MSS
MAKING STRONG SUCCESS

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

CYBERSECURITY AWARENESS TRAINING IN THE PHILIPPINES

CLICK SMART, WORK SECURE

Practical Cybersecurity Skills for Protecting Accounts, Devices, Information, Customers, and Organizational Operations

---

TRAINING OVERVIEW

Cybersecurity is not solely the responsibility of the Information Technology department.

A technically secure system can still be exposed when an employee clicks a fraudulent link, approves an unexpected authentication request, shares a password, sends confidential information to the wrong recipient, installs an unauthorized application, uses an unprotected device, or fails to report suspicious activity promptly.

Employees interact daily with email, messaging applications, cloud platforms, mobile devices, online meetings, shared files, customer information, financial records, internal systems, and artificial intelligence tools. Every interaction creates an opportunity to either protect or expose the organization.

Republic Act No. 10175, or the Cybercrime Prevention Act of 2012, defines cybersecurity broadly to include tools, policies, risk-management approaches, actions, training, practices, assurance, and technologies used to protect the cyber environment and organizational or user assets. The Philippines has also adopted the National Cybersecurity Plan 2023–2028 through Executive Order No. 58 as the country's whole-of-nation roadmap toward a trusted, secure, and resilient cyberspace.

Click Smart, Work Secure: Cybersecurity Awareness Training in the Philippines equips employees, supervisors, managers, executives, administrative personnel, customer-facing teams, remote workers, and organizational leaders with practical behaviors for preventing, recognizing, and reporting common cyber threats.

Participants learn how to:

- Recognize phishing, impersonation, and social-engineering attempts;
- Verify unusual requests involving money, credentials, confidential data, or account changes;
- Use passwords, password managers, and multifactor authentication responsibly;
- Protect work devices, mobile phones, files, and cloud accounts;
- Handle personal, customer, employee, and business information securely;
- Avoid malware, ransomware, unsafe downloads, and unauthorized applications;
- Apply safer practices when working remotely or using public networks;
- Respond appropriately to suspicious links, unexpected authentication prompts, and possible account compromise;
- Protect information when using generative artificial intelligence platforms;
- Report possible cybersecurity incidents through approved organizational channels; and
- Understand that immediate reporting is more valuable than hiding an honest mistake.

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

The Data Privacy Act of 2012 requires organizations to implement reasonable and appropriate organizational, physical, and technical safeguards against unlawful access, disclosure, alteration, destruction, misuse, and other security risks involving personal information. It also requires employees handling nonpublic personal information to maintain strict confidentiality.

The program incorporates widely recognized cyber-hygiene practices such as recognizing and reporting phishing, using strong and unique passwords, enabling multifactor authentication, and installing software updates. These are among the fundamental protective behaviors promoted through the Cybersecurity and Infrastructure Security Agency's Secure Our World initiative.

Consistent with MSS Corporation's **EnterTRAINment** methodology, this **Training on Cybersecurity Awareness in the Philippines** minimizes technical lectures. Participants analyze realistic messages, inspect suspicious requests, make cybersecurity decisions, respond to simulated incidents, and prepare practical workplace commitments.

The program may be customized according to the client's industry, cybersecurity policy, information-classification rules, approved applications, reporting channels, remote-work arrangements, data privacy requirements, employee responsibilities, and actual anonymized security situations.

TRAINING GOAL

To equip participants with the awareness, practical judgment, responsible habits, and incident-reporting skills needed to recognize common cyber threats, protect organizational information and systems, reduce preventable security risks, and contribute actively to a stronger cybersecurity culture.

TRAINING OBJECTIVES

By the end of the program, participants should be able to:

1. **Explain** cybersecurity awareness in practical workplace terms;
2. **Recognize** the shared cybersecurity responsibilities of employees, managers, IT personnel, data protection officers, cybersecurity teams, and organizational leaders;
3. **Differentiate** cybersecurity threats, security incidents, personal data breaches, technical problems, and ordinary user errors;
4. **Describe** the importance of confidentiality, integrity, and availability in protecting organizational information and systems;
5. **Identify** common social-engineering methods, including phishing, spear phishing, business email compromise, smishing, vishing, impersonation, malicious QR codes, and fraudulent authentication requests;
6. **Inspect** messages, links, attachments, identities, websites, and unusual requests before acting;
7. **Apply** safer practices involving passwords, password managers, multifactor authentication, account access, and credential protection;

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

8. **Protect** work devices, removable media, cloud files, mobile phones, applications, and remote-work environments;
9. **Handle** personal data, confidential business information, customer records, financial information, and internal documents according to approved policies;
10. **Recognize** malware, ransomware, account compromise, unauthorized access, and other possible incident indicators;
11. **Respond** appropriately after clicking a suspicious link, sharing information, losing a device, receiving an unexpected MFA prompt, or observing unusual system behavior;
12. **Report** potential incidents promptly without deleting evidence, circulating information unnecessarily, or attempting unauthorized investigation;
13. **Apply** the MSS S.H.I.E.L.D. Cybersecurity Awareness Guide to common workplace situations; and
14. **Prepare** a personal or team action plan for strengthening cybersecurity behavior after the training.

