Preventative Measures: Security Awareness Training

Blue Team Level 1 Certification (Standard) > PA6) Taking Defensive Actions > Preventative Mea... IN PROGRESS

Always remember, phishing is a form of social engineering attack, using emails as a delivery method. These emails are targeting human weakness, and exploiting that to get them to open an attachment, enter their credentials into a malicious site, or to give out information that they normally wouldn't do.

It is **crucial** for organizations to take phishing seriously, and to ensure that they run routine user awareness training sessions, so that anyone can detect and report a suspicious email when they see one. There are two main ways to educate users on the importance of phishing, and how to quickly identify it.

AWARENESS TRAINING

Preferably during the on-boarding process (where a new employee joins a company), users should be put through either an in-person or an online training course that teaches them how to spot phishing emails, and the actions they should take (generally reporting them to the security team). This should cover identifiers of a phishing email such as:

- **Coming from an unknown sending address.**
- **Improper grammar and spelling mistakes.**
- **Poor styling.**
- **Trying to get the recipient to click on a button or complete an action.**
- **Suspicious URLs and attachments.**

If employees are able to spot these common issues with phishing emails, then they become less likely to click on any malicious artifacts, therefore not creating a security incident that needs to be handled by the security team. It is impossible for email defenses to catch every single phishing email, so users need to be ready to identify and report any that land in their mailboxes.

SIMULATED PHISHING ATTACKS

It is common for security-conscious organizations to launch simulated phishing attacks against their own employees in order to determine how effective their current security awareness training is. There are a number of security services that offer phishing attacks as a service, and allow you to customize the email that will be sent to mailboxes under the organization's domain. If the user clicks on a "malicious" link, they will be redirected to a safe website (typically owned by the company conducting the simulated attack) and will inform them that they have just fallen for a phishing email. Security teams can also monitor how many individuals report the phishing email to them, identifying employees that have understood the training and are able to identify suspicious emails. These events should be conducted every few months to test employees and identify any that are consistently falling for phishing emails so that they can receive additional training.

Some great platforms for doing this include:

- Sophos Phish Threat – Link
- GoPhish Open-Source – Link
- Trend Micro's Phish Insight – Link
- PhishingBox – Link

● 8 Topics | 1 Quiz

○ DF4) Windows Investigations

● 3 Topics | 3 Quizzes

○ DF5) Linux Investigations

● 4 Topics | 2 Quizzes

○ DF6) Volatility

● 3 Topics | 1 Quiz

‹ Previous Topic

Mark Complete ✓

Back to Lesson

Next Topic ›