Computer security, also known as cybersecurity or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures.

1. What the information technology is used to prevent the threat in the computer world?

Answer: Computer security

General Knowledge: Computer security (can be defined as) an information technology/ protection … from (Synonym: is similar to) prevent the threat

1. What are the ways an operator can misbehave?

Answer: intentional, accidental, or due to them being tricked.

General Knowledge: malpractice (Synonym) misbehave

1. What must an operator depart from to damage the computer?

Answer: secure procedures.

General Knowledge: deviate (Synonym) depart

Denial of service attacks are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points \u2013 and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet, but a range of other techniques are possible including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

1. What causes a machine or network resource out of service to its intended users?

Answer: Denial of service attacks

General Knowledge: unavailable (can be defined as) out of service

1. Which way makes victims cannot login to the system?

Answer: deliberately entering password enough consecutive times

General Knowledge: account (attribute) login system

1. What makes defending harder in DDoS attacks?

Answer: attack comes from a large number of points

General Knowledge: more difficult (Synonym) harder

1. What may be a source of DDoS attacks?

Answer: zombie computers of a botnet.

General Knowledge: originate (Synonym) source

If access is gained to a car's internal controller area network, it is possible to disable the brakes and turn the steering wheel. Computerized engine timing, cruise control, anti-lock brakes, seat belt tensioners, door locks, airbags and advanced driver assistance systems make these disruptions possible, and self-driving cars go even further. Connected cars may use wifi and bluetooth to communicate with onboard consumer devices, and the cell phone network to contact concierge and emergency assistance services or get navigational or entertainment information; each of these networks is a potential entry point for malware or an attacker. Researchers in 2011 were even able to use a malicious compact disc in a car's stereo system as a successful attack vector, and cars with built-in voice recognition or remote assistance features have onboard microphones which could be used for eavesdropping.

1. What type of cars have more effect from the attack?

Answer: self-driving cars

General Knowledge: further (can be defined as) more effect

1. Which wireless technology can be used to link onboard consumer devices?

Answer: wifi and bluetooth

General Knowledge: connection (Synonym) link/ wifi (can be defined as) wireless technology

1. In cars with innated voice recognition features, what can the onboard microphones be used for?

Answer: eavesdropping

General knowledge: built-in (Synonym) innated / entry point (is the definition of) entrance

However, relatively few organisations maintain computer systems with effective detection systems, and fewer still have organised response mechanisms in place. As result, as Reuters points out: \"Companies for the first time report they are losing more through electronic theft of data than physical stealing of assets\". The primary obstacle to effective eradication of cyber crime could be traced to excessive reliance on firewalls and other automated \"detection\" systems. Yet it is basic evidence gathering by using packet capture appliances that puts criminals behind bars.

1. What is the main concern on efficiency cyber crime elimination?

Answer: excessive reliance on firewalls and other automated \"detection\" systems.

General Knowledge: primary obstacle (can be defined as ) the main concern / eradication (Synonym) elimination

One use of the term \"computer security\" refers to technology that is used to implement secure operating systems. In the 1980s the United States Department of Defense (DoD) used the \"Orange Book\" standards, but the current international standard ISO/IEC 15408, \"Common Criteria\" defines a number of progressively more stringent Evaluation Assurance Levels. Many common operating systems meet the EAL4 standard of being \"Methodically Designed, Tested and Reviewed\", but the formal verification required for the highest levels means that they are uncommon. An example of an EAL6 (\"Semiformally Verified Design and Tested\") system is Integrity-178B, which is used in the Airbus A380 and several military jets.

1. Which terminology can be used for performing security of operating systems?

Answer: computer security

General Knowledge: implement secure operating systems (attribute) performing security of operating systems

1. What is the normal requirement for many common operation systems?

Answer: EAL4

General Knowledge: standard (can be defined as) normal requirement/common (Synonym) typical

China's network security and information technology leadership team was established February 27, 2014. The leadership team is tasked with national security and long-term development and co-ordination of major issues related to network security and information technology. Economic, political, cultural, social and military fields as related to network security and information technology strategy, planning and major macroeconomic policy are being researched. The promotion of national network security and information technology law are constantly under study for enhanced national security capabilities.

