IR Plan, Playbook and Policy

For Canadian Tire Corporation

Author: Sumit Giri

LHL Project #: 07

Date: 27-10-2024

Table of Contents

1. Revision History

This Incident Response Plan has been updated as follows:

Date	Version	Modification	Modifier
2024-10-25	1.0	Initial version established	Sumit

2. Testing & Review Cycle

To ensure the Cyber Security Incident Response Team (CSIRT) is well-informed of its responsibilities, annual testing of the Incident Response Plan is essential. In the absence of real incidents that fully engage the process, testing can be conducted through walkthroughs and practical simulations of possible incident scenarios.

1. **Annual Testing**: The Incident Response Plan will undergo testing at least once a year.
2. **Evaluation of Response**: The testing will evaluate the organization's response to potential incident scenarios, identifying any gaps in processes and areas that require enhancement.
3. **Record of Insights**: The CSIRT will record insights gained during testing, noting any steps that were executed poorly or misunderstood by participants, as well as aspects that require improvement.
4. **Plan Updates**: The Incident Handler will be responsible for updating the Incident Response Plan and distributing it to CSIRT members as needed.

3. Purpose & Scope

3.1 Purpose

This Incident Response Plan ensures Canadian Tire Corporation (CTC) is prepared to effectively manage data breach incidents. With cyber threats becoming more frequent and sophisticated, it's vital for CTC to have a structured approach to respond swiftly to any breaches, as well as to prevent and detect them. By implementing this plan and conducting regular training, CTC aims to minimize the impact of incidents, quickly contain damage, and mitigate risks.

This document outlines how CTC will respond to Phishing incident, detailing team structures, roles, responsibilities, and processes for preparation, identification, containment, eradication, recovery, and post-incident analysis.

3.2 Scope

This plan applies to all of CTC's networks, systems, data, and stakeholders, including employees, contractors, and third-party vendors. Members of the Cyber Security Incident Response Team (CSIRT) are expected to lead the response efforts. All team members should be familiar with this plan and ready to collaborate to minimize the impact of Phishing incident.

This document provides a framework for handling Phishing incidents but does not list every possible action to address such incidents.

4. Authority

The responsibility for the security of Canadian Tire Corporation's data and that of its customers rests with the President and CEO of CTC. In the event of a phishing incident, this responsibility is delegated to the Chief Information & Technology Officer (CITO). The CITO, in coordination with the Cyber Security Incident Response Team (CSIRT), will lead a swift and structured response to contain the threat, mitigate risks, and safeguard sensitive information across all systems and stakeholders.

5. Definitions

The following definitions are based on the definitions given in the Cybersecure Canada, Incident Response Plan template & example (Government of Canada, 2021).

- **Acceptable Interruption Window:** In Canadian Tire Corporation's business continuity planning, this represents the maximum time allowed for critical systems to restore basic functionality following a disruption. It is a crucial factor in formulating disaster recovery strategies to minimize operational impact.
- **Confidentiality:** Refers to the classification of Canadian Tire Corporation's sensitive data, often involving personally identifiable information (PII), such as customer account numbers, employee social insurance numbers, and financial data, which must be safeguarded to prevent unauthorized access and maintain trust.
- **Cybersecurity Event:** An observable occurrence in CTC's systems or network, which may include employee logins, transactions in a system, or email exchanges. These events can indicate normal activity or potentially lead to incident detection when analyzed collectively.
- **Cybersecurity Incident:** Any intentional or accidental occurrence that negatively impacts CTC's information processing systems. Incidents may compromise the confidentiality, integrity, or availability of CTC's data or services, including unauthorized access, modification, or data destruction.
- **Denial of Service (DoS) Attack:** An attack method where the target system, often CTC's customer-facing portals, is overwhelmed with excessive requests, disrupting service for legitimate users and impairing business operations.
- **Exploit:** In cybersecurity terms, this is any software or command sequence that leverages a vulnerability to trigger unintended actions on CTC's systems, potentially compromising data or system integrity.
- **Indicators of Compromise (IoCs):** Forensic clues on CTC's network that may signify a security breach. IoCs might include unusual patterns in log entries, abnormal files, or indicators from threat intelligence sources, which assist in identifying potential threats.
- **Integrity:** This refers to ensuring the accuracy, consistency, and authenticity of CTC's data, protecting it from unauthorized modifications and ensuring that information remains reliable across its lifecycle.

