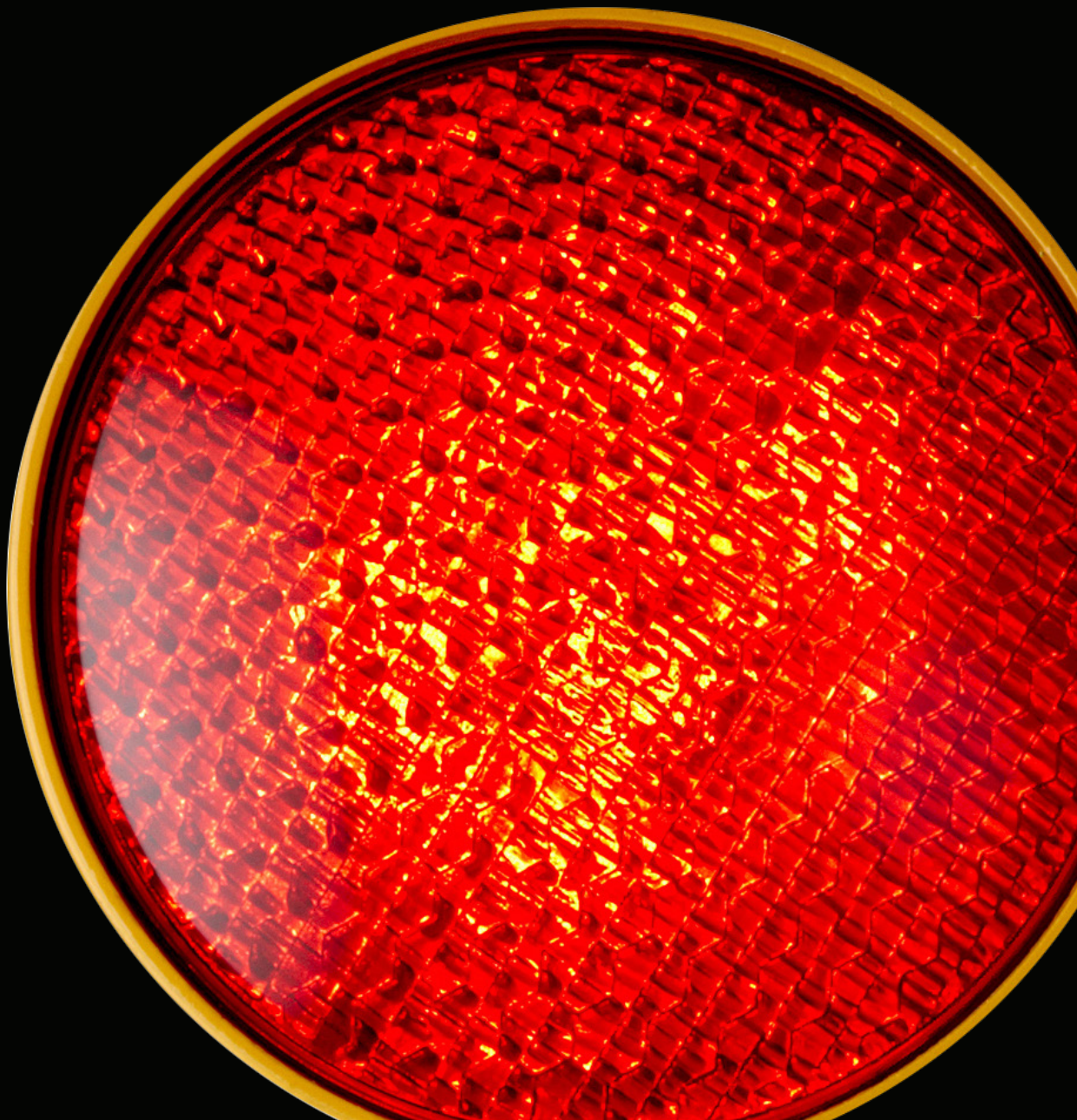
Deloitte.

Assessing risk for a secure future.
Phishing simulations as a service

2020



Content

Get to know phishing

Phishing is a form of social engineering. Phishing attacks involve the use of email or malicious websites to solicit personal information by masquerading as a trustworthy organisation.

