Policies for Phishing Playbook

By: Danielle Daza

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The following document are recommended policies relevant to the phishing playbook also proposed in a separate document. The following policies are the four most important policies to authorize first as they cover the base requirements needed in being able to follow the playbook as well as the addressing the base legal consequences in the event of a successful phishing attack. The policies are as follows: phishing incident response policy (for allowing the use of the playbook), email security and filtering policy (for the use of necessary software and applied configurations for proper phishing prevention), phishing awareness training policy (to mandate and solidify the training requirements and expected outcomes), and data breach notification policy (for formalizing internal and external notifications with appropriate criteria and considerations). Within each policy heading, there will be the purpose, scope, responsible groups and/or individuals, procedures, compliance, and frequency of revisions all thoroughly defined for clear comprehension. For each policy, however, some distinct headings will be included for each policy which depends on the nature of the policy itself. The policies are for the viewing of all employees as it falls under Traffic Light Protocol (TLP): Green meaning that it is useful for the everyone within the company and does not contain any substantially sensitive information.

PHISHING INCIDENT RESPONSE POLICY

PURPOSE

The purpose of this policy is to define the process for identifying, responding to, and recovering from phishing attacks that affect the organization. This policy aims to minimize the impact of phishing incidents and protect the confidentiality, integrity, and availability of the organization's data and systems.

SCOPE

The policy applies to all employees, contractors, and third-party vendors who have access to the organization's networks and systems. It covers all types of phishing attacks including email-based phishing, spear-phishing, and social engineering attempts via other communication channels.

DEFINITIONS

Phishing: A type of cyberattack where attackers impersonate legitimate entities to steal sensitive information, such as login credentials, financial information, or personal data.

Spear-phishing: A targeted phishing attack that is personalized and often directed at a specific individual or organization.

Whaling: A type of spear-phishing that targets high-level executives with the goal of stealing financial data or sensitive organizational information.

RESPONSIBILITIES

Incident Response Team (IRT):

- The Incident Response Team (IRT) is responsible for managing and coordinating the response to phishing incidents.
- Key members include: IT Security Team, Security Operations Center (SOC), Legal, Communications, and HR.

IT Security Team:

- Detect and block phishing emails using security tools and filters
- Investigate potential phishing incidents and escalate as necessary
- Implement technical controls to mitigate further risks

Employees:

- Employees must report any suspected phishing emails or incidents to the IT Security Team immediately.
- Employees must complete annual phishing awareness training and participate in simulated phishing exercises.

PROCEDURES AND GUIDELINES

Incident Response Process:

1. **Prepare:**
    - Formal phishing awareness training will be conducted company-wide and reviewed for revision at least once a year.
    - Appropriate security measures and controls to protect the systems from phishing are in place and updated appropriately.
2. **Detection:**
    - Employees report suspicious emails through the organization's designated reporting channels (e.g., email, helpdesk).

- The IT Security Team uses phishing detection tools to scan and identify phishing attempts.

3. **Incident Analysis:**
   - The incident is assessed to determine its severity (low, medium, high) based on factors like the number of affected users, the type of information targeted, and the likelihood of a breach.
   - A decision is made whether the phishing attack is an isolated incident or part of a larger campaign.
4. **Containment:**
   - If an attack is confirmed, IT Security and Incident Response Team will immediately block access to any affected systems or accounts.
   - Employees who clicked on links or provided sensitive information will be contacted for further investigation.
5. **Eradication:**
   - The source of the phishing attack is identified (e.g., malicious emails, compromised accounts).
   - Any malicious files, links, or compromised credentials are removed or reset.
6. **Recovery:**
   - Affected systems and accounts are restored to a secure state.
   - Monitoring continues to ensure the attack has been fully eradicated and no further damage occurs.
7. **Post-Incident Review:**
   - A post-incident analysis is conducted to assess the effectiveness of the response, identify lessons learned, and make improvements where needed.

