Cyber Security Awareness

Created by

**UPTOWN IT**

by

**James Eastman**

**PROJECT REFERENCE: BSBXCS402\_UptownIT Cyber Security Solution**

**DATE: 17 August 2024**

Contents

[PART 1 Establish the current level of cyber security awareness and required awareness program 4](#_Toc108773108)

[Review of Cyber Security Audit Report 4](#_Toc108773109)

[Communication and Feedback – Audit Review and Assessment 5](#_Toc108773110)

[Cyber Security Program Proposal 5](#_Toc108773111)

[Cyber Security Procedure 6](#_Toc108773112)

[Conversation with relevant stakeholder 7](#_Toc108773113)

[PART 2 Support cyber security awareness and organise and review training 8](#_Toc108773114)

[Training Program One (Replace with real name) 8](#_Toc108773115)

[Training Program Two (Replace with real name) 9](#_Toc108773116)

[PART 3 Review cyber security awareness in the workplace 10](#_Toc108773117)

[Review and communicate the latest cyber security threats and trends 10](#_Toc108773118)

[Communication and Feedback – Latest Cyber Security Threats and Trends 10](#_Toc108773119)

[PART 4 Contingency task and cyber security knowledge 11](#_Toc108773120)

[Contingency Task 11](#_Toc108773121)

[Cyber Security Knowledge 11](#_Toc108773122)

[REFERENCES 12](#_Toc108773123)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document Name | Version | Date Completed | Completed by | Approved by | Date Approved |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# PART 1 Establish the current level of cyber security awareness and required awareness program

**Introduction** A recent cybersecurity audit at Uptown IT has revealed several significant gaps in our current practices. These findings underscore the urgent need to enhance our staff’s cybersecurity awareness to protect sensitive company data and ensure the integrity of our IT infrastructure. This report analyses the identified cybersecurity issues, their impact on the workplace, and their associated risk levels. Based on this analysis, we will prioritize areas for cybersecurity awareness training to address these issues effectively.

## Review of Cyber Security Audit Report

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Cyber Security Problem | Cyber Security Area | Workplace Impact | Risk Level  (High, Moderate, Low) | Awareness Training Priority  (1 Highest – 10 Lowest) |
| Staff members opening all emails, including suspicious ones | Email Security | Increased risk of phishing attacks and malware infections | High | 1 |
| Use of personal pen drives and external hard drives | Data Security | Potential for data leaks and introduction of malware | High | 4 |
| Use of personal devices on home networks for work | Network Security | Compromised data security and potential network vulnerabilities | High | 3 |
| Unlocked workstations during lunch breaks | Physical Security | Unauthorized access to sensitive information | Moderate | 6 |
| Use of mobile phone data for work-related tasks | Network Security | Potential data interception and increased security vulnerabilities | Moderate | 5 |
| Display of passwords on sticky notes near workstations | Password Security | Easy access to passwords by unauthorized individuals | High | 2 |
| Increased calls for forgotten passwords due to stricter policy | Password Management | Reduced productivity and increased support workload | Low | 7 |

## 

## Communication and Feedback – Audit Review and Assessment

Great summary James.  I like the priority you placed on passwords on sticky notes.  This is a bad habit to fall into and promotes a careless attitude towards cyber security within the company.

## Cyber Security Program Proposal

**Introduction** In light of the recent cybersecurity audit findings, Uptown IT is committed to enhancing its cybersecurity practices through a comprehensive Cyber Security Awareness Policy. This policy outlines specific procedures to mitigate identified risks and foster a secure working environment. The proposed procedures will address all seven issues highlighted in the audit report, ensuring that all employees understand their roles and responsibilities in maintaining cybersecurity. Below is a detailed proposal of the procedures to be included in the Cyber Security Awareness Policy.