For example, an attacker may send an email seemingly from a reputable credit card company or financial institution that requests account information, often indicating a problem. When users respond with the requested information, attackers can use it to gain access to accounts.

Phishing attacks may also appear to come from other types of organisations, such as charities. Attackers often take the advantage of current events and certain times of the year that includes:

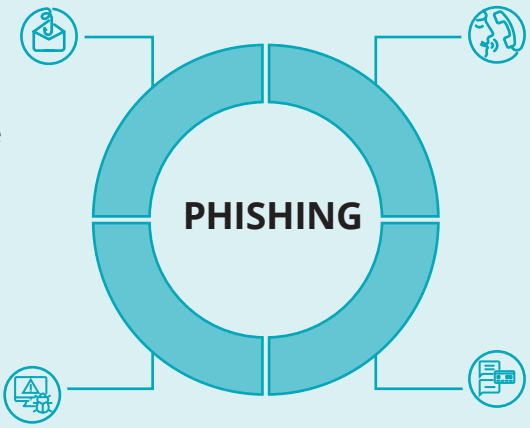
- Natural disasters (e.g., Hurricane Katrina and Indonesian tsunami)
- Epidemics and health scares (e.g., H1N1)
- Economic concerns (e.g., IRS scams)
- Major political elections
- Holidays

Pause before you respond
Our key services

Taking into account the current market's requirements, Deloitte India offers the following simulation solutions, which include a set of initiatives aimed at making participants aware and reinforcing their basic concepts of cybersecurity and cyber-risks, while learning how to protect themselves from cyber threats.

Email phishing
It is an the attempt to obtain sensitive information, such as usernames, passwords, and credit card details (and money), by disguising as a trustworthy entity through an email. Phishing emails contain malicious links that entice users to click them.

Learning management system
Deloitte intends to create better awareness among its client partners through a series of global security training programmes.



Voice phishing
Voice phishing or vishing is the criminal practice of using social engineering over the telephone system to gain access to private personal and financial information from the public for the purpose of financial reward.

SMShing
It is a form of fraud that uses mobile phone text messages, to lure victims into calling back a fraudulent phone number, visiting fraudulent websites, or downloading malicious content via phone or web.

