

**OzCazual**

**Staff Training**

rectangle

HOW TO IDENTIFY CYBERSECURITY THREATS IN YOUR ORGANISATION

**Prepared By :** *Mauricio G. Guerra* **Prepared on :** *July 2023*

**Table of Contents**

[Introduction 3](#_heading=h.1t3h5sf)

[Password Security 5](#_heading=h.44bxrr4l93ll)

[Phishing Awareness 6](#_heading=h.13bmd0s9qvlo)

[Social Engineering Awareness 7](#_heading=h.n7yrac894x47)

[Data Protection and Privacy 8](#_heading=h.k8vlnwm8niji)

[Safe Internet and Email Practices 9](#_heading=h.rigtmnft0ak5)

[Device Security 10](#_heading=h.4qq859hwd1ek)

[Physical Security 10](#_heading=h.4hmfiyt4c4wb)

[Reporting Security Incidents 11](#_heading=h.iln6vrn15o1j)

[Ongoing Training and Awareness 11](#_heading=h.9w5llf93uuaf)

| Introduction |
| --- |
| Welcome to the Cyber Security Training Program. This training is designed to raise awareness and promote best practices in cybersecurity to protect our organisation's assets. Understanding cybersecurity threats and their potential impact is crucial in maintaining a secure working environment.  **Purpose:** The purpose of this Cyber Security Training Document is to educate and empower general employees within our organisation with the knowledge and best practices necessary to contribute to a secure and resilient cyber environment. By providing comprehensive training, we aim to raise awareness about cyber threats, promote responsible behaviour, and mitigate the risks associated with cybersecurity incidents. This training will help employees understand their role in safeguarding organisational assets, protecting sensitive information, and minimising potential vulnerabilities.  **Scope:** This Cyber Security Training Document is designed for all general employees within our organisation, regardless of their technical background or job roles. It covers fundamental concepts and practical guidance related to various cybersecurity domains. The training will focus on the following key areas:   * **Password Security:**   + Educating employees on the significance of strong and unique passwords.   + Providing guidelines for creating and managing passwords securely.   + Highlighting the importance of two-factor authentication (2FA) as an additional layer of security. * **Phishing Awareness:**   + Developing employees' ability to identify and respond to phishing attacks.   + Providing practical examples and real-life scenarios to enhance awareness.   + Equipping employees with strategies to detect and report suspicious emails or messages. * **Social Engineering Awareness:**   + Raising awareness about social engineering techniques and their potential impact.   + Training employees to recognize and respond to manipulative tactics employed by threat actors.   + Encouraging employees to practise caution when sharing sensitive information or granting access to unauthorised individuals. * **Data Protection and Privacy:**   + Highlighting the importance of safeguarding sensitive data and maintaining privacy.   + Guiding employees on best practices for secure data handling, encryption, and secure file sharing.   + Ensuring compliance with data protection regulations and internal policies. * **Safe Internet and Email Practices:**   + Educating employees on safe internet browsing habits and responsible email practices.   + Providing guidance on identifying and avoiding malicious websites and suspicious email attachments.   + Promoting safe online behaviours to minimise the risk of malware infections and data breaches. * **Device Security:**   + Empowering employees to maintain the security of their devices.   + Providing recommendations for keeping software and antivirus programs up to date.   + Advising on secure Wi-Fi usage, especially when connecting to public networks. * **Physical Security:**   + Highlighting the importance of physical security measures in protecting organisational assets.   + Encouraging employees to practise secure physical access control and reporting any suspicious activities. * **Reporting Security Incidents:**   + Informing employees about the significance of reporting security incidents promptly.   + Providing clear channels and procedures for reporting incidents, potential breaches, or suspicious activities.   + Reinforcing the organisation's commitment to supporting and addressing cybersecurity concerns. * **Ongoing Training and Awareness:**   + Encouraging employees to stay updated on emerging threats, trends, and best practices.   + Promoting a culture of continuous learning and sharing cybersecurity knowledge within the organisation.   + Communicating the organisation's commitment to providing ongoing training and resources to support employees' cybersecurity awareness. |