LEARNING DOMAINS ADDRESSED

Cognitive Domain
Participants understand cybersecurity concepts, common threats, social engineering, account protection, information handling, device security, incident indicators, and organizational reporting responsibilities.

Affective Domain
Participants strengthen vigilance, responsibility, healthy skepticism, willingness to verify unusual requests, respect for confidentiality, and readiness to report honest mistakes without concealment.

Psychomotor and Behavioral Domain
Participants practice inspecting suspicious communications, verifying identities, applying secure account habits, responding to cybersecurity scenarios, preserving relevant information, and using approved reporting channels.

FROM POINT A TO POINT B

Point A: Before the Training

Participants may:

- Believe that cybersecurity is exclusively an IT concern;
- Click links before verifying the sender or destination;
- Trust a message because it uses a familiar name, logo, or email signature;
- Respond immediately to urgent requests involving payments or confidential information;
- Reuse the same password across multiple accounts;
- Share credentials with colleagues for convenience;
- Approve unexpected multifactor authentication prompts;
- Leave devices unlocked and unattended;
- Download files or applications from unverified sources;

- Connect unauthorized storage devices to work equipment;
- Use personal email or messaging accounts for official information;
- Upload confidential information into unapproved online or AI platforms;
- Share cloud links without reviewing permissions;
- Ignore software-update reminders;
- Assume that public Wi-Fi is safe because it requires a password;
- Conceal an accidental click or information disclosure out of embarrassment;
- Delete suspicious messages before reporting them;
- Forward possible phishing messages to colleagues as a warning;
- Attempt to investigate a cybersecurity incident without authority; or
- Delay reporting because no visible damage has occurred.

Point B: After the Training

Participants should be better able to:

- Recognize their role in protecting organizational systems and information;
- Pause before acting on unusual or urgent requests;
- Verify identities through separate and trusted communication channels;
- Inspect senders, links, attachments, domains, and message context;
- Treat unexpected MFA prompts as possible warning signs;
- Use strong, unique credentials and approved password-management practices;
- Protect devices through locking, updates, and approved configurations;
- Follow information-classification and sharing requirements;
- Use only approved applications, storage services, and AI tools;
- Limit access according to legitimate business need;
- recognize indicators of phishing, malware, ransomware, or account compromise;
- preserve relevant information when an incident may have occurred;
- report mistakes and suspicious activity immediately;
- avoid gossiping, forwarding suspicious content, or confronting suspected attackers;
- follow organizational reporting and escalation procedures;
- cooperate appropriately with authorized incident responders; and
- contribute actively to a stronger cybersecurity culture.

ORGANIZATIONAL CHALLENGES ADDRESSED

This **Cybersecurity Training in the Philippines** may help organizations address situations such as:

- Employees regularly receive suspicious emails and messages;
- Staff cannot distinguish legitimate requests from phishing attempts;
- Payment instructions are accepted without independent verification;
- Employees share passwords or reuse them across accounts;
- Multifactor authentication is enabled but users approve unexpected prompts;
- Confidential files are sent to incorrect recipients;
- Cloud links provide broader access than intended;

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

- Employees install unauthorized applications or browser extensions;
- Personal devices are used for work without adequate safeguards;
- Employees upload company information into public AI platforms;
- Software updates are repeatedly postponed;
- Work devices are left unlocked;
- Lost devices are reported late;
- Employees use removable media from unknown sources;
- Remote employees work through unsecured or shared networks;
- Staff members do not know where or how to report suspicious activity;
- Employees hide mistakes because they fear punishment;
- Managers treat cybersecurity as a purely technical responsibility;
- Security policies exist but are written in language employees do not understand;
- New employees receive limited cybersecurity orientation;
- phishing simulations produce repeated failures without sufficient coaching;
- Security awareness is treated as a once-a-year compliance activity;
- Incident reporting lacks consistency; or
- The organization wants to build more resilient human behavior around its technical controls.

WHAT CYBERSECURITY AWARENESS MEANS

Cybersecurity awareness is the ability and willingness of employees to recognize digital risks, apply approved protective behaviors, make safer decisions, and report suspicious activity promptly.

It involves:

- Understanding what information and systems require protection;
- Recognizing how attackers manipulate people;
- Knowing which actions increase or reduce risk;
- Following organizational policies;
- Verifying unusual requests;
- Protecting identities and credentials;
- Handling information responsibly;
- Recognizing possible compromise;
- Reporting promptly; and
- learning continuously as threats and technologies change.