1. What is the duty of management group?

Answer: national security and long-term development and co-ordination of major issues related to network security and information technology

General Knowledge: leadership team (can be defined as) management group / duty (Synonym) task

1. Which areas of Internet safety are explored?

Answer: Economic, political, cultural, social and military fields as related to network security and information technology strategy, planning and major macroeconomic policy

General Knowledge: network security (attribute of) Internet safety / research (Synonym) explore

Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, programs such as Carnivore and NarusInsight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon via monitoring the faint electro-magnetic transmissions generated by the hardware; TEMPEST is a specification by the NSA referring to these attacks.

1. What is the act of spying on exclusive conversation?

Answer: Eavesdropping

General Knowledge: Listening (can be defined as) Spying / Exclusive (similar to) private

1. What softwares can be used to listen on internet service providers system?

Answer: Carnivore and Narus Insight

programs (can be defined as) softwares / eavesdrop (synonym) listen on

1. How can devices that cannot be reached by outsiders be spied upon?

Answer: via monitoring the faint electro-magnetic transmissions generated by the hardware

General Knowledge: Machines (can be defined as) devices / closed (can be defined as) cannot be contacted by outsiders / eavesdropped (synonym) spied

Desktop computers and laptops are commonly infected with malware either to gather passwords or financial account information, or to construct a botnet to attack another target. Smart phones, tablet computers, smart watches, and other mobile devices such as Quantified Self devices like activity trackers have also become targets and many of these have sensors such as cameras, microphones, GPS receivers, compasses, and accelerometers which could be exploited, and may collect personal information, including sensitive health information. Wifi, Bluetooth, and cell phone network on any of these devices could be used as attack vectors, and sensors might be remotely activated after a successful breach.

1. What is the aim of infecting electronic devices with virus-bugs?

Answer: to gather passwords or financial account information, or to construct a botnet to attack another target.

General knowledge: Desktop computers and laptops (can be defined as electronic devices) malware (synonym of virus-bugs).

1. What part of mobile devices can be manoeuvred to get confidential details?

Answer: sensors.

General knowledge: exploited (synonyms) manoeuvred, personal information, including sensitive health information (synonyms) confidential details.

1. What are the main points of targets when trying to break into devices?

Answer: Wifi, Bluetooth, and cell phone network.

General knowledge: attack vectors (synonyms) target point, breach (can be defined as) break into.

Within computer systems, two of many security models capable of enforcing privilege separation are access control lists (ACLs) and capability-based security. Using ACLs to confine programs has been proven to be insecure in many situations, such as if the host computer can be tricked into indirectly allowing restricted file access, an issue known as the confused deputy problem. It has also been shown that the promise of ACLs of giving access to an object to only one person can never be guaranteed in practice. Both of these problems are resolved by capabilities. This does not mean practical flaws exist in all ACL-based systems, but only that the designers of certain utilities must take responsibility to ensure that they do not introduce flaws. [citation needed].

1. What are the security models that have the ability to apply privilege separations within electronic devices?

Answer: access control lists (ACLs) and capability-based security

General knowledge: capable (can be defined as) have the ability, enforcing (synonym) apply, computer systems (synonyms) electronic devices.

1. Which of the security models has been proven to be unsafe when used to restrict programs?

Answer: access control lists (ACLs).

General knowledge: insecure (synonym) unsafe, confine (synonym) restrict.

1. Can the promise of ACLs of giving permission to only one person be assured in application?

Answer: NO, It can never be guaranteed.

General knowledge: access (can be defined as) permission, guaranteed (synonym) assured, practice (synonym) application.