| Password Security |
| --- |
| Protecting our accounts with strong passwords is vital. Ensure that your passwords are unique, complex, and not easily guessable. Use a mix of uppercase and lowercase letters, numbers, and special characters. Avoid using personal information or common words. Remember to update passwords regularly and never share them with others. Enable two-factor authentication (2FA) for an added layer of security.  **1. Educating employees on the significance of strong and unique passwords:** Passwords play a critical role in protecting our accounts and sensitive information. Employees must understand the importance of using strong and unique passwords for every account they have. Weak or easily guessable passwords can be easily compromised, leading to unauthorised access and potential data breaches. By using strong passwords, employees contribute to the overall security of the organisation's digital assets.  **2. Providing guidelines for creating and managing passwords securely:** To ensure password security, employees should follow these guidelines:  **a. Length and Complexity:** Encourage employees to create passwords with a minimum length of eight characters, including a mix of uppercase and lowercase letters, numbers, and special characters. The longer and more complex the password, the harder it is for attackers to crack.  **b. Avoiding Personal Information:** Advise employees to avoid using personal information like names, birthdays, or addresses in their passwords. Attackers can easily guess such information from public sources or social media profiles.  **c. Unique Passwords:** Stress the importance of using different passwords for each account. Reusing passwords across multiple accounts increases the risk of a single compromised password leading to multiple security breaches.  **d. Regular Updates:** Encourage employees to update their passwords periodically, ideally every three to six months. Regularly changing passwords reduces the likelihood of successful brute force or dictionary-based attacks.  **3. Highlighting the importance of two-factor authentication (2FA) as an additional layer of security:** Two-factor authentication (2FA) provides an additional layer of security beyond passwords. It requires users to provide a second form of verification, such as a unique code sent to their mobile device or a biometric scan, along with their password. Emphasise the importance of enabling 2FA whenever available, especially for critical accounts and systems. 2FA adds an extra barrier for attackers even if they manage to obtain or crack passwords. It significantly reduces the risk of unauthorised access and strengthens overall account security. |

| Phishing Awareness |
| --- |
| Phishing attacks attempt to trick you into revealing sensitive information or downloading malicious content. Be cautious of emails, attachments, or links from unknown sources. Look out for suspicious requests for personal or financial information. Avoid clicking on links in suspicious emails, and verify the legitimacy of websites before entering login credentials. When in doubt, report suspicious emails to the IT department.   * **1. Examine the Sender:** Check the email sender's address carefully. Be cautious of emails from unfamiliar or suspicious domains or email addresses that imitate legitimate organisations. Look for misspellings or variations in the sender's name or email address. * **2. Assess the Content:** Pay attention to the content of the email. Be wary of urgent requests, overly generic greetings, or poor grammar and spelling. Phishing emails often use fear tactics or urgency to pressure recipients into taking immediate action. * **3. Hover Over Links:** Before clicking on any links in an email, hover the mouse cursor over them to reveal the actual URL. Ensure that the URL matches the expected destination or website. Be cautious of shortened URLs or URLs that redirect to suspicious or unfamiliar domains * **4. Beware of Attachments:** Exercise caution when opening email attachments, especially if they come from unknown senders or if they are unexpected. Malicious attachments can contain malware or viruses that can compromise your system or steal sensitive information. * **5. Check for Personalization:** Legitimate organisations usually personalise their communications. Be suspicious of generic greetings like "Dear Customer" instead of using your name. Phishing emails often lack personalization or use incorrect personal information. * **6. Verify Requests for Information:** Be cautious of emails requesting sensitive information, such as passwords, credit card details, or social security numbers. Legitimate organisations typically do not ask for such information via email. When in doubt, contact the organisation directly through a verified and trusted channel to verify the request. * **7. Look for Red Flags:** Be alert to common red flags indicating a phishing attempt, such as unexpected prize winnings, unsolicited job offers, or requests for financial assistance. Be sceptical of emails promising unrealistic rewards or benefits. * **8. Report Suspicious Emails:** If an email appears suspicious, report it to your IT or security team following the organisation's reporting procedures. By reporting phishing attempts, you contribute to the organisation's overall security posture and help protect others from falling victim to similar attacks. * **9. Stay Informed:** Stay updated on the latest phishing techniques and trends through regular cybersecurity awareness training. Stay informed about the common tactics used by phishers to maintain a proactive stance against evolving threats. |

