DUBAI HOLDING

Information Security Awareness Program

August 2020

15 YEARS
For the Good of Tomorrow

Agenda

- Avoiding Social Engineering and Phishing Attacks
- Account Security and Access Rights
- Identity Theft
- Internal Threats
- Online Security and Mobile Computing
- Software Licensing and Usage
- Laptop and Workstation Security
- Personally, Identifiable Information (PII) & Information Protection
- Self Assessment Questions and Scenarios

Dubai Holding Information and Cyber Security Policy

Dubai Holding Information and Cyber Security Policy

What is the Security Policy?

- Dubai Holding information and cyber security policy along with procedures, standards and guidelines provide a management framework for the protection of information assets within Dubai Holding and its subsidiaries.

Who Does the Security Policy Apply to?

- This policy is applicable to all the employees and third-party personnel who use information assets that are owned or leased by Dubai Holding.

Why is the Security Policy Important?

- Dubai Holding recognizes that information assets are of significant value to the business and therefore require appropriate and adequate protection. Dubai Holding is committed to providing appropriate levels of security and continuity across all its departments and companies.

Where to Know More about the Security Policy?

- The security policies, procedures and guidelines are published on SharePoint and are accessible here: Security Portal https://dubaiholding.sharepoint.com/sites/IS/

Employee Responsibility

- Employees must comply with Dubai Holding's information security policies.
- Employees must confirm their compliance with Dubai Holding's information security policies upon joining and on annual awareness and policy refreshment programs

Dubai Holding Information Asset Classification

What is Information Asset Classification?

- Information in Dubai Holding's possession is classified as either public, internal, confidential or secret, based upon its sensitivity by the respective Information Asset Owners.
- The default classification for Dubai Holding information assets is 'Confidential' until a specific classification is assigned to them.
- The classification of an information system must correspond to the highest classification of data hosted on or passing through it.
- The classification of information assets have to be regularly reviewed by the information assets' respective Service Owners in coordination with the Information Security department.
- A business impact analysis must be undertaken whenever reclassification of an information asset is required, and the relevant stakeholders have to be informed about the reclassification.

Information Handling and Labelling

- Secure handling controls over information assets, including labelling are established to correspond to the identified information classification categories. Secure handling controls must be applied accordingly to ensure Dubai Holding's information assets are sufficiently protected against misuse and harm.
- Information that has been entrusted to Dubai Holding or companies is protected against misuse and harm in a manner consistent with the information's classification and corresponding handling requirements. Security measures must be applied irrespective of the media on which information is stored, the systems that process it, or the methods by which it is transmitted. Information must be sufficiently protected against misuse and harm throughout the lifecycle from collection, use, storage and destruction.

Avoiding Social Engineering and Phishing Attacks

What is a social engineering attack?

- In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.
- An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity.
- However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network.
- If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a phishing attack?

- Phishing is a form of social engineering; phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization.
- For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem.
- When users respond with the requested information, attackers can use it to gain access to the accounts.
- Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as
  - Natural disasters (e.g., Indonesian tsunami)
  - Epidemics and health scares (e.g., H1N1, COVID-19)
  - Economic concerns
  - Major political elections
  - Holiday

What is a vishing attack?

- Vishing is the social engineering approach that leverages voice communication.
- This technique can be combined with other forms of social engineering that entice a victim to call a certain number and divulge sensitive information.
- Advanced vishing attacks can take place completely over voice communications by exploiting Voice over Internet Protocol (VoIP) solutions and broadcasting services.
- VoIP easily allows caller identity (ID) to be spoofed, which can take advantage of the public's misplaced trust in the security of phone services, especially landline services.
- Landline communication cannot be intercepted without physical access to the line; however, this trait is not beneficial when communicating directly with a malicious actor

What is a Smishing attack?

- Smishing is a form of social engineering that exploits SMS, or text, messages.
- Text messages can contain links to such things as webpages, email addresses or phone numbers that when clicked may automatically open a browser window or email message or dial a number.
- This integration of email, voice, text message, and web browser functionality increases the likelihood that users will fall victim to engineered malicious activity

What is a Phone Spear Phishing Attack?

