DATARISK
CANADA

Cybersecurity Awareness Checklist

Use this checklist to create a cybersecurity and privacy awareness & training program to fit your organization and ensure workplace vigilance and accountability, in compliance with NIST CSF, ISO 27001:2022 & applicable data protection laws.

1. Anti-Phishing Training.

- ☐ Initial Training: Provide comprehensive training to all employees on how to identify and avoid phishing attacks, including real-life examples and interactive simulations.
- ☐ Regular Updates: Conduct periodic refresher courses to keep employees updated on the latest phishing tactics and trends.
- ☐ Simulated Phishing Tests: Regularly test employees with simulated phishing emails to assess their awareness and improve their ability to recognize phishing attempts.

2.Annual Cybersecurity Training.

❑ Comprehensive Curriculum: Develop an annual training program that covers all aspects of cybersecurity, including password management, secure browsing, and data protection.

❑ Mandatory Participation: Ensure that all employees, contractors, and third-party partners complete the annual training.

❑ Certification and Assessment: Provide certification upon successful completion of the training and conduct assessments to gauge understanding and retention.

3. Monthly Awareness Updates.

❑ Cybersecurity Newsletters: Distribute monthly newsletters that highlight recent cyber threats, security tips, and best practices.

❑ Awareness Campaigns: Launch monthly campaigns focusing on different aspects of cybersecurity, such as mobile device security, secure file sharing, and recognizing social engineering.

❑ Interactive Workshops: Organize workshops and webinars to engage employees in discussions about current cybersecurity challenges and solutions.

Other Recommendations for Cybersecurity Awareness

- Policy Enforcement: Ensure that cybersecurity policies are clearly communicated and strictly enforced across the organization.
- Incident Reporting: Establish a straightforward process for employees to report suspicious activities or potential security incidents.
- Access Control: Regularly review and update access controls to ensure that employees have the appropriate level of access based on their roles.
- Security Champions: Appoint security champions within departments to promote cybersecurity awareness and serve as a point of contact for security-related questions.
- Continuous Improvement: Regularly review and update the cybersecurity awareness program to address emerging threats and incorporate feedback from employees.

Let's create a cybersecurity awareness program:
https://www.securityeducation.ca