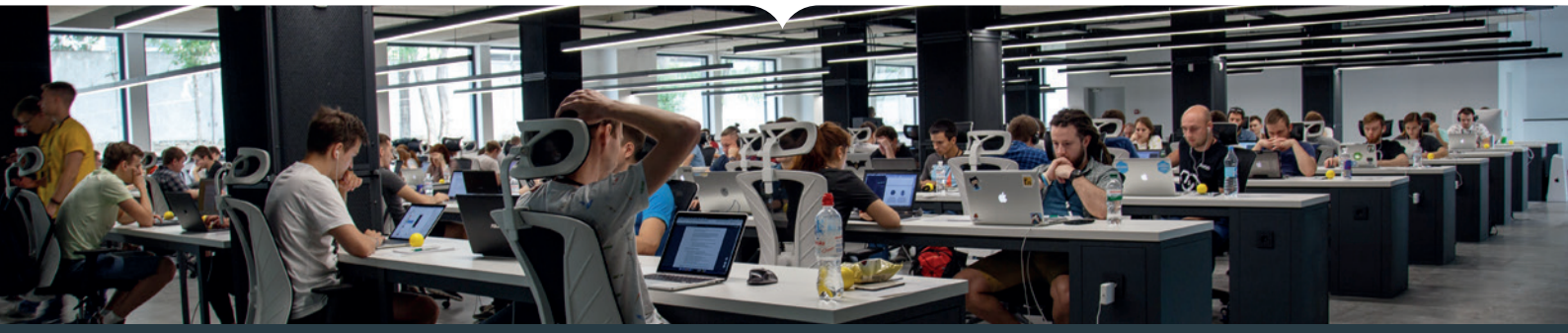
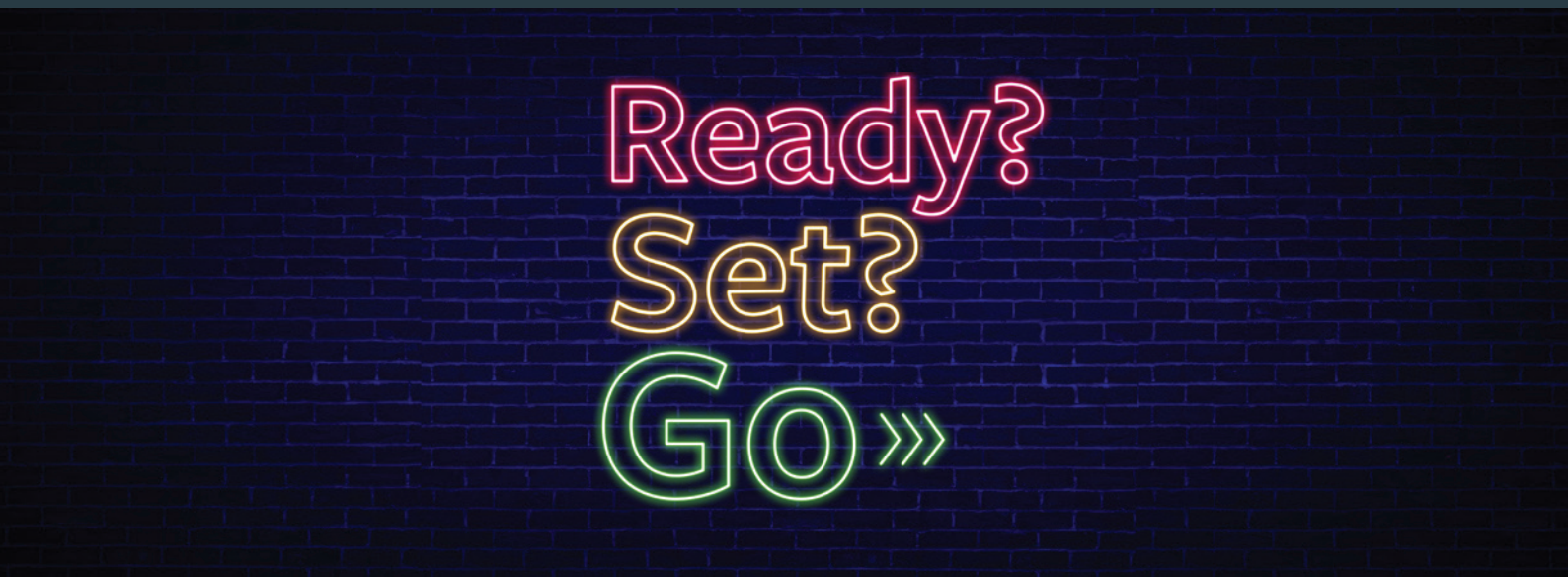
TRAVELERS



TRAVELERS RISK CONTROL



Cyber Security Training for Employees

Empowering your employees to recognise common cyber threats can be beneficial to your organisation's computer security. Security awareness training teaches employees to understand vulnerabilities and threats to business operations. Your employees need to be aware of their responsibilities and accountabilities when using a computer on a business network.

New hire training and regularly scheduled refresher training courses should be established in order to instill the data security culture of your organisation. Employee training should include, but not be limited to:

Responsibility for Company Data
Continually emphasise the critical nature of data security and the responsibility of each employee to protect company data. You and your employees have legal and regulatory obligations to respect and protect the privacy of information and its integrity and confidentiality.

Document Management and Notification Procedures
Employees should be educated on your data incident reporting procedure in the event an employee's computer becomes infected by a virus or is operating outside its norm (e.g., unexplained errors, running slowly, changes in desktop configurations, etc.). They should be trained to recognise a legitimate warning message or alert. In such cases, employees should immediately report the incident so your IT team can be engaged to mitigate and investigate the threat.

Passwords
Train your employees on how to select strong passwords. Passwords should be cryptic so they cannot be easily guessed but also should be easily remembered so they do not need to be in writing. Your company systems should be set to send out periodic automatic reminders to employees to change their passwords.

Unauthorised Software

Make your employees aware that they are not allowed to install unlicensed software on any company computer. Unlicensed software downloads could make your company susceptible to malicious software downloads that can attack and corrupt your company data.

Internet Use

Train your employees to avoid emailed or online links that are suspicious or from unknown sources. Such links can release malicious software, infect computers and steal company data. Your company also should establish safe browsing rules and limits on employee Internet usage in the workplace.

Email

Responsible email usage is the best defence for preventing data theft. Employees should be aware of scams and not respond to email they do not recognise. Educate your employees to accept email that:

- Comes from someone they know.
- Comes from someone they have received mail from before.
- Is something they were expecting.
- Does not look odd with unusual spellings or characters.
- Passes your anti-virus program test.

Social Engineering and Phishing

Train your employees to recognise common cybercrime and information security risks, including social engineering, online fraud, phishing and web-browsing risks.

Social Media Policy

Educate your employees on social media and communicate, at a minimum, your policy and guidance on the use of a company email address to register, post or receive social media.

Mobile Devices

Communicate your mobile device policy to your employees for company-owned and personally owned devices used during the course of business.

Protecting Computer Resources

Train your employees on safeguarding their computers from theft by locking them or keeping them in a secure place. Critical information should be backed up routinely, with backup copies being kept in a secure location. All of your employees are responsible for accepting current virus protection software updates on company PCs.