- Phone spear phishing is a form of social engineering. In Phone spear phishing attacks, attacker may call a potential victim to solicit personal information by posing as a trustworthy organization.
- For example, an attacker may claim that he or she from a reputable bank, work in same organization or financial institution that requests account information, often suggesting that there is a problem.
- When users respond with the requested information, attackers can use it to gain access to the accounts.

What are common indicators of phishing attempts?

- **Suspicious sender's address.** The sender's address may imitate a legitimate business. Cybercriminals often use an email address that closely resembles one from a reputable company by altering or omitting a few characters.
- **Generic greetings and signature.** Both a generic greeting—such as "Dear Valued Customer" or "Sir/Ma'am"—and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.
- **Spoofed hyperlinks and websites**. If you hover your cursor over any links in the body of the email, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.
- **Spelling and layout.** Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.
- **Suspicious attachments.** An unsolicited email requesting a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first

How do you avoid being a victim?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the internet before checking a website's security.
    - Pay attention to the Uniform Resource Locator (URL) of a website. Look for URLs that begin with "https"—an indication that sites are secure—rather than "http."
    - Look for a closed padlock icon—a sign your information will be encrypted.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.
- Take advantage of report phishing features offered by your email client.

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organization, report it to your line manager and information security team. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.

Account Security and Access Rights

Account Security and Access Rights

- One of the most fundamentally important aspects of information security is protecting your unique username and log-in credentials to any number of Dubai Holding system components, and to your personal accounts.
- Stop and think of all the highly sensitive and confidential information you access each and every day, all with a quick stroke of the keyboard or punching in pin numbers.
- Our lives truly are controlled by technology, yet you have a responsibility to protect Dubai Holding information, which means doing the following:
    - Using strong passwords, passcodes, and changing them on a frequent basis.
    - **Use strong passwords.** While most passwords will be enforced by group policy settings from I.T. personnel, it' still important to make them unique, never using information pertaining to your favorites sports team, home address, middle name, etc. With password complexity requirements in place often requiring the use of symbols and numbers and other mandates, it's also a good idea to adopt the same policies to other systems and websites that you personally have administrative password access right to, such as online banking, social media accounts, or any business accounts that are not group policy enforced by I.T. personnel
    - Never giving your username, password or any other account login credentials to anyone.
    - Never writing down your username, password or any other account login credentials and leaving such information available for public viewing.
    - Never trying to gain access to information for which you are not authorized.
    - Double your login protection. Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token.

Identity Theft

Identity Theft

- Identity theft is one of the fastest growing crimes today.
- Advances in technology, though plentiful with benefits, also leave everyone vulnerable to malicious individuals. Identity theft, is when someone steals your personal information and uses it without your permission.
- Three important aspects worth discussion on identify theft are:
    1. Looking for signs it has occurred.
    2. Protective measures to undertake.
    3. What to do if you're a victim.
- As for watchful signs, consider the following to be possible indicators of identity theft - remember - the earlier it's caught, the great the chances of minimizing the damages to you:
    - The type of mail you are receiving changes, or you stop getting certain bills or other items. Many times, fraudsters change somebody's mailing address, forwarding to another location.
    - You receive a statement for a credit card or some other type of purchase you never made.
    - Money is withdrawn from your bank account for unknown charges.
    - You receive calls from debt collection agencies for debts unknown to you.
    - You receive bills from medical services performed that you are unaware of. (Health care fraud is rampant).
    - Upon examining your credit report, you find unfamiliar accounts.
    - You've been notified that a data breach has occurred, and your personal information has been compromised.

