



Awareness Content & Work from Home Toolkit



phishrod.co

Executive Summary

As we speak, more than 182,000+ cases have been identified for COVID-19 across 151 countries and the number is increasing at an alarming rate. It is an unusual situation where organizations are trying to run their business as normal while emphasizing on the safety of the employees, customers and other stakeholders to be first and foremost. A lot of organizations are promoting work from home to limit the spread of this deadly virus.

While the world is struggling to control the spread of this virus, there are opportunists trying to cash in the opportunity. Hackers are no different. As the curiosity grows amongst end users to know more about Corona, there is a sudden increase in the websites related to Covid-19. While many are serving the purpose by educating people and raising awareness, a large number of websites are also being used for phishing attacks and to lure end users into clicking a link or downloading an attachment to trigger a cyber-attack.

COVID-19 spread has a lot in common with a computer virus with no signature available. Under such circumstances, the ability to quarantine the infected and to create awareness about the virus have proven to be most effective remedies.

Believing in "It's time to Aware, Not Scare", PhishRod has put together a "Work from Home" toolkit. The tool kit contains General Awareness Content on Covid-19, Awareness Content for Corona related Phishing Scams, Screen Savers & a Work from Home Policy Template. The awareness content is available in both English and Arabic. You can download the toolkit at www.phishrod.co/workfromhometoolkit

PhishRod phishrod.co

CORONAVIRUS PHISHING SCAMS

How to Recognize & Avoid them?

Hackers are taking full advantage of the chaos and panic created by Covid-19. As end users are desperate for updates, they can easily be lured into clicking on phishing emails.

HERE ARE A FEW HELPFUL TIPS:

- REPORT EMAILS IMPERSONATING WORLD HEALTH ORGANIZATION (WHO) OR GOVERNMENT AGENCIES ASKING YOU TO PROVIDE PERSONAL INFORMATION
- HOVER YOUR MOUSE OVER THE EMAIL LINKS AND ATTACHMENTS TO SEE WHERE THEY LEAD
- KEEP A LOOK OUT FOR GRAMMATICAL AND SPELLING ERRORS
- REPORT SUSPICIOUS EMAILS THAT CREATE A SENSE OF URGENCY

PhishRod phishrod.co

What You Should Know

COVID-19 is highly contagious virus that causes respiratory illness in people.

What are the Symptoms?

- Cough
- Fever
- Shortness of breath
- Body aches
- Pneumonia
- Diarrhea

How does it Spread?

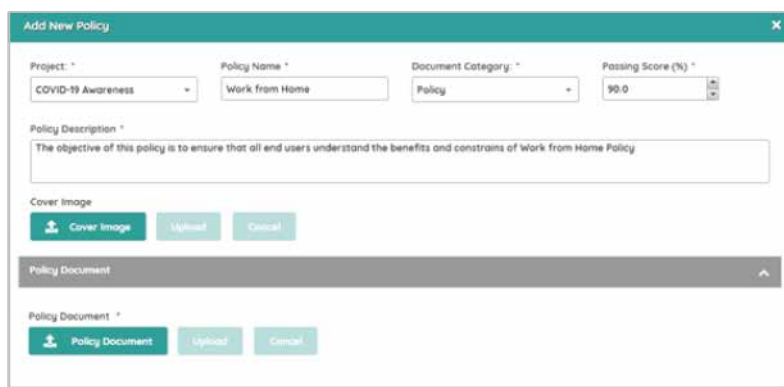
- Through droplets when an infected person coughs or sneezes
- Close personal contact with an infected person

Publishing Work from Home Policy & End User Consent

Work from home is not a usual scenario for most of the organizations. Besides operational impact, it has technical and legal impacts too. It is mandatory for an organization to have a Work from Home policy that must be clearly understood by all employees. Their agreement and official consent to it is important.

As part of the Toolkit, PhishRod is providing a Work from Home Policy that you can customize, publish and share with end users. PhishRod is also providing a 1-month free access to PhishRod Policy Compliance Manager which you can use to publish and share the policy with end users. Automated reminders can be configured while centralized dashboard will provide analytics related to consent & compliance across the organization, department & individual users. Here is a step-by-step approach for Work from Home Policy Consent.

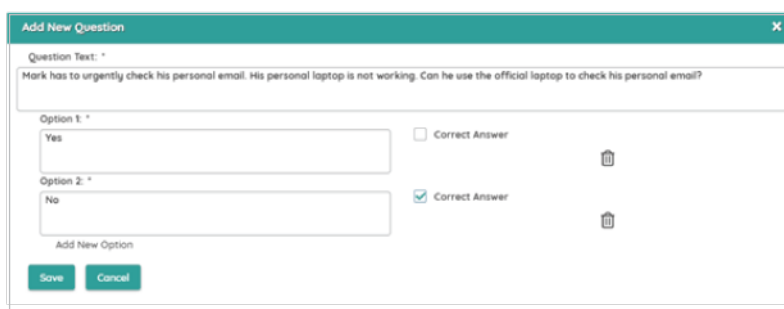
Step 1: Download the Work from Home Policy Template provided by PhishRod and customize it based on your parameters.



