Government of Canada
Gouvernement du Canada

Canada's Cyber Security Strategy

FOR A STRONGER AND MORE PROSPEROUS CANADA

Canada

Cat. No.: PS4-102/2010E-PDF

ISBN: 978-1-100-16934-7

Printed in Canada

Message from the Minister

Canadians' personal and professional lives have gone digital: we live, work, and play in cyberspace. Canadians use the Internet, computers, cell phones and mobile devices every day to talk, email, text and twitter with family, friends and colleagues. We do business online everyday, from banking to shopping to accessing government services – and we do it from wherever we happen to be. Digital infrastructure makes all this possible, and also keeps essential services up and running.

Canadians – individuals, industry and governments – are embracing the many advantages that cyberspace offers, and our economy and quality of life are the better for it. But our increasing reliance on cyber technologies makes us more vulnerable to those who attack our digital infrastructure to undermine our national security, economic prosperity, and way of life.

Our systems are an attractive target for foreign military and intelligence services, criminals and terrorist networks. These groups are breaking into our computer systems, searching through our files, and causing our systems to crash. They are stealing our industrial and national security secrets, and our personal identities.

We don't see them, we don't hear them, and we don't always catch them. At times they are mere nuisances. At other times, they present real threats to our families, companies and to our country.

Canada's Cyber Security Strategy is our plan for meeting the cyber threat. It delivers on the Government's 2010 Speech from the Throne commitment to work with provinces, territories and the private sector to implement a cyber security strategy to protect our digital infrastructure. It leverages the partnerships being established under the *National Strategy and Action Plan for Critical Infrastructure,* and supports the ongoing efforts by our law enforcement community to work with partners and international allies in cracking down on those who use the Internet for crime and illegal activities.

Canada's Cyber Security Strategy is a cornerstone of our Government's commitment to keep Canada – including our cyberspace – safe, secure and prosperous.

The Honourable Vic Toews, P.C., Q.C., M.P.
Minister of Public Safety

Introduction

Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship.

The Canadian economy relies heavily on the Internet:

- Canadian online sales in 2007 were estimated at $62.7 billion;[1] and
- In 2007, 87% of Canadian businesses used the Internet.[1]

Canadian businesses are moving quickly to adopt the most modern digital applications, including next generation and mobile technologies.

Canada's governments have also become increasingly dependent on the Internet. The federal Government alone now offers more than 130 commonly used services online, including tax returns, employment insurance forms and student loan applications.

Our success in cyberspace is one of our greatest national assets. Protecting this success means protecting our cyber systems against malicious misuse and other destructive attacks. This is a daunting challenge. There is no simple way

Canadians are embracing cyberspace:

- 74% of Canadian households had paid Internet service in 2008;[2]
- 59% of personal tax filings were electronic in 2008;[3]
- 67% of Canadians banked online in 2009.[4]

[1] Statistics Canada, "The Daily," April 24, 2008
[2] Canadian Radio-television and Telecommunications Commission, "Communications Monitoring Report," August 2009
[3] Canada Revenue Agency, "National Processing Status Report," September 2009
[4] Statistics Canada, "Canadian Internet Use Survey," 2009

to detect, identify and recover from attackers who cannot be seen or heard, who leave no physical evidence behind them, and who hide their tracks through a complex web of compromised computers.

Cyber security affects us all, in part because even attackers with only basic skills have the potential to cause real harm. Sophisticated attackers can disrupt the electronic controls of our power grids, water treatment plants and telecommunications networks. They interfere with the production and delivery of basic goods and services provided by our governments and the private sector. They undermine our privacy by stealing our personal information. Dealing with cyber threats in isolation is not enough. Through the implementation of this Strategy, the Government will continue to work with the provinces, territories and the private sector in a concerted effort to address the threats facing Canada and Canadians.

Every year, we detect more attackers than the year before. And every year, those seeking to infiltrate, exploit or attack our cyber systems are more sophisticated and better resourced than the year before. They are investing in their capabilities. We must respond by investing more in ours.

