THE
SOFTWARE
PRACTICE

ACCEPTABLE USE POLICY

Version 1.12
The Software Practice Pte Ltd

Change Log

Version	Date	Author	Remarks
1.0	8/02/2023	IT Ops	First Version
1.1	31/03/2023	IT Ops	Update on 3. Network
1.2	6/07/2023	IT Ops	Migration to Wiki
1.3	19/07/2023	IT Ops	Update on 4. Confidentiality and Integrity and updated formatting
1.4	26/07/2023	IT Ops	Tips with hyperlinks added in section 1.9 and 4.1 Name of section 4.1 changed to 'Password and Information Security'
1.5	16/08/2023	IT Ops	Move all URL links to the ‘References’ section
1.6	17/11/2023	IT Ops	Updated formatting and minor content updates
1.7	19/12/2023	IT Ops	Migration from Outline to Doks and minor content update on 3. General
1.8	8/01/2024	IT Ops	Minor content update on 3. General
1.9	16/01/2024	IT Ops	Updated References
1.10	5 Feb 2024	IT Ops	Minor content update on 6.2 Use of Data, Computers, and Portable Storage Media
1.11	27 May 2024	IT Ops	Updates on 3. General, 5. Network Security and 7. References
1.12	7 June 2024	IT Ops	Updated content on 6.1 Password and Information Security

Contents

1 Introduction

The Acceptable Use Policy outlines the security measures that all TSP staff will have to adhere to ensure strong IT security in TSP.

**Staff refers to all individuals engaged in the provision of services for TSP, including but not limited to employees, contractors, and interns, whether on a full-time or part-time basis*.

2 Scopes

This policy is applicable to the following key domains.

- General
- Use of Software Applications and Tools/Utilities
- Network
- Confidentiality and Integrity

3 General

3.1. ✅ DO use either your TSP-authorized laptops or TSP-Virtual Machines for all your work.

3.2. ✅ DO carry TSP-authorized devices (laptops, portable storage devices, etc.) as hand luggage when traveling.

- Not Applicable to ODC Staff. For ODC Staff, please refer to **TSP Asset Management – Bandung Office [1]**.

3.3. ✅ DO take good care of the TSP devices assigned to you.

You are accountable for any damage or loss of the assigned devices resulting from your lack of due care.

Report to IT Ops Team via the Youtrack TSP Helpdesk [2] immediately if the device is damaged or lost.

3.4. ✅ ALWAYS set Calendar Event's visibility as **'Private'** for events related to Project Meetings.

- The default visibility is 'Public', you would need to change it to **'Private'** to ensure meeting agendas are not visible to anyone outside of your project.

3.5. ❌ DO NOT let others use your TSP-authorized devices.

Report all IT security incidents immediately to the IT Ops Team and the Management via the Youtrack TSP Helpdesk [2].
For example, phishing attempts, malware attacks, and theft / loss of laptops / mobile phones.

3.6. ❌ DO NOT use any cloud service for synchronizing other than TSP's Microsoft OneDrive or TSP's Google Drive.

3.7. ❌ DO NOT share company's and client's personal information with external parties without permission from the Management.

3.8. ❌ DO NOT work on TSP projects from a public location e.g., cafes, libraries, etc.

3.9. ❌ DO NOT leave confidential material on printers or photocopiers.

4 Use of Software Applications and Tools / Utilities

4.1. ❌ DO NOT run software from untrusted sources.

- ✅ DO request access to third-party software by submitting a ticket via the **YouTrack TSP Helpdesk [2]**. Software applications that do not require approval are Zoom, Teams, Meet.
- ❌ DO NOT download, install, or run third-party software from the internet, without prior approval from IT Ops Team. (This is more relevant for non-developers).

4.2. ❌ DO NOT upload code to any code hosting service (github.com, gitlab.com, etc.) other than official TSP git repositories.

- ✅ DO inform IT Ops Team immediately if any code has been uploaded.
- ✅ ALWAYS use TSP's services only e.g., TSP's Gitlab, TSP's Google Drive, TSP's Microsoft OneDrive, etc. If you are unsure if a type of service belongs to TSP or is authorized by TSP for usage, confirm with IT Ops Team before using it.

