Managed Security Awareness Training (MSAT) – Onboarding a New SMB

To onboard your customer to the next available Security Awareness Training Campaign run due to start on the 8th of any month we will need to have the following implemented on or before the 28th of any month prior:

Having the address book and allow lists managed early in the conversations is advantageous

Customer Address Book A copy of the template is available.

Customer Mail Service/filtering technologies 'Allow/Lists' updated to reduce the risk of content submitted by MSAT ending up in spam folders, and thus adversely affecting the experience of the Security Awareness Training Campaigns.

Test message: As soon as the 'Allow lists' have been put into place, we can submit a test message, just to make sure it filters through the technologies to the recipient's inbox.

Communications: Once all the components are in place, it is advised that the customer communicates with their userbase of the Security Awareness Training program, Online Training videos that will be delivered by email, of which there will be a time period to complete them.

The Schedule:
Our campaigns run Monthly. It is a requirement for us to have all the components in place on or before the 28th of any month to prepare for the following months run of campaigns. Should delays occur in having any of the key parts in place for our cut off time, we cannot guarantee that your setup for your customer will make it to the next scheduled run.

Deadline for submission	Responsibility	Action
28th of Month	MSP/SMB	Cut off date: MSP PhishLine team to have received requests for next campaign • New Account set-ups in full (Address book received & Allow lists implemented by MSP/SMB) • Updates to any existing address books Anything received after, will be applied for the following month.
1st of Month	Barracuda	Schedules are updated
1st-4th of Month	Barracuda	Implement pre-prepared campaign content for the months run
5th of Month	Barracuda	Campaigns Audited
8th of Month	Barracuda	Campaigns go live, service will start submitting email
16th of Month	Barracuda	Design next months campaign content
22nd of Month	Global	Campaigns will end, no further submissions from the service
23rd of Month	Global	Campaign cut off date, Training must be completed by
26-28th of Month	Barracuda	Reports are generated and populated into secure report library
28th of Month	MSP/SMB	Cut off date for new and updates

Allow Lists:

Please note that if you are already using Barracuda Email Gateway Defense, no additional allow listing steps should be required unless you are using any additional spam filters like Microsoft 365 for example.
If non-Barracuda Spam filtering is in use, please review the following Barracuda Campus article link below for assistance with Allow Listings for Managed Security Awareness Training:

https://campus.barracuda.com/product/phishline/doc/78153005/email-allow-list-and-best-practices/

If you are using Microsoft 365 and would like to bypass it's filtering, please see the following document on the Managed Security Awareness Training Campus Site (requires you to be logged into campus.barracuda.com first):

https://campus.barracuda.com/to/16ES

Once all is in place, communicate back to the MSAT team for them to submit a test message to a local administrator/contact, just to make sure the messages are not restricted from delivery.

Campaign Schedules:

We publish the schedules online, detailing the campaigns that will be run and the content for any given month. These pages are updated for the new content a month ahead. All the schedules can be seen here: *(note that a login will be required, please register if you have not done so before)*

For all new customers starting the Security Awareness course, we have the cornerstone of every training program! Four modules over 4 months cover everything you need to know about phishing scams and the tactics cybercriminals use to trick unwitting targets into clicking or downloading malicious links and attachments.

Checklist:

The Following is a list of the action items. We will require to ensure this implementation is successful:

- √ Customer Address Book.
- √ Customers Mail Service, 'Allow' lists applied.
- √ Test Message submitted and verified delivered.
- √ Customer Communicated to the recipient audience of the up-and-coming training that will be delivered to their inboxes.

What to expect:

Campaign delivery: The customer will in the first 4 months receive our Core 4 campaigns.

Month 1: Video Training, an introduction to Phishing (What is Phishing?) is a high-level introductory training video describing the concept of Phishing.

Month 2: Video Training, Types of Phishing which provides an overview of phishing, spear phishing, smishing and vishing.

Test Phishing email, A message will be delivered to the recipients that will be questionable in nature but designed to try to influence the recipient into making an action.

Month 3: Video Training, Understanding URLs which provides Insights into web addresses that protect browsers from threats.

Month 4: Video Training, Spotting Phishing Scams, many of the most popular phishing techniques revealed.

Test Phishing email, A message will be delivered to the recipients that will be questionable in nature but designed to try to influence the recipient into making an action.

Month 5 and ongoing:

Once the customer has completed the first 4 Core months content, they will join the global campaign group where we will select a topic of the month for the Training Videos. Additionally, at our choosing of when it will be delivered, we shall submit a 2nd campaign in any given month that will contain a test phishing message.

Reports:

After each month's campaigns have completed, we will publish the reports to the SharePoint location we shall provide to yourself.

Please note that for some months, you will have two reports for each SMB customer in any given month. 1 report for the results of training and the other report being related to the Test Phishy Mail Campaign.

How do we recognise the Video Training messages?

All Video Training messages we send will all have the same familiar look when received in the recipient's mailbox. An example is shown below.

Can I see the content that is being published each month?

Customer's that are on the first four Core months, as well as the monthly published content is available on our Campus pages here: *(please note a login is required to access all the pages).*

How do we recognise the Phishy test messages?

The test messages will all vary each month and are designed to try to be as legitimate as possible. There may be some glaring spelling and grammar mistakes that give the 'email' away, but it could also be very convincing with very few, if any grammatical errors. The content we deliver for a given month will be published upon our campus page – *Documents – Managed Phishline Campaigns*.

When can we expect the Security Awareness training to start?

We operate the Managed PhishLine service under a strict schedule, to ensure we can facilitate delivery of the service to all our customers, globally. Key dates to be aware of are:

28th of any month:	Customer set-up / Any updates, submitted to the MPL Team
8th of any month:	Campaigns start to deliver to the recipients' mailboxes
23rd of any month:	All Campaigns end
25th-28th of any month:	Reports are generated and delivered to your SharePoint folders.

If you have any questions, please do contact the team via Email at:
PhishLineMSP@Barracuda.com

Kind regards

Managed Security Awareness Training
Technical Partner Success Team