**CONTENT CREATION WEBINAR**

**Outline, Learning Outcomes and Potential Resources**

You are my digital assistant and co-developer of a 10-module 24-hour-long microcredential for people in work to upgrade their skills, knowledge and capabilities related to cybersecurity. I need you to help me create content, assessment tools and ideas for presentations. I'd like to start with you providing an outline of each of the 10 modules. Each module should have: (a) learning outcomes and objectives; (b) up to 10 items of critical content; (c) some suggested open educational resources; and (d) five suggested self-assessment questions.

**Self-Assessments**

Create a 15 item multiple choice self-assessment for Module 9. Provide the answer key at the end. Make sure that a student has to use different responses – correct answer cannot always be a!

**Exam Questions**

For each module, suggest six exam questions that could appear on a final exam for the micro-credential.

**Suggest a Video Script**

For Module 9, suggest a script with scene changes and image ideas, The video should be 5-7 minutes long and be highly engaging.

**Suggest the Lecture Notes**

Suggest the teaching notes needed for module 0, assuming each involves a 140 minute presentation lecture or formal presentation.

**Translation**

Translate each of these lecture notes into French.

**Suggest Activities**

The micro-credential may involve a 2-day, 8 hours a day boot camp where students get hands-on experience. Suggest a design for a fun, highly interactive, yet very practical boot camp with both team building and hands-on experiences built in. Offer your design in English.

**Resource Finding**

Suggest 5 videos I could use for module 9 which are available freely online. Offer five bullets summarising each.

**OER**

Suggest open education resources appropriate for cybersecurity

**Comparison**

Suggest five similar micro-credentials or short courses from Canada, US or UK that are focused on cybersecurity for this same target audience.

**Case Studies**

Suggest ten case studies related to the themes of Module 9 that we could use. Make sure some are from business, some from higher education and some from a government.

**Fact Finding**

Generate 20 facts about cybersecurity which highlight the severity of the threat. Use Canadian examples.

**Exploring**

What is missing in most courses and training programs focused on cybersecurity?

**Write Code**

Create code that would enable text to speech. Then do the same for speech to text.

**CHAT GPT RESPONSES**

# CHATGPT GENERATED OUTLINES LIKE THIS FOR ALL 10 MODULES.

**Module 9: Social Engineering and Physical Security**

(a) Learning outcomes and objectives:

* Understand the basics of social engineering and physical security
* Identify common social engineering tactics and physical security threats
* Recognize the importance of protecting against social engineering and physical security threats

(b) Critical content:

1. Social engineering concepts and principles
2. Social engineering tactics (phishing, pretexting, baiting, tailgating, etc.)
3. Physical security concepts and principles
4. Physical security threats and vulnerabilities
5. Access control systems (badges, biometrics, etc.)
6. CCTV and surveillance systems
7. Alarms and intrusion detection systems
8. Physical security best practices
9. Physical security testing and auditing
10. Physical security compliance and regulations

(c) Suggested open educational resources:

* Social Engineering by SANS Institute
* Physical Security Fundamentals by FEMA
* Social Engineering and Manipulation by University of California, Davis

(d) Suggested self-assessment questions:

1. What is social engineering and why is it a security concern?
2. What are some common social engineering tactics?
3. What is physical security and why is it important?
4. What are some physical security threats and vulnerabilities?
5. What are some best practices for physical security?

# **Multiple Choice Self-Quiz**

Sure, here are 15 multiple-choice questions with the answer key at the end for Module 9: Social Engineering and Physical Security:

1. What is social engineering? a. A type of computer virus b. A practice of manipulating people into giving up confidential information or access to secure systems c. A type of encryption algorithm d. A method of securing physical assets

Answer: b

1. What is pretexting? a. Using social media to gather information about someone b. Creating a fake scenario to gain access to confidential information or systems c. Stealing information by intercepting wireless signals d. Using biometrics to authenticate users

Answer: b

1. What is baiting?

a. Leaving a physical device, such as a USB drive, in a public place to entice someone to use it and infect their system with malware

b. Tricking someone into revealing their password

c. Pretending to be a legitimate company or organization to gather information d. Physically following someone into a secure area

