TitanHQ
SafeTitan

Start Now! Your 3-Month Roadmap to a Mature Security Awareness Program

As an MSP, you'll want to plan and roll out phishing and training campaigns to help make your customers more cyber-risk aware. But you may be wondering how to make your campaigns most effective? This roadmap provides some tips for planning the first three months of your cyber security awareness campaign strategy.

Before You Start

Set up your MSP Dashboard. Your users must be synced with the SafeTitan Portal, so that phishing and training emails can be received by them. For help with this as well as an overview of the MSP Dashboard, see SafeTitan MSP Setup.

MONTH ONE

Assess threats and the security awareness of your people

- Assess your risk landscape and identify your assets. What are the threats and vulnerabilities faced by your clients and their industries?
- Assess your clients. How do they view security? Do they understand their roles, company policies and procedures? Consider running a survey to identify their level of security awareness.

Consider the phishing and training strategy you need and begin developing it

- Build a learning ladder. What priorities and security gaps have you identified? Create a list of targeted learnings for the year.
- Combine learning goals with your phishing campaigns. Understand each risk and use them to teach your targeted lesson.
- Apply follow-up training. After you've analyzed the results of a campaign, you can determine where vulnerability exists, and create training campaigns to raise awareness and mitigate risk.

Run a baseline campaign

- Get a controlled, unbiased set of data around the phishing susceptibility of your organization. You can then run it again in six months or a year, which will enable you to compare the results and see where improvements have been made. You'll want to keep the complexity and sophistication of the campaign low. You can read more about this in Setting Up Campaigns: Tips for MSPs.

MONTH TWO

Analyze baseline campaign results

- Review the results to determine where the vulnerabilities are in your organization.

Run training campaign as follow-up to baseline campaign

- Depending on the theme you chose for your baseline campaign, select an appropriate follow-up training course, as shown in the Twelve-Month Campaign Planner for MSPs. You may have sent the baseline campaign to a random number of recipients, but you can send the training to everyone in the organization.

Run first official phishing campaign

- Next you can run your first official phishing campaign. Select a different theme and send the campaign to everyone this time. You want to encourage people to realize the importance of cyber security and engage on a regular basis with training.

TitanHQ SafeTitan

Start Now! Your 3-Month Roadmap to a Mature Security Awareness Program

MONTH THREE

Analyze first official phishing campaign results

- The results of your first official phishing campaign should be now available and will highlight where the gaps are in the recipients' security awareness. Next you'll want to create a training campaign to encourage behavioral change where needed.

Create next training campaign

- Refer to the Twelve-Month Campaign Planner for MSPs for suggestions.

Create next phishing campaign

- You could consider increasing the complexity and sophistication of your phishing campaigns for your fourth or fifth campaign but keep it simple again for this campaign. You are building a learning ladder for your customers, and it's important to help them proceed along that ladder together, so frequent bursts of phishing campaigns followed by training reinforces the learning.

Analyzing Results

When you receive the results of a phishing campaign, there are several ways to analyze the results. Results can differ based on region, language, department, and time of employment. Also, what actions are people performing if they've interacted with the lure? You'll be analyzing results to determine the number of people who opened files, clicked on links, entered data, and so on. Based on this, you'll want to develop training to create behavioral change to effect change in these areas. And, apart from keeping an eye on the progress of your clients, it's important to check the progress of organizations and their ability to mitigate risk. Use your SafeTitan Reporting tool to see how organizations are benchmarked against their susceptibility to phishing.

Tips for Ongoing Best Practice

Review trends and threats regularly. What are the phishing scams being received at your organization or by others in your industry? Learn from these and hone your phishing strategy.

Training should be a constant conversation to keep security at the forefront. Follow up phishing with targeted responsive training. Provide annual training on basic information security tenants. Ensure role-based training is provided and includes important processes like incident response, and so on.

Monitor behavior change. Is there more reporting of phishing emails through Phishhuk? Are vulnerabilities reported more often? Consider rewarding and recognizing positive behavior.

Likewise, correct and encourage action for negative behavior with additional training and real-time communications. Based on behavioral changes, adjust your learning ladder and learning goals.

GET IN TOUCH

General queries: info@titanhq.com

titanhq.com