Cybersecurity awareness does not require every employee to become a technical specialist.

Employees do not need to configure firewalls, analyze malware, conduct digital forensics, or investigate attackers. They need to know how to avoid preventable risk, recognize warning signs, and involve the right authorized personnel quickly.

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

Cybersecurity aims to protect three essential qualities of information and systems.

Confidentiality
Information is accessed, used, and disclosed only by authorized individuals.

Examples of confidentiality failures include:
- Sending employee records to the wrong recipient;
- Sharing a password;
- Exposing customer information through an open cloud link;
- Discussing confidential information in a public place; or
- Uploading restricted data to an unauthorized platform.

Integrity
Information remains accurate, complete, trustworthy, and protected from unauthorized alteration.

Examples include:
- An attacker changing bank-account details;
- Unauthorized modification of records;
- Altered reports or contracts;
- Manipulated payment instructions; or
- accidental overwriting of important information.

Availability
Authorized users can access information and systems when needed.

Examples of availability concerns include:
- Ransomware preventing access to files;
- Deleted records;
- System outages;
- damaged equipment;
- unavailable backups; or
- accounts locked or taken over by unauthorized persons.

The National Privacy Commission similarly distinguishes confidentiality, integrity, and availability breaches when addressing personal data security incidents.

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

CYBERSECURITY AWARENESS VERSUS RELATED PROGRAMS

Cybersecurity Awareness Training
Develops practical protective behaviors among general employees and managers.

Technical Cybersecurity Training
Develops specialized competencies involving networks, systems, penetration testing, threat detection, incident response, security architecture, digital forensics, or other technical functions.

Data Privacy Awareness Training
Focuses on lawful and responsible collection, use, sharing, storage, retention, and disposal of personal data. Cybersecurity supports data privacy, but not every cybersecurity concern involves personal information.

Information Security Training
May cover a broader range of digital, physical, administrative, and personnel controls protecting organizational information.

Cybercrime Awareness Training
Focuses more directly on illegal acts involving computer systems, networks, online communication, fraud, and other offenses addressed by applicable laws.

Security Incident Response Training
Prepares authorized incident-response personnel to assess, contain, investigate, recover from, document, and report cybersecurity incidents.

General employees need reporting awareness but should not perform unauthorized technical response or investigation.

COMMON CYBERSECURITY THREATS ADDRESSED

Phishing
Fraudulent email or online communication designed to make recipients click harmful links, open malicious attachments, disclose information, transfer money, or enter credentials into a fake website.

Spear Phishing
A more targeted message designed for a particular person, department, role, or organization.

Business Email Compromise
An attacker impersonates or compromises an executive, supplier, client, finance employee, or other trusted party to request payment, information, or account changes.

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

Smishing
Phishing delivered through SMS, messaging applications, or mobile communication.

Vishing
Voice-based social engineering through calls, voice messages, or online meeting platforms.

QR-Code Phishing
A malicious or substituted QR code directs the user to a fraudulent website or unsafe download.

Impersonation
An attacker pretends to be a manager, customer, vendor, government representative, IT support person, courier, recruiter, or another trusted person.

Credential Theft
The attacker attempts to obtain usernames, passwords, one-time codes, recovery information, or session access.

MFA Fatigue or Authentication-Prompt Abuse
The attacker repeatedly sends login approvals or contacts the user and pressures them to approve a request.

Malware
Malicious software intended to damage, disrupt, monitor, steal, or gain unauthorized access to systems and information.

Ransomware
Malware or related attacker activity that restricts access to systems or data and may be accompanied by demands for payment.

Account Takeover
An unauthorized person gains control of an email, cloud, social-media, banking, or organizational account.

AI-Enabled Deception
Artificial intelligence may be used to create more polished phishing messages or manipulate audio, video, and images. Employees should therefore verify unusual requests based on context and trusted procedures rather than relying only on spelling, grammar, appearance, or familiarity.

THE MSS S.H.I.E.L.D. CYBERSECURITY AWARENESS GUIDE

The program introduces a practical six-step guide for safer workplace decisions.

S — Stop Before You Click, Send, Approve, or Pay

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

Pause when a message:

- Creates extreme urgency;
- pressures secrecy;
- requests credentials or verification codes;
- changes payment instructions;
- asks for confidential information;
- contains an unexpected attachment;
- directs you to a login page;
- asks you to approve an authentication prompt; or
- appears inconsistent with normal procedures.

A short pause can prevent a much longer incident.

H — Handle Information, Accounts, and Devices Safely

Apply approved practices involving:

- Information classification;
- file sharing;
- passwords;
- password managers;
- device locking;
- physical documents;
- cloud storage;
- removable media;
- mobile devices; and
- disposal of information.