| Social Engineering Awareness |
| --- |
| Social engineering is the manipulation of individuals to gain unauthorised access or confidential information. Be alert to unsolicited phone calls or visitors asking for sensitive information or attempting to gain physical access to restricted areas. Verify the identity and authorization of individuals before sharing any information or granting access.   * **1. Understand Social Engineering:** Educate employees about social engineering tactics, which involve manipulating individuals to gain unauthorised access to systems or sensitive information. Explain the various methods used, such as impersonation, pretexting, baiting, or tailgating, to help employees recognize when they may be targeted. * **2. Verify Requests:** Instruct employees to independently verify requests for sensitive information or access to systems or facilities, especially if they come from unfamiliar or unexpected sources. Encourage them to use established communication channels or contact known individuals within the company to authenticate the legitimacy of such requests. * **3. Be Mindful of Personal Information:** Remind employees to be cautious about sharing personal or sensitive information, both online and offline. Emphasise the importance of protecting personal details that could potentially be used in social engineering attacks, such as birth dates, home addresses, or financial information. * **4. Promote a Security-Conscious Culture:** Foster an environment where employees feel comfortable reporting suspicious activities or potential social engineering incidents. Create clear channels and procedures for reporting and provide assurance that concerns will be taken seriously and addressed promptly. |

| Data Protection and Privacy |
| --- |
| Safeguarding sensitive data is critical. Handle data securely by encrypting files, using secure file transfer methods, and properly disposing of confidential documents. Only access and share data on a need-to-know basis. Comply with data protection regulations, such as the General Data Protection Regulation (GDPR), to maintain the privacy and integrity of personal information. |

* **1. Understand the Importance of Data Protection:** Educate employees about the significance of data protection and privacy in safeguarding sensitive information. Explain the potential consequences of data breaches, including financial losses, reputational damage, and legal implications. Help them understand their role in maintaining data confidentiality and integrity.
* **2. Identify Sensitive Data:** Teach employees how to identify different types of sensitive data within the organisation, such as personal identifiable information (PII), financial data, trade secrets, or intellectual property. Provide examples and specific guidelines on what constitutes sensitive information in the context of your company's operations.
* **3. Data Handling Best Practices:** Establish clear guidelines on how employees should handle sensitive data. This may include proper encryption methods, secure file transfer protocols, or data retention policies. Emphasise the importance of securely storing physical documents and protecting digital files with strong passwords or encryption.
* **4. Access Control:** Explain the concept of access control and the principle of least privilege. Train employees on the importance of restricting access to sensitive data only to those who require it to perform their job responsibilities. Encourage the use of strong passwords, multi-factor authentication, and regular review of access rights.
* **5. Data Sharing and Third Parties:** Educate employees about the risks associated with sharing sensitive data outside the organisation. Emphasise the need to exercise caution when sharing information with external parties or using cloud-based services. Train employees on how to verify the security practices of third-party vendors and the importance of data protection agreements.

| Safe Internet and Email Practices |
| --- |
| Exercise caution when browsing the internet and opening emails. Avoid visiting untrusted or suspicious websites, as they may contain malware or attempt to deceive you. Be sceptical of unexpected or unsolicited emails, especially those with attachments or links. Verify the legitimacy of email senders and exercise discretion when sharing sensitive information over email.   * **1. Phishing Awareness:** Educate employees about phishing attacks and how to identify suspicious emails. Train them to be cautious of unsolicited emails, requests for personal information, or urgent messages that create a sense of urgency. Encourage employees to report any suspicious emails to the appropriate IT or security personnel. * **2. Verify Email Senders:** Instruct employees to verify the authenticity of email senders before interacting with the email. Teach them to scrutinise the email address, look for signs of impersonation, and be cautious of emails from unknown or unexpected sources. * **3. Be Wary of Email Attachments:** Train employees to exercise caution when opening email attachments, particularly from unknown or suspicious senders. Emphasise the importance of scanning attachments with antivirus software before opening them * **4. Think Before Clicking:** Encourage employees to think twice before clicking on links in emails or on websites. Remind them to hover their mouse over links to view the actual URL and verify that it matches the expected destination. If in doubt, employees should navigate to the website directly through a trusted browser. * **5. Secure Internet Browsing:** Promote safe internet browsing practices by advising employees to visit reputable websites, avoid clicking on suspicious ads or pop-ups, and be cautious when downloading files or software from the internet. Encourage the use of secure websites (HTTPS) for online transactions or when sharing sensitive information. * **6. Regular Software Updates:** Stress the importance of keeping software, browsers, and plugins up to date. Regular updates often include security patches that address vulnerabilities and protect against known threats. Encourage employees to enable automatic updates whenever possible. |