1. How are the above listed issues settled?

Answer: By capabilities

General knowledge: Problems (synonym) issues, resolved (synonym) settled

1. Who must make sure that practical mistakes are not instigated into development of the utilities?

Answer: the designer

General knowledge: take responsibility (can be defined as) make sure, flaws (can be defined as) mistakes, introduced (synonym) instigated.

In 1994, over a hundred intrusions were made by unidentified crackers into the Rome Laboratory, the US Air Force's main command and research facility. Using trojan horses, hackers were able to obtain unrestricted access to Rome's networking systems and remove traces of their activities. The intruders were able to obtain classified files, such as air tasking order systems data and furthermore able to penetrate connected networks of National Aeronautics and Space Administration's Goddard Space Flight Center, Wright-Patterson Air Force Base, some Defense contractors, and other private sector organizations, by posing as a trusted Rome center user.

1. In what year was over a hundred encroachments made by anonymous crackers into the Rome Laboratory, the US Air Force's main command and research facility?

Answer: 1994

General knowledge: intrusions (can be defined as) encroachments, unidentified (synonym) anonymous.

1. How did hackers gain unlimited access to Rome's networking systems and get rid of evidence of their activities?

Answer: Using trojan horses

General knowledge: obtain (can be defined as) gain, unrestricted (synonym) unlimited, remove (similar to) get rid of, traces (synonym) evidence.

1. How were the trespassers able to secure categorized files and invade connected networks?

Answer: by posing as a trusted Rome center user.

General knowledge: intruders (can be defined as) trespassers, obtain (synonym) secure, classified (synonym) categorized, penetrate (similar to) invade.

In July of 2015, a hacker group known as \"The Impact Team\" successfully breached the extramarital relationship website Ashley Madison. The group claimed that they had taken not only company data but user data as well. After the breach, The Impact Team dumped emails from the company's CEO, to prove their point, and threatened to dump customer data unless the website was taken down permanently. With this initial data release, the group stated \u201cAvid Life Media has been instructed to take Ashley Madison and Established Men offline permanently in all forms, or we will release all customer records, including profiles with all the customers' secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails. The other websites may stay online.\u201d When Avid Life Media, the parent company that created the Ashley Madison website, did not take the site offline, The Impact Group released two more compressed files, one 9.7GB and the second 20GB. After the second data dump, Avid Life Media CEO Noel Biderman resigned, but the website remained functional.

1. When did a hacker group known as \"The Impact Team\" victoriously break into the extramarital affair website Ashley Madison?

Answer: July of 2015.

General knowledge: successfully (synonym) victoriously, breached (can be defined as) break into, relationship (similar to) affair.

1. What facts and statistics did the group affirm to extract?

Answer: The group claimed that they had taken not only company data but user data as well.

General knowledge: data (can be defined as) facts and statistics, claim (synonym) affirm, take (similar to) extract.

1. What did the impact team threaten to do if the website wasn’t removed indefinitely?

Answer: threatened to dump customer data

General knowledge: take down (similar to) removed, permanently (synonym) indefinitely.

1. Which group was ordered to disconnect Ashley Madison and Established Men from the internet permanently in all forms?

Answer: the group stated \u201cAvid Life Media

General knowledge: instructed (can be defined as) ordered, take offline (can be defined as) disconnect from the internet.

1. What were the sizes of the two more compressed files that were exposed by the Impact Group?

Answer: 9.7GB and the second 20GB.

General knowledge: released (synonym) exposed.

1. When did Avid Life Media CEO Noel Biderman voluntarily leave office and was the website still in operation?

Answers: After the second data dump and YES the website was still functional.

General knowledge: resign (can be defined as) voluntarily leave office, functional (similar to) in operation.