I — Inspect Identities, Messages, Links, and Requests

Examine:

- The complete sender address;
- domain spelling;
- link destination;
- attachment type;
- message context;
- unusual tone;
- unexpected changes;
- identity claims;
- payment details; and
- whether the request follows normal procedures.

Do not rely solely on logos, signatures, display names, caller identification, voices, or video appearance.

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

E — Employ Secure Access and Approved Tools

Use:

- Strong and unique credentials;
- approved password managers;
- multifactor authentication;
- approved applications;
- authorized cloud platforms;
- updated software;
- secure connection methods; and
- organization-issued devices where required.

MFA provides protection beyond a password, although employees must never approve an authentication request they did not initiate. More phishing-resistant methods should be used where the organization makes them available.

L — Limit Exposure, Sharing, and Access

Ask:

- Does this person genuinely need the information?
- Am I sending only what is necessary?
- Are the sharing permissions correct?
- Is the recipient verified?
- Is the platform approved?
- Does the application need these permissions?
- Should this information be discussed in this location?
- Am I exposing organizational information through social media or AI tools?

D — Detect, Document, and Report Promptly

When something appears suspicious:

- Stop the action;
- follow immediate safety instructions;
- preserve the message or relevant information;
- take screenshots only when permitted;
- avoid forwarding suspicious content;
- use the approved reporting channel;
- state what happened honestly; and
- follow the instructions of authorized responders.

Employees should not delay reporting while trying to determine whether the incident is serious. Authorized personnel can assess the situation more effectively when they receive timely and accurate information.

MSS
MAKING STRONG SUCCESS

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

ONE-DAY CYBERSECURITY AWARENESS TRAINING OUTLINE

Time	Modules and Essential Topics	Major Activity and Participant Output
8:00 AM–10:00 AM	**MODULE 1: EVERY EMPLOYEE IS PART OF CYBERSECURITY** **1. Understanding Workplace Cybersecurity** • Cybersecurity as a shared organizational responsibility • People, processes, technology, information, and physical environments **2. What Organizations Protect** • Accounts, devices, systems, personal data, business information, finances, reputation, and operations • Confidentiality, integrity, and availability **3. How Cyber Incidents Begin** • Human error, manipulation, weak access, unsafe tools, delayed updates, and unauthorized sharing • Why attackers target people as well as technology **4. Common Cyber Threats** • Social engineering, phishing, malware, ransomware, credential theft, and account takeover • Internal, external, accidental, and intentional risks **5. The MSS S.H.I.E.L.D. Guide** • Stop, Handle, Inspect, Employ, Limit, and Detect • Applying the framework to daily workplace decisions	**Major Activity: Cyber Risk Workplace Scenario Laboratory** — Participants analyze realistic workplace situations, identify the information or asset at risk, determine the possible threat, examine the employee behavior involved, and select the safest response. **Major Output:** Workplace Cybersecurity Risk and Responsibility Map
10:00 AM–10:15 AM	**MORNING BREAK**	

MSS
MAKING STRONG SUCCESS

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L. Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

Time	Modules and Essential Topics	Major Activity and Participant Output
10:15 AM–12:00 NN	**MODULE 2: THINK BEFORE YOU CLICK—DEFENDING AGAINST SOCIAL ENGINEERING** **1. How Social Engineering Works** • Urgency, authority, fear, curiosity, reward, familiarity, and helpfulness • Manipulating human judgment rather than directly attacking technology **2. Phishing and Impersonation Channels** • Email, text, calls, social media, chat, QR codes, shared documents, and online meetings • Phishing, spear phishing, smishing, vishing, and business email compromise **3. Inspecting Messages and Requests** • Sender, domain, links, attachments, context, timing, tone, and requested action • Why grammar and appearance alone are unreliable indicators **4. Verifying High-Risk Requests** • Payments, account changes, password resets, confidential information, and executive instructions • Using trusted and separate verification channels **5. Protecting Credentials and Authentication** • Strong unique passwords, password managers, MFA, recovery information, and one-time codes • Unexpected MFA prompts and account-compromise indicators	**Major Activity: Phish, Fraud, or Legitimate? Verification Simulation** — Teams inspect increasingly realistic messages and requests, identify manipulation techniques and warning signs, and demonstrate how they would verify and report each situation. **Major Output:** S.H.I.E.L.D. Message Verification and Phishing-Response Checklist
12:00 NN–1:00 PM	**LUNCH BREAK**	
1:00 PM–3:00 PM	**MODULE 3: PROTECTING INFORMATION, DEVICES, AND DIGITAL WORKPLACES**	**Major Activity: Secure Digital Workday Simulation** — Participants navigate a simulated workday involving email, cloud