- The results of the analysis are shared with relevant stakeholders, and corrective actions are taken as necessary.

COMPLIANCE AND CONSEQUENCES

The organization will comply with relevant legal and regulatory requirements related to phishing and data breaches. If a data breach occurs as a results of phishing, notification to affected individuals and regulatory bodies will occur within the specific timeframes.

REVIEW AND REVISION

The policy will be reviewed annually or after each significant phishing incident to ensure its effectiveness and relevance. Necessary updates will be made with all employees being informed of changes as they occur.

EMAIL SECURITY AND FILTERING POLICY

PURPOSE

The purpose of this policy is to ensure all incoming, outgoing, and internal email communications are secured and monitored to prevent phishing attacks, malware infections, and unauthorized access to the organization's systems and sensitive data.

SCOPE

The policy applies to all employees, contractors, and third-party vendors who use Canadian Tire's email system. It covers all email communications (i.e. external and internal sources, email archiving, data retention)

RESPONSIBILITIES

IT Security Team:

- Responsible for configuring, maintaining, and monitoring email security tools and filters.
- Conducting regular audits to ensure compliance with email security protocols.

Incident Response Team:

- Responding to identified threats (e.g., flagged phishing emails) and managing incident response.
- Verifying the email security and filtering procedures and guidelines are effective and kept up-to-date.

Employees:

- Responsible for adhering to the organization's email usage guidelines, such as not opening suspicious attachments or clicking on links in unsolicited emails.
- Reporting any suspicious or potential phishing emails to the IT Security Team.

EMAIL SECURITY STANDARDS AND TECHNOLOGIES

Email Filtering Software:

- The organization will use anti-phishing and anti-malware email filtering software to scan all incoming and outgoing messages for malicious attachments, links, and other suspicious content.
- Spam filters will be used to block unsolicited or suspicious messages before they reach the inbox.

Sender Authentication (What is Email Authentification?, 2022):

- SPF (Sender Policy Framework): Used to authenticate that emails are sent from authorized mail servers.
- DKIM (DomainKeys Identified Mail): Ensures that emails are not tampered with during transit.
- DMARC (Domain-based Message Authentication, Reporting & Conformance): Helps prevent email spoofing and provides instructions for how email should be handled if SPF or DKIM checks fail.

Attachment Scanning:

- All email attachments will be scanned for malware or suspicious content before being allowed into the organization's network.
- Emails with potentially dangerous attachments (e.g., executables, macros) will be blocked or flagged for review.

URL Filtering:

- All embedded URLs within emails will be scanned in real-time to ensure they are not linking to malicious or phishing websites.
- Malicious or blacklisted URLs will trigger a block, warning, or flag for investigation.

COMPLIANCE AND MONITORING

Ensure that the email security systems are continuously monitored and meet compliance requirements.

Monitoring:

- Continuous monitoring of email traffic for suspicious patterns and unauthorized access attempts.

- Regular update to email filtering systems based on emerging threats and trends.

Compliance:

- Ensure email security practices comply with industry standards.
- Maintain logs and records for auditing purposes.

REVIEW AND REVISION

The policy will be reviewed annually or as frequently as there are significant changes in technology, threats, or regulatory requirements.

PHISHING AWARENESS AND TRAINING POLICY

PURPOSE

The purpose of this policy is to educate employees with the knowledge and skills to recognize and respond to phishing attempts, ensuring that employees do not fall victim to phishing attacks that could compromise sensitive information, data integrity, and the organization's security posture.

SCOPE

The policy applies to all employees, contractors, and third-party vendors who use Canadian Tire's email system.

RESPONSIBILITIES

CISO:

- Support and enforce the phishing awareness training.
- Manage the allocation of resources for the phishing awareness training development,

Incident Response Team:

- Design and update training content with attest phishing threats and tactics taken into consideration.
- Develop and conduct phishing attack campaigns to assess employees' ability to recognize phishing attempts and modify the awareness training as necessary.

