KPMG

Strengthen your security posture with KPMG's Managed Phishing, Cyber Range and Training

Seamless, strategic frameworks for effective phishing protection

At a glance: Key challenges

Emerging tech like AI and machine learning are revolutionising the way businesses operate and communicate with clients and customers. In the face of persistent and emerging cyber trends, business leaders are increasingly having to navigate new challenges in digital security. These include:

Demand for process excellence

As the global economy evolves, businesses are constantly looking for smart solutions to enhance their cyber posture while maximising productivity and efficiency.

Talent gap

Even as the demand for trained cybersecurity professionals grows, scarcity in talent supply is creating potential gaps in security.

Increased regulatory frameworks

The increasing frequency and sophistication of cyber threats is driving the demand in regulation and compliance.

Adopt a robust phishing simulation program aligned with industry best practices and current threats

- **Modern phishing attacks** continue to cause chaos on an unprecedented scale.
- **Impacts** ranging from **severe financial losses** to declining market share and consumer trust, phishing attacks are increasingly becoming more rampant and sophisticated
- Made harder to detect when malicious actors use advanced social engineering techniques and leverage on **artificial intelligence** to generate more authentic looking content to exploit security gaps.

Achieve your goals securely in a dynamic, digital world

At KPMG in Singapore, our **managed phishing and awareness training services** help clients address existing and emerging cyber threats to build an integrated, intelligent and more dynamic future.

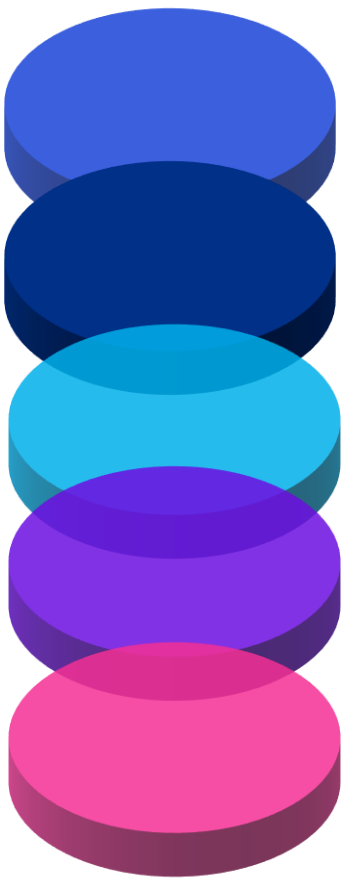
Break away from traditional annual phishing exercises and transform towards phishing **as an ongoing activity.**

Improve the cyber security vigilance of your workforce by **inculcating cyber security mindsets.**

Combining next-gen innovation and critical industry insights, our **comprehensive solutions** can help you build resilience, mitigate risk and create new value across your organisation.

Past notable phishing related cyber incidents

Phishing remains one of the most common and dangerous threats organizations face today. Despite advances in cybersecurity, phishing attacks continue to breach even the most secure environments, as seen in high-profile incidents targeting tech companies, healthcare systems, and critical infrastructure in 2023 and 2024.



01

Identity and Access Management service provider (2024)

Breached through a phishing attack on a third-party contractor. This incident affected multiple downstream clients, emphasizing the risks posed by supply chain vulnerabilities made worse by phishing.

02

Healthcare IT provider (2024)

A healthcare IT provider, suffered a phishing-based ransomware attack which resulted in disruptions to the healthcare provider it was supporting. Nationwide healthcare service was disrupted, and sensitive patient data were exposed.

03

Small Office / Home Office routers (2023)

A state sponsored attack group used phishing to compromise small office / home office (SOHO) routers to form a botnet which was later used to target U.S. critical infrastructure.

04

Major technology company (2023)

Phishing campaign targeted the tech company's employees, compromising accounts which lacked multi-factor authentication and gained access to emails of senior executives and security staff, resulting in exposure of internal communications.

05

Ride hailing platform service provider (2023)

A phishing attack against the platform provider allowed attackers to steal an employee's login credentials, which was then used to infiltrate critical internal systems. This led to significant operational disruption and raised concerns about employee training in detecting phishing.

Enhance your digital security with our managed phishing services

Our commitment to innovation and bringing new ideas to life can help empower you with the right tools to combat cyber threats through advanced phishing simulation and tailored security awareness training.