4.3. ❌ DO NOT use online tools/utilities for splitting and/or merging PDF files, etc. for any document that belongs to TSP or TSP's project. In general, do not use online tools/utilities. DO reach out to Dev team or PMO team for recommendations.

- ❌ DO NOT use online tools/utilities for processing data/code e.g., do not use online JSON serialisers or code prettifiers. Use DevToys or equivalent that runs locally.
- There are many open-source and command-line options for such use cases. When in doubt, you can google and share the best options you found with Dev team who can give you advice.

4.4. ❌ DO NOT use online tools/utilities for notetaking, project management, task management, e.g., Trello, Notion, Asana, etc.

- ✅ DO use OneNote from your Microsoft 365 account for notetaking.
- ✅ DO use our issue trackers for project management. You might find the above less convenient; however, we should not place any work we do for our clients into these online tools/utilities.

4.5. ❌ DO NOT use screenshots or screen-recording services that automatically upload a copy online.

- ✅ DO configure Xbox game bar for local usage only. For screen recording, press Windows + G (on Windows) to bring up the Xbox game bar.
- For screenshots, press Windows + Shift + S to bring up Windows Snipping tool.

5 Network Security

5.1. ✅ DO use strong and secure passwords for your home’s WIFI network especially when you connect your laptops with TSP information to your home’s WIFI network.

- ❌ DO NOT perform any port scanning or any security scanning on TSP resources.
- Note: This is not applicable to ODC Staff.

5.2. ❌ DO NOT use BitTorrent, Onion, and I2P networking protocols on your TSP laptops or on TSP’s network.

- Users with TSP laptops or TSP Virtual Machines (VM) are prohibited from using BitTorrent clients on their laptops.
- Users logged into any VPN provided by TSP are prohibited from using BitTorrent clients when connected to TSP VPN.

5.3. ❌ DO NOT connect any non-TSP authorized device to TSP network or IT Systems.

5.4. ❌ DO NOT allow guests to connect TSP network:

- ✅ DO request guests to use their own hotspot.
- ❌ DO NOT allow them to use TSP network via Ethernet cables.

- ❌ DO NOT share TSP Wi-Fi passwords to guests.

5.5. ❌ DO NOT use commercial or third-party VPN to access TSP network or IT Systems e.g., Mullvad, Nord VPN, PIA etc.

- ✅ DO only use VPN provided by TSP.
- TSP VPN should only be installed on a TSP-authorized laptop or TSP Virtual Machine.

5.6. ❌ DO NOT use free public Wi-Fi networks on TSP-authorized devices.

6 Confidentiality and Integrity

6.1 Password and Information Security

- ✅ DO keep all secrets, keys, or passwords on Bitwarden
    - ✅ DO set Bitwarden to automatically clear the clipboard 1 minute after copying the password. Refer to **Bitwarden Guideline [3]** for further instructions.
    - ✅ DO use **YouTrack TSP Helpdesk [2]** to request if you do not have a Bitwarden account.
- ✅ DO use secure and strong passwords.
    - ✅ DO use Bitwarden password auto generator.
    - ✅ DO ensure passwords are at least 16 characters in length.
    - ✅ DO ensure that Passwords should be comprised of a mix of letters, numbers, and symbols (at least 2 each).
    - ❌ DO NOT reuse any password.
    - ❌ DO NOT use personal information in passwords e.g., birthdays, names etc.
- ✅ DO ensure files (MS Word, MS Excel etc) with personal data or sensitive information are password protected.
- ✅ DO remove any personal data from documents if it is not required.
- ✅ DO use Multi-Factor Authentication, whenever possible, especially for **Google Account [4]**, **Microsoft Account [5]**, and **Bitwarden Account [6]**.
- ✅ DO ensure laptops, mobile devices, and desktop computers are protected by:
    - Using a lock-screen password of at least 8 characters in length.
    - Enabling auto lock after 10 minutes of inactivity.
- ❌ DO NOT allow others to access your accounts (GitLab, VPN, Google Accounts, etc.) without explicit clearance from Management.
- ❌ DO NOT share any confidential information or passwords in plaintext with anyone or on Google Chat/Email or any other communication channels.

- ❌ DO NOT store passwords in plain text anywhere i.e., should not write down passwords on your notes or paste the passwords on your laptops.
- ❌ DO NOT use any browser extension password managers e.g., Google, Firefox, etc., including Bitwarden browser extension to store or access your passwords. (Only use web-based or desktop versions of Bitwarden).