- **Maximum Tolerable Downtime (MTD):** Defines the longest period that critical Canadian Tire operations can remain inactive before facing severe impact, making this metric essential to assessing acceptable risks in continuity planning.
- **Response Playbook:** A reference guide with prescriptive cybersecurity measures that CTC can adopt to fortify its defenses. It outlines best practices, response protocols, and structured actions to take in incident scenarios, improving both preventative and reactive strategies.
- **Service Availability:** Indicates the system's responsiveness and accessibility to end users, often represented as a percentage. For example, maintaining a 99.9% availability rate on CTC's customer interface ensures that the portal is accessible for nearly all operational hours.
- **Service Level Agreement (SLA):** A contractual performance measure often detailing CTC's uptime commitments for core systems. Falling short of the SLA threshold may incur financial penalties, especially with vendors and external service providers.
- **Stakeholder Relationship Map:** A visual diagram representing CTC's internal and external stakeholders in cybersecurity. It helps outline responsibilities, improving the organization's capacity to manage IT risks and cybersecurity interactions across departments.
- **Vulnerability:** A flaw or bug within CTC's systems that could lead to unwanted behavior or exploitation. Vulnerabilities necessitate prompt attention to avoid potential misuse by attackers.
- **War Room:** A dedicated, secure meeting space for handling significant incidents at CTC. Equipped with advanced communication tools, it serves as the hub for coordinating response efforts and maintaining privacy during active incidents.
- **Zero-Day:** Describes a vulnerability that lacks a vendor-provided patch, which makes it particularly critical for CTC to monitor, as attackers may exploit it before mitigation is available.

6. How to Recognize a Phishing Incident

Recognizing phishing incidents within Canadian Tire Corporation (CTC) is essential to protect sensitive information. The identification process includes proactive and reactive measures, often guided by key leads and indicators.

1. Leads: Proactive signs can help suggest that a phishing attempt may be occurring. For CTC, relevant leads include:

- **Suspicious Email Patterns**: Phishing emails commonly use tactics like impersonating trusted companies, claiming account issues, or creating urgency to trick recipients into clicking malicious links or providing personal information. Scammers may send unexpected messages resembling those from banks or utility companies, often including fake invoices or requests for personal data (Federal Trade Commission, 2024).
- **Unusual Network Activity**: Alerts from cybersecurity tools detecting anomalies in network traffic or email patterns can signal a phishing attempt targeting CTC's systems. For example, repeated logins from unknown IP addresses might indicate attempts to exploit user credentials.

2. Indicators: Reactive signs are key to identifying whether phishing has already compromised a user or system. Critical indicators include:

- **Unusual Email Behaviour**: Phishing emails often feature generic greetings or appear to address billing issues, directing recipients to update payment information on fake websites (Federal Trade Commission, 2024). Monitoring for suspicious email activity—especially those with links or attachments from unknown senders—can help reveal compromised accounts.
- **Unauthorized Access Attempts**: Numerous failed or out-of-region login attempts are signs of potentially compromised credentials, as phishing attacks often aim to steal user access information.

By recognizing both leads and indicators, CTC can improve its ability to detect and respond to phishing incidents swiftly, securing its data and maintaining customer trust.

7. Cyber Security Incident Response Team (CSIRT) for Phishing Incidents at Canadian Tire Corporation (CTC)

7.1 CSIRT Structure

The following roles are established within CTC's CSIRT for managing Phishing incidents:

CSIRT Role	Role Definition
Executive Lead	**President and CEO** (Greg Hicks): Provides overall strategic direction for cybersecurity, approves high-impact decisions during phishing incidents, and reports to the Board on incidents as needed.
Incident Response Coordinator	**Chief Information & Technology Officer (CITO)** (Rex Lee): Activates the Incident Response Plan, oversees incident management activities, and coordinates cross-functional teams.
Communications Lead	**Executive VP & Chief Brand & Customer Officer** (Susan O'Brien): Manages internal and external communications regarding the incident to protect CTC's reputation and keep stakeholders informed.
Operations Lead	**Chief Supply Chain Officer** (Paul Draffin): Manages IT operations during incidents to ensure business continuity across critical systems, including supply chain networks.
Legal Advisor	**Executive VP & General Counsel** (Lisa Damiani): Advises on legal obligations, ensures regulatory compliance, and assists

