ESTABLISHING AND IMPLEMENTING A CYBERSECURITY EMPLOYEE TRAINING & TESTING PROGRAM

This publication was produced at the request of the United States Agency for International Development. It was prepared independently by implementing partner, Catalisto LLC for the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The authors' views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States government.

MODULE 2 - INTRODUCTION

You can force complex passwords, install drive encryption, and use three different types of security applications, yet, none of that matters unless you tackle the primary cause of security issues: your employees. While typically not a malicious act, employee caused security incidents are quite common, with phishing attacks accounting for 43 percent of all data breaches. Besides technical means, a comprehensive Security Awareness Training program is essential when it comes to your overall security plan. While many businesses conduct formal training seminars, send email updates, and even test employees on their overall security knowledge, there is one question that IT leaders often have a difficult time answering…is it working?

WHAT IS SECURITY AWARENESS TRAINING?

Security Awareness Training is the process of educating employees on proper information security best practices, policies, and general guidelines. Security Awareness Training should be an ongoing process that teaches employees how to best protect themselves and a business from potentially harmful threats. Empowering employees with knowledge, while reminding them of the possible repercussions from a security breach should be a core pillar of every company's overall security practice.

WHY TRAIN EMPLOYEES & HOW?

Empowering your employees to recognize common cyber threats can be beneficial to your organization's cybersecurity. Security awareness training teaches employees to understand vulnerabilities and threats to business operations. Your employees need to be aware of their responsibilities and accountabilities when using a computer on a business network.

New hire training and regularly scheduled refresher training courses should be established to instil the data security culture of your organization. Employee training should include, but not be limited to:

1. **Responsibility for Company Data**

Continually emphasize the critical nature of data security and the responsibility of each employee to protect company data. You and your employees have legal and regulatory obligations to respect and protect the privacy of information and its integrity and confidentiality.

2. **Document Management & Notification Procedures**

Employees should be educated on your data incident reporting procedure in the event an employee's computer becomes infected by a virus or is operating outside its norm (e.g., unexplained errors, running slowly, changes in desktop configurations, etc.). They should be trained to recognize a legitimate warning message or alert. In such cases, employees should immediately report the incident so your IT team can be engaged to mitigate and investigate the threat.

3. **Passwords**

Train your employees on how to select strong passwords. Passwords should be cryptic so they cannot be easily guessed but also should be easily remembered so they do not need to be in writing. Your company systems should be set to send out periodic automatic reminders to employees to change their passwords.

4. **Unauthorized Software**

Make your employees aware that they are not allowed to install unlicensed software on any company computer. Unlicensed software downloads could make your company susceptible to malicious software downloads that can attack and corrupt your company data.

5. Internet Use

Train your employees to avoid emailed or online links that are suspicious or from unknown sources. Such links can release malicious software, infect computers and steal company data. Your company also should establish safe browsing rules and limits on employee Internet usage in the workplace.

6. Email

Responsible email usage is the best defence for preventing data theft. Employees should be aware of scams and not respond to email they do not recognize. Educate your employees to accept email that:

- Comes from someone they know.
- Comes from someone they have received mail from before.
- Is something they were expecting.
- Does not look odd with unusual spellings or characters.
- Passes your anti-virus program test.

7. Social Engineering and Phishing

Train your employees to recognize common cybercrime and information security risks, including social engineering, online fraud, phishing, and web-browsing risks.

8. Social Media Policy

Educate your employees on social media and communicate, at a minimum, your policy and guidance on the use of a company email address to register, post or receive social media.

9. Mobile Devices

Communicate your mobile device policy to your employees for company-owned and personally owned devices used during the course of business.

10. Protecting Computer Resources

Train your employees on safeguarding their computers from theft by locking them or keeping them in a secure place. Critical information should be backed up routinely, with backup copies being kept in a secure location. All of your employees are responsible for accepting current virus protection software updates on company PCs.

11. Build a culture of security

A culture of security has long been seen as the holy grail for chief information security officers (CISOs). Equally, such a culture is seen as notoriously difficult to achieve.

With the aid of security awareness training, some are heading in the right direction.

Creating a culture of security means building security values into the fabric of your business. Training that covers situational awareness (why someone might be at risk), plus work and home-life benefits is a good way to bring people onboard.

Advanced training platforms can help monitor and develop a culture of security, making people your first line of defence.

12. Be socially responsible as a business

As WannaCry and NotPetya demonstrated in 2017, cyberattacks can spread at rapid speeds. The more networks that become infected, the more at-risk other networks become. And one network's weakness increases the overall threat for others.

The absence of security awareness training in one organisation makes other organisations vulnerable. It's a little like leaving your house door unlocked – with the keys to next door waiting inside.

Security awareness training doesn't just benefit you. It benefits your customers, your suppliers and everyone else interlinked with your network.

HOW TO MAKE IT STICK?

1. Lead By Example

Good security habits start from the top. If the boss has passwords affixed to his monitor with sticky notes, a computer left unattended and unlocked during lunch, or an unsecured laptop sitting on his desk overnight, why should employees behave any differently? The best way to instil good security behaviours in employees is to model them yourself as a manager. Follow security protocols to the letter; otherwise you can't admonish others in good faith for failing to do so.