The question of whether the government should intervene or not in the regulation of the cyberspace is a very polemical one. Indeed, for as long as it has existed and by definition, the cyberspace is a virtual space free of any government intervention. Where everyone agree that an improvement on cybersecurity is more than vital, is the government the best actor to solve this issue? Many government officials and experts think that the government should step in and that there is a crucial need for regulation, mainly due to the failure of the private sector to solve efficiently the cybersecurity problem. R. Clarke said during a panel discussion at the RSA Security Conference in San Francisco, he believes that the \"industry only responds when you threaten regulation. If industry doesn't respond (to the threat), you have to follow through.\" On the other hand, executives from the private sector agree that improvements are necessary, but think that the government intervention would affect their ability to innovate efficiently.

1. Is government intercession in the management of cyberspace critical?

Answer: yes it is very polemical.

General knowledge: intervene (can be defined as) intercession, regulation (synonym) management, polemical (similar to) critical.

1. Is the cyberspace exempted from any government intercession?

Answer: yes it is.

General knowledge: intervention (can be defined as) intercession, Free of (synonym) exempted from.

1. Where everyone concur that an advancement on cybersecurity is more than important, who thinks that the government officials should step and resolve this problem?

Answer: Many government officials and experts.

General knowledge: agree (can be defined as) concur, improvement (synonym) advancement, vital (similar to) important.

1. Why do many government officials and experts think that the government should step in and that there is an urgent need for management?

Answer: Due to the failure of the private sector to solve efficiently the cybersecurity problem.

General knowledge: crucial (synonym) urgent, regulation (synonym) management.

1. Who concurs that advancements are necessary, but think that the government intercession would influence their ability to develop effectively?

Answer: executives from the private sector

General knowledge: agree (can be defined as) concur, improvement (synonym) advancement, intervention (can be defined as) intercession, affect (synonym) influence,

Innovate (similar to) develop, efficiently (similar to) effectively.

On October 3, 2010, Public Safety Canada unveiled Canada\u2019s Cyber Security Strategy, following a Speech from the Throne commitment to boost the security of Canadian cyberspace. The aim of the strategy is to strengthen Canada\u2019s \"cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world.\" Three main pillars define the strategy: securing government systems, partnering to secure vital cyber systems outside the federal government, and helping Canadians to be secure online. The strategy involves multiple departments and agencies across the Government of Canada. The Cyber Incident Management Framework for Canada outlines these responsibilities, and provides a plan for coordinated response between government and other partners in the event of a cyber incident. The Action Plan 2010\u20132015 for Canada's Cyber Security Strategy outlines the ongoing implementation of the strategy.

1. When did Public Safety Canada disclose Canada\u2019s Cyber Security Strategy following a Speech from the Throne commitment to uplift the security of Canadian cyberspace?

Answer: On October 3, 2010

General knowledge: unveil (can be defined as) disclose, boost (synonym) uplift.

1. What is the objective of the strategy?

Answer: To strengthen Canada\u2019s \"cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world.

General knowledge: Aim (can be defined as) objective.

1. What are the three fundamental pillars that explain the strategy?

Answer: securing government systems, partnering to secure vital cyber systems outside the federal government, and helping Canadians to be secure online.

General knowledge: main (can be defined as) fundamental, define (synonym) explain.

1. Who summarizes these responsibilities, and provides a plan for harmonized response between government and other partners in case of the occurrence of a Cyber incident?

Answer: The Cyber Incident Management Framework

General knowledge: Outlines (synonym) summarizes, coordinated (can be defined as) harmonized, event (can be defined as) occurrence.

1. Who summarizes the proceeding execution of the strategy?

Answer: The Action Plan 2010\u20132015 for Canada's Cyber Security Strategy.

General knowledge: Outlines (synonym) summarizes, ongoing (can be defined as) proceeding, implementation (synonym) execution.

Computers control functions at many utilities, including coordination of telecommunications, the power grid, nuclear power plants, and valve opening and closing in water and gas networks. The Internet is a potential attack vector for such machines if connected, but the Stuxnet worm demonstrated that even equipment controlled by computers not connected to the Internet can be vulnerable to physical damage caused by malicious commands sent to industrial equipment (in that case uranium enrichment centrifuges) which are infected via removable media. In 2014, the Computer Emergency Readiness Team, a division of the Department of Homeland Security, investigated 79 hacking incidents at energy companies.