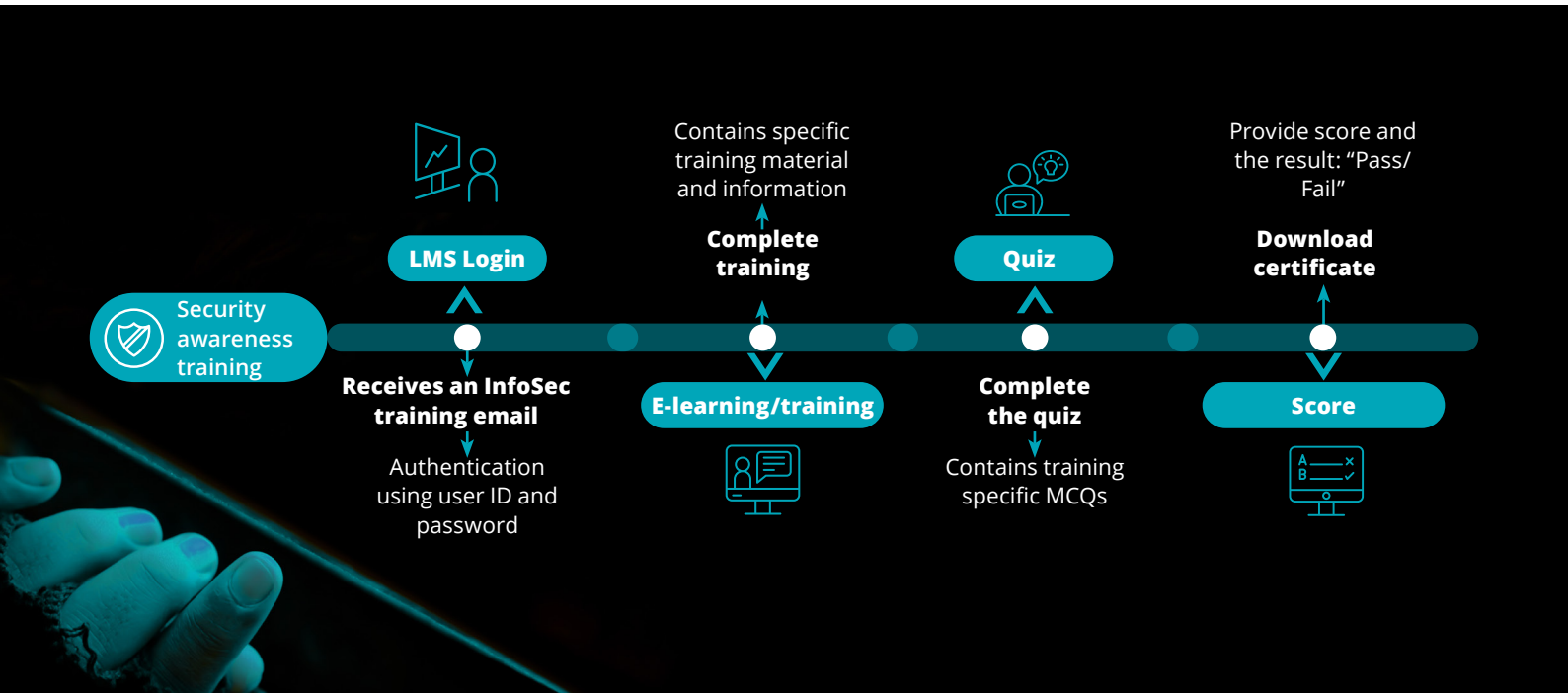
Think Deloitte, think secure

Email phishing, Vishing, and SMShing simulations

Taking into account the current market's requirements, Deloitte India offers the following simulation solutions, which include a set of initiatives aimed at making participants aware and reinforcing their basic concepts of cybersecurity and cyber-risks, while learning how to protect themselves from cyber threats.

Email phishing	**Entice to click**	Email may contain malicious links with a sense of urgency to lure users into clicking it.	**Please give me your credentials!**	Phishing attempts may try and extract your sensitive account information.	**To open that attachment or not?**	Emails may contain malicious attachments that can infect your device with a virus.
Voice phishing (Vishing)	**Voice response capturing**	You may receive a 'legitimate-looking' call asking for your personal or confidential information.	**IVR response capturing**	A voice call may be in the form of a IVR, which records your responses and seems legitimate.	**Conference call**	Vishing could be in the form of a conference call where you may find fake users sharing their personal information, leading you to believe it.
SMS phishing (SMShing)	**Entice to click**	Email may contain malicious links with a sense of urgency to lure users into clicking it.	**Please give me your credentials!**	You may receive an SMS requesting for your credentials on the basis of false information.	**Do me a favour!**	You may receive an SMS from a known source, asking for a favour.