2. Send Out a Daily Security Tip

Dropping a hundred-page policy manual on every employee's desk that outlines your security policy is a sure-fire way to guarantee it is never read or referenced. While formal security documentation has its place, security advice and tips delivered in manageable, bite-sized chunks are more likely to be effective at both training and reinforcing good security habits. These tips can be delivered in a daily email missive, either highlighting one point of your security policy, explaining a common security term ("What is phishing?"), or focusing on a recent security-related story in the news to help bring home the real risks of loss.

3. Rigorously Enforce Security Policies

In many companies, particularly smaller ones, it's a common habit to let security protocols slide from time to time. You may (smartly) require an in-person appearance from someone before resetting their password, but when time is tight and people are busy, the IT staff may go ahead and perform the reset over the phone. Mandate that procedure be followed on all such activities, even if the person on the other end of the line is a good friend and there's no question of identity. Make sure both the IT department and the employee calling for help know that this isn't a matter of distrusting either of them, it's about protection from outsiders looking for holes in your internal processes.

4. Put Employees to the Test

Telling employees to watch out for things like social engineering doesn't mean much. You might also want to see if they actually follow your corporate guidelines when a hacker calls. Why not put them to the test in a real-world simulation? In a social engineering situation, you can either pay a security expert or do the job internally. Either way, you only need to call an employee who has access to sensitive information – be it password resets or customer data – and attempt to coerce them into bypassing your security protocols. If they crack, you know you have additional training work to do.

5. Make Security Tools Freely Available

Employees won't use tools like data encryption, VPNs, and malware scanners unless they're widely available and easy to use. Make these tools default products on every computer in the building. Extend this concept to anything related to security, including drawers and file cabinets that lock as well as paper shredders. Employees often have access to shredders or other secure document destruction bins, but they simply don't use them because they're a hassle or are located too far from their desk to bother making the trip. The overarching theory: Make it easy to adopt good security behaviours, and employees will catch on.

HOW DO I KNOW IF MY SECURITY AWARENESS TRAINING PROGRAM IS WORKING?

Security Awareness Training can be costly. Given the time commitment required from employees, many executives are cautious about pulling the trigger on funding for security training because it is hard to know if it actually helps. One modern way businesses are gaining quantifiable stats on their security awareness training program for an affordable price is through phishing simulation tests.

1. Simulated Phishing Test

Phishing tests are simulated phishing emails that try and trick your employees into opening a possibly fraudulent email, click on a link, and enter private credentials on a bogus landing page designed to look like the real thing (i.e., LinkedIn, DropBox, PlayStation, etc.). These emails appear to be coming from a known source, such as the president of the company, a well-known employee or client, social media site, or even a bank or government entity. These simulations exploit common email security best practice guidelines, meaning that employees who have a decent understanding of information security should pass the test. These simulations are incredibly useful as they paint a fairly clear picture of your company's overall level of security awareness by reporting on who was duped by the test, including who actually entered their private credentials on the dummy landing page. Also, most phishing simulation programs can force employees who failed the test to learn where they went wrong and what they should have done.

Simulated phishing tests can be a relatively low cost, high reward activity as it helps re-educate your entire team, while finding where the holes and gaps might be.

2. Password Enumeration Tests

Passwords are one of the most basic forms of security, yet many employees often ignore tips and guidelines for creating strong passwords. In a recent study by Thycotic, 30% of people admitted to still using their birthday, address, pet names, or children's names for their password…which are all big password no-nos.

One quick and inexpensive way to test your Security Awareness Training plan is to have a 3rd party Consulting team conduct a Password Enumeration Test. A Password Enumeration Test is when a trained and qualified security professional acts like a hacker and tries to discover employee passwords using common hacking methods such as dictionary and brute force attacks. The results of this tests come as an executive friendly report that shows you how many passwords were uncovered during the test, and where employees went wrong when they created their password. This will help you and your security team create stronger password policies when needed and know where to better focus your next security awareness training class.

3. USB Drop

Social engineering is when a cybercriminal tricks an employee into installing malware or revealing private information. One common form of social engineering is through USB keys or flash drives that contain malware being left in the open or given to someone to use. USB drives have fallen somewhat out of fashion over the years due to a rise in Cloud storage and security concerns, yet many people still save critical and sensitive data on USB drives.

A USB Drop is a form of social engineering testing where "dummy" USB keys are left around your facility in common places like the parking lot, break room, or even on an employee's desk. These dummy keys are actually installed with software that will let you remotely know when and where they were plugged in, which will inadvertently reveal employees that do not fully understand the dangers of using an unknown USB drive.

4. The "Eye Test"

A lot of security violations come from common mistakes, such as walking away from your desktop without locking it, leaving sensitive data on a printer for an extended period of time, and by not following proper visitor policies. Take a walk around your office, or better yet, get a trained security consultant to do it, and ask the following questions:

- Do you see PCs that are logged in and unattended?
- Are there documents left unattended on a printer?
- Is a contractor in your facility unattended or without a visitor's badge?
- Are employees using non-approved file sharing methods such as DropBox or a USB drive?
- Is anyone using a non-sanctioned device for business purposes? (i.e. laptop, tablet, phone, etc.)
- Do employees take devices or material home?

Remember, for security to be effective, it needs to be everybody's responsibility, so make sure to push the importance of Security Awareness Training early and often.

READING MATERIAL

1. Module_2_Whitepaper1-JL_Privacy_Training_White_Paper_2021
2. Module_2_Whitepaper2-Employee Training as a Tool for Cyber Security