Identity Theft

Let's discuss some protective measure to take against identity theft, which consist of the following:

- Always keep sensitive and confidential information physically secure, such as in locked files, cabinets, safe, etc. When you have friends, relative, guests over, be sure to put personal documentation away and not viewable by anyone.
- Limit what you carry in your wallet and purse to just the minimum - credit card or two, driver's license, important health care information, etc.
- Always ask "why". More specifically, if somebody asks for your personal information (date of birth, National ID, etc.) always politely ask why they need it, how it will be used, where will it be stored, etc.
- Shred documents such as receipts, financial account statements, along with peeling off labels from prescription bottles before discarding of them.
- If you've unfortunately become a victim of identity theft, it's time to act quickly for protecting yourself, which means cancelling credit cards and contacting all financial institutions and alerting them.
- What's extremely important is to report the incident to respective authority.

Internal Threats

Internal Threats

- Often the greatest enemy for any organization is its very own employees that undertake malicious acts that cause severe damage in terms of security.
- From stealing files to accessing privileged and sensitive information, insider threats are unfortunately on the rise. Yet it's more than just deliberate and fraudulent activities that create so many security challenges for businesses, it's also unintentional acts, such as opening virus infected attachments, visiting websites that result in executables infecting computers, and other unfortunate practices by employees.
- Not knowing is just as bad as the deliberate acts, at least in terms of consequences for the organization, so keep that in mind. What's interesting to note about insider threats are the following:
    - A negative event in the workplace triggered such an event.
    - The malicious individual had planned the event in advance maybe also been given prior disciplinary action for some other incident.
    - The vast majority of events used simple tools, commands, etc., and not elevated system administrative privileges.
    - A statistically significant amount took place using remote access protocols from outside of the organization's network, such as from their home.

Internal Threats

A list of recent and notable insider incidents that caused severe damage to organizations consist of the following:

- Theft of highly sensitive and confidential documents with the use of USB hard drives, which are easy to obtain, conceal, and use.
- Obtaining company secret information by accessing privileged folders in a cloud computing environment by a vendor who had supposedly been removed from access.
- Hundreds of checks forged for various amounts, ranging from $50 to $25,000, all from a company checkbook that was thrown into a garbage dispenser outside of the company's headquarters.

This list goes on and on, from deliberate acts to dangerous, unintended mishaps and actions, internal threats are everywhere. All employees have a responsibility to live and act by the motto, "if you see something, say something" – and report immediately.

Internal Threats

With that said, be alert and on the lookout for the following suspicious activities by others:

- Mood swings, violent and/or aggressive actions.
- Sudden change in behavior, work ethic, morals, etc.
- Discussion of suicide, harming others, general negativity, etc.
- Combative, argumentative, etc.
- Appearing intoxicated or using illegal substances.
- Verbal and/or email threats towards others.
- Unexplained absence and tardiness at work.
- Disregard for company rules and regulations.
- Not being a "team player", etc.

Online Security and Mobile Computing

Online Security and Mobile Computing

Security awareness is also about understanding today's ever-growing online threats, many of which can result in serious security issues for Dubai Holding along with identify theft for yourself. We all spend large amounts of time online, for both professional and personal reason - using laptops and portable devices, so it's important to take note of the following tips:

- **Trust, but verify.** It essentially means knowing who is requesting or asking for any type of information from you, from highly sensitive and confidential customer information to your own personal information. Social engineering - tactics used to gain access and steal valuable assets - is on the rise, so be watchful and mindful always.
- **Enable security.** This means making sure that you have anti-virus on whatever computer being used to access the Internet. It also means using a username and password for protecting the contents on your laptop should it ever be lost, stolen, or misplaced.
- **Protect your physical assets**. This means not leaving your laptop, mobile phone, tablet, etc. unattended for any time period. Going to the bathroom at the coffee house while leaving your notebook alone is not wise. For company-owned laptops, verify with your I.T. department that the serial number has indeed been recorded. For your own personal laptop, record the serial number also.
- **Secure Browsing.** Only download files and applications from websites that you trust, such as official app stores or legitimate organizations such as your bank, think carefully before clicking on links in emails, messages or on web sites. Don't click on links in messages if you don't know the sender or if the message is unexpected.