|  |  |  |
| --- | --- | --- |
| Proposed Procedure | Purpose | Content Description |
| Email Security Procedure | To prevent phishing attacks and malware infections | Identify and report suspicious emails, avoid opening unknown attachments or links, use email filtering and anti-phishing tools, regularly update email security software |
| Data Transfer and Storage Policy | To secure data transfer between work and home | Prohibit use of personal pen drives and external hard drives, use company-approved encrypted storage devices, implement secure file transfer methods (e.g., VPN, encrypted email), conduct regular audits of data transfer practices |
| Remote Work Security Guidelines | To ensure secure remote working practices | Mandate use of company-issued devices, require use of VPN for remote access, enforce secure home network practices (e.g., strong passwords, firewall), conduct remote work security training sessions |
| Workstation Security Procedure | To prevent unauthorized access to workstations | Implement automatic screen lock after inactivity, educate staff on manually locking screens when leaving desks, use secure workstation setup guidelines, monitor and enforce compliance regularly |
| Mobile Device Security Protocol | To secure use of mobile devices for work purposes | Restrict use of personal mobile data for work-related tasks, require mobile device management (MDM) software, implement secure mobile access policies, educate employees on risks and best practices |
| Password Management Policy | To enhance password security and reduce risk of breaches | Prohibit displaying passwords in unsecured locations, implement strong password creation guidelines, enforce regular password changes, use password managers for secure storage |
| Password Support Procedure | To streamline password management and support | Provide training on creating and remembering strong passwords, offer self-service password reset options, implement multi-factor authentication (MFA), reduce support workload through user education |

## Cyber Security Procedure

**Introduction** The implementation of comprehensive cybersecurity procedures is essential for Uptown IT to mitigate identified risks and strengthen our cybersecurity posture. These procedures ensure that all employees adhere to best practices for securing sensitive data and maintaining the integrity of our IT infrastructure. The following document outlines the detailed procedure for "Email Security Protocol" to address the issues highlighted in the recent cybersecurity audit.

|  |  |
| --- | --- |
| **UPTOWN IT**  **Cyber Security Awareness Procedure**  **Email Security Procedure** | |
| Purpose | To safeguard Uptown IT's email communication channels from phishing attacks, malware infections, and other email-based threats. This procedure ensures employees can identify and handle suspicious emails appropriately, reducing the risk of cybersecurity incidents. |
| Scope | This procedure applies to all employees, contractors, and third-party partners who use Uptown IT's email systems for any form of communication. |
| Responsibilities | * **All Employees:** Adhere to the guidelines outlined in this procedure and participate in required training sessions. * **IT Support Group:** Implement email security tools, monitor email traffic, and provide support for email-related security issues. * **Management Group:** Ensure compliance with the procedure and address any violations promptly. * **Cybersecurity Team:** Regularly update the procedure and provide ongoing training and awareness programs. |
| Version Control | * **Version:** 1.0 * **Date:** 17 July, 2024 |
| Rules/Guidelines | 1. **Identifying Suspicious Emails:**    * Check the sender's email address for authenticity.    * Look for unusual or unexpected email content.    * Be wary of emails requesting sensitive information or urgent actions. 2. **Handling Suspicious Emails:**    * Do not open attachments or click on links in suspicious emails.    * Report suspicious emails to the IT Support Group immediately.    * Move suspicious emails to the junk/spam folder. 3. **Using Email Security Tools:**    * Enable and regularly update email filtering and anti-phishing tools.    * Ensure antivirus software is active and updated.    * Use encryption for sensitive email communications. 4. **Regular Training and Updates:**    * Participate in mandatory email security training sessions.    * Stay informed about the latest email-based threats and best practices.    * Review and adhere to updates in the email security protocol. 5. **Monitoring and Compliance:**    * The IT Support Group will monitor email traffic for suspicious activity.    * Non-compliance with the procedure will result in disciplinary actions as per company policy.    * Regular audits will be conducted to ensure adherence to the protocol. |
| Referenced Documents | * Uptown IT Infrastructure Diagram * Cybersecurity Awareness Training Materials * IT Support Group's Monitoring and Reporting Procedures |
| Approval | DRAFT |
| Review Date | 17 July 2025 |

## Cyber security maintenance procedure schedule

**Introduction** To ensure Uptown IT's cybersecurity procedures remain effective and up-to-date, a regular maintenance schedule must be established. This schedule outlines the periodic review and update of our cybersecurity protocols, ensuring they adapt to emerging threats and evolving business needs. Below is the proposed schedule for maintaining the "Email Security Protocol" and "Password Support Procedure" documents.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Procedure Name** | **Weekly** | **Monthly** | **6 Monthly** | **Yearly** |
| Email Security Procedure |  |  | **✔** |  |
| Data Transfer and Storage Policy |  |  | **✔** |  |
| Remote Work Security Guidelines |  |  |  | **✔** |
| Workstation Security Procedure |  |  | **✔** |  |
| Mobile Device Security Protocol |  |  |  | **✔** |
| Password Management Policy |  |  | **✔** |  |
| Password Support Procedure |  |  | **✔** |  |
| Internet and Social Media Procedure |  |  | **✔** |  |

