

 **Phishing & Training Assessment – Get Your Foot in the Door**

Preparation

**Prepare for the campaign:**

* Access the portal with your Partner Admin login
* Create a new client for your prospect
	+ Enter Company Name under Name
	+ Scroll down and check the “DWBA” check box
	+ Enter up to 3 different domains for your prospect
	+ Click submit
* Find created client in client list, click view
* Under “Employee Vulnerability Assessment (EVA)” click the blue “Run DWBA” button
* Enter the approximate number of employees
* Click the checkbox “I have read and agree to the Terms of use”
* Click the blue arrow on the bottom right hand side to start the scan
* Once scan is complete, click okay on the pop-up box
* You will then be taken to their results where you can view fully redacted, partially redacted, or non-redacted passwords.
* Click the print symbol on the top right side to print your report!
* Fill in all [red boxes] with prospect-specific information!

**Phishing & Training Assessment – Get Your Foot in the Door**

Call Script

**If low completion rate on security awareness training**

Hi <prospect’s name>, this is <insert name here> with <insert company name here>. I’m calling to let you know that your phishing campaign has been completed and the deadline for the training course has passed. During the phishing campaign, [insert number] employees took the bait and clicked on the simulated phishing email. We are also concerned with the outcome of your training completion rate. I’d like to get together to discuss these results and how we can continue to ensure your employees keep security top of mind. Does [date & time] work for you?

**If high completion rate on security awareness training**

Hi <prospect’s name>, this is <insert name here> with <insert company name here>. I’m calling to let you know that your phishing campaign has been completed and the deadline for the training course has passed. During the phishing campaign, [insert number] employees took the bait and clicked on the simulated phishing email. We are impressed with the outcome of your training completion rate. I’d like to get together to discuss these results and how we can continue to ensure your employees keep security top of mind. Does [date & time] work for you?

**IF NO EMPLOYEES CLICKED ON THE PHISHING LINK**

**Swap out:** During the phishing campaign, [insert number] employees took the bait and clicked on the simulated phishing email.

**With:** Upon analyzing the phishing results, no employees took the bait – this time. These are great baseline results! With cybercriminals becoming more sophisticated, social engineering scams are constantly changing, meaning success today does not guarantee success tomorrow.

**Phishing & Training Assessment – Get Your Foot in the Door**

Initial EVA Email Template

**Subject Line**: Your phishing & training results are in!

[First Name],

Now that your phishing campaign is complete and the deadline you have set for your employees to complete their training has come, I’d like to go over the results of both of those items with you! I am requesting a meeting to review the valuable and potentially dangerous information that I collected from both the phishing and training.

During the phishing campaign, we found that [insert number] employees took the bait and clicked on the simulated phishing email. With **85% of organizations** being targeted by phishing emails, this is a major cause for concern, as just one click could lead to detrimental consequences.

When we meet, I will provide you with further details on which of your employees fell victim to the simulated attack, as well as the results of who completed and passed their security awareness training.

This information will be very helpful in assessing the current security posture of your organization and determining next steps to alleviate any risks you may be facing.

I value your time and anticipate this meeting will only require 30 minutes of your day. Are you available to meet [Insert Date and Time]?

Thank you,

[Email signature]

**Tips:**

* **If no employees take the bait on the simulated phishing attack**, you will want to alter the text of this email. We recommend the below changes:
	+ **Remove these lines**: “During the phishing campaign, we found that [insert number] employees took the bait and clicked on the simulated phishing email. With **85% of organizations** being targeted by phishing emails, this is a major cause for concern, as just one click could lead to detrimental consequences.”
	+ **Remove this line**: When we meet, I will provide you with further details on which of your employees fell victim to the simulated attack, as well as the results of who completed and passed their security awareness training.
	+ **Replace with this line**: “When we meet, I will provide you with further details on the simulated attack as well as the results of who completed and passed their security awareness training.”