	with phishing incident notification requirements.
HR Liaison	**Chief Human Resources Officer** (Bob Hakeem): Coordinates staff communication, manages employee support in case of compromised personal data, and addresses cybersecurity training needs.
Cybersecurity Architect	**Cybersecurity Architect** (In-house role): Designs secure system architectures, evaluates potential vulnerabilities, and collaborates with incident handlers to address structural risks.
Threat Intelligence Analyst	**Threat Intelligence Analyst** (In-house role): Identifies, analyzes, and monitors potential cyber threats to CTC, ensuring early detection and proactive response measures.
Database Specialist	**Senior Database Administrator**: Ensures database security, protects data integrity, and supports data restoration efforts if phishing incidents compromise database access.
IT Support Specialist	**IT Systems Engineer**: Provides technical support to systems impacted by phishing attempts, aiding in the restoration of services and securing operational environments.
Network Security Specialist	**Network Security Architect**: Monitors network traffic for phishing-related anomalies, performs forensic analysis, and collaborates on containment of network threats arising from phishing activities.
Forensic Analyst	**Cyber Forensics Analyst**: Investigates phishing incidents to identify the source and scope, preserving digital evidence and supporting post-incident analysis.
Finance Liaison	**Executive VP & CFO** (Gregory Craig): Assesses financial implications of phishing incidents, allocates necessary budgets for response efforts, and reports on financial risks associated with phishing attacks.

7.2 CSIRT Responsibilities

Executive Lead Responsibilities

- **President and CEO**:
    1. Provides executive oversight for CSIRT activities and makes strategic decisions on cybersecurity investments.

2. Communicates the impact and response strategies for significant phishing incidents to the Board.

Incident Response Coordinator Responsibilities

- **Chief Information & Technology Officer (CITO)**:
  1. Leads the CSIRT, activates the Incident Response Plan upon detection of a phishing incident, and coordinates all response efforts.
  2. Delivers regular progress updates and detailed incident reports to the CEO and executive team.

Communications Lead Responsibilities

- **Chief Brand & Customer Officer**:
  1. Manages communications for internal and external stakeholders regarding phishing incidents.
  2. Ensures that any external information aligns with Canadian Tire Corporation's brand reputation and addresses public concerns.

Operations Lead Responsibilities

- **Chief Supply Chain Officer**:
  1. Ensures continuity of supply chain and IT operations affected by phishing incidents.
  2. Coordinates with IT and cybersecurity teams on mitigating phishing threats that could impact operational functions.

Legal Advisor Responsibilities

- **General Counsel**:
  1. Advises on legal compliance and phishing incident notification protocols.
  2. Reviews response actions to ensure regulatory adherence in handling phishing incidents.

HR Liaison Responsibilities

- **Chief HR Officer**:
  1. Communicates phishing-related best practices and supports affected staff during incidents.
  2. Coordinates post-incident training and awareness to prevent future phishing attempts.

Cybersecurity Architect Responsibilities

- **Cybersecurity Architect**:
  1. Reviews system architecture for vulnerabilities related to phishing threats.
  2. Collaborates with the CITO and IT teams to implement structural safeguards and defenses.

Threat Intelligence Analyst Responsibilities

- **Threat Intelligence Analyst**:
    1. Monitors emerging phishing techniques and indicators of compromise to proactively address risks.
    2. Shares threat intelligence with the CSIRT to strengthen detection and response to phishing incidents.

Senior Database Administrator Responsibilities

- **Senior Database Administrator**:
    1. Assesses potential impacts on database security due to phishing compromises and aids in data recovery if necessary.
    2. Assists in safeguarding data integrity during and after a phishing incident.

IT Systems Engineer Responsibilities

- **IT Systems Engineer**:
    1. Provides technical support for restoring functionality to systems impacted by phishing attempts.
    2. Assists in implementing enhanced security configurations post-incident.

Network Security Architect Responsibilities

- **Network Security Architect**:
    1. Monitors network traffic for phishing-related anomalies and supports threat containment efforts.
    2. Contributes to forensic analysis and implements enhanced network defense measures.

