Information Security Quiz

QUESTION

Once an individual consents to a fingerprint procedure, his or her fingerprints remain forever in the R.C.M.P. labyrinth?

ANSWER

Once the work of fingerprinting in the civil context is completed, the submission for fingerprinting is deleted from the R.C.M.P. system. In other words. The RCMP does not retain civil fingerprint submissions. Civil fingerprints, at no time, are populated in a data base where they could be subject to further research.

WHY IS IT RIGHT

AWARENESS TRAINING FOR EMPLOYEES

Provide Employee with Awareness Training

Cyber threat actors continue to evolve their attack tactics and techniques. A lack of awareness of cyber threats can lead to cyber incidents. Your organization should focus on creating tailored cyber security training to help users avoid cyber incidents and strengthen the overall cyber security culture in the workplace.

Include in training programs

Cyber threat actors take advantage of human error and deception to compromise information systems and assets. For example, cyber threat actors can access devices and information if easily guessed passwords are used for accounts. Or cyber threat actors can compromise your organization’s networks and systems by sending emails that contain malicious links or attachments.

Educating employees about common cyber threats can protect your organization and minimize risks.

Examples:

- Creating unique passphrases and complex passwords for all accounts
- Using the Internet and social media safely in the workplace
- Using approved software and mobile applications
- Identifying malicious emails

Recommendations for organization:

- Invest in cyber security training for employees
- Consider creating a cyber security training policy

Remote Workers – Security Tips

Remote work introduces some challenges when trying to balance functionality with security. When working remotely, your employees need to access the same internal services, applications, and information that they would have access to in the office. However, your organization also needs to protect its systems and information, as remote work introduces new vulnerabilities. You need to implement additional security precautions to prevent threat actors from taking advantage of those vulnerabilities.

THREATS TO REMOTE WORKERS

Remote work can increase the likelihood of compromises to your organization’s sensitive information. These actors use different methods to target remote workers:

- **Physical access to a device:** If employees leave devices unattended in public, threat actor can tamper with them or steal them.
- **Phishing:** A threat actor emails, texts, or calls victims and poses as a legitimate organization requesting sensitive information (e.g. passwords, credit card numbers).
- **Social engineering:** A threat actor may gather information about your organization, or an employee, online (e.g. corporate website, social media accounts) to craft a targeted phishing message.
- **Ransomware:** A threat actor uses malware to access a device and the data on it and then denies access until a sum of money is paid.
- **Wireless hijacking:** A threat actor spoofs a Wi-Fi network by creating a network that uses the same name as a legitimate one (e.g. a coffee shop’s public Wi-Fi network).
- **Eavesdropping:** A threat actor listens to Wi-Fi traffic and records online activities and account passwords.
- **Traffic manipulation:** If a mobile device is infected with malicious code, a threat actor can insert their own traffic to influence data and obtain access to your organization’s network.

EMPLOYEES – PRePARATION, preparation, preparation

If an employee has never worked remotely before, the transition can be surprisingly difficult. Set your employees up for success and clearly communicate the measures that they need to take to contribute to your organization’s cyber security.

- Have policies and procedures in place that outline, for example, the acceptable use of corporate devices and the management of corporate information.
- Ensure your employees know who to contact (and have the correct contact information), especially if they experience security issues or their devices are lost or stolen.
- Train your employees on cyber security issues and best practices, such as spotting phishing attempts, creating strong passphrases and passwords, and using secure Wi-Fi networks.

WHY IS EVERYTHING ELSE WRONG

SECURITY SCREENING/CIVIL SCREENING MODERNIZATION PROJECT

Fingerprinting and Credit Checks

- Explanations for each of what is changing and why.
- How the change will affect employees (including deemed employees).
- How the change will affect the organization.

FINGERPRINTING

The change and why

1. Changes implemented to conduct criminal record checks

The Royal Canadian Mounted Police (RCMP) has re-engineered its processes for criminal record checks through a project called Civil Screening Modernization, which involves transitioning from a name-based screening method to a fully electronic fingerprint-based model. Effective immediately, the RCMP will only accept digitized fingerprint records for processing. Like all other federal government departments, Statistics Canada must adopt this new method to conduct criminal record checks.

2. The myths about name-based criminal record checks

Name-based checks have inherent weaknesses arising from variances in spelling, common surnames, use of nicknames and name changes (both legal and those where an individual takes on a name for deceptive purposes). Fingerprint verification is the only way to effectively and accurately confirm identity, thereby preventing individuals from being falsely associated with a criminal record that is not theirs, and ensuring that individuals cannot evade their criminal past.

To date, the RCMP has used name-based checks for criminal record verifications because the technology to support fingerprint checks was not sufficient to meet the demand. If a name-based check indicated the possibility of an existing criminal record, fingerprints were required to confirm the identity prior to the release of any information. The RCMP now has a biometric (fingerprint) system capable of supporting the demand for all criminal record checks.