Check out about Password Security [7] for more information.

- ❌ DO NOT send passwords in plain text via email / Google Chat or any other communication channels.
    - ✅ DO use Bitwarden to securely store and share passwords.
- ❌ DO NOT share passwords with anyone (including your TSP colleagues) without explicit approval from the Management.

6.2 Use of Data, Computers, and Portable Storage Media.

- ✅ ALWAYS lock all devices that contain data pertaining to projects, financial information, organizational information, and personnel information when you step away from your laptops.
- ✅ ALWAYS enable disk encryption on TSP-authorized portable and non-portable devices.
    - ✅ DO use BitLocker if you are using Windows. If you don't have Windows Pro, please submit a ticket via the **YouTrack TSP Helpdesk [2]** to request.
- ✅ DO use Windows Defender as your anti-virus software for TSP VMs and TSP-authorized Laptops.
    - ✅ DO perform continuous and/or schedule full system scanning. If you use Windows, this can be done with Windows Defender.
    - ✅ DO ensure Windows Defender is updated regularly. DO ensure to schedule automatic updates.
    - ✅ DO ensure Windows Defender is always operating in real-time scan mode. Please refer to this **Windows Security Guideline [8]** for further instructions.
- ✅ ALWAYS enable the built-in firewall in your computer – contact IT Ops Team if you need help with this.
- Follow the steps below before sharing any TSP data with any internal or external party:
    - ✅ ALWAYS get permission to transfer data to an internal or external party – this will be Project Manager / Management – if in doubt, use the highest escalation level or contact IT Ops Team.
    - ✅ DO use TLS/SSL encryption to transmit the data to an internal or external party e.g., HTTPS, SSH, SCP, and VPN.
    - ✅ DO share files e.g., Word Documents, Google Docs, Excel, Google Sheets via Google Drive's "share" options or emails.
        - ✅ DO ensure to give access to the file only to the person who needs it.

        - ✅ ALWAYS set access to “Restricted” under **General Access** when sharing files using the Google workspace with people who need access.
    - ✅ DO password-protect sensitive documents in non-Microsoft (MS) Office file format using 7zip or similar tools.
    - ❌ DO NOT send passwords in the same email where password-protected files are attached.
    - ❌ DO NOT use HTTP, FTP, and Telnet protocols to transfer data.
- ✅ DO check for vendor security updates (e.g., Adobe, Windows) and apply them.

    Occasionally, vulnerabilities in the operating system and/or application's security are discovered, and the vendor will then release security updates to fix these vulnerabilities.

- ✅ DO ensure the major operating systems’ e.g., Windows and Mac auto-update mechanisms are enabled.
- ❌ DO NOT share TSP and clients' personal information with external parties without explicit permission from Management.
- ❌ DO NOT use someone else’s username and password to access the TSP IT System.
- ❌ DO NOT store any TSP data on non-TSP-authorized devices.
- ❌ DO NOT give or transfer TSP data, software, or software licenses to any person or organization without approval from Management.
- ❌ DO NOT share any code you write with anyone outside your project team.
- ❌ DO NOT share any code in any cloud service for synchronizing e.g., Dropbox, Microsoft OneDrive, etc. This applies to all documents and data belonging to TSP.
- ❌ DO NOT share codes anywhere e.g., in Stack Overflow to get answers, GitHub Gists, online code-editors such as repl.it etc.
- ❌ DO NOT mention any specific details of the projects, client names, etc., anywhere online.

6.3 For Internet Access and Email / Other Communications

- ❌ DO NOT click or open unexpected or suspicious emails or email attachments.
- ❌ DO NOT forward messages containing general appeals or warnings like virus warnings, or request for help, by mass mail or otherwise. For example, be careful with forwarding emails that include files with .exe or .dll extensions.
- ❌ DO NOT send confidential data/information via commercial messaging platforms (e.g., WhatsApp, Signal, Telegram etc).
- ❌ DO NOT send TSP-related documents/files via personal email/personal devices.

6.4 Actions upon Termination of Contract

- All TSP-authorized devices must be returned to TSP at the termination of the contract, i.e., on the last day at work.
- All TSP data or intellectual property developed or gained during the period of employment remains the property of TSP and must not be retained beyond the termination or reused for other purposes.