1

Phishing curation with tailored platform integration

With a focus on your organisation's needs, we can ensure that the phishing content are carefully tailored to deliver an optimal phishing simulation experience.

By modelling the content to mirror real-world threats, we can help your employees gain knowledge to effectively recognise and combat potential cyber risks.

2

Data analysis and reporting

Analysing data from simulations and training sessions provide us with valuable insights into your employees' security awareness levels. This allows us to identify key areas that require improvement or added training.

3

Deep industry experience

With a strong background in cyber incident response, our team possesses extensive knowledge of real-world threats and tactics employed by malicious actors. This allows us to design simulations and training that reflect the risks facing your organisation.

4

Project management

Our dedicated transition team comprising of a project manager and dedicated subject matter experts can help ensure a smooth onboarding process for your organisation.

5

Targeted learning approach for your cybersecurity curriculum

Our teaching approach combines a tailored cybersecurity learning curriculum that incorporates proven adult learning methodologies. By understanding your organisation's specific needs and desired outcomes, we can design a curriculum that caters to unique learning styles.

Phishing curation with tailored platform integration solutions

From comprehensive eLearning modules to employee-centric simulations, our integrated solutions means you can choose a strategy to suit your needs, no matter where you might be on the cyber security journey.

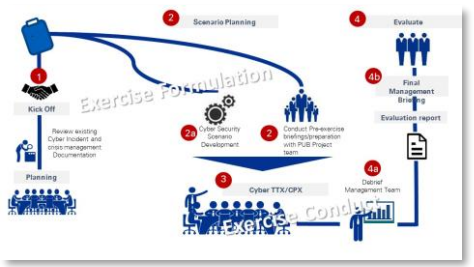
- Our comprehensive library of past exercises serve as a valuable resource for our team to ensure efficient and effective execution of phishing exercises, allowing us to draw upon our past experiences to tailor phishing exercises specifically to the needs of our clients.

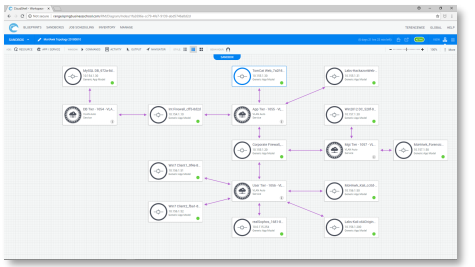
- Each phishing email template is also paired with microlearning content tailored to the specific email. For example, your staff will immediately receive short training lessons that highlight the red flags missed and reminders on how to identify and report similar emails in future.

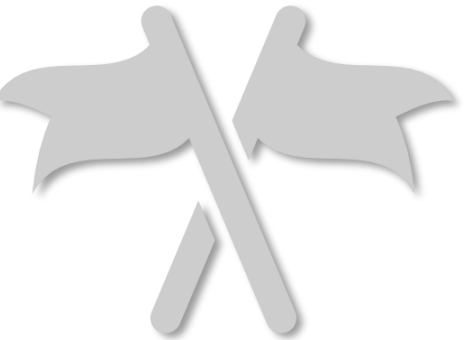
- Target specific employees by creating highly personalized phishing emails that appear to come from internal sources or business partners. This increases the likelihood of engagement and tests users' vigilance against more sophisticated threats.

- With over 1,000 learning assets in our content library of industry- and role-based training resources that is updated weekly, you will be able to build and customise training plans to deliver fresh, relevant training to every member of your organisation.
- You can also easily customise the learning plan to suit your various needs and target audience. By delivering a customised training experience for each employee, you can boost engagement rates, reduce repeat offenses and prepare employees for existing and emerging threats.

Our Cyber Training Programmes







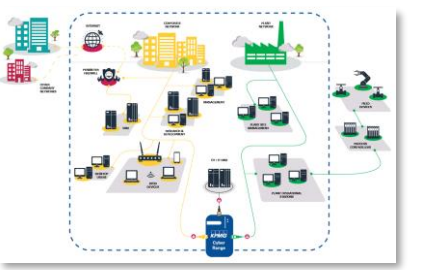


Table-Top Exercises

- Escalation plans focused, execution of steps
- Blend of management and technology teams

DFIR & Cyber Range

- Incident Response technical skill sets
- CSIRT team collaboration / technical competencies focused
- Hands-on experience in Range environment
- Either with live attacks or static snapshots
- In-Class & Virtual Session