The screenshot shows the 'Add New Policy' form. It has the following fields and sections:

- Project:** COVID-19 Awareness
- Policy Name:** Work from Home
- Document Category:** Policy
- Passing Score (%):** 90.0
- Policy Description:** The objective of this policy is to ensure that all end users understand the benefits and constrains of Work from Home Policy
- Cover Image:** Includes a 'Cover Image' button, an 'Upload' button, and a 'Cancel' button.
- Policy Document:** Includes a 'Policy Document' button, an 'Upload' button, and a 'Cancel' button.

Step 2: Define the key learning points, develop the quiz that you want the end users to answer and define the passing percentage for the Work from Home Policy.

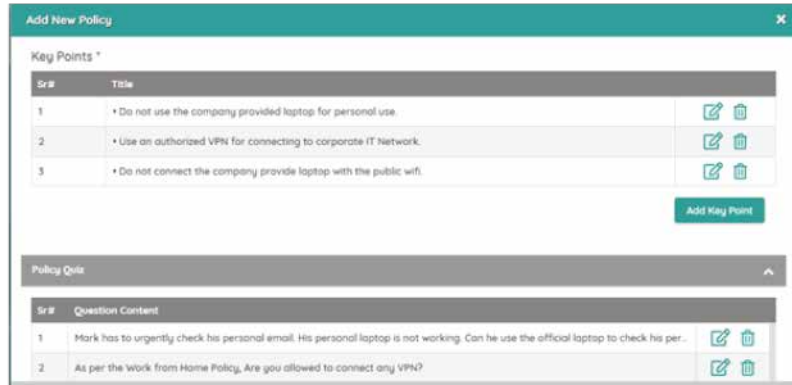


The screenshot shows the 'Add New Question' form. It has the following fields and sections:

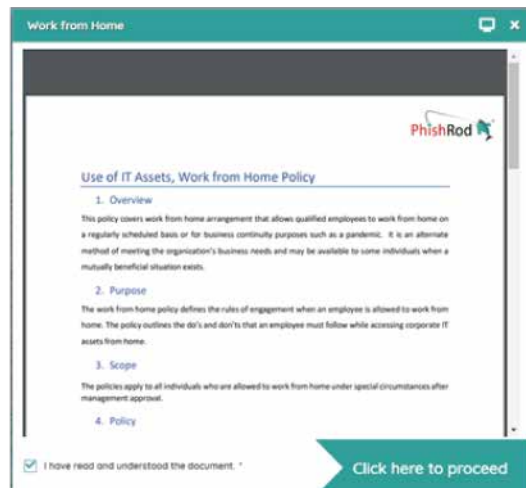
- Question Text:** Mark has to urgently check his personal email. His personal laptop is not working. Can he use the official laptop to check his personal email?
- Option 1:** Yes
- Option 2:** No
- Correct Answer:** The 'Correct Answer' checkbox is checked for the 'No' option.
- Buttons:** 'Save' and 'Cancel' buttons are at the bottom.

Publishing Work from Home Policy & End User Consent

Step 3: Get the Policy approved by defining the relevant approvers in the PhishRod Policy Compliance Manager.



Step 4: Publish the Policy to all End users so that they are aware and provide their consent to it.



Step 5: Keep tracking the consent on the dashboard and send reminders to those who have not provided the consent.



It's time to Aware, Not Scare



Employees are the most critical assets of an organization. Whether it's a computer virus or Covid-19, it is important to get the employees onboard and provide them awareness to curb the spread of the virus.

PhishRod has bundled general security awareness content & phishing scams content related to Covid-19. The content is available in both English as well as in Arabic in the form of Posters & Screen Savers. The content can be customized according to your organization branding guidelines.

Here are a few steps to ensure the outreach of the awareness campaign & its effectiveness.

Step 1: Download the awareness content from the toolkit and request for any customization if required.

Step 2: Upload the final version of content in the Content Library section of PhishRod Security Awareness Manager.

Step 3: Create a new awareness campaign, select the audience list, select the content and send it all target end users.

Step 4. End users would receive this content and they will have to provide their consent & acknowledgement.

Step 5: Measure the outreach of the campaign on the analytics driven dashboard.

You can request for the content customization & free subscription of PhishRod Security Awareness Manager for 1 month [here](#).