Cyber attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security.

The Government is continuing its efforts to help secure Canada's cyber systems and protect Canadians online. Indeed this Strategy is but one element in a series of initiatives designed to protect Canadians. The Government has established the Canadian Cyber Incident Response Centre to monitor and provide mitigation advice on cyber threats, and coordinate the national response to any cyber security incident. The Government will soon introduce legislation to modernize law enforcement's investigative powers, and ensure that technological innovations are not used to evade lawful interceptions of communications supporting criminal activity.

These are important initiatives, but they are no longer sufficient. The threat is becoming more serious. We cannot allow our cyber security efforts to remain fixed on the threat as we understood it in the past. To ensure that our advanced use of cyberspace remains a strategic asset, Canada must anticipate and confront emerging cyber threats. *Canada's Cyber Security Strategy* is our plan for making cyberspace more secure for all Canadians.

Understanding Cyber Threats

There are various ways to gain access to information in cyberspace. Attackers can exploit vulnerabilities in software and hardware. They can exploit security vulnerabilities by tricking people into opening infected emails or visiting corrupted websites that infect their computers with malicious software. They can take advantage of people who fail to follow basic cyber security practices, such as changing their passwords frequently, updating their antivirus protection on a regular basis, and using only protected wireless networks.

Once they have access to a computer, attackers can steal or distort the information stored on it, corrupt its operations and program it to attack other computers and the systems to which they are connected. In many cases, victims suffer a theft of their identity and/or their personal assets. According to a study by McMaster University,[5] 1.7 million Canadians were victims of identity theft in 2008. The annual cost of identity theft in Canada has been estimated at nearly $1.9 billion. For this reason the Government has amended the *Criminal Code* to better protect Canadians from identity theft.

Canadian companies can lose the race to bring a product to market, or experience other harm without ever realizing that their losses were caused by a cyber attack. It has been estimated that in a recent one year period, 86% of large Canadian organizations had suffered a cyber attack. The loss of intellectual property as a result of these attacks doubled between 2006 and 2008.[6]

Though certain attack tools and techniques are more costly and sophisticated than others, most cyber attacks share four characteristics that, in part, account for their growing popularity. Cyber attacks are often:

- **Inexpensive** – Many attack tools can be purchased for a modest price or downloaded for free from the Internet;
- **Easy** – Attackers with only basic skills can cause significant damage;

[5] McMaster University, *Measuring Identity Theft in Canada: 2008 Consumer Survey*

[6] CA Technologies, "Canada 2008 Security and Privacy Survey"

- **Effective** – Even minor attacks can cause extensive damage; and
- **Low risk** – Attackers can evade detection and prosecution by hiding their tracks through a complex web of computers and exploiting gaps in domestic and international legal regimes.

While there is some similarity in the targets and methods of cyber attackers, the nature of the threat posed by each is made distinct by their differing motivations and intentions. Three types of threats are discussed below.

STATE SPONSORED CYBER ESPIONAGE AND MILITARY ACTIVITIES

The most sophisticated cyber threats come from the intelligence and military services of foreign states. In most cases, these attackers are well resourced, patient and persistent. Their purpose is to gain political, economic, commercial or military advantage.

All technologically advanced governments and private businesses are vulnerable to state sponsored cyber espionage. Reports from Canada and across the world confirm that these attacks have succeeded in stealing industrial and state secrets, private data and other valuable information.

Some foreign states have declared publicly that cyber attacks are a central element of their military strategy. Some states have been widely accused of using cyber attacks to coincide with – and magnify the effects of – traditional military operations. These cyber attack programs are typically designed to sabotage an adversary's infrastructure and communications. They may also support electronic attacks on an adversary's military equipment and operations. Cyber attacks that disrupt emergency response and public health systems would put lives in danger.