Answer: a

1. What is tailgating?

a. Using a pretext to gain access to secure systems

b. Pretending to be a legitimate company or organization to gather information c. Following someone into a secure area without proper authorization

d. Stealing information by intercepting wireless signals

Answer: c

1. What is phishing?

a. A type of social engineering attack that uses email or other electronic communication to trick people into revealing sensitive information

b. Leaving a physical device, such as a USB drive, in a public place to entice someone to use it and infect their system with malware

c. Following someone into a secure area without proper authorization

d. Stealing information by intercepting wireless signals

Answer: a

# Possible Exam Questions for Module 9

1. What is social engineering, and why is it a security concern? a. Define social engineering and describe why it is a security concern.
2. What are some common social engineering tactics? a. List and describe some common social engineering tactics.
3. What is phishing, and how does it work? a. Define phishing and describe how it works.
4. What is baiting, and how does it work? a. Define baiting and describe how it works.
5. What is tailgating, and why is it a security concern? a. Define tailgating and explain why it is a security concern.
6. What is physical security, and why is it important? a. Define physical security and explain why it is important.
7. What are some physical security threats? a. List and describe some common physical security threats.
8. What are access control systems, and why are they important for physical security? a. Define access control systems and explain why they are important for physical security.
9. What is CCTV, and how does it work? a. Define CCTV and describe how it works.
10. What are some best practices for physical security? a. List and describe some best practices for physical security.

# **Video Script for Module 9**

For Module 9, suggest a script with scene changes and image ideas, The video should be 5-7 minutes long and be highly engaging.

Opening Shot: The video opens with an aerial view of a busy city, with the narrator introducing the topic of social engineering and physical security.

Scene 1: The narrator is standing in front of a busy office building, explaining how social engineering attacks can happen anywhere and anytime.

Image Idea: Showing footage of people entering and exiting an office building, with text overlay highlighting the potential for social engineering attacks.

Scene 2: The video cuts to a graphic of a computer screen, with the narrator explaining how phishing attacks work.

Image Idea: Showing a graphic animation of a phishing email, with the narrator pointing out the common features of a phishing email.

Scene 3: The video cuts to a security guard monitoring a CCTV system, with the narrator explaining the importance of physical security.

Image Idea: Showing footage of a security guard monitoring a CCTV system, with text overlay highlighting the importance of physical security.

Scene 4: The video cuts to a reenactment of a tailgating attack, with the narrator explaining how these attacks can happen in seemingly secure areas.

Image Idea: Showing a reenactment of a tailgating attack, with the narrator pointing out the vulnerabilities in the security system.

Scene 5: The video cuts to a graphic of an access control system, with the narrator explaining how access control systems can improve physical security.

Image Idea: Showing a graphic animation of an access control system, with the narrator pointing out the benefits of using an access control system.

Scene 6: The video cuts to a security expert demonstrating a physical security audit, with the narrator explaining the importance of regular security audits.

Image Idea: Showing a security expert conducting a physical security audit, with text overlay highlighting the benefits of regular security audits.

Scene 7: The video cuts to a group of employees in a training session, with the narrator explaining the importance of security awareness training.

Image Idea: Showing a group of employees in a training session, with text overlay highlighting the importance of security awareness training.

Closing Shot: The video ends with the narrator summarizing the main points of the module, with a graphic of a padlock symbolizing the importance of security.

Image Idea: Showing a graphic animation of a padlock, with text overlay summarizing the key points of the module.

# **Lecture Notes Module 9 – 40 minutes**

**Slide 1 (Title Slide): Social Engineering and Physical Security**

* Introduce the topic and provide an overview of the presentation.

**Slide 2 (2 minutes): What is Social Engineering?**

* Define social engineering and provide examples of common social engineering tactics.
* Suggested image: A graphic of a phishing email or a social engineering scenario.

**Slide 3 (5 minutes): Types of Social Engineering Attacks**

* Describe various types of social engineering attacks, such as phishing, pretexting, baiting, and tailgating.
* Provide examples and explain how each attack works.
* Suggested image: A chart or infographic showing the different types of social engineering attacks.

**Slide 4 (5 minutes): How to Protect Against Social Engineering Attacks**

* Discuss best practices for protecting against social engineering attacks, such as security awareness training, using strong passwords, and being cautious with email and social media.
* Provide examples of how to implement these best practices.
* Suggested image: A graphic of a padlock or a security awareness training session.

**Slide 5 (5 minutes): What is Physical Security?**

* Define physical security and describe the various aspects of physical security.
* Suggested image: A graphic of a building with various physical security measures.