At the end of your contract, please delete all TSP related code/folders/files from your laptops/computers.

6.5 Compliance

- All TSP personnel shall be compliant with the following regulatory requirements:
    - Personal Data Protection Act 2012.
    - Computer Misuse Act 1993.

7 References

[1] TSP Asset Management – Bandung Office > https://wiki.tsp.sg/docs/policies/tsp-assets-storage-management-bandung-office/

[2] YouTrack TSP Helpdesk > https://youtrack.tsp.dev/form/c5fe35f0-0c20-4636-abb6-d8c53929b11f

[3] Bitwarden - Clearing Clipboards > https://docs.google.com/presentation/d/1UfPh-_jrA05fs13KiU5sYQufp_ffhOVfSOm-Ox8vO40/preview?slide=id.g28d600eef7c_0_5

[4] Google Multi Factor Authentication Guideline > https://wiki.tsp.sg/docs/it/file-sharing/multi-factor-authentication/google-multi-factor-authentication/

[5] Microsoft Multi Factor Authentication Guideline > https://wiki.tsp.sg/docs/it/file-sharing/multi-factor-authentication/microsoft-multi-factor-authentication/

[6] Bitwarden Multi Factor Authentication Guideline > https://wiki.tsp.sg/docs/it/file-sharing/multi-factor-authentication/bitwarden-multi-factor-authentication/

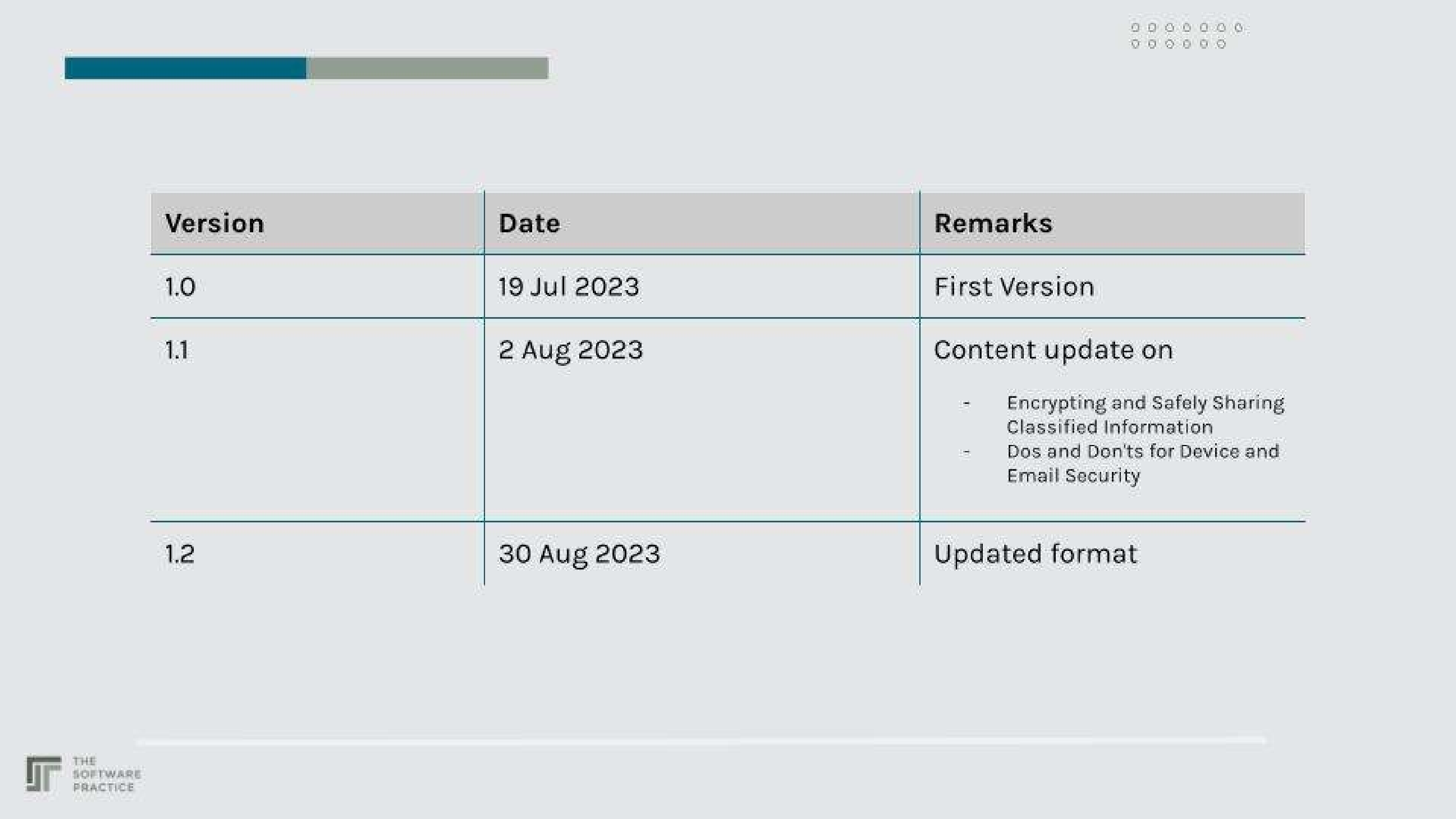
[7] Password Security Guideline > https://wiki.tsp.sg/docs/it/references/password-security/