Canada and our allies understand that addressing these risks requires modernizing our military doctrines. It is for this reason that the North Atlantic Treaty Organization (NATO) has adopted several policy documents regarding cyber defence, and like the militaries of our closest allies, the Department of National Defence and the Canadian Forces are examining how Canada can best respond to future cyber attacks.

TERRORIST USE OF THE INTERNET

Terrorist networks also are moving to incorporate cyber operations into their strategic doctrines. Among many activities, they are using the Internet to support their recruitment, fundraising and propaganda activities.

Terrorists are aware of the potential for using the Western world's dependence on cyber systems as a vulnerability to be exploited. For example, there are now online resources providing advice to terrorists on how to defend their own websites while launching cyber attacks on their enemies. In addition, a number of terrorist groups, including Al-Qaeda, have expressed their intention to launch cyber attacks against Western states. Though experts doubt that terrorists currently have the ability to cause serious damage via cyber attacks, they recognize that this capacity will likely develop over time.

CYBERCRIME

In much the same way as states have expanded their operations into cyberspace, so too have organized criminals. The more sophisticated among them are turning to skilled cyber attackers to pursue many of their traditional activities, such as identity theft, money laundering and extortion.

Criminals now sell information stolen online, such as credit and debit card numbers, login passwords for computer servers, and malicious software designed to infiltrate and damage targeted systems. Even those of us who are diligent in protecting our personal information online are at risk of having our personal data stolen from the third parties we share it with.

Some criminal organizations are now developing customized attack software. They are using advanced encryption technologies to protect their own assets and trade secrets. Some in the law enforcement and security communities argue that the capabilities of some cyber criminals now rival those of developed states.

THE THREAT IS EVOLVING

Much like bacteria developing drug resistance to antibiotics, cyber viruses and malicious code are continually evolving to evade our defences and antivirus software. The evolution of cyber attack tools and techniques has accelerated dangerously in the recent past. Statistics compiled by two well known Internet security companies, Akamai and Symantec, together show that malicious computer programs now originate in more than 190 countries.[7] More than 60% of all the malicious code ever detected was introduced into cyberspace in 2008[8] alone.

There is no doubt that the frequency and severity of the cyber threat is accelerating. Protecting Canadians in cyberspace will be a constantly evolving challenge. To effectively address this challenge will require a range of actions and responses, accompanied by continuing investment and vigilance over the long term.

[7] Akamai, "State of the Internet Report," March 2009

[8] Symantec, "Global Internet Security Threat Report," April 2009

Canada's Cyber Security Strategy

Canadian researchers have been at the forefront of making cyberspace a reality. This same ingenuity must continue to be applied to predicting, detecting and defeating the cyber threats of tomorrow, and exploiting cyberspace to further Canada's national interests.

Canada's Cyber Security Strategy is our plan for meeting the cyber threat. The Strategy is built on three pillars:

1. **Securing Government systems** – Canadians trust Government with their personal and corporate information, and also trust Government to deliver services to them. They also trust that the Government will act to defend Canada's cyber sovereignty and protect and advance our national security and economic interests. The Government will put in place the necessary structures, tools and personnel to meet its obligations for cyber security.

2. **Partnering to secure vital cyber systems outside the federal Government** – Canada's economic prosperity and Canadians' security depend on the smooth functioning of systems outside the Government. In cooperation with provincial and territorial governments and the private sector, the Government will support initiatives and take steps to strengthen Canada's cyber resiliency, including that of its critical infrastructure sectors.

3. **Helping Canadians to be secure online** – The Government will assist Canadians in getting the information they need to protect themselves and their families online, and strengthen the ability of law enforcement agencies to combat cybercrime.

Canada's Cyber Security Strategy will strengthen our cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world. We all have a role to play as we take full advantage of cyberspace to build a safe, resilient and innovative Canada.

The Government has sought input from stakeholders on a wide range of cyber threats and security practices. Collaboration, especially internationally, is essential if cyberspace is to be secured. Canada will benefit from being seen internationally and domestically as a trusted partner in making cyberspace safer.

