

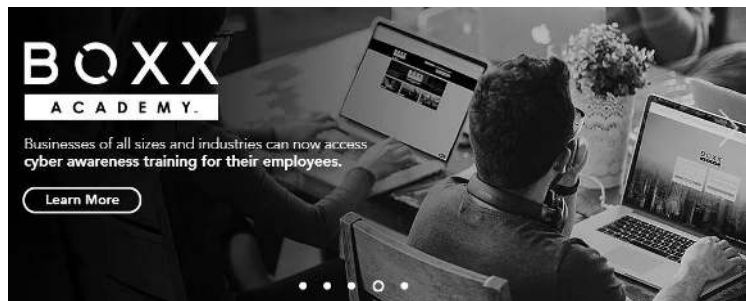
# Members can help reduce their cyber risk by educating employees to 'stop clicking around'

Employee Education Program – Online enrollment and assessment

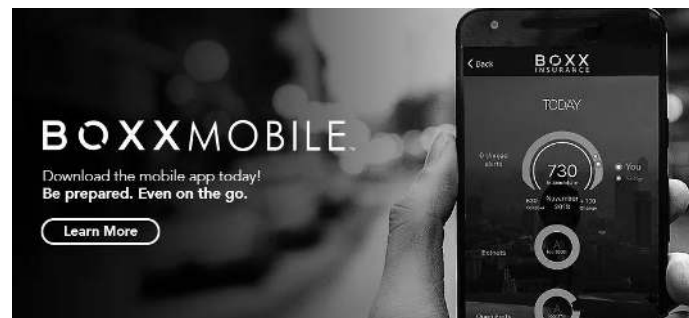


# Welcome to cyberboxx

We go beyond insurance. Our 3 features helps reduce your risk of being hacked as well as ensuring you can respond and recover from a breach



Train your employees for free on BOXX's e-learning platform

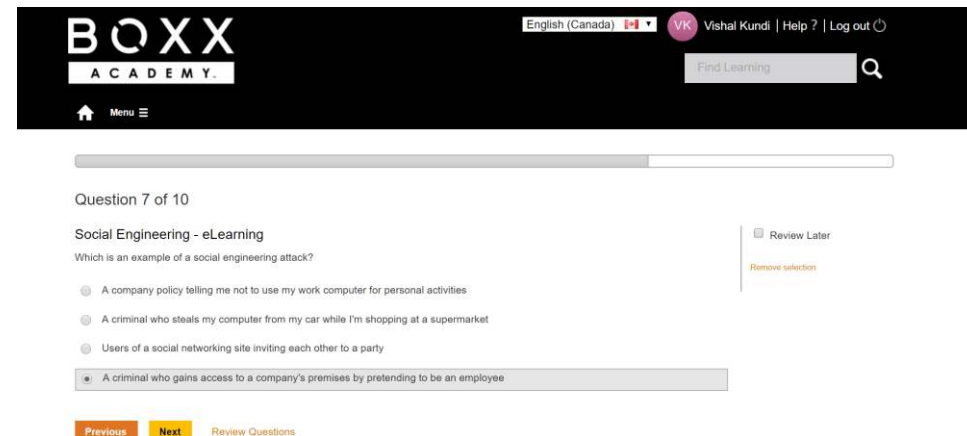
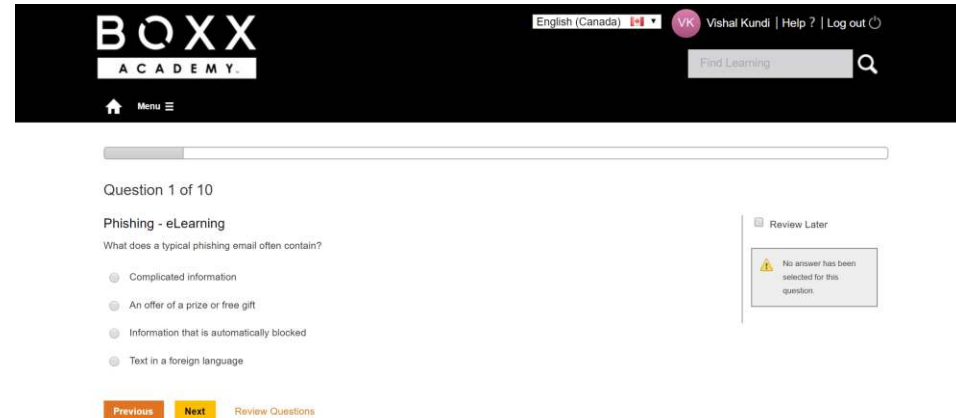
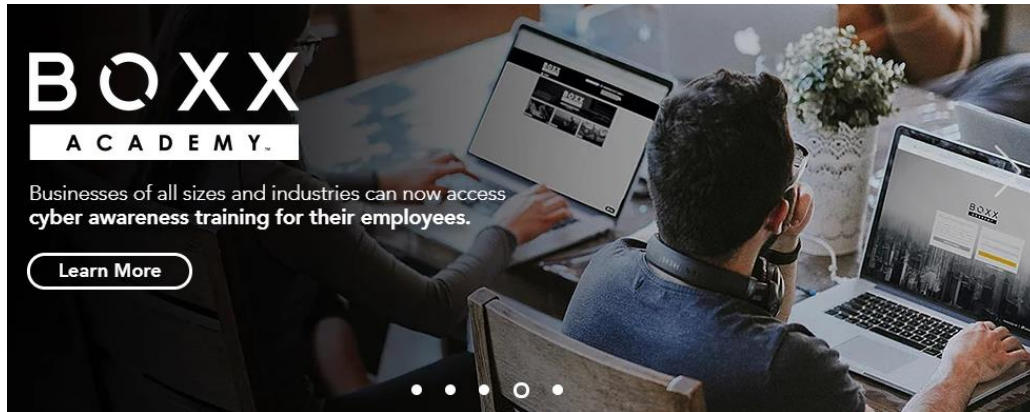