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

Time	Modules and Essential Topics	Major Activity and Participant Output
	1. Handling Organizational Information • Public, internal, confidential, restricted, and personal information where applicable • Minimum necessary access, correct recipients, and secure sharing **2. Securing Work Devices and Accounts** • Screen locking, updates, approved applications, account separation, and physical protection • Lost, stolen, borrowed, shared, or unattended devices **3. Email, Cloud, and File-Sharing Safety** • Permissions, external recipients, shared links, attachments, version control, and misdirected messages • Personal accounts and unauthorized storage services **4. Remote, Mobile, and Public-Space Security** • Home networks, public Wi-Fi, screen privacy, online meetings, travel, and shared equipment • Following approved remote-access arrangements **5. Emerging Workplace Risks** • Unauthorized AI use, shadow IT, removable media, browser extensions, oversharing, and malicious downloads • Protecting confidential information when using generative AI	files, remote work, mobile devices, public spaces, AI tools, and document sharing while making security decisions at each stage. **Major Output:** Secure Digital Workday Protection Plan
3:00 PM–3:15 PM	**AFTERNOON BREAK**	
3:15 PM–5:00 PM	**MODULE 4: WHEN SOMETHING GOES WRONG—RESPONDING AND REPORTING QUICKLY** **1. Recognizing Possible Security Incidents**	**Major Activity: Cybersecurity Incident Tabletop Challenge** — Groups respond to a developing workplace incident, determine immediate actions, prepare an initial report, distinguish employee responsibilities from

Time	Modules and Essential Topics	Major Activity and Participant Output
	• Unusual login alerts, unexpected MFA prompts, missing files, device behavior, account changes, malware warnings, and unauthorized messages • Lost devices, incorrect recipients, exposed links, and accidental disclosure **2. Immediate Employee Actions** • Stop, preserve, report, and follow authorized instructions • What not to delete, forward, alter, conceal, or investigate **3. Responding After a Mistake** • Suspicious-link clicks, credential entry, attachment opening, information disclosure, or authentication approval • Why immediate honesty reduces organizational risk **4. Reporting and Escalation** • IT, cybersecurity, supervisor, HR, Data Protection Officer, service desk, or designated incident channel • Information needed for a useful initial report **5. Building a Cybersecurity Culture** • Psychological safety for reporting, manager role-modeling, reinforcement, simulations, and continuous learning • Personal responsibility and post-training application	authorized technical response, and identify preventive improvements. **Major Output:** Cybersecurity Incident Response Record and 30-, 60-, or 90-Day Cyber-Safe Action Plan
5:00 PM	**PROGRAM CLOSING**	Learning synthesis, commitments, evaluation, and recommended next steps

MAJOR PARTICIPANT OUTPUTS

Participants are expected to complete:

1. **Workplace Cybersecurity Risk and Responsibility Map;**

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

2. **S.H.I.E.L.D. Message Verification and Phishing-Response Checklist;**
3. **Secure Digital Workday Protection Plan;** and
4. **Cybersecurity Incident Response Record and 30-, 60-, or 90-Day Cyber-Safe Action Plan.**

SAMPLE CYBERSECURITY SITUATIONS

Activities may be customized around situations such as:

- An executive allegedly requests an urgent bank transfer;
- A supplier submits new payment-account details by email;
- An employee receives an unexpected password-reset message;
- A user receives repeated MFA approval prompts;
- A caller claims to be from IT and asks for a verification code;
- An employee scans an unfamiliar QR code displayed in a public area;
- A shared cloud link allows anyone with the link to access a confidential file;
- A staff member sends an employee file to the wrong recipient;
- An employee uses a personal email account to continue work from home;
- A user uploads a confidential document into a public AI platform;
- A laptop is left unattended in a café;
- An employee finds an unknown USB device in the office;
- A browser extension requests extensive account permissions;
- A mobile phone containing workplace applications is lost;
- A colleague's email account sends unusual messages;
- A ransomware message appears on a workstation;
- An employee clicked a link but is afraid to report it;
- A manager asks staff to share one account for convenience;
- A remote worker uses a family computer for sensitive work; or
- Employees circulate screenshots of a possible data leak.

PHILIPPINE CYBERSECURITY AND DATA-PROTECTION CONTEXT

The Philippines' National Cybersecurity Plan 2023–2028 provides a national direction for strengthening cyber resilience and developing a trusted and secure cyberspace. Executive Order No. 58 directs national government bodies to align their cybersecurity plans with it and encourages local governments to do likewise.

Republic Act No. 10175 protects the confidentiality, integrity, and availability of computer data and systems and identifies offenses such as illegal access, illegal interception, data interference, and system interference.

Republic Act No. 10173 requires reasonable and appropriate safeguards for personal information. The National Privacy Commission also requires personal information controllers and processors to maintain security-incident management policies, develop response procedures, build personnel capability, and document security incidents and personal data breaches.