**Slide 6 (5 minutes): Common Physical Security Threats**

* Describe common physical security threats, such as theft, vandalism, and natural disasters.
* Provide examples of how these threats can be prevented or mitigated.
* Suggested image: A chart or infographic showing the different types of physical security threats.

**Slide 7 (5 minutes): Access Control Systems**

* Discuss the importance of access control systems for physical security and provide examples of different types of access control systems.
* Suggested image: A graphic of an access control system or a chart comparing different types of access control systems.

**Slide 8 (5 minutes): CCTV and Surveillance Systems**

* Describe how CCTV and surveillance systems can enhance physical security.
* Provide examples of different types of CCTV and surveillance systems.
* Suggested image: A graphic of a CCTV camera or a chart comparing different types of CCTV and surveillance systems.

**Slide 9 (5 minutes): Best Practices for Physical Security**

* Discuss best practices for physical security, such as conducting regular security audits, implementing security protocols, and training employees on security awareness.
* Provide examples of how to implement these best practices.
* Suggested image: A graphic of a checklist or a security audit in progress.

**Slide 10 (3 minutes): Ethics and Professionalism in Social Engineering and Physical Security**

* Discuss the ethical considerations and professional standards in social engineering and physical security.
* Suggested image: A graphic of a code of ethics or a security professional in action.

**Slide 11 (1 minute): Conclusion**

* Summarize the main points of the presentation and emphasize the importance of social engineering and physical security.
* Suggested image: A graphic of a padlock or a security symbol.

*Note: These are just suggested lecture notes, and the actual content, timing, and images should be tailored to the specific learning objectives and critical content of the module, as well as the instructor's style and audience*.

# **Translation**

Translate the last 3 slides into French

**Slide 9 (5 minutes): Meilleures Pratiques pour la Sécurité Physique**

* Discuter des meilleures pratiques pour la sécurité physique, telles que la réalisation d'audits de sécurité réguliers, la mise en place de protocoles de sécurité, et la formation des employés à la sensibilisation à la sécurité.
* Fournir des exemples de mise en œuvre de ces meilleures pratiques.
* Image suggérée : une image d'une liste de contrôle ou d'un audit de sécurité en cours.

**Slide 10 (3 minutes): Éthique et Professionnalisme en Ingénierie Sociale et Sécurité Physique**

* Discuter des considérations éthiques et des normes professionnelles en matière d'ingénierie sociale et de sécurité physique.
* Image suggérée : une image d'un code d'éthique ou d'un professionnel de la sécurité en action.

**Slide 11 (1 minute): Conclusion**

* Résumer les points principaux de la présentation et souligner l'importance de l'ingénierie sociale et de la sécurité physique.
* Image suggérée : une image d'un cadenas ou d'un symbole de sécurité.

# **Design for a Boot Camp**

Day 1:

Morning Session (2 hours)

* Icebreaker: Have students pair up and share a story about a time they were tricked or fooled, either in person or online. This will help break the ice and get everyone comfortable sharing their experiences.
* Lecture: Provide an overview of social engineering and physical security, including common tactics and threats. Use interactive visuals and real-world examples to keep students engaged.

Afternoon Session (3 hours)

* Hands-on Exercise: Divide students into small teams and have them conduct a social engineering attack against another team. This could involve creating a fake phishing email or pretexting scenario, and the team that successfully tricks the other team wins a prize.
* Debrief: Have each team share their experience and discuss what they learned. This will help reinforce the concepts covered in the morning session.

Evening Session (2 hours)

* Team Building: Have students participate in a fun activity, such as an escape room or a scavenger hunt. This will help build teamwork and encourage students to get to know each other outside of the classroom.

Day 2:

Morning Session (2 hours)

* Lecture: Cover advanced topics in social engineering and physical security, such as spear phishing and physical security audits. Use real-world case studies to illustrate the importance of these topics.

Afternoon Session (3 hours)

* Hands-on Exercise: Have students conduct a physical security audit of a simulated building or facility. This could involve identifying vulnerabilities and making recommendations for improvement.
* Debrief: Have students present their findings to the class and discuss the importance of physical security.

Evening Session (2 hours)

* Group Discussion: Have students participate in a group discussion about the ethical considerations of social engineering and physical security. Use scenarios and case studies to prompt discussion and debate.