The Strategy:

- Reflects Canadian values such as the rule of law, accountability and privacy;
- Allows continual improvements to be made to meet emerging threats;
- Integrates activity across the Government of Canada;
- Emphasizes partnerships with Canadians, provinces, territories, business and academe; and
- Builds upon our close working relationships with our allies.

Three of our closest security and intelligence partners, the United States, the United Kingdom and Australia, recently released their own plans to secure cyberspace. Many of the guiding principles and operational priorities set out in those reports resemble our own. This complementarity reflects our shared experiences in dealing with cyber security, and demonstrates our determination to enhance our collective security by leveraging each ally's domestic cyber regimes. Like Canada, our allies intend to review and update their plans regularly in response to evolution in cyber security technologies and practices, and the cyber threat environment.

Canada will also build on its existing engagement in cyber security discussions at key international fora, such as the United Nations, NATO and the Group of Eight. We are one of the non-European states that have signed the Council of Europe's *Convention on Cybercrime*, and the Government is preparing legislation to permit ratification of this treaty.

Canada supports international efforts to develop and implement a global cyber governance regime that will enhance our security. To the extent possible, Canada will support efforts to build the cyber security capacity of less developed states and foreign partners. This will help forestall adversaries from exploiting weak links in global cyber defences.

WORKING COOPERATIVELY

The Strategy will be implemented by the departments and agencies most directly responsible for securing the Government's cyber systems. We will work with our provincial and territorial partners, as they are jointly responsible for protecting much of the critical infrastructure in Canada.

Canada's academic community, non-governmental organizations and private sector must join the Government in securing Canada's cyber systems. Each of these communities has unique technological and analytical capabilities to offer, and a strong incentive to secure their own systems. Their collaboration is essential to our shared success to secure Canada and increase our productivity and prosperity.

Individual Canadians must also play a primary role in securing Canada's cyber future. The Government can introduce and support important cyber security initiatives, but it cannot protect each of us from every threat we encounter when we go online. Canadians must become aware of these threats, and of the tools available to recognize and avoid them. Most importantly, they must use these tools to protect themselves and their families.

Cyber security matters to everyone, everyday. It matters for a safer and more prosperous Canada.

Specific Initiatives

Canada's Cyber Security Strategy is built on three pillars:

- Securing Government systems;
- Partnering to secure vital cyber systems outside the federal Government; and
- Helping Canadians to be secure online.

SECURING GOVERNMENT SYSTEMS

The cyber world in which Canadians live, work and play lacks the regimes of law and order that govern our physical world. The Government is entrusted with safeguarding some of our most personal and sensitive information in its electronic databases. It provides services to Canadians and the private sector through its websites and electronic processing systems. And the Government transmits highly classified information essential to our military and national security operations via its classified communications systems.

There have been many cyber attacks directed at Government systems. Cyber attackers regularly probe these systems, looking for vulnerabilities. Securing these links is not simply a matter of operational efficiency. It is a matter of national security and sovereignty, protecting the lives of our foreign service, military and law enforcement personnel, the integrity of our economy, and safeguarding the personal information of Canadians.

We must and will strengthen the Government's capability to detect, deter and defend against cyber attacks while deploying cyber technology to advance Canada's economic and national security interests. Achieving the cyber integrity of Government requires that roles and responsibilities are clear, systems are strengthened and Government employees are aware of proper procedure.

Establishing Clear Federal Roles and Responsibilities

With a subject as critical as cyber security, there is no room for ambiguity in terms of who does what. This Strategy sets out the required clarity.

Public Safety Canada will coordinate implementation of the Strategy. It will design a whole-of-Government approach to reporting on the implementation of the Strategy. It will provide central coordination for assessing emerging complex

threats and developing and promoting comprehensive, coordinated approaches to address risks within the Government and across Canada. Within Public Safety Canada, the Canadian Cyber Incident Response Centre will continue to be the focal point for monitoring and providing advice on mitigating cyber threats, and directing the national response to any cyber security incident. Public Safety Canada will also lead public awareness and outreach activities to inform Canadians of the potential risks they face and the actions they can take to protect themselves and their families in cyberspace.