| Device Security |
| --- |
| Keep your devices secure by installing software updates promptly. Use reputable antivirus software and enable firewalls. Be cautious when connecting to public Wi-Fi networks and avoid transmitting sensitive data on unsecured connections. When working remotely, use a virtual private network (VPN) to encrypt your internet traffic and ensure secure access to company resources.   * **1. Secure Network Connections:** Advise employees to be cautious when connecting to Wi-Fi networks, particularly public or unsecured ones. Encourage the use of secure, password-protected Wi-Fi networks, or recommend the use of a virtual private network (VPN) to encrypt internet traffic and enhance security. * **2. Encryption:** Promote the use of device-level encryption, such as full-disk encryption or file-level encryption, to protect sensitive data in case of loss or theft. Encourage employees to enable encryption features available on their devices. * **3. App and Software Downloads:** Remind employees to download apps and software only from reputable sources, such as official app stores or verified websites. Encourage them to read user reviews and check app permissions before installation to ensure they are legitimate and safe |

| Physical Security |
| --- |
| Physical security is essential for protecting our assets. Lock your workstation when leaving your desk, even for a short time. Secure laptops and mobile devices to prevent unauthorised access. Restrict access to sensitive areas and report any suspicious individuals or activities to the appropriate authorities.   * **1. Access Control:** Emphasise the importance of controlling physical access to facilities, offices, and sensitive areas. Instruct employees to always lock doors, use access control systems (such as keycards or biometric scanners), and not allow unauthorised individuals to enter restricted areas. * **2. ID Badge Policy:** Educate employees about the organisation's ID badge policy. Encourage them to prominently display their ID badges at all times and report any lost or stolen badges immediately. Remind employees to challenge individuals without proper identification who attempt to access company premises. * **3. Visitor Management:** Train employees on the organisation's visitor management procedures. Instruct them to escort and monitor visitors, ensuring they are appropriately identified and have authorised access. Encourage employees to report any suspicious or unauthorised visitors to the designated personnel. |

| Reporting Security Incidents |
| --- |
| Promptly report any security incidents or suspicious activities to the IT department or designated personnel. This includes potential data breaches, unusual system behaviour, or suspected phishing attempts. Your vigilance plays a crucial role in maintaining a secure environment.   * **1. Know What Constitutes an Incident:** Educate employees on what constitutes a cybersecurity incident. Provide clear examples of incidents, such as data breaches, unauthorised access attempts, suspicious emails, malware infections, or suspicious network activity. This helps employees understand the types of incidents they should report. * **2. Recognize Indicators:** Train employees to recognize indicators of a cybersecurity incident, such as unusual system behaviour, unauthorised access or use of company resources, unexpected pop-ups or error messages, or unusual network activity. Encourage them to trust their instincts and report anything that seems suspicious or out of the ordinary. * **3. Understand Reporting Channels:** Communicate the designated reporting channels and procedures within the organisation. This may include contacting the IT department, a dedicated cybersecurity hotline, or an incident response team. Ensure employees are aware of who to contact and how to report incidents promptly and effectively. * **4. Encourage Timely Reporting:** Stress the importance of reporting incidents in a timely manner. Emphasise that early detection and response are crucial in mitigating potential damage and minimising the impact of cybersecurity incidents. Encourage employees to report incidents as soon as they are identified or suspected. |

| Ongoing Training and Awareness |
| --- |
| Cybersecurity threats evolve constantly. Stay informed and updated through ongoing training and awareness programs. Participate in periodic refresher courses, review security policies and guidelines, and keep up to date with emerging threats and best practices. Stay proactive and share your knowledge with your colleagues to foster a culture of cybersecurity within our organisation.   * **1. Regular Training Sessions:** Conduct scheduled training sessions on relevant cybersecurity topics. These sessions can be conducted by internal IT or security teams, external trainers, or a combination of both. Cover emerging threats, new technologies, best practices, and policy updates. Use a variety of training formats, such as presentations, workshops, interactive activities, and case studies, to engage employees effectively. * **2. E-Learning Modules: I**mplement an e-learning platform or online training modules that employees can access at their convenience. These modules can cover a wide range of cybersecurity topics and allow employees to learn at their own pace. Include quizzes or assessments to reinforce learning and track progress. * **3. Security Awareness Campaigns:** Launch periodic security awareness campaigns to promote cybersecurity knowledge and best practices. These campaigns can be themed around specific topics or aligned with cybersecurity awareness months. Use posters, newsletters, emails, intranet articles, and other communication channels to share tips, reminders, and success stories. |