[8] Windows Security Guideline > https://wiki.tsp.sg/docs/it/security/windows-security/

Annex A

THE SOFTWARE PRACTICE

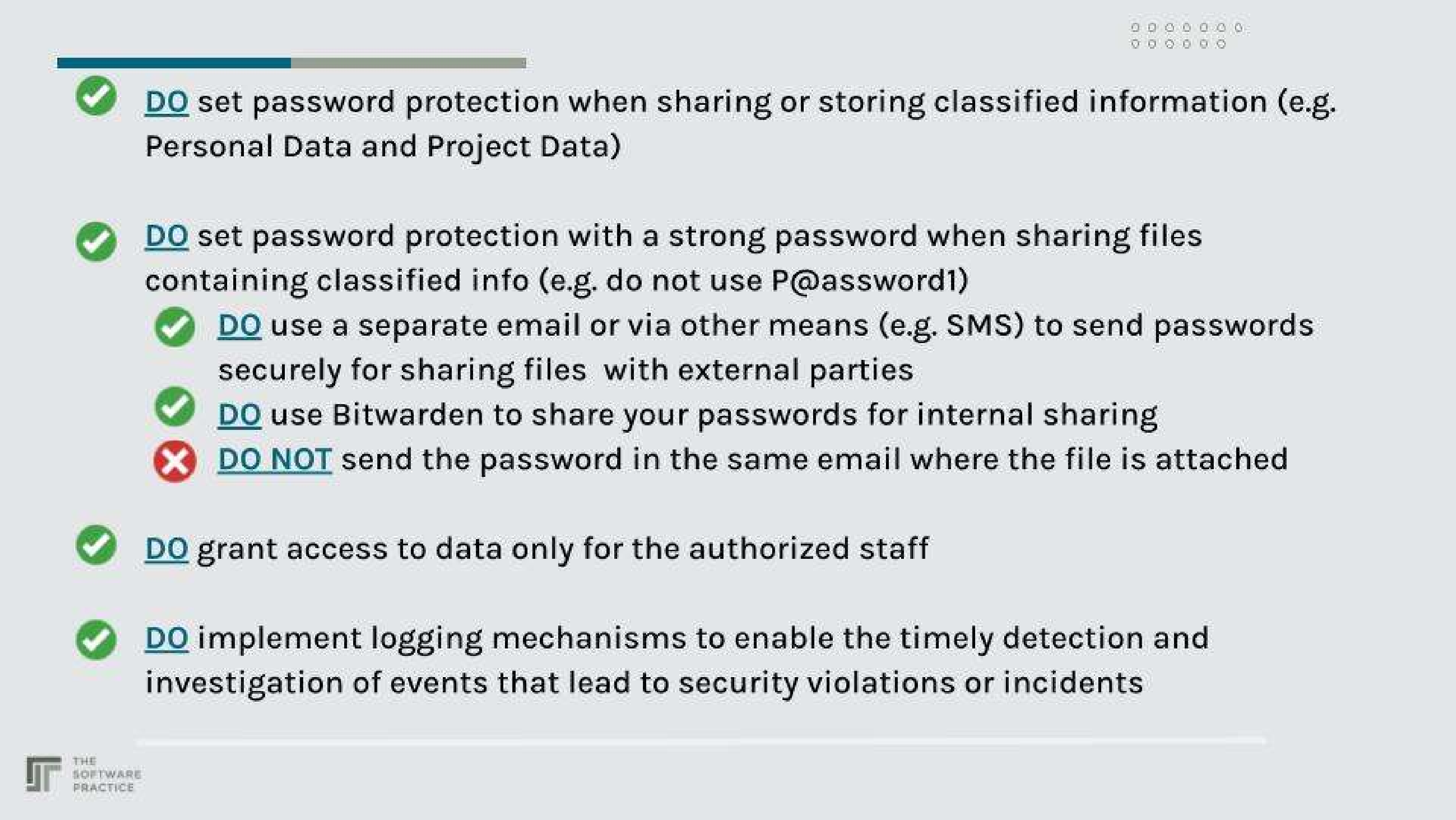
Information Security



Version	Date	Remarks
1.0	19 Jul 2023	First Version
1.1	2 Aug 2023	Content update on - Encrypting and Safely Sharing Classified Information - Dos and Don'ts for Device and Email Security
1.2	30 Aug 2023	Updated format

Securing and Safely Sharing Classified Information

THE
SOFTWARE
PRACTICE



- ✓ DO set password protection when sharing or storing classified information (e.g. Personal Data and Project Data)

- ✓ DO set password protection with a strong password when sharing files containing classified info (e.g. do not use P@assword1)
  - ✓ DO use a separate email or via other means (e.g. SMS) to send passwords securely for sharing files with external parties