The Communications Security Establishment Canada has internationally recognized expertise in dealing with cyber threats and attacks. With its unique mandate and knowledge, the Communications Security Establishment Canada will enhance its capacity to detect and discover threats, provide foreign intelligence and cyber security services, and respond to cyber threats and attacks against Government networks and information technology systems.

The Canadian Security Intelligence Service will analyze and investigate domestic and international threats to the security of Canada. The Royal Canadian Mounted Police will investigate, as per the *Royal Canadian Mounted Police Act*, suspected domestic and international criminal acts against Canadian networks and critical information infrastructure.

The Treasury Board Secretariat will support and strengthen cyber incident management capabilities across Government, through the development of policies, standards and assessment tools. The Treasury Board Secretariat is also responsible for information technology security in the Government of Canada.

Foreign Affairs and International Trade Canada will advise on the international dimension of cyber security and work to develop a cyber security foreign policy that will help strengthen coherence in the Government's engagement abroad on cyber security.

The Department of National Defence and the Canadian Forces will strengthen their capacity to defend their own networks, will work with other Government departments to identify threats and possible responses, and will continue to exchange information about cyber best practices with allied militaries. The Department of National Defence and the Canadian Forces will also work with allies to develop the policy and legal framework for military aspects of cyber security, complementing international outreach efforts of Foreign Affairs and International Trade Canada.

Given the speed and complexity of many cyber attacks, barriers to cooperation and information sharing between federal partners must be eliminated. The Strategy includes measures to address this need, and provides the additional financial and personnel resources required to allow the Government to fulfill its cyber security obligations.

Strengthening the Security of Federal Cyber Systems

For each new technology or practice adopted to enhance our cyber security, another is developed to circumvent it. We will continually invest in the expertise, systems and governing frameworks required to keep pace with these evolving threats. We will also review our options for increasing the risks and consequences applied to those who attack our cyber systems.

The Government will enhance the security of its cyber architecture. It will continue to reduce the number of Internet gateways into its computer systems, and take other measures to secure systems.

In 2009 the Government made a number of important amendments to its *Policy on Government Security*. Administered by the Treasury Board Secretariat, the Policy sets out safeguards to assure the delivery of Government services to Canadians. Since the Government relies extensively on information technology to provide these services, the Policy emphasizes the need for departments and agencies to monitor and secure their electronic operations.

The globalization of the technology industry makes it difficult to assess suppliers' trustworthiness. Cyber attackers are well aware of the opportunities created for them by security gaps in the global supply chain. Some organized crime syndicates and foreign intelligence services have already exploited these vulnerabilities in an effort to disseminate exploitable technologies. The Government will strengthen processes to reduce the risk related to compromised technologies.

Enhancing Cyber Security Awareness throughout Government

While clear roles and responsibilities, and strengthened systems are important to achieving cyber security, the Government's success in securing its systems is largely dependent on its employees. As countless incidents in all segments of society have shown, even the most sophisticated security systems can be undermined by simple human error. In Government, as elsewhere, people can fail to follow basic cyber security practices by:

- Not changing their passwords on a regular basis;
- Assuming that an office email system is more secure than it is; and
- Importing malicious viruses into workplace computers by visiting corrupted websites.

PARTNERING TO SECURE VITAL CYBER SYSTEMS OUTSIDE THE FEDERAL GOVERNMENT

The economic success of Canada's private sector depends in large measure on its ability to secure cutting edge research and intellectual property, business transactions and financial data. Failing to secure these assets inevitably leads to lost market share, fewer customers and corporate breakdown.

In much the same way, our personal wellbeing depends on access to secure and reliable services from our transportation systems, communication networks and financial institutions. It is increasingly important to protect two of the primary contributors to our quality of life – private companies that drive our economic prosperity and the infrastructure systems that support our daily activities – against cyber threats. Failure to do so will have adverse economic impacts and undermine consumer confidence.