Cyber Forensics Analyst Responsibilities

- **Cyber Forensics Analyst**:
    1. Conducts in-depth investigations to identify the origin and scope of the phishing incident.
    2. Compiles and preserves evidence for potential legal proceedings.

Finance Liaison Responsibilities

- **Chief Financial Officer (CFO)**:
    1. Evaluates the financial impact of phishing incidents and allocates necessary budgets for response activities.
    2. Communicates financial risks associated with phishing threats to relevant stakeholders.

All Staff Responsibilities

- **All Employees**:
    - All staff must understand procedures for identifying and reporting phishing-related activities.
    - Employees should report any suspicious emails or activities to the Incident Response Coordinator or a CSIRT member immediately.

8. Contact Information

8.1 CSIRT Contacts

CSIRT Role	Title	Phone	Email	Availability
Executive Lead	President and CEO	647-555-0001	executivelead@canadiantire.ca	M-F, 9 AM - 5 PM
Incident Response Coordinator	Chief Information & Technology Officer	647-555-0002	incidentresponse@canadiantire.ca	M-F, 9 AM - 5 PM
Communications Lead	Executive VP & Chief Brand & Customer Officer	647-555-0003	communications@canadiantire.ca	M-F, 9 AM - 5 PM
Operations Lead	Chief Supply Chain Officer	647-555-0004	operations@canadiantire.ca	M-F, 9 AM - 5 PM
Legal Advisor	Executive VP & General Counsel	647-555-0005	legal@canadiantire.ca	M-F, 9 AM - 5 PM
HR Liaison	Chief Human Resources Officer	647-555-0006	hr@canadiantire.ca	M-F, 9 AM - 5 PM
Cybersecurity Architect	Cybersecurity Architect	647-555-0007	cybersecurity@canadiantire.ca	M-F, 9 AM - 5 PM
Threat Intelligence Analyst	Threat Intelligence Analyst	647-555-0008	threatintel@canadiantire.ca	M-F, 9 AM - 5 PM
Database Specialist	Senior Database Administrator	647-555-0009	dbadmin@canadiantire.ca	M-F, 9 AM - 5 PM
IT Support Specialist	IT Systems Engineer	647-555-0010	itsupport@canadiantire.ca	M-F, 9 AM - 5 PM
Network Security Specialist	Network Security Architect	647-555-0011	networksecurity@canadiantire.ca	M-F, 9 AM - 5 PM
Forensic Analyst	Cyber Forensics Analyst	647-555-0012	forensics@canadiantire.ca	M-F, 9 AM - 5 PM
Finance Liaison	Executive VP & Chief Financial Officer	647-555-0013	finance@canadiantire.ca	M-F, 9 AM - 5 PM

8.2 External Contacts

Role	Organization	Title	Phone	Email	Availability
Network Security Vendor	Cybersecurity Vendor Ltd.	Support Lead	647-555-0014	support@canadiantire.ca	M-F, 9 AM - 5 PM
Network Security Vendor	Cybersecurity Vendor Ltd.	Helpdesk	1-888-555-0014	helpdesk@canadiantire.ca	24/7
Lawyer	Legality Corp.	Lawyer	647-555-0025	legal@canadiantire.ca	M-F, 9 AM - 5 PM
Parts Supplier	Supplier Co	Account Manager	647-555-0036	gina@supplier.co	M-F, 9 AM - 5 PM
Card Acquirer Service	POS Ltd.	Account Manager	647-555-0047	richard@pos.ca	M-F, 9 AM - 5 PM
Cyber Insurance Provider	Insurance Ltd.	Account Manager	647-555-0058	mandy@insurance.ca	M-F, 9 AM - 5 PM
Law Enforcement (local)	Toronto Police	Toronto Police	647-911-0911	report@police.ca	24/7
Law Enforcement (federal)	RCMP National Cybercrime	Cybercrime Reporting	613-993-7267	NA	NA

9. Incident Severity Matrix

The Incident Severity Matrix for Canadian Tire is utilized by the Cyber Security Incident Response Team (CSIRT) to assess the severity of a phishing incident. The CSIRT will leverage this matrix to guide the response based on the severity of the incident. Based on the listed incidents by the Federal Trade Commission (Federal Trade Commission, 2021), here are some of the considerations bellow.

