

Spear phishing services – COVID-19



In this crisis, hackers are looking to lure victims to gain an advantage. Especially with work from home (WFH), many of an organisation's assets are vulnerable in case an employee's system is compromised. Spear phishing simulation tests the awareness of employees and the preparedness of the defence team to respond to cyber-attacks that may impact operations, brand image, financials, regulatory requirements, etc.

Cyber criminals are hoping your employees will take the bait and give them your sensitive information.

Phishing is

- An attempt to obtain your sensitive personal information
- Criminals posing as a trustworthy organisation or institute to gain your employees' trust.



How we can help

- KPMG in India will simulate an attacker and target the employees of your organisation with phishing emails to test them for their awareness. This in turn will also test the various email and defense controls your organisation has in place
- We will help increase the awareness among employees in handling and reporting the phishing emails and phishing attempts
- We will benchmark the results to see where you stand.

Sample phishing scenarios

- Update the details of self and family member for communication, online meeting or collaboration tools, etc.
- Warning against fraudulent emails and calls
- Warning from IT compliance team for suspicious behaviour
- Raise donations for victims.

Potential benefits of the simulation

- Simulates a real-life threat in a controlled environment
- Focusses on training and familiarisation with various cyber-attacks
- Helps verify the efficiency of the email controls
- Helps understand the efficiency of the defence systems and controls.



90% of organisations experienced targeted phishing attacks in 2019. 88% of organisations worldwide faced spear phishing attacks and 86% dealt with business email compromise (BEC) attacks.

- State of the Phish report, Proofpoint, 2020

KPMG in India contacts:

Akhilesh Tuteja **Partner and Head**

Risk Consulting - Global
Co-Leader Cyber Security
T: +91 124 254 9191
E: atuteja@kpmg.com

Atul Gupta **Partner and Head**

Risk Consulting - IT Advisory,
India Cyber Security Lead
T: +91 124 336 9065
E: atulgupta@kpmg.com

Pratiksha Doshi **Director**

Risk Consulting - IT Advisory
T: +91 99672 28986
E: pratikshadoshi@kpmg.com



Follow us on:
home.kpmg/in/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2020 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

This document is meant for e-communication only. (002_FLY0420_SB)

home.kpmg/in