A 2008 study by McMaster University[9] on identity theft in Canada found that 20% of consumers have eliminated or reduced the amount of shopping they do online, and that 9% have eliminated or reduced online banking activities due to the risks they perceive in doing business online. By building a secure and trusted business environment, we will help foster the productivity and innovation that drive our economic prosperity.

The public needs to be more aware of the vulnerabilities inherent in the cyber systems that these industries use to deliver their services. Increased awareness will equip Canadians to avoid identity theft and potential financial loss. The Government will partner with the provinces, territories and private sector to improve the cyber security posture of Canada and Canadians.

The Government will build on existing programs and expertise, such as Defence Research and Development Canada's Public Security Technical Program to better support cyber security research and development activities. We will also collaborate with our private sector and academic partners to enhance information sharing activities.

Partnering with the Provinces and Territories

Strengthened partnerships among all levels of government are an essential component in delivering a comprehensive cyber security strategy for Canada and Canadians. Our provincial and territorial counterparts provide a range of essential services whose delivery is dependent on the safe and secure operation of their cyber systems. For example, they hold sensitive personal information in their electronic databases, including health records, marriage and driver licenses, and provincial tax return information. The provinces

[9] McMaster University, *Measuring Identity Theft in Canada: 2008 Consumer Survey*

and territories have a key role to play in promoting awareness among Canadians, especially young Canadians in the education system where first exposure to the Internet often occurs. Only when all levels of government are working together can Canadians be assured that their private information is secure and the services that they depend on will be delivered.

Partnering with the Private Sector and Critical Infrastructure Sectors

Many of the risks and impacts of cyber attacks are shared between the Government and private sector. For example, untrustworthy technology is harmful to both government and industry. Identifying these risks must be done in partnership.

Fortunately, Canada's public and private sectors share a long history of working together to achieve shared economic and national security goals. This cooperation needs to be further strengthened. Each partner must share accurate and timely cyber security information regarding existing and emerging threats, defensive techniques and other best practices.

Strengthened public/private partnerships will be fostered through existing structures and organizations, such as critical infrastructure sector networks. Cross sector mechanisms will also be established, providing opportunities for governments and industry to collaborate on a broad range of critical infrastructure issues, including cyber security.

Another key area for collaboration is the security of process control systems. These systems control everything from our machines and factories to our critical infrastructures. They keep our dams from overflowing, our electrical grids from collapsing and our transportation networks from malfunctioning. Their security is critical to the safe delivery of the services and products upon which Canadians depend. Joint public/private sector initiatives will be struck to identify and share best practices for addressing threats to these systems.

Our collective cyber security efforts will be further refined through training and exercise programs. The result of these exercises, some of which are already underway, will be an improved understanding of the dynamic among partners in cyber security. Participation in these exercises will also support the improvement of procedures to prevent cyber security failures.

The disruption of critical infrastructure and cyber systems can have direct impacts on businesses and communities on both sides of the Canada–United States border. Attacks on interconnected cyber networks can have cascading effects across industrial sectors and national borders. For this reason, Canada will be active in international fora dealing with critical infrastructure protection and cyber security.

HELPING CANADIANS TO BE SECURE ONLINE

Our success in harnessing cyberspace has helped us achieve unprecedented personal productivity and prosperity. But it has also allowed the world's criminals to commit traditional crimes with 21st century technologies. The Government is taking steps to protect cyberspace from becoming a criminal haven. We will deny cyber criminals the anonymity they are seeking while at the same time protecting the privacy of Canadians.

Combatting Cybercrime

Criminals are learning quickly that cybercrime can be inexpensive, low risk and profitable. In one well known incident uncovered in 2007,[10] over 45 million customer records were stolen from a well known North American retailer. The breach occurred over a three year period, during which criminals monitored wireless signals from point of sale credit card terminals. These attacks cost the retailer over $130 million and inflicted unknown financial harm on individual victims.