Key Considerations:

1. **Scope of the Incident:** The CSIRT will evaluate whether the incident affects a single user or multiple users within Canadian Tire's network.
    - **Example:** A phishing attempt targeting a single employee versus a widespread campaign affecting multiple departments.
2. **Criticality of Affected Systems:** The impact will be assessed based on how critical the affected systems are to Canadian Tire's core business operations.
    - **Example:** A breach impacting financial systems versus an isolated incident involving employee email accounts.
3. **Number of Affected Individuals or Teams:** The CSIRT will determine if the phishing incident impacts a single individual or multiple teams within Canadian Tire.

   - **Example:** An incident affecting finance and HR teams versus an isolated incident involving IT support staff.
4. **Business Context:** The CSIRT will also consider the business operations relevant at the time of the incident. The urgency may increase if the phishing attack coincides with a major sales event or promotional period.

Additional Factors Considered by CSIRT:

- **Magnitude of Impact:** The team will evaluate the known and potential size of the incident, whether it is contained, or if there is a risk of it spreading.
- **Likelihood of Spread:** The CSIRT will assess the risk of the phishing attack spreading to other users or departments and the pace at which this may occur.
- **Potential Damage:** The incident's potential impact on Canadian Tire's financial position, reputation, and customer trust will be considered.

Threat Characteristics:

The phishing incident may stem from various sources, such as:

- **Automated or Manual Attacks:** Phishing emails designed to trick employees into revealing sensitive information or credentials (T1598 | MITRE, n.d.).
- **Nuisance or Vandalism:** Less severe phishing attempts targeting non-critical systems.

CSIRT Assessment Process:

The CSIRT will consider the following criteria when assessing the incident:

1. **Vulnerability Exploitation:** Is there evidence that a known vulnerability was exploited?
2. **Patching:** Is there a patch available to address any identified vulnerabilities?
3. **Type of Threat:** Is this a new phishing threat, or is it a known tactic that can be mitigated quickly?
4. **Effort to Contain:** What resources are required to contain and remediate the incident?

Incident Severity Categories

Category	Indicators	Scope	Action
1 – Critical	Significant data loss, widespread credential theft	Widespread across critical systems (e.g., financial data, customer information)	Activate CSIRT, execute Incident Response Plan (IRP), organization-wide response, notify executive leadership.
2 – High	Exploitation of vulnerabilities, data theft	Affects major systems (e.g., email systems, network infrastructure)	Activate CSIRT, execute IRP, notify relevant stakeholders, and initiate organization-wide response.

3 – Medium	Phishing attempts with limited spread	Multiple users or departments affected (e.g., sales and marketing)	Initiate CSIRT, execute IRP, notify IT support, and monitor the incident closely.
4 – Low	Phishing or suspicious activity on one host	Individual workstation or person affected	Notify CSIRT, monitor the situation, escalate if necessary, and notify IT support for containment.

This matrix helps Canadian Tire assess and respond to phishing incidents swiftly, ensuring that critical systems and sensitive data are prioritized. If an incident affects a major part of Canadian Tire's operations or data, it escalates to "Critical" status, triggering a comprehensive response involving the CSIRT and executive leadership (T1566 | MITRE, n.d.).

10. Incident Handling Process

10.1 Overview

This playbook is activated for phishing threats based on specific triggers, such as phishing detection alerts, suspicious email reports from employees, or potential breaches. Based on guidance by NIST (Phishing | NIST, 2024) and the NIST Risk Management Framework (NIST, n.d.) each stage assigns tasks to relevant teams, with the goal of protecting sensitive data, systems, and customer information.

10.2 Conditions for Activating the Playbook

Trigger Points:

- Alerts from phishing detection systems.
- User reports of suspicious emails.
- Verification of phishing attempts by security analysts.

10.3 Preparation

Objective: Establish a strong foundation for phishing incident response.