3. Asking for fingerprints is not treating individuals like criminals

Fingerprints have been used for many years to confirm identity and are an internationally accepted ‘best practice.’ Fingerprints are used increasingly to confirm identity for purposes unrelated to criminality, including immigration and visas, unlocking digital devices or paying for goods at major attractions. In the case of criminal records checks, fingerprinting is the only definitive way to determine whether an individual has a criminal record, thereby eliminating false associations with criminality.

4. Submitting fingerprints is not overly complex and time consuming and is more effective

Submitting fingerprints electronically is easy and convenient. The immediacy of electronic results will be a direct benefit to employers and applicants, especially those individuals whose application otherwise would have been unnecessarily delayed as a result of their names being incorrectly associated with those of convicted offenders. The results of name-based searches are not as accurate as fingerprint-based searches.

5. RCMP and Fingerprints

The RCMP does not retain civil fingerprint submissions. Once the work in progress is completed, the submission is deleted from the RCMP system. At no time are civil fingerprints populated on a database where they could be subject to further search.

Employee Concerns

1. Costs for fingerprint-based criminal record checks

For employees who cannot present themselves to a Statistics Canada regional office, local service fees may be required for fingerprinting by a police service or an accredited fingerprinting company.

2. Prints taken for volunteer for community work, sports association or other organizations, be used.

Unfortunately, they cannot. They need to be retaken because the RCMP does not store fingerprints.

Statistics Canada – The Effect

1. What are the options available for recording and submitting fingerprints?

The RCMP will only accept electronic fingerprints. Electronic submissions must meet the RCMP standards and must be created by using either an Electronic Fingerprint Capture Device (Livescan) or Cardscan, in which paper-based fingerprints are scanned and converted into electronic submissions.

Statistics Canada has installed electronic fingerprint capture devices in Ottawa and in each of the regional offices: Halifax, Sherbrooke, Montréal, Toronto, Sturgeon Falls, Winnipeg, Edmonton and Vancouver. In addition, a Cardscan device will be installed in the security office located in Ottawa.

Statistics Canada is investigating the feasibility of partnering with other federal government departments that have locations outside its regional office network.

The final option is to refer the individual to an accredited third party fingerprint agency or local law enforcement office. In this case, the applicant will be responsible for any cost incurred.

CREDIT CHECKS

The Change, and why?

1. Standard on Security Screening

The *Standard on Security Screening* ensures that security screening in the Government of Canada is effective, efficient, consistent and fair. The Government of Canada is standardizing security screening processes and leveraging new technologies across all departments and agencies. As you know, security screening is an integral component of the hiring process, and obtaining and maintaining a valid security level is a condition of employment with the Government of Canada.

2. Key changes in the *Standard on Security Screening*

Security checks conducted under ‘standard’ (or ‘reliability status’) screening—which involves the majority of Statistics Canada employees—will essentially remain the same. A mandatory credit check will be introduced immediately for new hires and as security screenings for current employees require updating or renewal.

A credit check is only one of a number of factors considered during the security screening process. Screening activities relating to ’enhanced‘ screening for positions involving security and intelligence duties will see additional checks being conducted according to the duties of the position occupied. Reliability status and secret clearances are valid for 10 years if there is no break in service that exceeds one year.

3. Screening activities for reliability status

- verification of identity and background
- verification of educational and professional credentials
- personal and professional references
- criminal background check.

4. Credit checks mandatory for security screening

The new Treasury Board Secretariat (TBS) Standard on Security Screening that came into effect on October 20, 2014, for all Government of Canada departments and agencies established a risk-based approach to security screening. As part of this new standard, a credit check—which is only one of a number of factors considered during the security screening process—is a mandatory requirement.

The new Standard on Security Screening will be implemented over 36 months. Effective October 20, 2014, credit checks are mandatory for all new requests for security screening. Credit checks for current employees and contractors will be implemented as security screening is required for updates, upgrades or reviews for cause.

5. The requirement is applicable to whom?

This new requirement applies to all individuals employed by or working in federal departments. This includes employees (including deemed employees), volunteers, students, private sector contractors and people on loan, assignment or secondment.

6. Practices of the Government of Canada

The practice of conducting mandatory financial inquiries (credit checks) for security screening dates back to 1986 when the first Treasury Board *Government Security Policy* was introduced. At that time, although optional for ‘reliability’ screening, some departments conducted mandatory credit checks for all levels of screening.

7. Purpose of conducting a credit check for security screening

An assessment of the trustworthiness and reliability of all individuals accessing sensitive information or assets must be undertaken to protect the interests and security of the Government of Canada. In addition to other information collected (e.g., criminal record check, employment history, personal character references), a credit report will be reviewed to assist in assessing an individual’s reliability and trustworthiness as an employee of or individual working with the Government of Canada.

