The Fraud Show
Technology-based Fraud Awareness Training

April 2017

kpmg.nl

What do you get?
Customised training
Not another boring PowerPoint training course but a highly engaging training to improve the awareness level of your employees towards technology-based external fraud risks.

Real-life cases
With use of impactful real-life case studies and optional simulations we demonstrate behavioural vulnerability in order to show how easily it can go wrong.

Tips & guidance
We provide effective tips and guidance to mitigate the risk of external technology-driven frauds. Useful tips and guidance to identify new types of technology-based fraud are provided.

Value for money
The show enables you to train groups up to 100 participants per event making the required investment per employee very cost efficient.

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 endeavor 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.

© 2017 KPMG Advisory N.V., registered with the trade register in the Netherlands under number 33263682a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. Printed in the Netherlands. The KPMG name and logo are registered trademarks of KPMG International.

Caroline Molenaar
Director
T: +31(0)70 3382138
E: molenaar.caroline@kpmg.nl

Paul Hulshof
Senior Manager
T: +31(0)20 656 8610
E: hulshof.paul@kpmg.nl

Tjores Maes
Manager
T: +31(0)20 656 7032
E: maes.tjores@kpmg.nl
Technology-based fraud has increased exponentially due to our augmented reliance on information technology. Social engineers are becoming more professional and convincing as a result of which they are able to steal millions relatively easily, with or without your (employees) help. Many organisations are aware of this emerging and growing threat but aren't necessarily doing much about it. However, a solution is at hand, based on real-life cases: Technology based Fraud Awareness Training.

A significant amount of time and money has been invested in making systems secure in order to mitigate the risk of fraud. However, the effective security of any system is primarily influenced by the human component, which is therefore considered to be the weakest link. Fraudsters are aware of this and abuse it increasingly through social engineering. A good example of social engineering is the CEO fraud, where a fraudster convincingly poses as the CEO of a certain organisation and overrides the organisations' internal controls to make large unlawful payments.

Fraudsters have therefore come to realize that targeting employees, who are involved in key processes within organisations, can offer them great rewards. Too many organisations have unfortunately already experienced this type of technology-based fraud and have come to realize adequate measures are required. We have assisted organisations in investigating the incident itself and also educating their employees to prevent similar situations from occurring again.

In the training course we explain the risks of social engineering arising from personal exposure of your employees on the internet and provide them with effective tips and guidance to manage these risks. This is all done based on real-life examples.

This is not another boring PowerPoint training course but an interactive gameshow that will include everyone. The fraudshow is modelled around various trending topics in the external technology-based fraud domain. First of all we brainstorm together with our clients on the required content. We include real-life case studies with respect to technology-based fraud, social engineering and cybercrime. We combine our knowledge and experience, in order to reach a tailor made set of case studies, red flags, rules of conduct and best practices, which are then used in a customised show.

Typically the fraudshow will include:
- Disconcerting real-life cases and facts that participants will not easily forget:
  - Recent incidents that occurred within the organization. Actual statistics on exposure to social engineering attacks, fraud losses and possible insufficient controls.
  - Real-life corporate intelligence gathering with respect to key employees, which will increase awareness of the potential impact.
- Simulation of social engineering attacks performed on the client. The organization will not be at risk at any point. This attack will not focus on technological flaws but on human susceptibility to social engineering, such as:
  - How well do employees handle USB sticks, phishing emails or a crafty social engineering attempt?
  - How many employees connect our fake USB stick to their work machines and what happens when they do?
  - Do employees click on a link in a sophisticated phishing email? What is the impact of clicking? Do they report it when they do recognize it as a phishing email?
  - How do employees deal with calls and requests from third parties?
- Resulting ultimately in one winner.

In an auditorium or theatre-sized room, a game show format is set up, specifically designed for this purpose. Music, video and sound effects will be combined to create a fast-paced interactive environment. Participants will be grouped in teams to compete with each other through a set of challenging questions around the tailored content and the results of the simulated social engineering attack.

Participants from the audience will be chosen at random to provide insights or share their opinion in support of the contesting teams.

The finale of the show will include participation from the entire audience. The simulation provides useful insights into the organisation’s resilience with respect to potential threats.

A safe targeted social engineering attack is performed on the client. The organization will not be at risk at any point. This attack will not focus on technological flaws but on human susceptibility to social engineering, such as:

- How well do employees handle USB sticks, phishing emails or a crafty social engineering attempt?
- How many employees connect our fake USB stick to their work machines and what happens when they do?
- Do employees click on a link in a sophisticated phishing email? What is the impact of clicking? Do they report it when they do recognize it as a phishing email?
- How do employees deal with calls and requests from third parties?

This simulation provides useful insights into the organisation’s resilience with respect to potential threats.

"This is not another boring PowerPoint training but an interactive gameshow…

- this course is a real eye-opener…"

© 2017 KPMG Advisory N.V. All rights reserved.
What do you get?

Customised training
Not another boring PowerPoint training course but a highly engaging training to improve the awareness level of your employees towards technology-based external fraud risks.

Real-life cases
With use of impactful real-life case studies and optional simulations we demonstrate behavioural vulnerability in order to show how easily it can go wrong.

Tips & guidance
We provide effective tips and guidance to mitigate the risk of external technology-driven frauds. Useful tips and guidance to identify new types of technology-based fraud are provided.

Value for money
The show enables you to train groups up to 100 participants per event making the required investment per employee very cost efficient.

Contact
Caroline Molenaar
Director
T: +31(0)70 338 2138
E: molenaar.caroline@kpmg.nl

Paul Hulshof
Senior Manager
T: +31(0)20 656 8610
E: hulshof.paul@kpmg.nl

Tjores Maes
Manager
T: +31(0)20 656 7032
E: maes.tjores@kpmg.nl