Online Security and Mobile Computing

- **Clear out browser sessions.** It's a good idea to periodically clean out your browser history for ensuring no pre-populated usernames and passwords exist especially on non-company owned desktops, laptops, and workstations. As for usernames and passwords, keep them secure (which is in your head!) and nowhere else. This means a clean desktop work policy, one that does not contain notes lying around with online login information.

- **Security updates.** Make sure your mobile and personal devices has all the required security updates for the operating system and all other applications running.

Online Security and Mobile Computing

- **Wireless Access Points.** Though they're free and easy to connect to, wireless access points can be extremely problematic in terms of security issues, so take note of the following precautions:
  - Turn off your actual wireless connectivity when not in use.
  - Connect only to trusted Wi-Fi "hotspots", thus if you aren't sure about a network that's being broadcasted, ask! If it seems suspicious, then do not connect - most Internet sessions can wait!
  - Do not use wireless access points for conducting business activities, unless you have approved VPN and secure, remote access software on your laptop.

- **Protect wireless handheld devices.** The continued growth and use of small, mobile devices capable of sending, receiving and storing information - though highly efficient - also requires putting in place protective measure, such as the following:
  - Use PIN and/or password security parameters for accessing and unlocking your phone, as this is critical if it's ever lost, stolen or misplaced.
  - When disposing of any wireless handheld devices, ensure that all sensitive and confidential data has been removed, such as with a secure wipe program

Social Media

Social Media

Be mindful on social media sites. You work for Dubai Holding , which means you represent us in everything you do, both inside and outside the walls of DH facilities. As such, be cognizant of information posted and please strive to use a professional tone and dialect at all times, even with your friends, family members, co-workers, and other online participants users you are engaging with. Just remember to ask yourself the following question: "Does the posting or uploading of content to any of my personal social media resources disclose any "sensitive information" related to my company, or does it in any way impact the safety and security of my organization? Remember to think before you post

- You are personally responsible for the content you publish on blogs, wikis or any other social media. You must be mindful of what you publish will remain public for a long time or will be archived.
- Always follow Dubai Holding's social media policy and respect your audience.
- Do not publish or post any inappropriate, defamatory, infringing, obscene, racist, terrorist, politically slanted, indecent or unlawful topic, name, material or information, ethnic slurs, personal insults, or engage in any conduct which would not be acceptable by Dubai Holding's policies.
- Do not use Dubai Holding and/or subsidiary address to establish any account on a social media platforms / Blogs etc.
- For any public posts, please identify yourself with minimal information such as your name and, your role at Dubai Holding, only if required or relevant, when associates discuss Dubai Holding or Dubai Holding related matters. Always write in the first person. You must make it clear that he/she is speaking for himself/herself and not on behalf of Dubai Holding.
- Do not not post any content (e.g. book, quotes, logos, etc.) which is property of Dubai Holding's or any third party including the confidential or other proprietary information. Seek permission to publish or report on conversations that are meant to be private or internal to Dubai Holding.

Social Media

- You should also show proper considerations for other's privacy and for topics which may be considered objectionable or provocative – such as politics and religion.
- Do not harass or advocate harassment of another person or organization.
- Do not post any material which contain nudity, violence or of offensive subject matter
- Do not publish information which is not verified or authentic or that is known to be false or misleading or promotes illegal activities or conduct that is abusive, threatening, obscene, defamatory or libelous.
- Do not exploit people in a sexual, violent or other manner not respectful of human rights.
- Do not commit or promote any criminal activity or provide instructional information about illegal activities, such as making or buying illegal weapons or violating someone's privacy.
- Don't pick fights or altercations, be the first to correct your own mistakes and don't alter previous posts without indicating you have done so.