# **Suggest Some Possible Videos**

1. ***"What is Social Engineering?" by Symantec Corporation (2:44)***

* Provides a brief overview of social engineering, including common tactics and how to protect against them.
* Includes helpful visuals and examples to make the content more accessible.

1. ***["Social Engineering: The Art of Human Hacking" by RSA Conference (1:01:38)](https://www.youtube.com/@RSAConference)***

* Features a keynote presentation by social engineering expert [Christopher Hadnagy,](https://www.youtube.com/watch?v=p40fZFAUz6U) covering the psychology of social engineering and how to defend against it.
* Provides in-depth information and real-world examples.

1. ***"The Basics of Physical Security" by Security Baron (3:43)***

* Provides an introduction to physical security and the importance of securing physical assets.
* Includes helpful visuals and real-world examples to illustrate key concepts.

1. ***"***[***Access Control Systems Explained***](https://www.youtube.com/watch?v=NSxK1WP4TLU)***" by Verkada (3:37)***

* Provides an overview of access control systems and how they can improve physical security.
* Includes a demonstration of how an access control system works and the benefits of using one.

1. ***"Introduction to CCTV Systems" by ITS (7:29)***

* Provides an introduction to CCTV systems and how they can enhance physical security.
* Includes a demonstration of how CCTV systems work and the benefits of using one.

# **Suggest 10 Case Studies**

1. **Business Case Study: Target Data Breach**

* In 2013, hackers stole the personal and financial information of up to 110 million Target customers, using a combination of social engineering tactics and malware.
* This case study highlights the importance of both physical and cyber security, and how social engineering attacks can have serious consequences.

1. **Higher Education Case Study: University of Iowa Social Engineering Attack**

* In 2020, the University of Iowa fell victim to a social engineering attack that compromised the personal information of thousands of students and staff.
* This case study demonstrates the importance of security awareness training for employees and students, and the need for strong access control systems.

1. **Government Case Study: U.S. Capitol Breach**

* In 2021, a mob of protesters breached the U.S. Capitol building, highlighting the vulnerabilities of physical security measures and the need for better access control systems and emergency protocols.

1. **Business Case Study: Google Phishing Attack**

* In 2017, a phishing attack targeting Google employees successfully compromised the personal information of some employees.
* This case study demonstrates the importance of email security and the need for strong access control systems and security awareness training.

1. **Higher Education Case Study: University of Maryland Data Breach**

* In 2014, the University of Maryland experienced a data breach that compromised the personal information of over 300,000 students and staff.
* This case study highlights the need for strong physical security measures and the importance of conducting regular security audits.

1. **Government Case Study: U.S. Office of Personnel Management Data Breach**

* In 2015, hackers gained access to the personal information of over 20 million current and former U.S. government employees through a social engineering attack on the U.S. Office of Personnel Management.
* This case study demonstrates the importance of both physical and cyber security, and the need for strong access control systems and security awareness trainin

1. **Business Case Study: Equifax Data Breach**

* In 2017, credit reporting agency Equifax experienced a data breach that compromised the personal information of up to 147 million customers.
* This case study highlights the importance of both physical and cyber security, and the need for strong access control systems and regular security audits.

1. **Higher Education Case Study: University of California Los Angeles (UCLA) Data Breach**

* In 2014, UCLA experienced a data breach that compromised the personal information of up to 4.5 million people.
* This case study emphasizes the importance of physical security measures and access control systems, as well as the need for security awareness training for employees and students.

1. **Government Case Study: U.S. Nuclear Regulatory Commission Data Breach**

* In 2013, the U.S. Nuclear Regulatory Commission experienced a data breach that compromised the personal information of thousands of employees and contractors.
* This case study highlights the need for strong access control systems and security awareness training in high-security environments.

1. **Business Case Study: Twitter Hack**

* In 2020, several high-profile Twitter accounts were compromised in a social engineering attack that allowed hackers to post fraudulent messages and solicit Bitcoin payments.
* This case study demonstrates the need for strong email security and access control systems, as well as the importance of security awareness training for employees.