Boost your cyber fitness with our automated monitoring at minimal cost



Cyber insurance included to help you respond and recover

# The course is already accredited by Regulatory body for Insurance Brokers of Ontario for 5.5. hours



11 topics grouped under 4 modules to educate employees. Own pace training @ [www.boxxacademy.com](http://www.boxxacademy.com)



MODULE ONE

Managing online risks



MODULE TWO

Keeping safe online



MODULE THREE

Protecting information



MODULE FOUR

Safe device use

# Each of the four modules include video and reading content users can study in their own time



# Learn how to avoid phishing attacks and keep sensitive information safe line and on social media

## 1. Managing Online Risks:

Avoiding phishing and social engineering attacks helps keep sensitive information secure. Understand what the online risks are and what you can do to avoid being successfully attacked.

- **Phishing** : Understand how phishing emails are used to steal sensitive information, launch cyber-attacks, and how to prevent them. The damages resulting from a successful attack are highlighted.
- **Social Engineering**: Learn how our willingness to help can be abused to launch cyber-attacks and what actions to take to avoid being social engineered.

## 2. Keeping Safe Online:

Online services are used by most of us for business and personal use. Understand what online risks you face and what sensible precautions will help keep you safe online.

- **Online Safety**: Learn the basics of how to work online safely and responsibly and how to protect sensitive information when browsing.
- **Social Media Protection**: Understand how to use social media securely and responsibly and where the boundary lies between personal and organization information.

# Understand how to protect PII data and how to protect information on your mobile devices

## 3. Protecting Information:

Information is precious and critical to both individuals and organizations. Understand what the risks are and how best you can protect it.

- **Personal Information:** Learn what constitutes personally identifiable information and what you need to do to help keep this secure.
- **Information Handling:** Learn how different types of information should be stored, shared and used, using appropriately secure methods.
- **Data Protection and Regulation: All Staff General Awareness:** Personal data needs to be protected and used correctly in order to be compliant with regulation – using GDPR as the benchmark.
- **Removable Media:** Understand the risks of using removable media, when it should be used and what precautions to take to protect information

## 4. Safe Device Use:

Devices provide a way to access information and services whenever we need. Understand what the risks are to devices and how to keep them well protected to limit unauthorized access.

- **Bring Your Own Device (BYOD):** Understand what the risks are with Bring your own device and what measures should be taken to protect sensitive information.
- **Password Safety:** Learn how passwords should be securely set and stored to help prevent your password being compromised to gain unauthorised access to critical information and services.
- **Remote and Mobile Working:** Understand the risks when working outside your organization's secure premises and networks and how to protect information when working remotely.