Software Licensing and Usage

Software Licensing and Usage

It's also important to understand the company's general policy on software usage, which includes numerous responsibilities that all employees need to be aware of. Software is used by all of us, each and every day, as it's vital to performing daily tasks for one's job function. With that said, please be mindful of the following issues:

- **Use only approved software.** Only software approved and purchased from the company may be installed and used on any company-wide system components. This includes your workstation and any other device provided to you from the company. Unapproved software that has not been fully vetted by authorized I.T. personnel and can often contain dangerous or malicious code that's extremely harmful to computers. Simply stated, only load and use legally approved software on computers.
- **Do not duplicate software.** The licensing rights for software are strict and extremely rigid, allowing only a predetermined number of installations for a given data set. This means you are not allowed to copy or duplicate any company approved and purchased software – no exceptions. Copyright laws – and other regulations throughout the world – often place strict guidelines on software usage, so please keep this in mind.
- **Use caution on your own devices.** When using your own personal workstation, laptop, or other device, please consider and be mindful of the software you install, especially when such computing systems are used for potentially accessing the corporate network. While the guidelines on software for your personal computers are less restrictive, we still ask that you use extreme caution when loading any type of application onto your devices.

Software Licensing and Usage

- **Accept updates.** For software to function efficiently and safely, security and patch updates have to be applied on a regular basis, so make sure to accept such updates when pushed out and also take time to update any software on your personal computers that do not rely on updates pushed out by I.T. personal.
- **Downloading from the Internet.** Any software obtained from the Internet is to be considered copyright protected, which means accepting any copyright agreements, and also comprehensively scanning the software for ensuring no dangerous or malicious code exists. The Internet can be an extremely dangerous forum when it comes to software as many products seem harmless, only to contain viruses that can wreak havoc on computers. Think before you start downloading any software online.
- **Software audits.** As an employee of the company, we have the right to conduct random software compliance audits on workstations, including laptops issued to you. The audits are for ensuring compliance with software licensing rules, while also ensuring your computers are free of any potentially dangerous applications.
- **Penalties and fines.** Did you know that we as a company and you as an employee can actually be levied fines for improper software use? Yes, it's that serious and it's why we're taking the time to discuss this important issue with you.

Laptop and Workstation Security

Laptop Security

Securing your laptop always is extremely critical, and it requires comprehensive measures regarding its physical security, while also protecting all electronic data residing on it. From travelling for meetings to connecting to open public wireless access points, your laptop is a constant source of target, so beware. Take the following precautions for securing what's arguably one of your most important possessions

- **It's your laptop.** Therefore, don't let other individuals use it, especially if it's somebody you don't know. When situations arise that require it to be used by someone other than you, create a guest account for their use with the help of IT support team.
- **Secure it physically.** Always lock your laptop when not in use in secure cabinet.
- **Keep a watchful eye.** Don't ever leave your laptop unattended in any public venue or location not considered safe. That means not using the coffee house phrase "can you watch my laptop for a minute as I go to the restroom", or any other similar thought process. Being vigilant and watchful at all times is a must for the safety and security of your laptop, so remember – do not leave it unattended – plain and simple. If you have to leave in your hotel room or some other location, then remove it from sight and place under a pillow, in a closet, or some other location. The best safety measure is always to carry it with you.
- **Place your contact information somewhere visible.** Because most people are honest and trustworthy, should your laptop be stolen, misplaced or lost – and then subsequently found by a good Samaritan – you'll clearly want your name, phone number, address, and/or email visible on it. Put a sticker on the cover or back of your laptop with all your relevant contact information
- **And if your laptop is stolen.** Laptops unfortunately do get stolen, so think and act quickly, which means reporting the theft to local authorities along with the I.T. department) immediately.

Workstation Security and Other Security Tips

Protecting your workstation area - specifically your desktop computer and other supporting devices - is an important duty all employees should take very seriously. While many of the workstation security best practices mentioned below are also discussed in other areas of the security awareness training program, you'll find additional requirements, tips, and suggestions considered important. Employees spend long hours at their workstations, so it's critical to implement the following best practices:

- **It's your workstation.** That means only you should be using it, and primarily for business purposes only. Sure, it's fine to conduct personal activities also, such as checking your email, logging into online banking, even accessing a few of the accepted social media platforms, such as Facebook and LinkedIn. Allowing other employees to use your workstation is strictly prohibited, so be aware of this. Imagine another employee using your workstation, accessing the Internet and possibly downloading unsuspected malware, sending an unprofessional email, or any other action? It happens all the time and you don't want to be blamed for something you didn't do, so don't share your workstation rights.
- **Security updates.** While most of the security updates are "pushed" out and managed by I.T. personnel, at times you'll still need to accept these updates.
- **Don't alter security settings.** Your workstation has been configured for maximum security along with performance, so do not attempt to disable or modify configuration settings to the operating system or any other applications. Doing so may increase security vulnerabilities that would ultimately allow malicious files and other harmful scripts to reside on the workstation.

Workstation Security and Other Security Tips

- **Don't install any unapproved software.** Your workstation has also been configured for providing you the necessary tools in performing daily roles and responsibilities, which means no additional software is needed. Do not download or install into any of the drives or ports additional software that has not been approved as it may contain malicious files, could consume additional resources, or is simply not professionally suitable for the work environment.
- **Removable storage devices.** They're easy-to-use, inexpensive, and a great way for transferring information, yet they're also incredibly dangerous when the wrong information is on them and in the wrong hands. With that said, USB ports, such as thumb drives, external hard drives, and other removal storage and memory devices are never to contain highly sensitive and confidential information, such as Personally Identifiable Information (PII), or any other data deemed privileged. Such information should be transferred over the network using approved protocols and residing on company servers only.
- **Use caution with email.** Be careful when opening emails from unknown parties, especially attachments. If it looks suspicious, do not open the email under any circumstances. Additionally, avoid clicking on links or banner advertisements sent to you as these often-containing spyware, malware, etc
- **Be mindful of Instant Messaging.** Instant messaging is considered fun, informal, and an easy and affordable way to communicate – all of which are true. Just be very careful as to the types of information you're sending and receiving via instant messaging, which ultimately means not transmitting any type of secret, confidential, or privilege information. This includes what's commonly known as Personally Identifiable Information (PII) – unique identifiers for any individual, such as national ID numbers, dates of birth, medical accounts, etc. If you're not sure as to the sensitivity of the information, don't send it over IM.

Workstation Security and Other Security Tips

- **Handle privileged information with care.** From emails containing sensitive information to hard copy documents for contracts, trade secrets, or any other type of confidential data, treat it with the utmost care and professionalism, making every effort to protect its confidentiality and integrity. Don't divulge such information to unintended parties and never leave items (both hard copy and electronic media) unattended in public at any time (i.e., coffee shops, training seminars, conferences, etc.).
- **Report security issues immediately.** Remember, if you see something, say something – and immediately. You have a responsibility for helping protect the organization, which means being aware of your surroundings and reporting suspicious activity to authorized personnel – immediately. From seeing a door ajar that shouldn't be to finding sensitive documents lying in a commons area, you need take action.
- **Shut down and protect your workstation.** When leaving your workstation area at the end of each day, make sure to completely shut down and turn off all computers and related devices. Additionally, pickup and store any documents, electronic media, or any business and/or professional items that should not be left unattended. Use your judgment by asking yourself the following simple question – "what risk or security danger is there for leaving something not securely locked up and put away?"

Personally, Identifiable Information (PII)
&
Information Protection

Personally, Identifiable Information (PII)

Personally, Identifiable Information (PII) has become a notable topic in information security as organizations are spending vast resources for ensuring the safety and security of such information, much of it revolving around personal consumer financial and health data. With growing cyber security threats and the ever-increasing numbers of data breaches and security compromises, protecting PII is now more important than ever. With the widespread use of technology, PII is everywhere, being stored, processed and transmitted all over the globe, at levels of efficiency once thought unimaginable. But with thousands - and counting - of PII breaches, organizations are finding themselves being constantly challenged by malicious threats, lawsuits, regulators, compliance auditors, and irate customers.

What exactly is PII?

- Any information about an individual, including (1). any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information".