Possible Exceptional Circumstances

* Major Security Incident: Significant security breach revealing vulnerabilities.
* Regulatory Changes: Updates in regulations requiring policy review.
* Technological Advancements: New technologies impacting security.
* Internal Audit Findings: Weaknesses or gaps uncovered in audits.
* Emerging Threats: New threats posing risks.
* User Feedback: Feedback indicating potential issues.

## Strategies for promoting cyber security awareness

**Introduction:** Promoting cybersecurity awareness is crucial for protecting sensitive information and ensuring adherence to best practices.

**Strategies:**

1. **Regular Training and Workshops:**
   * Conduct quarterly sessions on various cybersecurity topics.
   * Mandatory for all employees.
   * Use quizzes, simulations, hands-on activities.
   * Update content regularly.
   * Align with Uptown IT's policies.
2. **Cybersecurity Awareness Campaigns:**
   * Ongoing campaigns via emails, posters, intranet articles.
   * Informational emails, posters, Cybersecurity Awareness Month events.
   * Create intranet cybersecurity section.
   * Use real-life examples.
   * Support existing policies.
3. **Phishing Simulations and Drills:**
   * Monthly simulations to improve email security habits.
   * Analyze results for improvement.
   * Provide feedback and follow-up training.
   * Refine awareness program.
   * Follow email security protocol.

## Conversation with relevant stakeholder

Introduction.

Arrange a conversation with your manager and seek feedback regarding the following points:

* 1. The suitability of the procedure that you have written. Modify procedure if required. Document the conversation in the Conversation Log.
  2. The proposed maintenance schedule to review cyber security awareness procedures.
  3. Discuss and confirm proposed strategies to promote cyber security awareness amongst employees.

Document discussion and confirmed strategies in the Conversation Log.

Please email me your documents so I can review (or upload to draft assessments in Connect). Then, I can talk through my feedback with you during class. Make notes of my feedback and add to table below

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Conversation Log | | | | |
| Date | Topic | Discussion | Stakeholder | Medium  Any oral form of communication, e.g., F2F, Zoom and phone call. |
| 21/8/24 | Procedure | Rename "Email security protocol" to "email security procedure" | Company Employees | Zoom |
| 21/8/24 | Procedure | Only 1 procedure is necessary | Company Employees | Zoom |

# PART 2 Support cyber security awareness and organise and review training

**Introduction** After reviewing the Cyber Security Audit Report, it is clear that there are significant gaps in staff awareness regarding cybersecurity at Uptown IT. To address these gaps, it is essential to organize targeted training programs. Based on the highest priority areas identified in Part 1, two training programs have been developed to enhance cybersecurity awareness and practices among employees. These programs will focus on Email Security Protocol and Password Support Procedure.

This is a Training Program. Imagine that you are conducting the training.

## Training Program One *Email Security Procedure*

|  |  |
| --- | --- |
| **UPTOWN IT**  **Cyber Security Awareness Training program**  **Email Security Procedure** | |
| Referenced Procedure | Email Security Procedure |
| Learning Objectives | • Understand the importance of email security.  • Recognize common types of email threats, such as phishing.  • Learn how to handle suspicious emails.  • Implement best practices for email security. |
| Recommended Frequency of Training | 12 months. |
| Responsibilities | • All Employees: Participate in training and apply the learned practices.  • IT Support Group: Facilitate training sessions and provide ongoing support.  • Management Group: Ensure compliance with the training program. |
| Topic Overview | This training program covers essential aspects of email security, focusing on identifying and handling phishing attempts, secure email practices, and using email security tools effectively. |
| Training Materials | **Module 1: Introduction to Email Security**   * Overview of email threats * Importance of email security * Video: " [What is phishing? Learn how this attack works - YouTube](https://www.youtube.com/watch?v=Y7zNlEMDmI4)"   **Module 2: Recognizing Suspicious Emails**   * Common characteristics of phishing emails * Case studies of email breaches * Activity: Identifying phishing attempts in sample emails   **Module 3: Handling Suspicious Emails**   * Steps to take when receiving a suspicious email * Reporting procedures * Interactive quiz: What to do with suspicious emails   **Module 4: Best Practices for Email Security**   * Using email filtering and anti-phishing tools * Secure email communication practices * PowerPoint presentation: "Top 10 Email Security Tips" |
| Activities | • Pre-evaluation quiz on current email security knowledge.  • Scenario-based exercises for identifying and handling suspicious emails |
| Evaluation | • Post-training quiz to assess understanding of email security concepts.  • Practical test involving the identification of phishing emails.  • Feedback survey on training effectiveness. |