1. What utilities do computers command their tasks?

Answer: coordination of telecommunications, the power grid, nuclear power plants, and valve opening and closing in water and gas networks.

General knowledge: control (can be defined as) command, functions (synonym) tasks.

1. What is a possible attack vector for such devices if connected?

Answer: The Internet

General knowledge: potential (can be defined as) possible, machines (synonym) devices.

1. Who demonstrated that even machines commanded by computers not connected to the Internet can be at risk to physical damage caused by harmful commands sent to industrial equipment (in that case uranium enrichment centrifuges) which are infected via removable media?

Answer: the Stuxnet worm

General knowledge: equipment (can be defined as) machines, controlled (can be defined as) commanded, vulnerable (synonym) at risk, malicious (synonym) harmful.

1. Who scrutinized 79 hacking incidents at energy companies?

Answer: The Computer Emergency Readiness Team, a division of the Department of Homeland Security.

General knowledge: Investigated (can be defined as) scrutinized.

1. In what year was the 79 hacking incidents at energy companies scrutinized?

Answer: 2014

General knowledge: Investigated (can be defined as) scrutinized.

Today, computer security comprises mainly \"preventive\" measures, like firewalls or an exit procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the Internet, and can be implemented as software running on the machine, hooking into the network stack (or, in the case of most UNIX-based operating systems such as Linux, built into the operating system kernel) to provide real time filtering and blocking. Another implementation is a so-called physical firewall which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet.

1. What does computer security encompass?

Answer: \"preventive\" measures, like firewalls or an exit procedure.

General knowledge: comprise (synonym) encompass.

1. How can you describe a firewall?

Answer: a way of filtering network data between a host or a network and another network, such as the Internet, and can be implemented as software running on the machine, hooking into the network stack (or, in the case of most UNIX-based operating systems such as Linux, built into the operating system kernel) to provide real time filtering and blocking.

General knowledge: define (synonym) describe.

1. What is another execution that contain a separate device filtering network traffic?

Answer: A so-called physical firewall.

General knowledge: implementation (synonym) execution, Consists (synonym) contain,

Machine (synonym) device.

1. What is amongst devices that are perpetually connected to the Internet?

Answer: Firewall.

General knowledge: Machine (synonym) device, permanently (synonym) perpetually.

Serious financial damage has been caused by security breaches, but because there is no standard model for estimating the cost of an incident, the only data available is that which is made public by the organizations involved. \"Several computer security consulting firms produce estimates of total worldwide losses attributable to virus and worm attacks and to hostile digital acts in general. The 2003 loss estimates by these firms range from $13 billion (worms and viruses only) to $226 billion (for all forms of covert attacks). The reliability of these estimates is often challenged; the underlying methodology is basically anecdotal.\"

1. What is the cause of financial loss?

Answer: security breaches.

General knowledge: financial damage (synonym) financial loss.

1. What is the consequence of not having an established model for calculating the cost of an incident?

Answer: the only data available is that which is made public by the organizations involved.

General knowledge: standard (can be defined as) established, estimating (can be defined as) calculating.

1. Many computer security consulting companies produce estimates of total worldwide losses that are traceable to???

Answer: to virus and worm attacks and to hostile digital acts in general.

General knowledge: several (can be defined as) Many, firms (synonym) companies, attributable (synonym) traceable.

1. In what year did the loss estimates by these companies span from $13 billion (worms and viruses only) to $226 billion (for all forms of covert attacks)?

Answer: 2003

General knowledge: firms (synonym) companies, range (can be defined as) span.

While hardware may be a source of insecurity, such as with microchip vulnerabilities maliciously introduced during the manufacturing process, hardware-based or assisted computer security also offers an alternative to software-only computer security. Using devices and methods such as dongles, trusted platform modules, intrusion-aware cases, drive locks, disabling USB ports, and mobile-enabled access may be considered more secure due to the physical access (or sophisticated backdoor access) required in order to be compromised. Each of these is covered in more detail below.