  - ✓ DO use Bitwarden to share your passwords for internal sharing
  - ✗ DO NOT send the password in the same email where the file is attached

- ✓ DO grant access to data only for the authorized staff

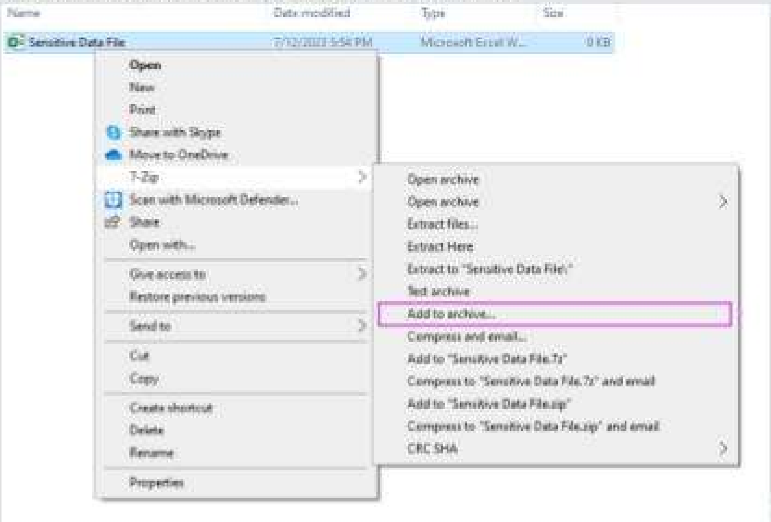
- ✓ DO implement logging mechanisms to enable the timely detection and investigation of events that lead to security violations or incidents

- **Password protect document in Non-Microsoft (MS) Office file format**

  7zip is a free tool that can be used to protect any general document and it would be made available to all government laptops. All attachments with sensitive information need to be password protected

Steps 1:

Right click on the file that you want to password protect and select "Add to archive"



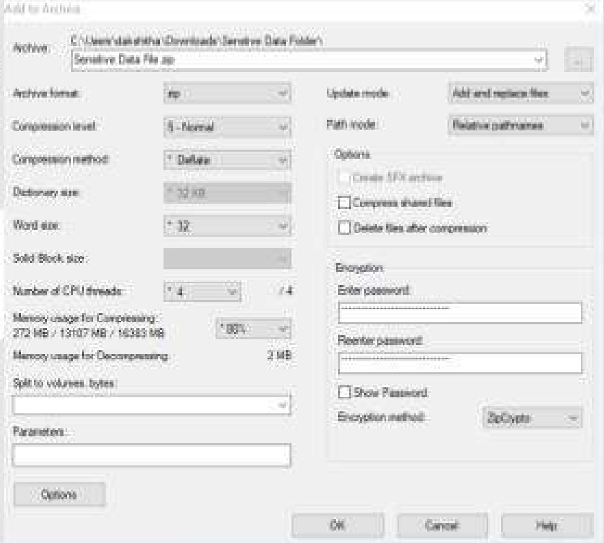
Name	Date modified	Type	Size
Sensitive Data File	7/12/2023 5:54 PM	Microsoft Excel W...	0 KB