## Training Program Two *Password Support Procedure*

**Introduction** Effective password management is a cornerstone of cybersecurity and ensuring that employees understand and adhere to best practices is crucial for protecting Uptown IT's sensitive information. This training program focuses on the Password Support Procedure, aiming to educate employees on creating strong passwords, using multi-factor authentication (MFA), and managing password resets. The program is designed to reinforce secure password practices and reduce the number of password-related support requests, aligning with Uptown IT's cybersecurity policies.

|  |  |
| --- | --- |
| **UPTOWN IT**  **Cyber Security Awareness Training program**  **Password Support Procedure** | |
| Referenced Procedure | Password Support Procedure |
| Learning Objectives | • Understand the importance of strong password practices.  • Learn how to create and manage secure passwords.  • Utilize multi-factor authentication (MFA) effectively.  • Know the process for password resets and support. |
| Recommended Frequency of Training | 12 months. |
| Responsibilities | • All Employees: Participate in training and apply the learned practices.  • IT Support Group: Facilitate training sessions and provide ongoing support.  • Management Group: Ensure compliance with the training program. |
| Topic Overview | This training program covers essential aspects of password security, focusing on creating strong passwords, using MFA, and handling password resets securely. |
| Training Materials | Module 1: Introduction to Password Security  • Importance of strong passwords  • Risks of weak passwords  • Video: [Why Strong Passwords Really Do Matter (youtube.com)](https://www.youtube.com/watch?v=T4DxErjgWpE)  Module 2: Creating and Managing Strong Passwords  • Guidelines for creating strong passwords  • Using password managers  • Activity: Creating strong passwords using guidelines  Module 3: Multi-Factor Authentication (MFA)  • Benefits of MFA  • Setting up and using MFA  • Interactive demo: Setting up MFA on a company account  Module 4: Password Resets and Support  • Self-service password reset process  • IT support for password issues  • PowerPoint presentation: "Steps for Secure Password Resets" |
| Activities | • Pre-evaluation quiz on current password security knowledge.  • Hands-on exercises for creating strong passwords and setting up MFA. |
| Evaluation | • Post-training quiz to assess understanding of password security concepts.  • Practical test involving creating strong passwords and setting up MFA.  • Feedback survey on training effectiveness. |

# PART 3 Review cyber security awareness in the workplace

## Review and communicate the latest cyber security threats and trends

|  |  |  |  |
| --- | --- | --- | --- |
| Cyber Security Threat | Trend | Source(S) | Proposed Improvement & Procedure to Update |
| Cyber Activity Impacting Cisco ASA VPNs | Exploitation of vulnerabilities in Cisco ASA VPNs | Australian Signals Directorate's Australian Cyber Security Centre  https://www.cyber.gov.au/acsc/view-all-content/advisories/exploitation-vulnerabilities-affecting-cisco-firewall-platforms | 1. Steps: Update Cisco ASA devices to the latest firmware. Monitor for signs of compromise, such as unusual network activity or specific IP addresses. 2. Procedures to Update:  * Remote Work Security Guidelines: Include the latest security measures for Cisco ASA devices. * Incident Response Plan: Add specific actions for handling VPN-related threats. |
| Microsoft Outlook Remote Code Execution Vulnerability (CVE-2024-21413) | Critical vulnerability allowing remote code execution through improper input validation | Australian Signals Directorate's Australian Cyber Security Centre  https://www.cyber.gov.au/acsc/view-all-content/advisories/microsoft-office-outlook-remote-code-execution-vulnerability-cve-2024-21413  Microsoft  <https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2024-21413> | 1. Steps: Apply the security updates provided by Microsoft to address the vulnerability. Ensure all systems using Microsoft Office are patched to the latest versions. Educate users about the risks of opening files in Protected View and enforce stricter email security policies. 2. Procedures to Update: Workstation Security Procedure, Email Security Policy |
| Advanced Persistent Threats 40 | Persistent, state-sponsored cyber operations targeting critical infrastructure and private sector networks | Australian Signals Directorate's Australian Cyber Security Centre  https://www.cyber.gov.au/acsc/view-all-content/advisories/apt40-advisory | 1. Steps: Conduct continuous monitoring for indicators of compromise associated with APT40. Implement multi-layered security controls. Regularly update and patch vulnerable systems and devices. Educate employees on identifying suspicious activity and responding to potential intrusions. 2. Procedures to Update: Incident Response Plan, Network Security Protocols, Employee Training Programs |