- **Phishing Incident Response and CSIRT Development**
  - **Responsible Group:** CSIRT Lead and Security Operations
  - **Actions:** Develop and document a comprehensive Phishing Incident Response Plan that outlines roles, responsibilities, and procedures. Form a dedicated response team trained specifically in phishing detection and response protocols to ensure effective action during incidents.
- **Enhancing Security Posture**
  - **Responsible Group:** Security Operations
  - **Actions:** Based on findings from post-incident reviews, enhance the organization's security posture by implementing additional security measures to prevent similar incidents in the future. This may include deploying or adjusting Anti-Phishing Software, DNS filters, email and web filters, and

implementing Two-Factor Authentication (2FA), as well as introducing new security tools (Cloudflare, n.d.).

- **Awareness and Reporting Initiatives**
  - **Responsible Group:** IT Security
  - **Actions:** Conduct phishing awareness campaigns and implement an easy reporting mechanism for employees to report phishing attempts (Canada, 2022a).

10.4 Detection and Analysis

Objective: Detect and confirm phishing incidents to assess their scope.

- **Phishing Detection**
  - **Responsible Group:** IT Monitoring
  - **Actions:** Use monitoring tools to detect phishing indicators, including suspicious email activity and unusual web form submissions.
- **Phishing Attack Scoping**
  - **Responsible Group:** Security Analysts
  - **Actions:** Assess the scale of the phishing attack, including the number of impacted users and any compromised accounts.
- **Phishing Analysis**
  - **Responsible Group:** Incident Response Team
  - **Actions:** Analyze email content, headers, links, and attachments to confirm the nature and potential impact of the phishing attempt (T1566 | MITRE, n.d.).

10.5 Containment

Objective: Limit the spread and impact of the phishing attack.

- **Trigger Point:** Confirmation of an active phishing incident.
- **Responsible Group:** Security Operations
- **Actions:** Block identified phishing emails, restrict access to suspicious links, and implement alerts to notify users of the ongoing threat (Kaspersky, 2016).

10.6 Eradication

Objective: Fully eliminate the phishing threat from affected systems.

- **Trigger Point:** Confirmation of compromised accounts or systems.
- **Responsible Group:** IT Support
- **Actions:** Disable compromised accounts, reset affected passwords, and work with users to secure access (Canada, 2022b).

10.7 Recovery

Objective: Restore systems and notify impacted users, returning operations to normal.

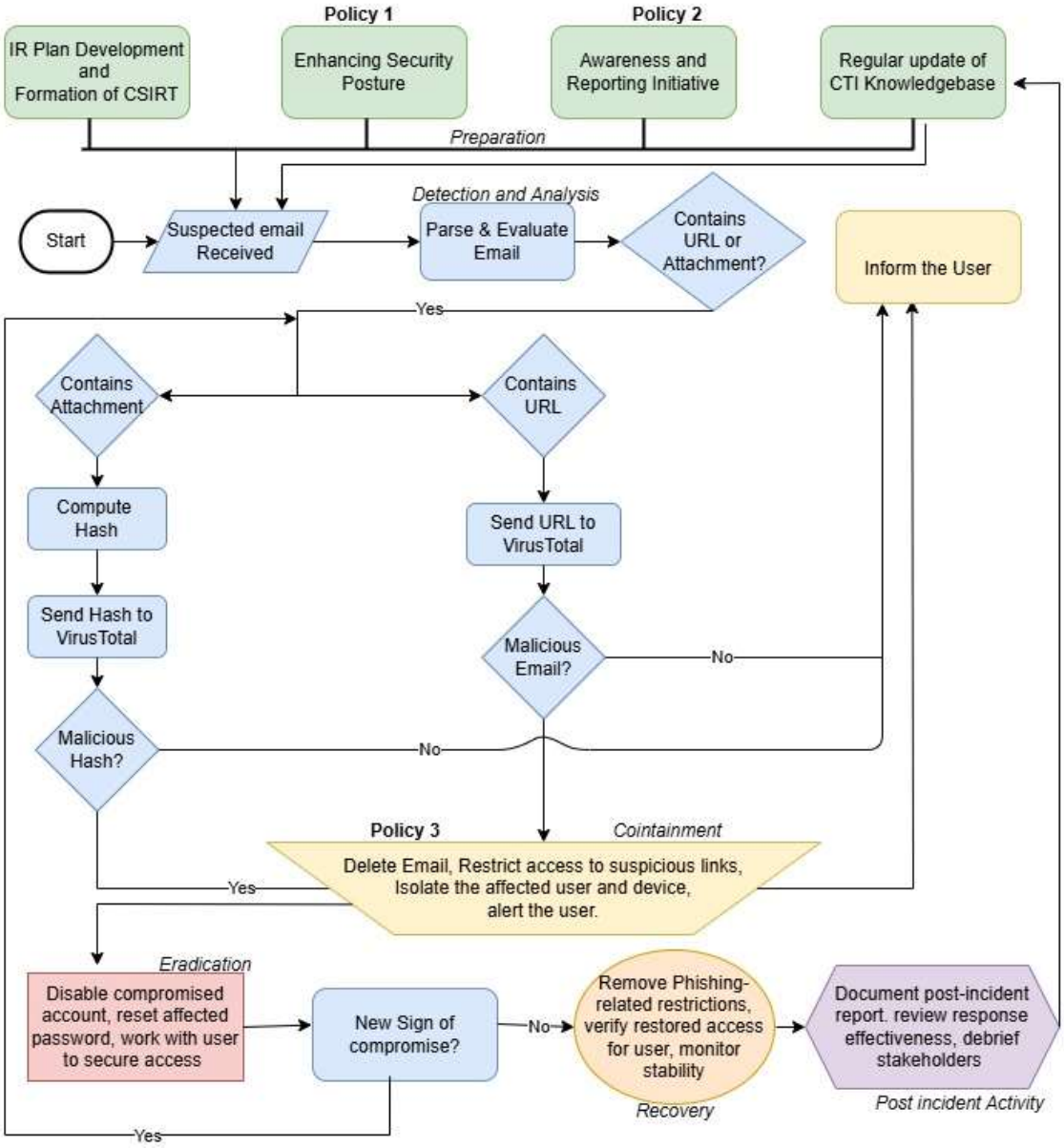
- **Trigger Point:** Full removal of the phishing threat.
- **Responsible Group:** IT Systems Recovery Team
- **Actions:** Remove phishing-related restrictions, verify restored access for impacted users, and monitor for recurrence to ensure stability.