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

The standard employee-awareness program does not teach participants to determine criminal liability, conduct legal compliance audits, perform digital forensics, or decide whether a particular event requires formal breach notification. Those responsibilities belong to authorized organizational and professional personnel.

TRAINING METHODS

The program follows MSS Corporation's **EnterTRAINment** design standard:

- Approximately **30% concise trainer input, demonstrations, facilitated discussion, and synthesis**; and
- Approximately **70% participant analysis, verification exercises, workplace simulations, incident-response decisions, feedback, and action planning**.

Methods may include:

- Anonymous cybersecurity knowledge checks;
- Threat-recognition exercises;
- Phishing-message analysis;
- Link and sender inspection demonstrations;
- Identity-verification practice;
- Password and MFA scenarios;
- Secure-data handling exercises;
- Remote-work risk analysis;
- Digital-workday simulations;
- Cybersecurity incident tabletop exercises;
- Peer feedback;
- Facilitator processing; and
- workplace action planning.

Participants are not required to disclose passwords, actual credentials, private incidents, or confidential organizational information during the workshop.

TARGET PARTICIPANTS

This **Cybersecurity Awareness Training in the Philippines** is recommended for:

- Rank-and-file employees;
- Newly hired employees;
- Administrative and executive-support personnel;
- Customer-service teams;
- Sales and marketing employees;
- Finance and accounting personnel;
- Human Resources professionals;
- Learning and Development practitioners;
- Operations employees;

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

- Procurement and supply-chain personnel;
- Remote and hybrid workers;
- Field-based employees;
- Project teams;
- Supervisors and team leaders;
- Middle and senior managers;
- Executives and business owners;
- Contractors and outsourced personnel;
- Internal trainers;
- customer-facing employees; and
- any employee who uses organizational accounts, devices, systems, or information.

Separate advanced programs should be developed for IT administrators, security operations personnel, incident responders, system developers, cybersecurity professionals, and other technical roles.

RECOMMENDED NUMBER OF PARTICIPANTS

A class size of approximately **15 to 25 participants** is recommended for meaningful discussion, simulations, facilitator feedback, and workplace application.

Larger groups may be accommodated through adjusted breakout structures, digital polling, additional facilitators, or modified cybersecurity exercises.

DELIVERY OPTIONS

The program may be delivered through:

- Face-to-face in-house training;
- Offsite corporate training;
- Live virtual instructor-led training;
- Hybrid training;
- Public seminar;
- New-employee cybersecurity orientation;
- Annual cybersecurity refresher;
- Cybersecurity Awareness Month program;
- Leadership cybersecurity briefing;
- Department-specific security workshop;
- Phishing-awareness campaign; or
- Customized cybersecurity learning journey.

AVAILABLE PROGRAM FORMATS

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

One- to Two-Hour Cybersecurity Awareness Briefing
Recommended for organization-wide awareness campaigns, employee assemblies, new-hire orientation, or executive briefings.

Half-Day Cybersecurity Awareness Training
Recommended for essential threat recognition, phishing prevention, account protection, and incident reporting. The half-day version contains exactly two modules.

One-Day Cybersecurity Awareness Training
Recommended for comprehensive awareness, phishing analysis, secure digital-work practices, incident-response simulation, and employee action planning.

Two-Day Cybersecurity Awareness and Behavior Workshop
Recommended when the organization requires:

- More extensive threat scenarios;
- Repeated phishing analysis;
- Department-specific simulations;
- remote-work and mobile-security exercises;
- data privacy integration;
- AI-related cybersecurity risks;
- incident-reporting practice;
- policy application; and
- individualized facilitator feedback.

Separate Employee and Leadership Sessions
The employee program focuses on protective habits, threat recognition, safe information handling, and reporting.

The leadership version may additionally address:

- Cybersecurity governance;
- manager responsibilities;
- reporting culture;
- business email compromise;
- third-party risks;
- incident escalation;
- business continuity;
- decision-making during incidents; and
- leadership communication.

Cybersecurity Awareness Learning Journey
May include:

- Pre-training risk-awareness survey;
- Core cybersecurity workshop;

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

- simulated phishing exercises;
- microlearning reminders;
- posters and communication materials;
- manager reinforcement guides;
- quarterly refreshers;
- scenario-based assessments;
- reporting-process review;
- behavioral pulse checks; and
- post-program recommendations.

CUSTOMIZATION OPTIONS

This **Training on Cybersecurity in the Philippines** may be customized using:

- The organization's cybersecurity policy;
- information-security policy;
- acceptable-use policy;
- password and MFA requirements;
- data-classification rules;
- incident-reporting channels;
- information-sharing procedures;
- remote-work policy;
- social-media policy;
- generative AI policy;
- cloud-storage standards;
- approved applications;
- employee handbook;
- Data Privacy Manual;
- business continuity arrangements;
- actual anonymized incidents;
- industry-specific threats;
- employee roles;
- customer and supplier interactions; and
- existing cybersecurity campaign materials.