Capture the Flag

- Attack focused with capstone quizzes
- 2 different flag programmes
- Gamified with leader board

Operational Technology

- Incident Response technical skill sets
- CSIRT team collaboration / technical competencies focused
- Hands-on experience in Range environment
- In-Class & Virtual Session

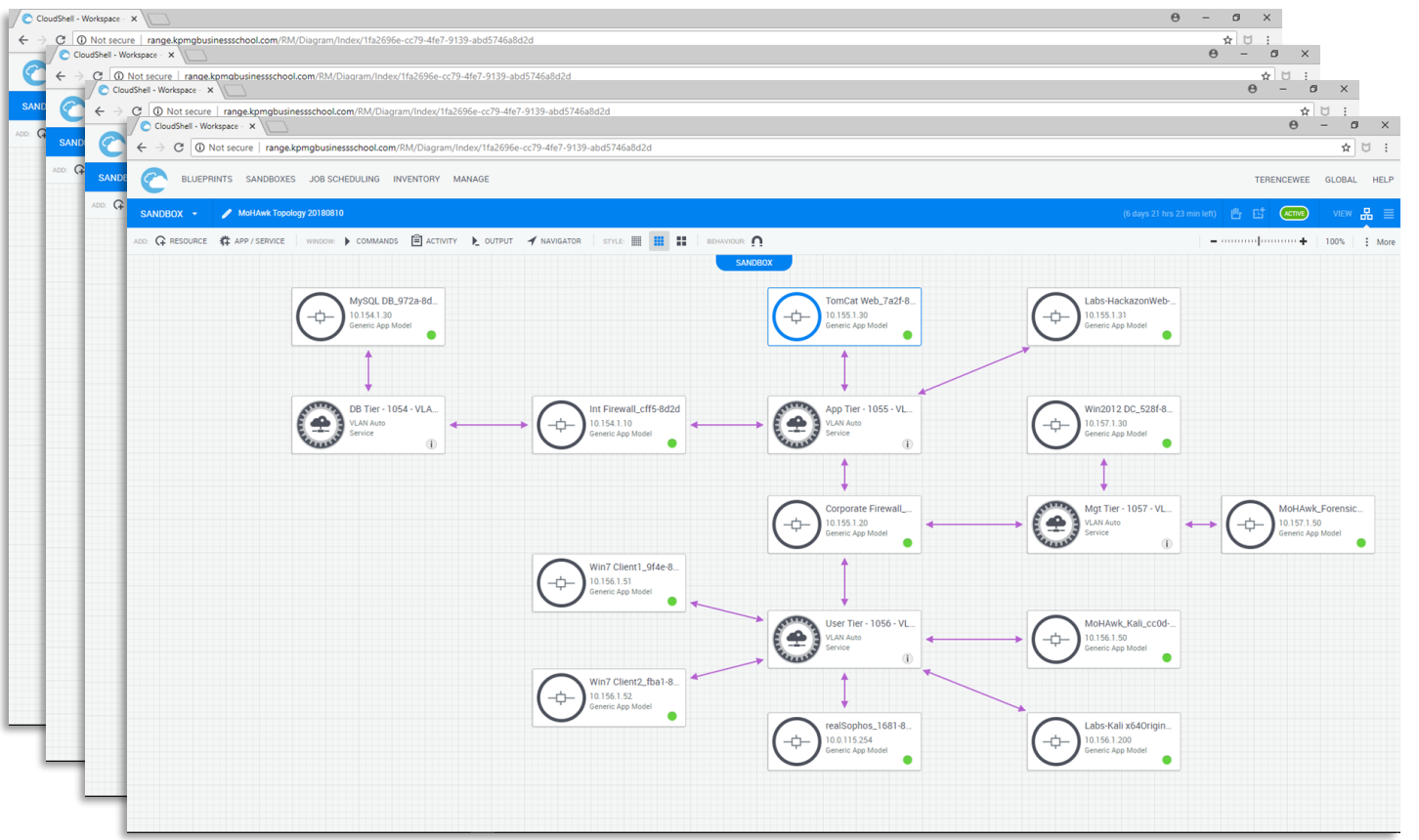
Cyber Range Simulation Environments

Our Cyber Range simulation environments are made up of instantiated blueprints called sandboxes.