Learning management system



Customised solutions customised needs

Phishing simulations as a service

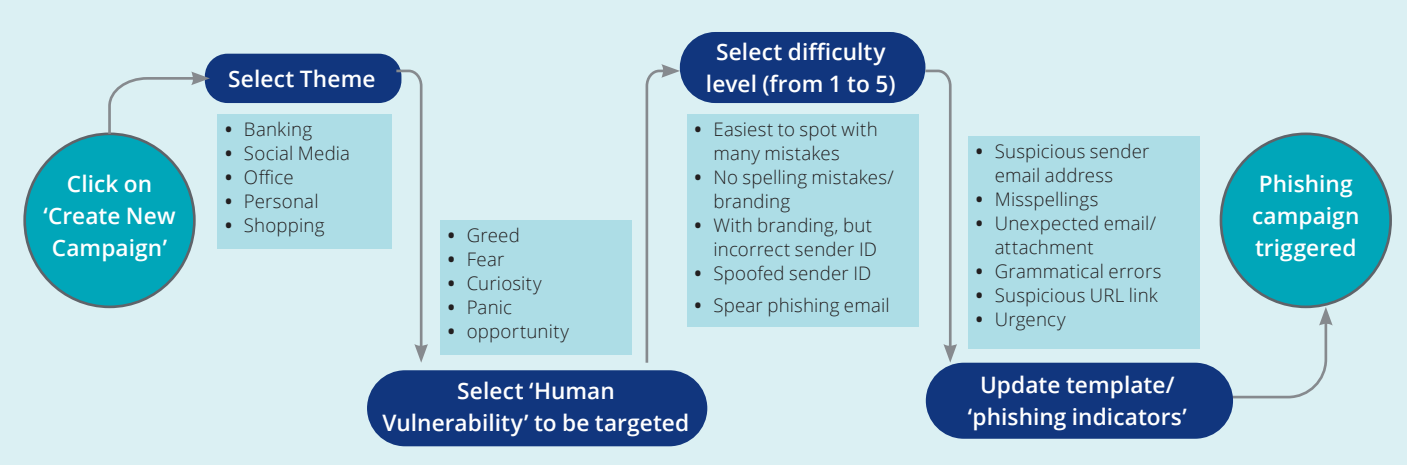
CLIENT DETAILS

Large IT service provider	The client faced an increased risk of being targeted by phishing emails. Deloitte supported continuously to stimulate employees by sending them regular phishing emails. • Value delivered: • Improved awareness among employees with respect to phishing • Change in employees' behaviour when faced with a potentially malicious email
Leading credit card industry	This engagement involves continuous support of the information security function ranging from vulnerability management and third-party risk assessment, to IT governance, information security awareness, and running phishing campaigns. This is an ongoing engagement where Deloitte has defined a process of awareness through continual training and regular email updates.
Large banking institute	The client engaged Deloitte to perform the following functions: • Development of an information security awareness programme (including executing a phishing campaign with an internal Phaas platform) • Selection of an identity governance and administration solution • Selection of an information classification solution
Large telecom provider	• The activities included defining and creating security policies, procedures, guidelines, and standards in line with ISO 27001, and aligning security policies to the relevant DOT and India IT Act, and other India regulations and guidelines. • Deloitte carried out a gap analysis and review, asset identification and classification, and a risk review, as well as implemented the ISMS. • Deloitte assisted in managing the client's IS awareness process: maintaining training records, and creating training manuals and sample campaigns for future use.

Selecting the right phishing template

Follow the steps given below to select the right phishing template:

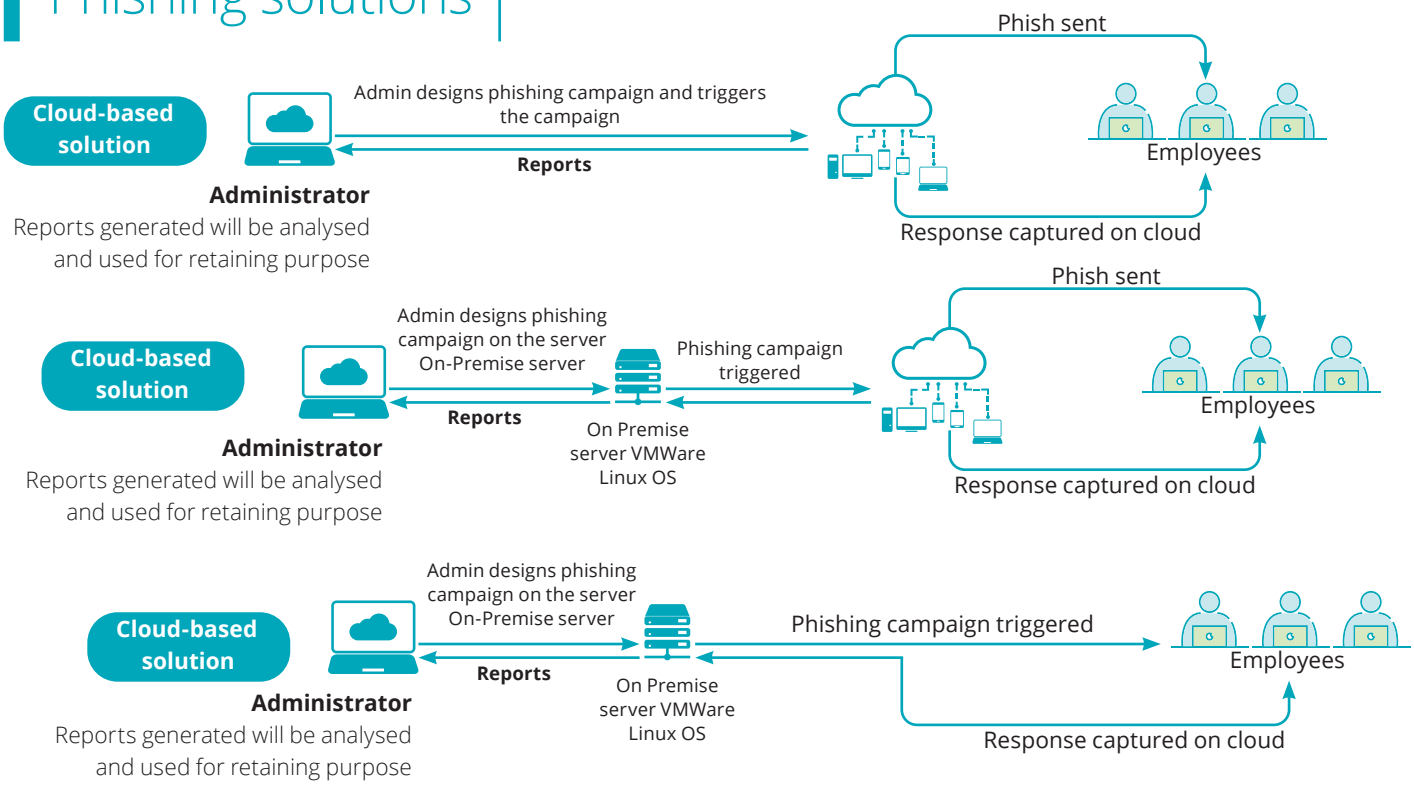
- Select the appropriate 'Theme', 'Human Vulnerability' (the template would attack), and 'Difficulty Level'.
- Update the template as required. Review the 'Phishing Indicators' in the pre-defined template that end-users would be expected to spot to identify a phishing email.
- Upload details of the target audience and the trigger campaign.



Our Phishing simulation solutions

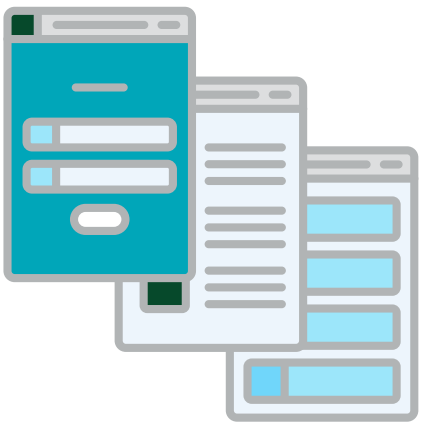
Taking into account the current market's requirements, Deloitte India offers the following simulation solutions, including a set of initiatives aimed at making the participants aware and reinforcing their basic concepts of cybersecurity and cyber-risks, while learning how to protect themselves from cyber threats

Phishing solutions



Mobile application

- Clients can login with authorised credentials and view reports for their live and completed phishing campaigns.
- The application also notifies the clients (through push notifications) of live events such as employee opening phishing simulation email, opening the attachment, and/or clicking on a phishing link during live campaigns.



Contacts

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Abhijit Katkar
Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Kamaljit Chawla
Leader – Cyber Operate
Risk Advisory, Deloitte India
kamaljitc@deloitte.com

Tarun Kaura
Leader – Cyber Advisory
Risk Advisory, Deloitte India
tkaura@deloitte.com

Ashish Sharma
Partner, Risk Advisory
Deloitte India
sashish@deloitte.com

Vikas Garg
Partner, Risk Advisory
Deloitte India
vikasgarg@deloitte.com

Deloitte.