Client-specific reporting instructions should be validated by the organization's IT, cybersecurity, legal, compliance, and data privacy personnel before delivery.

PROFESSIONAL AND TECHNICAL BOUNDARIES

This program develops general employee awareness and preventive behavior. It does not constitute:

- Penetration testing;

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

- vulnerability assessment;
- cybersecurity audit;
- network or application security review;
- digital forensics;
- malware analysis;
- incident investigation;
- legal advice;
- data breach determination;
- breach-notification preparation;
- system configuration;
- cybersecurity certification;
- emergency technical response; or
- evaluation of active threats against the organization.

Actual cybersecurity incidents must be handled by authorized personnel according to the organization's approved technical, legal, data privacy, communications, and incident-response procedures.

FREQUENTLY ASKED QUESTIONS

What is Cybersecurity Awareness Training in the Philippines?
Cybersecurity Awareness Training in the Philippines is an employee-development program that teaches participants how to recognize common cyber threats, protect workplace accounts and information, use devices and applications safely, and report possible incidents promptly.

It is designed primarily for general employees and managers rather than technical cybersecurity specialists.

What is included in Training on Cybersecurity Awareness in the Philippines?
The program may cover:

- Cybersecurity responsibilities;
- confidentiality, integrity, and availability;
- social engineering;
- phishing and business email compromise;
- fraudulent calls and text messages;
- password and MFA security;
- safe email and web use;
- device and mobile security;
- cloud-file sharing;
- remote-work security;
- malware and ransomware awareness;
- AI-related risks;
- incident recognition; and
- reporting procedures.

MSS
MAKING STRONG SUCCESS

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

Is Cybersecurity Training in the Philippines only for IT personnel?
No.

Technical cybersecurity training may be intended for IT and security specialists. Cybersecurity awareness training is designed for employees at all levels because every person who uses organizational information, accounts, devices, or systems can influence security.

What is the difference between cybersecurity and data privacy?
Cybersecurity protects systems, networks, devices, accounts, and information against unauthorized access, damage, disruption, manipulation, and other threats.

Data privacy focuses on the lawful and responsible processing of personal data and the rights of individuals. Cybersecurity supports data privacy, but the two disciplines are not identical.

What is phishing?
Phishing uses fraudulent messages or websites to manipulate recipients into revealing information, opening harmful files, clicking malicious links, making payments, or entering credentials.

Phishing may occur through email, text, social media, messaging platforms, phone calls, QR codes, or other channels.

Can employees identify phishing through poor grammar?
Poor grammar may sometimes be a warning sign, but it should not be relied upon.

Modern phishing messages may be polished, personalized, and supported by artificial intelligence. Employees should verify the sender, context, request, destination, and approved organizational process.

What is business email compromise?
Business email compromise is a social-engineering scheme in which an attacker impersonates or compromises a trusted business identity to request money, confidential information, account changes, or another high-risk action.

Payment and account-change requests should be verified through a separate trusted channel.

Why is multifactor authentication important?
MFA requires an additional method of verification beyond a password. It can make unauthorized account access more difficult even when a password has been compromised.

Employees should never approve an MFA request they did not initiate.

Should employees share passwords with colleagues?
No, unless an explicitly approved organizational process and system has been established for shared access.

Individual credentials support accountability and reduce unauthorized access. Employees should follow the organization’s password and access-control policies.

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

What should an employee do after clicking a suspicious link?
The employee should stop interacting with the page or message and immediately follow the organization's incident-reporting procedure.

The employee should explain honestly what was clicked, entered, downloaded, approved, or observed. They should not delete possible evidence, attempt unauthorized investigation, or delay reporting while waiting for visible damage.

What should an employee do after entering a password into a suspicious website?
The employee should contact the authorized IT or cybersecurity function immediately and follow its instructions. Changing a password may be necessary, but the authorized response team may also need to review sessions, devices, authentication settings, and related accounts.

What should employees do with unexpected MFA prompts?
They should not approve them.

Unexpected prompts may indicate that someone has obtained or is attempting to use the account credentials. The employee should deny the request where appropriate and report it through the approved channel.

Can employees use public Wi-Fi for work?
Employees should follow the organization's remote-access policy.

Sensitive work may require approved secure connections, organization-issued devices, virtual private networks, mobile hotspots, or other safeguards. A network's availability or password requirement does not automatically make it trustworthy.

Can employees upload company documents to an AI platform?
Only when the tool and intended use are authorized by the organization.

Employees should not enter personal, confidential, restricted, proprietary, customer, employee, financial, or legally sensitive information into an unapproved AI platform.

Does cybersecurity awareness training prevent every attack?
No.