# **Provide Summary Statistics and Key Information About Cybersecurity (Canada)**

1. In 2019, the cost of cybercrime in Canada was estimated at over $7 billion. (Source: Canadian Centre for Cyber Security)
2. Canada is the fourth most targeted country in the world for cyber attacks, behind the United States, United Kingdom, and India. (Source: Canadian Centre for Cyber Security)
3. The average cost of a data breach in Canada is $6.35 million, up from $5.78 million in 2020. (Source: IBM Security)
4. In 2020, Canadian organizations experienced an average of 14.8 security incidents per week. (Source: Canadian Centre for Cyber Security)
5. The most common type of cyber attack in Canada is phishing, which accounts for 65% of all reported incidents. (Source: Canadian Centre for Cyber Security)
6. Ransomware attacks have increased by 154% in Canada since 2019. (Source: Canadian Centre for Cyber Security)
7. In 2020, Canadian businesses spent an average of $3.3 million on cybersecurity, a 10% increase from the previous year. (Source: Canadian Centre for Cyber Security)
8. In 2019, the Canadian government announced a $1.9 billion investment in cybersecurity over the next five years. (Source: Government of Canada)
9. 84% of Canadian small and medium-sized enterprises (SMEs) reported experiencing a cybersecurity breach in the past year. (Source: Canadian Internet Registration Authority)
10. The average time to detect and contain a data breach in Canada is 306 days. (Source: IBM Security)
11. Cybersecurity incidents cost Canadian organizations an average of $12,000 per incident in 2020. (Source: Canadian Centre for Cyber Security)
12. In 2020, 52% of Canadian businesses reported that remote work had increased their risk of a cybersecurity incident. (Source: Canadian Centre for Cyber Security)
13. 70% of Canadian executives reported that cybersecurity risks are a top concern for their organization. (Source: Deloitte)
14. The Canadian Centre for Cyber Security responds to an average of 2,000 cybersecurity incidents per month. (Source: Canadian Centre for Cyber Security)
15. In 2020, the Canadian government launched the Cyber Secure Canada certification program to help small and medium-sized businesses improve their cybersecurity. (Source: Government of Canada)
16. The Canadian government's National Cyber Threat Assessment 2020 identified foreign cyber threats as the biggest cyber risk to Canada. (Source: Government of Canada)
17. The Canadian Anti-Fraud Centre received over 66,000 reports of fraud in 2020, resulting in over $110 million in reported losses. (Source: Canadian Anti-Fraud Centre)
18. In 2020, the University of British Columbia experienced a data breach that compromised the personal information of over 7,000 students. (Source: CBC)
19. In 2019, the Canadian government announced the creation of the Canadian Centre for Cyber Security Operations, which is responsible for monitoring and responding to cybersecurity threats. (Source: Government of Canada)
20. Cybersecurity threats are projected to increase in frequency and sophistication in Canada and around the world in the coming years. (Source: Canadian Centre for Cyber Security)

# **Exploring Ideas**

**We asked: What is missing in most courses and training programs focused on cybersecurity?**

One area that is often missing in most courses and training programs focused on cybersecurity is a focus on soft skills and human factors. While technical skills and knowledge are important in cybersecurity, it is equally important to develop skills related to communication, collaboration, and empathy.

For example, cybersecurity professionals often need to communicate complex technical information to non-technical stakeholders, such as executives or customers. They may also need to work collaboratively with other teams or departments within an organization. In addition, understanding human factors, such as how people make decisions and respond to security threats, is crucial in developing effective cybersecurity strategies and mitigating risks.

Therefore, training programs and courses that focus solely on technical skills and knowledge may be incomplete and may not adequately prepare individuals for the complex and ever-changing landscape of cybersecurity. A more holistic approach that incorporates soft skills and human factors could better equip individuals to tackle cybersecurity challenges in a comprehensive and effective manner.

# **Writing Code**

Create code that would enable text-to-speech. Then do the same for speech-to-text.

To enable speech-to-text, you can use the following Python code using the Speech Recognition library:

This code listens to the user's voice using the microphone and attempts to recognize speech using the Google Speech Recognition API. It then prints the recognized text to the console. If the speech cannot be recognized, it prints an error message.

**Text

Description automatically generated**

# **Improving Writing**

Suggest five ways to improve the following:

To make this more dramatic, Canada has a skills problem. At various points in 2022-23, Canada had over 1 million job vacancies which could not be filled due to a skills-talent mismatch between what employers were looking for and what was available from those seeking employment. Almost all developed nations have this same problem: Canada competes globally for skilled and qualified labour.

Universities and colleges cannot adapt quickly to the fast-changing market conditions or social expectations. Though some developments have taken place (e.g., targeted funding for expanding learning for skills in high demand; the growth and development of micro-credentials; the expansion of online and flexible learning; the emergence and expansion of boot camps; outcome-based funding), the potential demand for competency-based, short and on-demand learning is not been met by the existing post-secondary infrastructure.