HR and Compliance Teams:

- Ensure compliance with training requirements and coordinate a training schedule to ensure that all employees.
- Maintain records of training completion to comply with regulatory and legal requirements.
- Evaluate training effectiveness and assist in tracking metrics related to completion rates and employee performance.

Managers:

- Ensuring that their teams complete the phishing awareness training and are aware of email security policies and procedures.
- Support remediation for employees that fail to recognize phishing attempts or consistently fail phishing simulations.

Employees:

- Complete the required training sessions and simulated phishing campaigns as required by the policy
- Report phishing incidents to the IT department or security team promptly.

- Apply knowledge gained from the training in daily email interactions to identify and avoid phishing attempts.

TRAINING REQUIREMENTS

Mandatory Training

- All employees will undergo phishing awareness training as part of their onboarding process and annually thereafter.

Simulated Phishing Campaigns

- Employees will be subject to periodic simulated phishing exercises to assess their ability to identify phishing emails. These exercises will be conducted quarterly.

Training Content

The training will cover:

- What phishing is and how it works.
- Identifying red flags in phishing emails (e.g., urgent requests, suspicious links, strange attachments).
- How to report suspected phishing emails
- What to do if a phishing email is interacted with (e.g., what actions to take if login credentials are compromised).

Metrics and Reporting

Effectiveness of the training will be measured by:

- The percentage of employees who correctly identify phishing attempts during simulated campaigns.

- The number of phishing incidents reported by employees.
- Feedback surveys from employees after training sessions to assess engagement and understanding.

COMPLIANCE AND CONSEQUENCES

Employees who fail to complete the required training or demonstrate poor identification skills in phishing simulations will be required to undergo additional training as needed.

REVIEW AND REVISION

The policy will be reviewed and updated annually or as frequently as needed to address the latest phishing techniques and evolving security risks.

DATA BREACH NOTIFICATION POLICY

PURPOSE

The purpose of this policy is to provide guidelines on how to notify internal and external stakeholders when a phishing attack results in a data breach. A data breach refers to the unauthorized access, disclosure, alteration, loss or destruction of sensitive or protected data.

SCOPE

The policy applies to all employees, contractors, third-party vendors, and any other stakeholders who have access to or handle sensitive data within the organization.

The scope of data covered by this policy includes any personal data or sensitive information subject to regulatory requirements, including but not limited to (Meeting Data Compliance with a Wave of New Privacy Regulation, 2019):

- Personally identifiable information (PII)
- Health information (under HIPAA)
- Financial data
- Payment card information (under PCI-DSS)
- Protected health information (PHI)
- Intellectual property and trade secrets

RESPONSIBILITIES

CISO:

- Oversee the organization's response to data breaches, ensuring the appropriate notifications are made both internally and externally in a timely manner.
- Approve and coordinate external communication (e.g. regulatory bodies, customers, partners)

Incident Response Team:

- Leads the overall response to the data breach, coordinating across all teams.
- Provide regular updates to senior management regarding the breach status.

IT Security Team:

- Identify, contain, and mitigate the breach, then assist in determining the cause and the extent of the data exposure.
- Provide information on the nature of the breach, including compromised and affected systems.

Legal and Compliance Teams

- Ensure the organization complies the applicable laws and regulations regarding data breach notification (e.g. GDPR, CCPA, HIPAA (Meeting Data Compliance with a Wave of New Privacy Regulation, 2019))
- Assist in drafting formal breach notification letters to affected individuals and regulatory bodies.

Public Relations/Communications Teams

- Manage external communications regarding the breach to protect the organization's reputation and maintain transparency
- Monitor public response and manage media inquiries

HR

- Notify internal stakeholders and coordinate with IT to determine if employee data is affected.
- Provide support to employees if sensitive data (e.g. payroll data) is affected

TRIGGERS

Internal:

- Any unauthorized individual gains access to sensitive data, whether through hacking, accidental exposure, or internal misconduct.
- Loss of sensitive data through theft, accidental deletion, or mishandling (e.g., lost devices containing personal data).
- Data is altered or corrupted in a way that is irreversible or unauthorized.
- Exposure of Sensitive Data: Any case where sensitive data (e.g., PII, financial data, health data) is exposed or disclosed to unauthorized parties.