## Communication and Feedback – Latest Cyber Security Threats and Trends

Please include relevant website links in Source column of the table.  I can see the link in the references, but I think it is worthwhile to include the link in the table as well. Otherwise, great job!

# PART 4 Contingency task and cyber security knowledge

## Contingency Task

**Immediate Response and Incident Assessment**

* Assemble an incident response team with key personnel from IT, management, and other relevant departments.
* Gather all available information about the incident, including the type of attack, affected systems, and potential impact.
* Isolate affected systems from the network to prevent further spread.
* Inform stakeholders about the incident and the steps being taken.

**Incident Investigation and Mitigation**

* Conduct a thorough investigation to understand the root cause and extent of the breach.
* Work with cybersecurity experts to identify vulnerabilities and develop a mitigation plan.
* Communicate with external parties, such as law enforcement and cybersecurity agencies, if the incident involves significant data breaches or potential legal implications.

**Policy Review and Update**

* Document the incident in detail, including steps taken during the response and lessons learned.
* Update cybersecurity policies to prevent future occurrences.
* Provide additional training to employees to raise awareness and preparedness.
* Conduct regular reviews and updates of cybersecurity policies.

## Cyber Security Knowledge

For each item below, identify what would be the cyber security **legislative requirements** and **implications.** Provide examples to illustrate your answers

#### **a) Data Protection in Australia**

**Summary of Legislative Requirements:** The Privacy Act 1988 (Cth) regulates the handling of personal information by Australian government agencies and private sector organizations. It outlines 13 Australian Privacy Principles (APPs) that cover the collection, use, storage, and disclosure of personal information. Organizations must take reasonable steps to protect personal data from misuse, interference, loss, unauthorized access, modification, or disclosure.

**Implications if Laws are Broken:** If an organization breaches the Privacy Act, it can face significant penalties, including fines of up to $2.1 million per violation for serious or repeated breaches. Additionally, reputational damage and loss of customer trust can have long-term negative impacts on the business.

**Example:** In 2019, the Australian Information Commissioner fined HealthEngine $2.9 million for privacy breaches, including sharing patient information without consent and misleading reviews.

#### **b) Notifiable Data Breach in Australia**

**Summary of Legislative Requirements:** Under the Notifiable Data Breaches (NDB) scheme, part of the Privacy Act 1988, organizations must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm. Notifications must include the nature of the breach, the types of information involved, and recommendations for affected individuals.

**Implications if Laws are Broken:** Failing to comply with the NDB scheme can result in regulatory action by the OAIC, including fines and enforceable undertakings. Organizations may also suffer reputational damage and loss of consumer confidence.

**Example:** In 2018, PageUp, a recruitment software company, experienced a data breach affecting its clients' personal information. They notified affected individuals and the OAIC promptly, avoiding fines but highlighting the importance of compliance.

#### **c) Cyber Security in International Legislation Affecting Australia**

**Summary of Legislative Requirements:** International legislation such as the General Data Protection Regulation (GDPR) affects Australian organizations that handle the personal data of EU citizens. The GDPR mandates stringent data protection measures, including obtaining explicit consent, providing data access and deletion rights, and reporting breaches within 72 hours.

**Implications if Laws are Broken:** Non-compliance with the GDPR can result in fines of up to €20 million or 4% of the company's global annual turnover, whichever is higher. This poses significant financial and operational risks for Australian organizations dealing with EU data subjects.

**Example:** Australian businesses with EU customers, like online retailers, must comply with GDPR. Failure to protect EU citizens' data can lead to heavy fines and loss of access to the European market.