10.8 Lessons Learned

Objective: Reflect on the incident to improve future response capabilities.

- **Trigger Point:** Scheduled within one week post-incident.
- **Responsible Group:** Incident Analysis Team
- **Actions:** Document a post-incident report with key insights, review response effectiveness, and conduct a debrief with relevant stakeholders to identify improvement areas (Kaspersky, 2022).

10.9 IR Playbook Flowchart



11. Approval

Responsible Party
The responsibility for the development, updating, and enforcement of the Incident Response Plan rests with the following individuals:

Responsible Party Role	Responsible Party Signature	Version	Date
Chief Executive Officer		1.0	

The Responsible Parties have reviewed the Incident Response Plan and have delegated the responsibility for mitigating harm to the organization to the Incident Handler. In the event of a high or critical phishing incident, this responsibility is entrusted to the Incident Handler or their delegate.

---

12. Incident Handler

The Incident Handler for Canadian Tire's phishing incidents is the Chief Information & Technology Officer (CITO). The CITO has reviewed the Security Incident Response Plan and acknowledges that, during a phishing incident, the responsibility for managing the incident is entrusted to them or their delegate.

Incident Handler Role	Incident Handler Signature	Version	Date
Chief Information & Technology Officer		1.0	

The Incident Handler is expected to manage the incident in a manner that mitigates further exposure of the organization. This will involve following the established process, including identification, containment, eradication, recovery, and lessons learned.

13. Policy Outlines

13.1 Enhancing Security Posture

Purpose:
To continually improve the organization's defenses against phishing threats and related cybersecurity incidents.

Importance:
This policy is essential for proactively addressing vulnerabilities and reducing the likelihood of successful phishing attacks. By enhancing security measures, Canadian Tire can protect sensitive data and maintain customer trust.

Activities:

- Conduct post-incident reviews to identify weaknesses and implement recommended changes.
- Regularly assess and upgrade security measures, including Anti-Phishing Software, DNS filtering, email and web filters, and Two-Factor Authentication (2FA) (Cloudflare, n.d.).
- Schedule quarterly reviews of security policies and technologies to ensure they align with current threat landscapes.

Related Playbook:
The Phishing Incident Response Playbook will provide detailed instructions on implementing security enhancements, including assessments, tool deployments, and effectiveness evaluations.