Protecting Information (Hard Copy)

Call it PII or any other variant thereof – Secret, confidential, sensitive, restricted information - it all needs to be protected at all times, both physical hard-copy material and in electronic format. As for hard-copy documents, even in today's world the use of paper is still quite prevalent, thus protecting paper records in the following manner is a must:

- First and foremost, avoid printing any documentation containing PII if you can. If that's not possible, then limit it to the extent possible. Remember, paper records should only be generated, used, and/or retained if there's a true legitimate business need.
- For paper records containing PII, assign tracking and logging mechanisms as necessary for ensuring its use and whereabouts at any given time, along with assigning an approved data classification level (i.e., sensitive, secret, etc.) for such material.
- For paper records containing PII, they must be physically stored in a secure location at all times, such as locked file cabinets, office desks, or any other acceptable measure for ensuring their safety and security from unauthorized parties.
- When such records are no longer needed for business or compliance purposes (such as date retention laws, etc.), they are to be shredded and documented accordingly. This means having secure shredding bins strategically located throughout the facility, and it also means never throwing paper records containing PII - or any other sensitive and confidential company information into a garbage can without being shredded.
- Other acceptable means of destroying paper records containing PII may include, but are not limited to shredding, burning, pulping, or pulverizing the records so that PII is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
- Do not allow paper records containing PII to be viewable or accessible in general commons areas, or in an unsupervised fashion, such as residing on your desk or any other workstation | work areas while not being present.

Protecting Information (Electronic Format)

As for protecting PII in electronic format - or any other information - use your access rights granted to you specifically for legitimate business purposes, and nothing other. Logging into accounts with other employee usernames and passwords is strictly prohibited - remember - access rights to Dubai Holding system components is not a "right", it's an exclusive "privilege" granted to select employees, so act accordingly and do not abuse such privileges. More specifically, do not attempt or try to access information for which you are explicitly unauthorized to do, and do not engage in eavesdropping or snooping, such as looking up PII on customers, other employees, etc. Additionally, when displaying PII, never leave a workstation unattended as this information is now readily exposed to other parties. In short, treat someone's information the same you would want your data treated - with respect, privacy and security.

Employee Self assessment Questions and Scenarios

Employee Self assessment Questions and Scenarios

Scenario 1#

Your supervisor is very busy and asks you to log into the HR System using his/her user-ID and password to retrieve some reports. What should you do?

- A: It's your boss, so it's okay to do this.
- B: Ignore the request and hope she forgets.
- C: Decline the request and remind your supervisor that it is against DH policy.

Answer #1:

C - Decline the request and remind your supervisor that it is against DH policy.

- User-ID's and passwords must not be shared. If pressured further, report the situation to management and information security team

Scenario 2#

Dear User,

Beginning next week, we will be deleting all inactive email accounts in order to create space for more users. You are required to send the following information in order to continue using your email account. If we do not receive this information from you by the end of the week, your email account will be closed.

- Name (first and last):
- Email Login:
- Password:
- Date of birth:
- Alternate email:

Employee Self assessment Questions and Scenarios

Please contact IT Support with any questions. Thank you for your immediate attention.

What should you do?

- A: Respond and provide requested information
- B: Don't respond to email, instant messages (IM), texts, phone calls, etc., asking you for your password or other personal information. You should never disclose your password to anyone, even if they say they work for IT department

Answer #2:

B - Don't respond to email, instant messages (IM), texts, phone calls, etc., asking you for your password or other personal information. You should never disclose your password to anyone, even if they say they work for IT department.

- This email is a classic example of "phishing" – trying to trick you into "biting". They want your information.
- If you receive phishing or spam mail report using report message plugin

Employee Self assessment Questions and Scenarios

Scenario #3:

A friend sends an electronic greeting card (e-card) to your work email. You need to click on the attachment to see the card. What should you do?