1. What is a source of insecurity, such as with microchip exposure that are harmfully introduced during the manufacturing process?

Answer: hardware.

General knowledge: vulnerabilities (synonym) exposure, maliciously (synonym) harmfully, manufacturing (can be defined as) developing.

1. Why is the use of machines and procedures such as dongles, trusted platform modules, intrusion-aware cases, drive locks, disabling USB ports, and mobile-enabled access may be considered safer?

Answer: due to the physical access (or sophisticated backdoor access) required in order to be compromised.

General knowledge: Machine (synonym) device, methods (synonym) procedures, secure (can be defined as) safer.

Public Safety Canada\u2019s Canadian Cyber Incident Response Centre (CCIRC) is responsible for mitigating and responding to threats to Canada\u2019s critical infrastructure and cyber systems. The CCIRC provides support to mitigate cyber threats, technical support to respond and recover from targeted cyber attacks, and provides online tools for members of Canada\u2019s critical infrastructure sectors. The CCIRC posts regular cyber security bulletins on the Public Safety Canada website. The CCIRC also operates an online reporting tool where individuals and organizations can report a cyber incident. Canada's Cyber Security Strategy is part of a larger, integrated approach to critical infrastructure protection, and functions as a counterpart document to the National Strategy and Action Plan for Critical Infrastructure.

1. Who is in charge of alleviating and replying to threats to Canada\u2019s critical infrastructure and cyber systems?

Answer: Public Safety Canada\u2019s Canadian Cyber Incident Response Centre (CCIRC).

General knowledge: responsible (can be defined as) in charge, mitigating (synonym) alleviating, responding (synonym) replying.

1. Who gives support to alleviate cyber threats, technical support to reply and recuperate from targeted cyber-attacks?

Answer: The CCIRC

General knowledge: gives (can be defined as) provides, mitigate (synonym) alleviate, respond (synonym) reply, recover (synonym) recuperate.

1. Where does CCIRC publishes frequent cyber security bulletins?

Answer: on the Public Safety Canada website.

General knowledge: posts (can be defined as) publish, regular (synonym) frequent.

1. Where do individuals and organizations announce a cyber-occurrence?

Answer: CCIRC online reporting tool

General knowledge: report (can be defined as) announce, incident (synonym) occurrence.

1. What role does Canada's Cyber Security Strategy play as part of a larger, integrated approach to critical infrastructure protection?

Answer: It functions as a counterpart document to the National Strategy and Action Plan for Critical Infrastructure.

General knowledge: Role (can be defined as) function.

This has led to new terms such as cyberwarfare and cyberterrorism. More and more critical infrastructure is being controlled via computer programs that, while increasing efficiency, exposes new vulnerabilities. The test will be to see if governments and corporations that control critical systems such as energy, communications and other information will be able to prevent attacks before they occur. As Jay Cross, the chief scientist of the Internet Time Group, remarked, \"Connectedness begets vulnerability.\"

1. What are the recent terminologies that has been led to?

Answer: cyber warfare and cyber terrorism

General knowledge: new (can be defined as) recent, term (synonym) terminologies.

1. What happens when more polemical infrastructure is being commanded via computer programs?

Answer: increasing efficiency and exposes new vulnerabilities.

General knowledge: critical (synonym) polemical, controlled (synonym) commanded.

1. What is the aim of this experimental trial?

Answer: to see if governments and corporations that control critical systems such as energy, communications and other information will be able to prevent attacks before they occur.

General knowledge: test (can be defined as) experimental trial.