Consequences of Non-Compliance:

- **Individual:** Failure to follow security enhancement protocols may lead to disciplinary actions, including formal warnings or termination.
- **Company:** Inadequate enhancements can result in increased susceptibility to phishing attacks, leading to financial losses and reputational damage.

13.2 Awareness and Reporting Initiative

Purpose:
To foster a culture of security awareness and establish clear reporting mechanisms for suspected phishing incidents among all employees.

Importance:
This policy is critical for minimizing the risk of successful phishing attempts. Empowering employees to recognize and report suspicious activities enhances the overall security posture of Canadian Tire.

Activities:

- Conduct mandatory phishing awareness training for all employees bi-annually (Canada, 2022a).
- Implement an easy-to-use reporting mechanism for employees to report suspected phishing attempts.
- Regularly update training materials and awareness resources based on emerging phishing tactics.

Related Playbook:
The Phishing Incident Response Playbook will detail the reporting process, including how to document and escalate incidents effectively.

Consequences of Non-Compliance:

- **Individual:** Employees who fail to complete mandatory training or report incidents may face disciplinary actions, which could include formal warnings or termination.
- **Company:** Non-compliance can lead to increased vulnerability to phishing attacks, resulting in potential data breaches and financial losses.

13.3 User Management During Phishing Incidents

Purpose:
To outline procedures for managing users affected by phishing incidents to mitigate risks and protect sensitive information.

Importance:
Effective management of users and devices involved in phishing incidents is crucial for containing threats and preventing further compromises. This policy ensures prompt and coordinated actions are taken to protect organizational assets.

Activities:

- Immediately delete any emails identified as phishing attempts and restrict access to suspicious links (Kaspersky, 2016).
- Isolate affected users and devices from the network to prevent the spread of malware or data breaches (National Security Agency, 2023).
- Alert affected users about the incident and provide guidance on next steps.

Related Playbook:
The Phishing Incident Response Playbook will provide specific instructions for isolating users, communicating with affected parties, and restoring access after resolution.

Consequences of Non-Compliance:

- **Individual:** Failure to follow incident management protocols may result in disciplinary measures, including reassignment or termination.
- **Company:** Delayed action could lead to extensive data breaches, financial loss, and damage to customer trust.

14. References

1. Canada Centre for Cyber Security. (2022a, August 10). Don't take the bait: Recognize and avoid phishing attacks - ITSAP.00.101. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/dont-take-bait-recognize-and-avoid-phishing-attacks
2. Canada Centre for Cyber Security. (2022b, September 28). What to do if you are a victim of a phishing scam - Get Cyber Safe. Get Cyber Safe. https://www.getcybersafe.gc.ca/en/resources/what-do-if-you-are-victim-phishing-scam
3. Cloudflare. (n.d.). What is DNS filtering? | Secure DNS servers. https://www.cloudflare.com/learning/access-management/what-is-dns-filtering/
4. Federal Trade Commission. (2021, July 16). Phishing scams. https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams
5. Federal Trade Commission. (2024, October 11). How to recognize and avoid phishing scams. Consumer Advice. https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
6. Government of Canada. (2021, December 8). Develop an incident response plan: Fillable template and example. https://ised-isde.canada.ca/site/cybersecure-canada/en/certification-tools/develop-incident-response-plan-fillable-template-and-example
7. Kaspersky. (2016, March 8). Phishing scams & attacks - How to protect yourself. https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips
8. Kaspersky. (2022, May 17). What to do after a phishing attack. https://www.kaspersky.com/resource-center/threats/handling-phishing-attacks
9. Mimecast. (n.d.). How to stop phishing emails | Prevent phishing attacks. https://www.mimecast.com/content/how-to-stop-and-prevent-phishing-emails/
10. MITRE ATT&CK®. (n.d.). Retrieved October 27, 2024, from https://attack.mitre.org/
11. National Institute of Standards and Technology. (2024, March 14). Phishing. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing
12. National Institute of Standards and Technology. (n.d.). NIST Risk Management Framework | *CSRC*. https://csrc.nist.gov/projects/risk-management
13. National Security Agency. (2023, October 18). How to protect against evolving phishing attacks. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3560788/how-to-protect-against-evolving-phishing-attacks/