- A: Click on the link and open the attachment
- B: Verify the email and click on the link to open attachment
- C: Delete the message

Answer #3:

C- Delete the message:

This one has four big risks:

1. Some attachments contain viruses or other malicious programs, so just in general, it’s risky to open unknown or unsolicited attachments.
2. Also, in some cases just clicking on a malicious link can infect a computer, so unless you are sure a link is safe, don’t click on it.
3. Email addresses can be faked, so just because the email says it is from someone you know, you can’t be certain of this without checking with the person.
4. Finally, some websites and links look legitimate, but they're really hoaxes designed to steal your information.

Employee Self assessment Questions and Scenarios

Scenario #4:

The mouse on your computer screen starts to move around on its own and click on things on your desktop.

What do you do? <Select all that apply>

- A:Call your co-workers over so they can see.
- B: Disconnect your computer from the network.
- C: Unplug your mouse.
- D: Tell your supervisor.
- E: Turn your computer off.
- F: Run anti-virus.
- G: All of the above.

Answer #4:

B & D.

- This is suspicious. Immediately report the problem to your line manager and IT support team.
- Also, since it seems possible that someone is controlling the computer remotely, it is best if you can disconnect the computer from the network (and turn off wireless if you have it) until help arrives. If possible, don't turn off the computer.

Employee Self assessment Questions and Scenarios

Scenario #5:

One of the staff member subscribes through online to several free magazines. Among the questions she was asked in order to activate her subscriptions, one magazine asked for her month of birth, a second asked for her year of birth, and a third asked for her mother's maiden name.

Question: What do you think might be going on here?

- A: All three newsletters probably have the same parent company or are distributed through the same service. The parent company or service can combine individual pieces of seemingly-harmless information and use or sell it for identity theft. It is even possible that there is a fourth newsletter that asks for day of birth as one of the activation questions.
- B: This might be for legitimate purpose

Answer #4:

A.

- Often questions about personal information are optional. In addition to being suspicious about situations like the one described here, never provide personal information when it is not legitimately necessary, or to people or companies you don’t personally know.

Employee Self assessment Questions and Scenarios

Question #1:

What can you do if you fall victim to identity theft?

- A: Inform you friend
- B: Do not inform anyone
- C: Report the incident to your line manager
- D: Report the incident to your line manager & Information security

Answer #1: D

It is extremely important to report the incident to respective authority so that they can help you further.

Question #2:

Which of the following should be included in your password?

- A: Your name & phone number
- B: Your car license plate, spells backward
- C: Your favorite football team
- D: A combination of a certain number of alphanumeric, special characters with upper and lower case

Answer #2: D

A strong password consists of a com-bination of upper- and lower-case letters, special characters and upper and lower case.

Employee Self assessment Questions and Scenarios

Question #3:

Which of the following is an example of a "phishing" attack?

- A:Sending someone an email that contains a malicious link that is disguised to look like an email from someone the person knows
- B:Creating a fake website that looks nearly identical to a real website in order to trick users into entering their login information
- C:Sending someone a text message that contains a malicious link that is disguised to look like a notification that the person has won a contest
- D. All of the above

Answer #3: D

Yes, all of them. You can even be phished over the phone.

Question #4:

What kind of cybersecurity risks can be minimized by using a Virtual Private Network (VPN)?

- A:Use of insecure Wi-Fi networks
- B:Key-logging
- C:De-anonymization by network operators
- D:Phishing attacks

Answer #4:A

Use of insecure Wi-Fi networks

Employee Self assessment Questions and Scenarios

Question #5

What is employee's responsibility in Dubai Holding information and cyber security policy?

- A. Just read the policy and do not comply
- B. Partially comply with policy
- C. Employees must confirm their compliance with security policies upon joining and on policy refreshment programs

Answer #5: C

Question #6

Which of the statement is true

- A. Use your official company account to register your personal bank
- B. Company official account can be used to register social media accounts
- C. Use your company account only for official per pose

Answer #6: C

For the Good of Tomorrow

Please visit dubaiholding.com

Email: info@dubaiholding.com
T +971 4 362 2000
F +971 4 362 2091
P.O. Box 66000
Dubai, United Arab Emirates

15 YEARS
For the Good of Tomorrow