On September 27, 2010, Public Safety Canada partnered with STOP.THINK.CONNECT, a coalition of non-profit, private sector, and government organizations dedicated to informing the general public on how to protect themselves online. On February 4, 2014, the Government of Canada launched the Cyber Security Cooperation Program. The program is a $1.5 million five-year initiative aimed at improving Canada\u2019s cyber systems through grants and contributions to projects in support of this objective. Public Safety Canada aims to begin an evaluation of Canada's Cyber Security Strategy in early 2015. Public Safety Canada administers and routinely updates the GetCyberSafe portal for Canadian citizens, and carries out Cyber Security Awareness Month during October.

1. When did Public Safety Canada collaborate with STOP.THINK.CONNECT?

Answer: September 27, 2010

General knowledge: partner with (can be defined as) collaborate.

1. What is STOP.THINK.CONNECT committed to?

Answer: to informing the general public on how to protect themselves online.

General knowledge: dedicated (can be defined as) committed.

1. When did the Government of Canada inaugurate the Cyber Security Cooperation Program?

Answer: February 4, 2014

General knowledge: launched (can be defined as) inaugurate.

1. What is the goal of the program?

Answer: improving Canada\u2019s cyber systems through grants and contributions to projects in support of this objective.

General knowledge: aim (can be defined as) goal.

1. When does Public Safety Canada aspire to start an evaluation of Canada's Cyber Security Strategy?

Answer: Early 2015.

General knowledge: Aim to (synonym) aspire, begin (can be defined as) start.

1. Who organizes and regularly revises the GetCyberSafe portal for Canadian citizens?

Answer: Public Safety Canada

General knowledge: administer (synonym) organizes, routinely (synonym) regularly, updates (similar to) revises.

1. What month does Public Safety Canada perform Cyber Security Awareness?

Answer: October.

General knowledge: carry out (synonym) perform.

An unauthorized user gaining physical access to a computer is most likely able to directly download data from it. They may also compromise security by making operating system modifications, installing software worms, keyloggers, or covert listening devices. Even when the system is protected by standard security measures, these may be able to be by passed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and Trusted Platform Module are designed to prevent these attacks.

1. What can an unlicensed user that secures physical entrance to an electronic device, most likely do?

Answer: directly download data from it.

General knowledge: unauthorized (synonym) unlicensed, gains (can be defined as) secures, access (can be defined as) entrance, computer (can be defined as) electronic device.

1. How can security be jeopardized by unauthorized users?

Answer: by making operating system modifications, installing software worms, keyloggers, or covert listening devices.

General knowledge: compromised (can be defined as) jeopardized.

1. How can system protection by standard security measures be detoured?

Answer: Booting another operating system or tool from a CD-ROM or other bootable media.

General knowledge: bypassed (can be defined as) detoured.

1. What are formulated to avert these attacks?

Answer: Disk encryption and Trusted Platform Module.

General knowledge: designed (synonym) formulated, prevent (can be defined as) avert.

Clickjacking, also known as \"UI redress attack or User Interface redress attack\", is a malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to click on the top level page. This is done using multiple transparent or opaque layers. The attacker is basically \"hijacking\" the clicks meant for the top level page and routing them to some other irrelevant page, most likely owned by someone else. A similar technique can be used to hijack keystrokes. Carefully drafting a combination of stylesheets, iframes, buttons and text boxes, a user can be led into believing that they are typing the password or other information on some authentic webpage while it is being channelled into an invisible frame controlled by the attacker.

1. What is a harmful approach in which an attacker deceives a user into clicking on a button or link on another webpage while the user intended to click on the top level page?

Answer: Clickjacking, also known as \"UI redress attack or User Interface redress attack\".

General knowledge: malicious (can be defined as) harmful, technique (synonym) approach, tricks (can be defined as) deceives.

1. How is this performed?

Answer: This is done using multiple transparent or opaque layers.

General knowledge: done (synonym) performed.

1. What is consequence of cautiously drafting a mixture of stylesheets, iframes, buttons and text boxes?

Answer: A user can be led into believing that they are typing the password or other information on some authentic webpage while it is being channelled into an invisible frame controlled by the attacker.

General knowledge: Carefully (synonym) cautiously, combination (can be defined as) mixture.