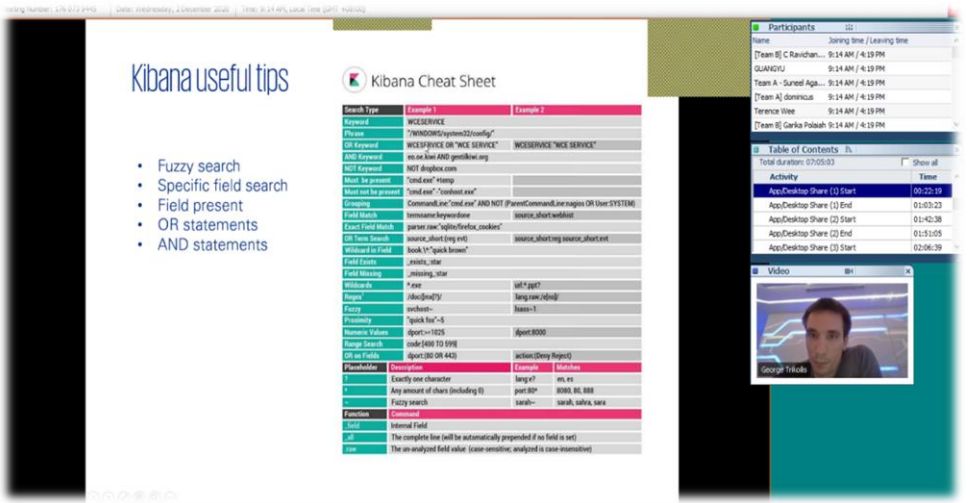
— Anything that can be virtualised can be built into the KPMG Cyber Range

— Hardware-in-the-loop model can be used for physical-only devices / components

— Multiple (identical) sandboxes can be instantiated to allow for parallel, yet diverging, team experiences

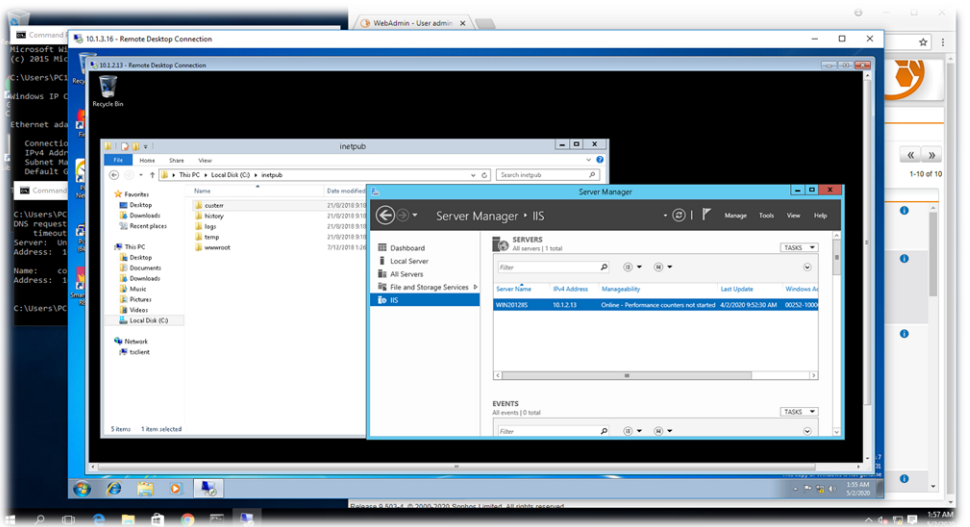


DIFR & Cyber Range – End User Views



DFIR Training (Virtual)

DFIR Training (Physical)



Cyber Range Training (Physical & Virtual)

- Remote Desktop sessions are the main way to access the simulation environment developed for a Cyber Range Exercise.
- Separate communication channel required for virtual exercises

Are you ready to focus on your business's priorities?

Our team of leading cybersecurity experts will help you achieve the best possible outcome when threats are detected, allowing you to focus on what matters.

KPMG

Contact us

Reach out to learn how we can support you on your cyber security compliance journey.

Eddie Toh
Partner
Cyber, Advisory
KPMG in Singapore
T: +65 6213 3028
E: eddietoh@kpmg.com.sg

Huang Weihan
Manager
Cyber, Advisory
KPMG in Singapore
T: +65 816 4601
E: weihanhuang1@kpmg.com.sg

kpmg.com.sg