Training reduces preventable behavioral risks and improves recognition and reporting. Organizations also need suitable technical controls, policies, leadership, monitoring, incident-response capabilities, backups, and other safeguards.

Is one day enough for Cybersecurity Awareness Training?
One day is sufficient for developing essential awareness, practicing threat recognition, improving digital work habits, and conducting an incident-response simulation.

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

Ongoing reinforcement, phishing simulations, microlearning, policy reminders, and periodic refreshers are recommended because threats, systems, and employee responsibilities change.

Can the training be delivered virtually?
Yes.

Virtual delivery may use digital polls, phishing-message analysis, breakout-room scenarios, cloud-sharing exercises, remote-work cases, and online incident-response simulations.

Can the program use our actual cybersecurity policy?
Yes.

MSS Corporation may incorporate the client's approved rules, reporting channels, terminology, applications, data classifications, and anonymized situations.

Does the training qualify participants as cybersecurity professionals?
No.

The program develops general employee awareness. Professional cybersecurity roles require specialized technical education, experience, tools, and possibly industry certifications.

How can the impact of cybersecurity awareness training be measured?
Possible measures include:

- Pre- and post-training knowledge results;
- phishing-simulation performance;
- reporting speed;
- quality of employee incident reports;
- use of MFA;
- compliance with password and access requirements;
- reduction in repeated unsafe behavior;
- secure file-sharing practices;
- completion of software updates;
- employee confidence in identifying threats;
- manager observations; and
- application of cyber-safe action plans.

Training results should not be measured only by the absence of reported incidents. Increased employee confidence may initially produce more reporting because previously hidden or ignored concerns are being surfaced.

RELATED MSS CORPORATION TRAINING PROGRAMS

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

Organizations considering this program may also explore:

- Data Privacy Awareness Training in the Philippines;
- Data Privacy Act Training;
- Information Security Awareness Training;
- Cybercrime Awareness Training;
- Phishing Awareness Training;
- Ransomware Awareness Training;
- Responsible AI Use in the Workplace;
- AI Prompting Training in the Philippines;
- Social Media Responsibility Training;
- Remote and Hybrid Work Security;
- Business Continuity Awareness;
- Risk Management Training;
- Fraud Awareness and Prevention;
- Business Email Compromise Prevention;
- Records Management Training;
- Digital Workplace Productivity;
- Code of Conduct Training; and
- Incident Reporting and Escalation Training.

WHY CHOOSE MSS CORPORATION FOR CYBERSECURITY AWARENESS TRAINING IN THE PHILIPPINES?

Behavior-Focused Rather Than Overly Technical
The program translates cybersecurity risks into practical decisions employees make during their daily work.

Built Around Real Workplace Situations
Participants analyze emails, requests, files, devices, cloud sharing, AI use, remote work, and possible incidents rather than memorizing technical definitions.

Clear Employee Responsibilities
Participants understand what they should prevent, verify, protect, preserve, and report—and what should be handled by authorized technical personnel.

Practical MSS S.H.I.E.L.D. Guide
The framework provides a repeatable process employees can use when confronted with unusual digital situations.

Immediate Reporting Without Blame
The program reinforces that rapid, honest reporting allows the organization to respond more effectively than delayed concealment.

MSS
MAKING STRONG SUCCESS

MSS SUCCESS SPACES
Units 2K–2L, 2nd Floor E.C. Valle Commercial Center M.L.
Quezon Avenue Brgy. San Isidro, Angono, Rizal
(02) 7255 5568
0995 846 2495 | 0917 123 1017
info@msscorporation.com.ph
www.MSSCorporation.com.ph

Philippine Workplace Context
The program considers the Data Privacy Act, Cybercrime Prevention Act, National Cybersecurity Plan, local workplace practices, and organizational compliance responsibilities.

Customized to Client Policies
Activities may use the organization's approved tools, reporting channels, data classifications, cybersecurity rules, and actual anonymized risks.

EnterTRAINment Methodology
Participants engage in scenario analysis, simulations, decision challenges, feedback, and workplace planning rather than listening to a day-long technical lecture.

Training and Consultancy Capability
MSS Corporation may support clients through employee awareness training, policy communication, leadership briefings, cybersecurity campaigns, reinforcement materials, and learning-program design.

CALL TO ACTION

Turn Employees from Possible Targets into Active Cybersecurity Defenders

Help your people recognize cyber threats, protect accounts and information, verify unusual requests, work more securely, and report possible incidents before they become larger organizational problems.

Partner with MSS Corporation for a customized:

- **Cybersecurity Awareness Training in the Philippines**
- **Training on Cybersecurity Awareness in the Philippines**
- **Cybersecurity Training in the Philippines**
- **Training on Cybersecurity in the Philippines**

designed around your employees, cybersecurity risks, digital workplace, organizational policies, approved platforms, and incident-reporting requirements.

With MSS, We Make Strong Success.