# Track employees progress. A quick diagnostic baselines their knowledge prior to taking the modules

You have answered 10 out of 10 Questions.

| Question   |
|--|
| <b>Phishing - eLearning</b>  |
| 1. What does a typical phishing email often contain?   |
| 2. What can you do to protect against phishing attacks?  |
| 3. What is spear phishing?   |
| 4. You have received an email from your bank asking you to log in to your account. What should you do? |
| 5. Which is an example of a typical phishing message?  |
| <b>Social Engineering - eLearning</b>  |
| 6. Which of these is NOT an example of social engineering?   |
| 7. Which is an example of a social engineering attack?   |
| 8. Which process verifies whether someone is who they say they are?                                    |
| 9. Which is an example of pretexting in a social engineering attack?                                   |
| 10. What is a social engineer?   |

Click the finish button below to end the assessment.

[Previous](#) [Finish](#)

## Your Diagnostic Assessment

Managing Online Risks - Diagnostic Assessment

**ATTEMPT FEEDBACK**

Questions: 10

Score: 80% (8 correct out of 10)

✔ Completed ○ Learning need

| TOPICS                          |         | QUESTIONS |                                      |                        |
|---------------------------------|---------|-----------|--------------------------------------|------------------------|
| ACTIVITY                        | DETAILS | SCORE     | STATUS                               | ACTIONS                |
| Phishing >                      |         | 4/5       | <span style="color: green;">✔</span> | <a href="#">Launch</a> |
| Social Engineering >            |         | 4/5       | <span style="color: green;">✔</span> | <a href="#">Launch</a> |
| <a href="#">Exit Assessment</a> |         |           |                                      |                        |

He



Each module has an assessment. 80% pass threshold.  
Certificates provided for proof of assessment.

The screenshot shows the BOXX Academy website header with the logo, language selector (English (Canada)), user profile (VK Vishal Kundi), and navigation links (Help, Log out). Below the header is a search bar and a breadcrumb trail: Home > Menu > My Activities > Managing Online Risks - L. >

## Managing Online Risks - International

### Description

When spending an increased amount of time online, it is important to understand what the online risks are and what you can do to avoid being successfully attacked.

Within this pathway are video animations, eLearning, summary document (PDF) and game learning modules covering:

- Phishing
- Social Engineering

The pathway starts with an optional diagnostic assessment and finishes with an assessment (20 questions).

| Filters       |
|---------------|
| Summary       |
| Not Completed |
| Completed     |
| All           |

|         |                     |
|---------|---------------------|
| Status: | All                 |
| Type:   | All (1) Pathway (1) |

| Activity  | Details | Status    | Planned Date |
|---|---------|-----------|--------------|
| Managing Online Risks  Print Certificate<br>★★★★★ | Info    | Completed | None         |

### Attempt Summary

|                       |           |
|-----------------------|-----------|
| Status:               | Completed |
| Percentage Completed: | 100.00%   |
| Result:               | Passed    |
| Time Spent:           | 00:08:36  |
| Total Views:          | 6         |
| Last Attempt:         | 8/15/2019 |
| Best Score:           | 80.00%    |
| Completed On:         | 8/15/2019 |



# 4 Cyberboxx membership to select from based on the level of your team's security expertise



ONE STAR

Cyber insurance plus  
free Employee training



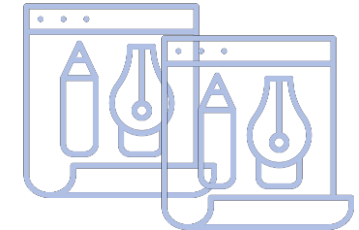
2 STAR

Adds the BOXX Mobile  
and daily monitoring



3 STAR

Adds 24/7 security  
including managed firewall  
at no additional cost



4 STAR

Add Managed Back up  
and Recovery service

# BOXXMOBILE. Risk control at your finger-tips. All we need is your website to monitor loopholes....

- 1** WE MONITOR YOUR SCORE  
You are keeping on top of your cyber health
- 2** REDUCE RISK OF BEING HACKED  
Catch, Match, Patch assessed daily
- 3** REPORT A BREACH  
Contact numbers and policy details stored in the digital wallet
- 4** SAVE ON INSURANCE COSTS  
Be rewarded for your cyberhealth overtime



+ Check BOXX score on a daily basis.



+ Track and action alerts with your team.



+ Report a breach to the Hackbusters™.



+ Be rewarded for being cyber healthy.