Understand security
Many organizations are still having major security incidents, simply because of inadequate security education, training and awareness. However, a cornerstone of any good security function is effective security training, education and awareness. Understanding what works and what doesn’t is an art, and what is apparent is that many organizations haven’t yet got the balance right.

How can we help?
KPMG offers security training, education and awareness activities to identify where you could enhance your current capabilities.

KPMG has defined a world-class security awareness contents based on the following key principles:
- focus on people’s behaviour, as key players in the protection of the organization’s information and, specifically, on what they can control.
- link rules/recommended behavior with the threats that may compromise the organization’s information.
- simple content, avoiding technical language, and where appropriate with a sense of humour.
- interactive content, based on practical real-world scenarios.
- content that can be easily adapted to existing information security policies and to organization specific security concerns, and
- content that can be easily produced and translated into any e-learning platforms.

KPMG’s e-Learning platform allows our clients access to a vast set of usage and management functionality:
- Training at a user’s pace, allowing each employee to return to the course exactly where they left off.
- Control mechanisms that allow reporting execution per module and escalation mechanisms.
- Shape the course based on information associated with the user (e.g. present the Internet module only to the employees that have access to Internet).
- Provide employees with a link to the various information security policies to the contents of each module.
- Establish KPIs based on Information Security Awareness (e.g. initial state versus after awareness course).
- Evaluation engine that can be customized to present a set of random questions per course module to each employee. If evaluation is not successful, a different set of questions is presented to the employee.
- Email notification of course completion.
- Various management reports are available.

Cases of cyber security are constantly in the media. Employees should fully understand what is expected of them when it comes to maintaining the security of their organization. Unfortunately this isn’t always the case.
KPMG’s Cyber Team works with organizations to help prevent, detect and respond to cyber threats.

We can help your organization be cyber resilient in the face of challenging conditions.

Have a cyber emergency? Contact our 24/7 Cyber response hotline.
1-844-KPMG-911
1-844-576-4911

KPMG Cyber Security professionals believe cyber security should be about what you can do – not what you can’t

An objective, knowledgeable advisor
As a global network of regulated member firms, we have an unwavering commitment to precision, quality and objectivity in everything we do. So you can rest assured that KPMG cyber security assessments and recommendations are based on what’s best for your business – not on market hype.

Knowledge of emerging issues
In our I-4 Forum, also known as the International Integrity Institute, we convene leading cyber security professionals from around the world to discuss emerging threats, regulatory challenges and solutions. So we can help you consider possible issues around the corner in financial services, oil and gas, pharmaceuticals, engineering and other industries.

Rated no. 1 In executive management
In fact, in a 2016 Forrester Wave™ study on information security consulting services, companies rated KPMG No. 1 for counseling senior leadership on cyber security. KPMG member firms surpass other professional services firms and technical firms to help board members understand cyber security, make informed decisions that align to the business strategy, and feel assured in their due diligence.

Transforming security across different geographies and cultures
KPMG member firms have deep local knowledge in nearly every market where you do business, so we understand cyber security risks, regulatory impacts, change management, forensic investigations and other factors that may change from one country to the next. We have a global network of more than 3,000 cyber security professionals, plus multi-disciplinary collaboration with 189,000 other professionals in KPMG member firms across more than 152 countries. With that global presence, we can help you drive security transformation across your operations, wherever they may be.