Also in 2008, 11 people operating in five different countries were charged[11] with breaking into the databases of nine major North American retailers, stealing some 40 million credit and debit card numbers from their databases, and selling the numbers (via the Internet) to other criminals.

[10] *SC Magazine*, "FTC Settles with TJX Over Breach," March 2008
[11] *Wired Magazine*, "Feds Charge 11 in Breaches at TJ Maxx, OfficeMax, DSW, Others," August 2008

Canada's law enforcement agencies cannot combat trans-national cybercrimes with outdated investigative powers and tools. Equipping our police to protect us in cyberspace requires that we provide them with new legislative authorities and supporting financial resources.

Accordingly, the Royal Canadian Mounted Police will be given the resources required to establish a centralized Integrated Cyber Crime Fusion Centre. This team will increase the ability of the Royal Canadian Mounted Police to respond, using a risk-based analysis approach, to requests from the Canadian Cyber Incident Response Centre regarding cyber attacks against Government or Canada's critical infrastructure.

The Government has already passed legislation to combat identity theft. Other legislative reforms will be re-introduced by the Government to enhance the capacity of law enforcement to investigate and prosecute cybercrime by:

- Making it a crime to use a computer system to sexually exploit a child;
- Requiring Internet service providers to maintain intercept capable systems, so that law enforcement agencies can execute judicially authorized interceptions;
- Requiring Internet service providers to provide police with basic customer identification data, as this information is essential to combatting online crimes that occur in real time, such as child sexual abuse; and
- Increasing the assistance that Canada provides to its treaty partners in fighting serious crimes.

Protecting Canadians Online

Canadian families want their privacy, identities and physical wellbeing protected from cyber predators. And Canadians know that risks exist. According to a Decima Research study:[12]

- Only 35% of Canadians believe their computer is very safe against online threats; and
- 77% are concerned about the security of personal information. Yet 63% use the Internet for sensitive transactions and 57% keep sensitive information on their computers.

As long as they know how to do so, Canadians will strengthen their own individual cyber security and that of Canada as a whole. We all need to follow basic cyber security practices, such as changing our passwords frequently, updating antivirus protection and using only protected wireless networks.

The Government will increase Canadians' awareness of common online crimes and will promote safe cyber security practices through the use of web sites, creative materials and outreach efforts.

The Government's ultimate goal is to create a culture of cyber safety whereby Canadians are aware of both the threats and the measures they can take to ensure the safe use of cyber-space. Creating such awareness will require a sustained effort over a period of several years. The effort must start now.

[12] Decima Research, *Cyber Security Practices in Canada*, Final Report, February 2008

Moving Forward

With each passing day, Canadians' dependence on cyberspace grows. There is no turning back to a world without an Internet. Just as previous generations took advantage of increasingly complex and helpful methods of communications, we have embraced the Internet.

But as we enjoy the benefits of cyberspace, we also recognize that it threatens us in a variety of ways. Those who choose to abuse the Internet are becoming more sophisticated and dangerous every day. We must invest now in cyber security to protect our economic prosperity, national security and quality of life.

Canada's Cyber Security Strategy is Canada's plan for securing our cyber systems. The Strategy will protect the integrity of Government systems and our nation's critical assets. It will combat cybercrime and protect Canadians as they use cyberspace in their daily lives. By promoting awareness of the need for cyber security, the Strategy will encourage individual Canadians, industry and all levels of government to adapt behaviour and adopt the technology required to confront evolving cyber threats.

The Government will begin implementing new initiatives under the Strategy in 2010. The initiatives outlined in this Strategy are important first steps. They will be adjusted and strengthened as required.

Cyber security is a shared responsibility, one in which Canadians, their governments, the private sector and our international partners all have a role to play. The Strategy reflects this shared responsibility. Implementation will be a collective effort. Its success will depend on our ability to work together.

Everyone must do their part.