External:

- Legal or regulatory requirements mandate notification (e.g., GDPR requires notification within 72 hours of detecting a breach if the breach risks the rights and freedoms of individuals (Meeting Data Compliance with a Wave of New Privacy Regulation, 2019)).
- If a third-party vendor or service provider suffers a breach and the organization's data is involved, this is a trigger for notification.
- If there is public exposure or the breach becomes publicly known (e.g., via media or external reports), notification must follow.

GENERAL TIMEFRAME FOR NOTIFICATIONS

Internal Notification:

- Notify Incident Response Team (IRT) and relevant stakeholders immediately.
- Senior management should be informed within 24 hours.

External Notification:

- Regulatory bodies (if applicable): Notify within 72 hours of breach detection (GDPR, etc.).
- Affected individuals: Notify within 72 hours.
- Public announcement (if needed): Notify within 48-72 hours if required.

NOTIFICATION PROCEDURES

Internal Notification

- Timeframe: The IT/Security team must notify the Incident Response Team (IRT) immediately after identifying the breach. The IRT will then notify the Data Protection Officer (DPO) and senior management within 24 hours.

- Content: The notification should include
    - Type of data compromised.
    - Estimated number of individuals affected.
    - Systems or departments impacted.
    - Steps taken to contain the breach.

External Notification

- Timeframe:
    - Regulatory Authorities: If required by law (e.g., GDPR, CCPA), the notification should be made within 72 hours of identifying the breach.
    - Affected Individuals: Notification must be sent to affected individuals without undue delay, generally within 7-30 days from the detection of the breach, depending on the severity and impact of the breach.
    - Public Communication: If necessary (depending on the scale of the breach), a press release or public statement should be made within 48-72 hours to maintain transparency.
- Content:
    - Regulatory Authorities: A formal breach report should be submitted to relevant regulators, including the nature of the breach, what data was compromised, and any corrective actions taken.
    - Affected Individuals:
        - A clear explanation of the breach, including the type of data exposed.
        - The potential consequences of the breach (e.g., identity theft, financial fraud).
        - Steps individuals can take to protect themselves (e.g., credit monitoring, password changes).

- A contact point for further inquiries or support (e.g., a hotline or email).
- If applicable, offer remediation (e.g., free credit monitoring services for affected individuals).

Press/Public Notification

- Clear, concise summary of the breach that includes information on the organization response and any steps individuals can take to mitigate risks.

COMPLIANCE AND MONITORING

Ensure that the email security systems are continuously monitored and meet compliance requirements.

Monitoring:

- Continuous monitoring of email traffic for suspicious patterns and unauthorized access attempts.
- Regular update to email filtering systems based on emerging threats and trends.

Compliance:

- Ensure email security practices comply with industry standards.
- Maintain logs and records for auditing purposes.

REVIEW AND REVISION

The policy will be reviewed annually and updated as necessary to ensure compliance with legal and regulatory requirements.

REFERENCES

Anderson, G. (2024, January 18). *The Role of Network Administrators in Ensuring Data Security*. Retrieved from MoldStud: https://moldstud.com/articles/p-the-role-of-network-administrators-in-ensuring-data-security

Meeting Data Compliance with a Wave of New Privacy Regulation. (2019, September 17). Retrieved from NetApp: https://bluexp.netapp.com/blog/data-compliance-regulations-hipaa-gdpr-and-pci-dss

Policy Statement Examples. (2024). Retrieved from Wayne State University: https://policies.wayne.edu/policy-statement-examples

Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook. (2012, January 31). Retrieved from NIST: https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter3.html

What is Email Authentification? (2022). Retrieved from Validity: https://www.validity.com/email-authentication/