Further, provincial governments' per capita spending on higher education continues to decline slowly. Institutions seek to secure income from growing their international student revenues with great success. But there are two challenges here: (a) local housing supply cannot cope with a substantial expansion of international students without it impacting communities , and (b) fees charged cannot meet the growing revenue challenges faced by institutions without considering the competitive nature of the international student market. As a surge in 18-year-old Canadians begins, institutions must make choices between domestic versus international students, and revenue versus service to the community.

1. **Use strong and emotive language:** The passage could be made more dramatic by using strong and emotive language that creates a sense of urgency and importance. For example, "Canada is facing a crippling skills crisis" or "The nation's economy is in peril due to a severe shortage of skilled workers." This will help to capture the reader's attention and emphasize the gravity of the situation.
2. **Provide specific examples and statistics:** The passage could be made more impactful by providing specific examples and statistics to illustrate the scale of the problem. For example, instead of stating that there were "over 1 million job vacancies," the passage could provide a breakdown of which industries and regions are most affected, and the specific number of unfilled positions in each.
3. **Use storytelling techniques**: A dramatic narrative can make the passage more engaging and memorable. For example, the story of a skilled worker who is unable to find a job due to a lack of demand for their particular skillset, or the story of an employer who is struggling to find qualified candidates for a critical position, could help to illustrate the challenges faced by both sides.
4. **Offer potential solutions:** While the passage outlines some of the challenges faced by the post-secondary education system and the labor market, it could be made more effective by offering potential solutions to address these issues. For example, the passage could discuss innovative programs or initiatives that have successfully addressed skills gaps in other countries, or propose policy changes that could incentivize employers to invest in training and development programs.
5. **Conclude with a call to action**: The passage could be made more impactful by concluding with a call to action that encourages readers to take steps to address the skills gap. For example, the passage could urge policymakers to prioritize investments in education and workforce development, or encourage employers to invest in training and development programs to help bridge the skills-talent gap.

**I then asked it to offer a rewrite:**

|  |  |
| --- | --- |
| **Original** | **ChatGPT** |
| To make this more dramatic, Canada has a skills problem. At various points in 2022-23, Canada had over 1 million job vacancies which could not be filled due to a skills-talent mismatch between what employers were looking for and what was available from those seeking employment. Almost all developed nations have this same problem: Canada competes globally for skilled and qualified labour.  Universities and colleges cannot adapt quickly to the fast-changing market conditions or social expectations. Though some developments have taken place (e.g., targeted funding for expanding learning for skills in high demand; the growth and development of micro-credentials; the expansion of online and flexible learning; the emergence and expansion of boot camps; outcome-based funding), the potential demand for competency-based, short and on-demand learning is not been met by the existing post-secondary infrastructure.  Further, provincial governments' per capita spending on higher education continues to decline slowly. Institutions seek to secure income from growing their international student revenues with great success. But there are two challenges here: (a) local housing supply cannot cope with a substantial expansion of international students without it impacting communities, and (b) fees charged cannot meet the growing revenue challenges faced by institutions without considering the competitive nature of the international student market. As a surge in 18-year-old Canadians begins, institutions must make choices between domestic versus international students, and revenue versus service to the community. | Canada's skills problem is a significant issue that affects the nation's economy. In 2022-23, there were over 1 million job vacancies that employers could not fill because job seekers did not possess the necessary skills. The skills-talent mismatch between what employers were looking for and what was available is a problem that most developed countries face.  Adapting to fast-changing market conditions and social expectations is difficult for universities and colleges. While there have been some developments such as targeted funding, micro-credentials, online learning, boot camps, and outcome-based funding, existing post-secondary infrastructure does not meet the potential demand for short, competency-based, and on-demand learning. Provincial governments' per capita spending on higher education is also declining, making it difficult for institutions to secure income.  To overcome this revenue challenge, institutions have turned to international students, but there are two challenges: housing supply and competition in the international student market. Housing supply is insufficient to cope with a significant expansion of international students, while fees charged by institutions cannot meet their revenue challenges without considering the competitive nature of the international student market. With a surge in 18-year-old Canadians, institutions must make choices between domestic versus international students and revenue versus service to the community.  Top of Form  Bottom of Form |