Open
New
Print
Share with Skype
Move to OneDrive
7-Zip
Scan with Microsoft Defender...
Share
Open with...
Give access to
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
Open archive
Open archive
Extract files...
Extract Here
Extract to "Sensitive Data File\"
Test archive
Add to archive...
Compress and email...
Add to "Sensitive Data File.7z"
Compress to "Sensitive Data File.7z" and email
Add to "Sensitive Data File.zip"
Compress to "Sensitive Data File.zip" and email
CRC SHA

Steps 2:

Enter the password and click "OK".

By default, the file would be saved in a zip format



Add to Archive

Archive: C:\Users\dakshitha\Downloads\Sensitive Data Folder\
Sensitive Data File.zip

Archive format: zip
Compression level: 5 - Normal
Compression method: * Deflate
Dictionary size: * 32 KB
Word size: * 32
Solid Block size:
Number of CPU threads: * 4 / 4
Memory usage for Compressing: 272 MB / 13107 MB / 16383 MB * 80%
Memory usage for Decompressing: 2 MB
Split to volumes, bytes:
Parameters:

Update mode: Add and replace files
Path mode: Relative pathnames

Options
□ Create SFX archive
□ Compress shared files
□ Delete files after compression

Encryption
Enter password: ••••••••••••••••••••
Reenter password: ••••••••••••••••••••
□ Show Password
Encryption method: ZipCrypto

THE SOFTWARE PRACTICE

- **When sharing documents with sensitive data**

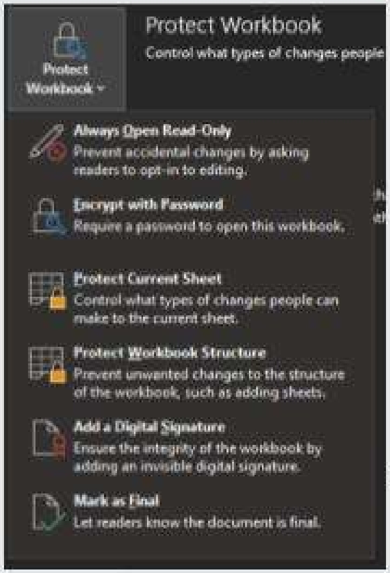
  To protect the integrity of the data in the document, you will need to digitally sign documents which contain sensitive information when you are sharing them, to ensure that they have not been modified.

  All documents that have sensitive data need to be password protected

Steps 1:

Click on Add Digital Signing:

- File Tab >> Info >> Protect Document, Protect Workbook or Protect Presentation



Always Open Read-Only
Prevent accidental changes by asking readers to opt-in to editing.

Encrypt with Password
Require a password to open this workbook.

Protect Current Sheet
Control what types of changes people can make to the current sheet.

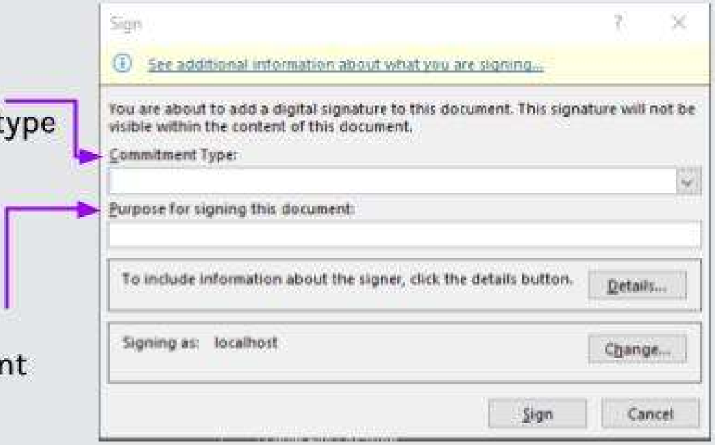
Protect Workbook Structure
Prevent unwanted changes to the structure of the workbook, such as adding sheets.