EMPLOYEE CONCERNS

1. Credit history and it’s content

A credit history is a record of an individual’s past borrowing and repaying, including information about late payments and bankruptcy. It is used as a measure of reliability.

The information in a credit history includes date of birth, addresses, employment information and a comprehensive history of the current credit or credit that has been used at any time in the past six years—or longer if bankruptcy was declared. This history is kept up to date by the financial institutions, credit card companies, retailers, auto lease financing companies and other establishments that provide an individual with credit.

2. Credit report information assessment

The overall assessment of reliability considers an individual’s trustworthiness in protecting government assets, information and facilities. An individual’s financial situation is relevant to this assessment, particularly as it relates to their ability to meet their financial obligations.

Information that may be of concern would be an inability to make payments on time, accounts placed for collections or written off by financial institutions as unrecoverable or a very high ratio of debt to income. Information contained in a credit report can also be used to validate other information provided by an individual such as previous address or date of birth.

3. What other lenders will know if the Government of Canada requested a credit report on an employee

Credit checks conducted for the purpose of security screening are masked so that a negative effect does not occur on the individual’s credit bureau file. Only credit checks performed by Canadian financial institutions (banks, credit unions, credit agencies, etc.), which are interpreted by credit reporting agencies as attempts by the individuals to obtain credit, have an impact on an individual’s credit score.

4. Credit checks – the legality

Yes, credit checks are legal. The *Policy on Government Security* and the *Standard on Security Screening* provide the legal basis for verifying the credit history for security screening purposes for those individuals working at Government of Canada departments and agencies.

5. Personal information protection during the credit check

The protection of personal information is governed by the *Privacy Act*, which establishes personal information-handling practices of federal government departments and agencies to respect the privacy of all Canadian citizens and permanent residents. The Office of the Privacy Commissioner of Canada oversees compliance with the *Privacy Act*.

With respect to the security of your information, the credit report is made available through the credit reporting agency’s website using secure connectivity methods (e.g., point-to-point connections, Secure Sockets Layer or ‘SSL’ encryption), and client identification information on each transaction is validated by the credit reporting agency before being processed. The encryption process transforms sensitive information into a string of unrecognizable characters before they are sent over the Internet and helps keep the information private between the computer system and the Internet browser.

In addition to encryption, a unique username and password would be required to authenticate the department or agency security official processing the credit check each time they access or use the service.

6. Where an individual does not want to consent to a credit check

A credit check is a component of the new *Standard on Security Screening*. For initial requests where the individual refuses to provide consent or the required information, screening activities will cease and an administrative cancellation will follow. When a security screening is being updated or upgraded, the individual's existing security screening must be suspended and reviewed for cause, and Human Resources should be consulted.

This administrative cancellation will result in the individual no longer meeting the condition of the screening standard and could result in an administrative termination of employment, or cancellation or termination of a contract.

7. The effect on a credit history due to a credit check

Your credit history will not be affected by the credit check

8. The results of credit checks

The results will remain within the Departmental Security office's personnel security screening files. They are protected and properly safeguarded in accordance with the *Policy on Government Security*, the *Standard on Security Screening* and the *Privacy Act*.

The Departmental Security office is not permitted to discuss an individuals' information with the credit bureau because of privacy reasons. The only information an individual will automatically receive is a confirmation that a reliability status or security clearance has been granted, denied or revoked. The individual may contact the credit bureau to discuss their results.

9. Negative credit checks

If the results of the credit check provide adverse information, such as a history of collection or missed payments, a more in-depth assessment is required that may require an interview with the individual by Departmental Security. The results of this interview will assist with the assessment and determination to grant, deny or revoke the reliability status or security clearance.

10. Where one does not pass the credit check?

A process will be applied to review individual cases that have extenuating circumstances.

11. Do the results of a credit check impact the position of an employee?

It would be very unlikely that a credit check would form the basis for a denial or revocation of a reliability status or a security clearance. It is one part of a comprehensive assessment of information collected to determine reliability and trustworthiness.

If it is deemed that the results of the credit check, along with other information found, could pose a risk to the functions being performed in an individual's position, there is a possibility that these results will affect the specific assessment. Before any decision is made, however, individuals will be informed and given an opportunity to respond to the information.

Statistics Canada – the affect

1. The responsibility for processing these checks

The Departmental Security office will process these checks as one of the verifications undertaken in the personnel security screening process and will protect personal information in accordance with the provisions of the *Privacy Act*.

2. Delays in processing a security screening request due to additional check.

This additional check should not cause any further delays as the report is available through the credit bureau’s supplier’s web interface. Should a report contain adverse information, delays may be incurred if a more in-depth assessment is required (e.g., an interview with the individual to better understand the circumstances).