For each listed policy/procedure, provide the scope of the procedure and three (3) rules or guidelines that should be included to protect the company against cyber security threats.

Provide the answers within the context of the company provided in the scenario.

|  |  |  |
| --- | --- | --- |
| Policy/Procedure For | Scope | Rules/Guidelines  Three (3) for each |
| 1. Securely storing, sharing and managing information | Applies to all employees, contractors, and third-party service providers handling company information. | 1. **Access Control:** Limit access to sensitive information to authorized personnel only. 2. **Data Encryption:** Encrypt sensitive information both in transit and at rest. 3. **Regular Audits:** Conduct regular audits to ensure compliance with data security policies. |
| 1. Encryption, and protocols for its uses | Applies to all digital data handled by the company, including emails, documents, and databases. | 1. **Encryption Standards:** Use industry-standard encryption protocols (e.g., AES-256) for all sensitive data. 2. **Key Management:** Implement robust key management practices, including regular key rotation and secure storage. 3. **Encryption Policies:** Ensure all data transmissions are encrypted using SSL/TLS. |
| 1. Data classification and management | Applies to all data created, received, maintained, or transmitted by the company. | 1. **Classification Levels:** Define data classification levels (e.g., public, internal, confidential) and handle data accordingly. 2. **Handling Guidelines:** Establish handling guidelines for each classification level to prevent unauthorized access. 3. **Data Inventory:** Maintain an up-to-date inventory of all classified data. |
| 1. Media/document labelling | Applies to all physical and electronic media and documents used by the company. | 1. **Labeling Protocols:** Implement labeling protocols for documents and media based on their sensitivity. 2. **Access Restrictions:** Restrict access to labeled documents to authorized personnel only. 3. **Disposal Procedures:** Ensure secure disposal of labeled documents and media, including shredding or secure digital deletion. |
| 1. Data governance   Overall data management, includes:  Change processes  Data flows  Data quality and regulation  Data processes  Policy and procedures | Covers overall data management, including change processes, data flows, data quality, and regulatory compliance. | 1. **Change Management:** Implement a formal change management process for data-related changes. 2. **Data Quality:** Regularly validate and clean data to maintain accuracy and integrity. 3. **Regulatory Compliance:** Ensure compliance with relevant data protection regulations and standards. |
| 1. Acceptable use | Applies to all employees and contractors using company IT resources. | 1. **Usage Restrictions:** Define acceptable and unacceptable uses of company IT resources. 2. **Monitoring:** Implement monitoring to detect and prevent misuse of IT resources. 3. **Disciplinary Actions:** Outline disciplinary actions for policy violations. |
| 1. Bring your own device | Applies to all employees using personal devices for work purposes. | 1. **Security Requirements:** Require personal devices to meet company security standards, including antivirus software and encryption. 2. **Access Control:** Limit access to company data and systems from personal devices to necessary functions. 3. **Data Wipe:** Implement remote wipe capabilities for lost or stolen devices to protect company data. |

# REFERENCES

 **Exploitation of Vulnerabilities Affecting Cisco Firewall Platforms**

* Source: Cyber.gov.au
* URL: https://www.cyber.gov.au/acsc/view-all-content/advisories/exploitation-vulnerabilities-affecting-cisco-firewall-platforms
* Description: This advisory provides information on vulnerabilities in Cisco firewall platforms and recommended mitigation steps.

 **Microsoft Office Outlook Remote Code Execution Vulnerability (CVE-2024-21413)**

* Source: Cyber.gov.au
* URL: https://www.cyber.gov.au/acsc/view-all-content/advisories/microsoft-office-outlook-remote-code-execution-vulnerability-cve-2024-21413
* Description: Details the critical vulnerability in Microsoft Office Outlook that allows remote code execution.

 **CVE-2024-21413 - Security Update Guide**

* Source: Microsoft
* URL: <https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2024-21413>
* Description: Security update guide for Microsoft’s remote code execution vulnerability CVE-2024-21413.

 **APT40 Advisory**

* Source: Cyber.gov.au
* URL: https://www.cyber.gov.au/acsc/view-all-content/advisories/apt40-advisory
* Description: Advisory on Advanced Persistent Threat (APT) group APT40, including indicators of compromise and recommended defensive measures.