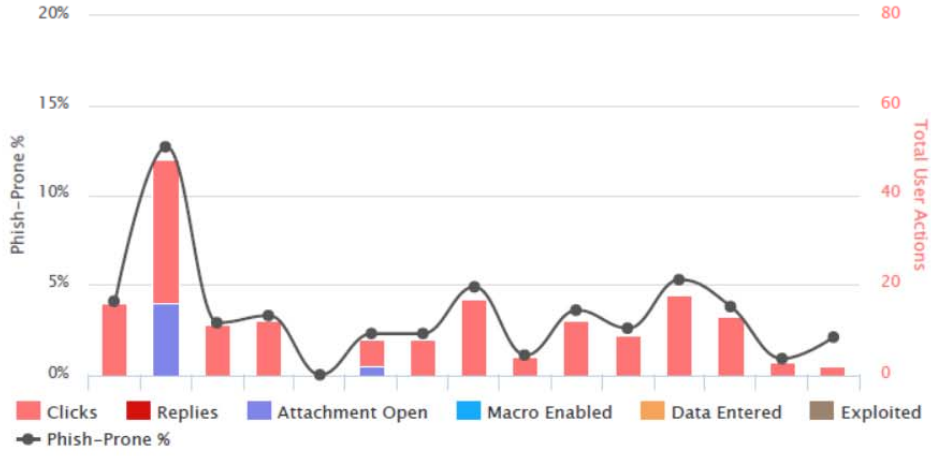
Create

1 / 1 130%

Tools Comment Share

Phishing Security Tests 6/5/17 - 12/5/17

163 Clicks 0 Replies 18 Attachment Open 0 Macro Enabled 0 Data Entered



Email Address	Phish-Prone %	Delivered	Failures	Clicks	Replies	Attachments	Macros	Data	Exploits

QUESTIONS?