Add a Digital Signature
Ensure the integrity of the workbook by adding an invisible digital signature.

Mark as Final
Let readers know the document is final.

Steps 2:

Choose the appropriate commitment type



You are about to add a digital signature to this document. This signature will not be visible within the content of this document.

Commitment Type:

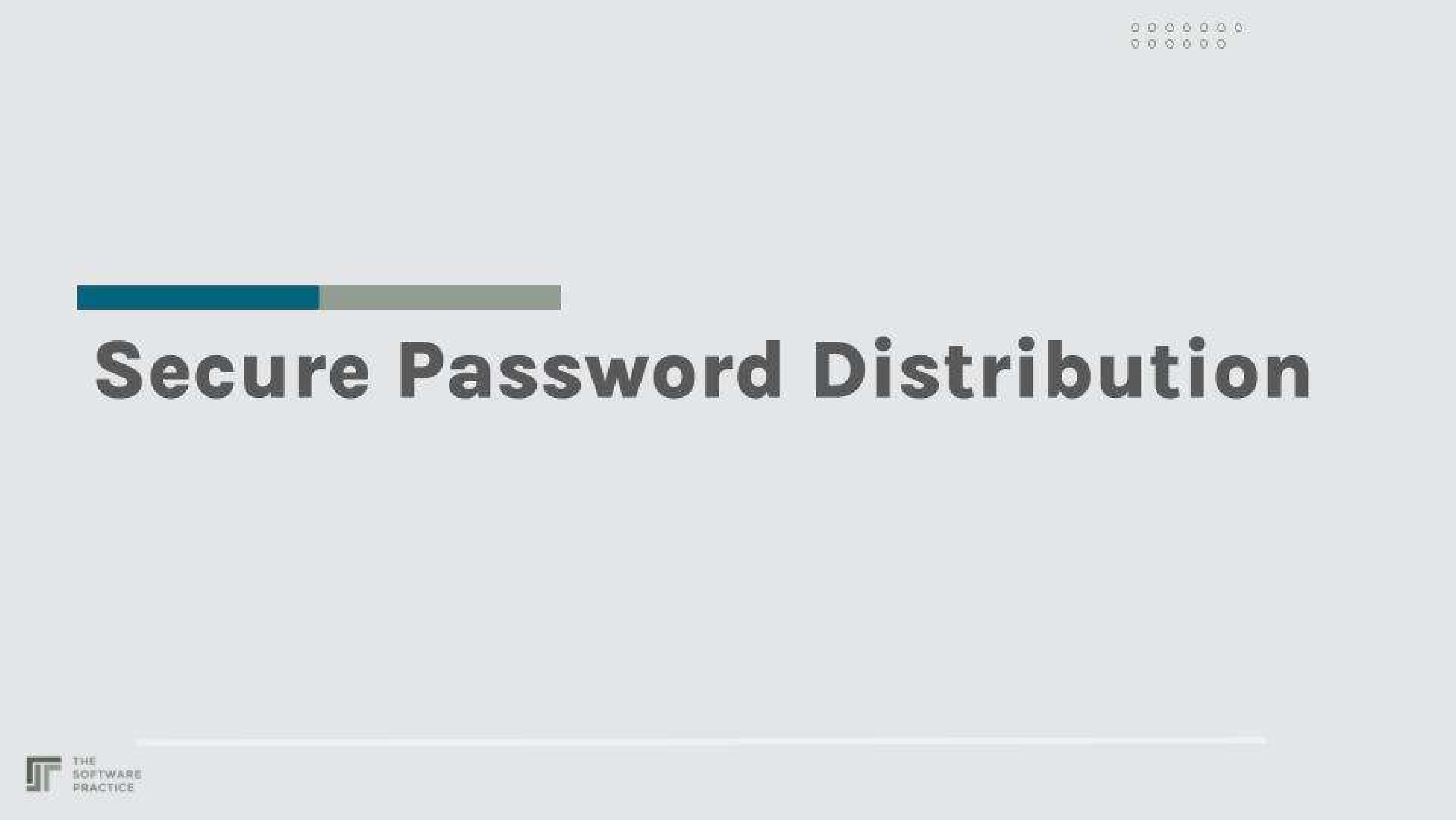
Purpose for signing this document:

To include information about the signer, click the details button.

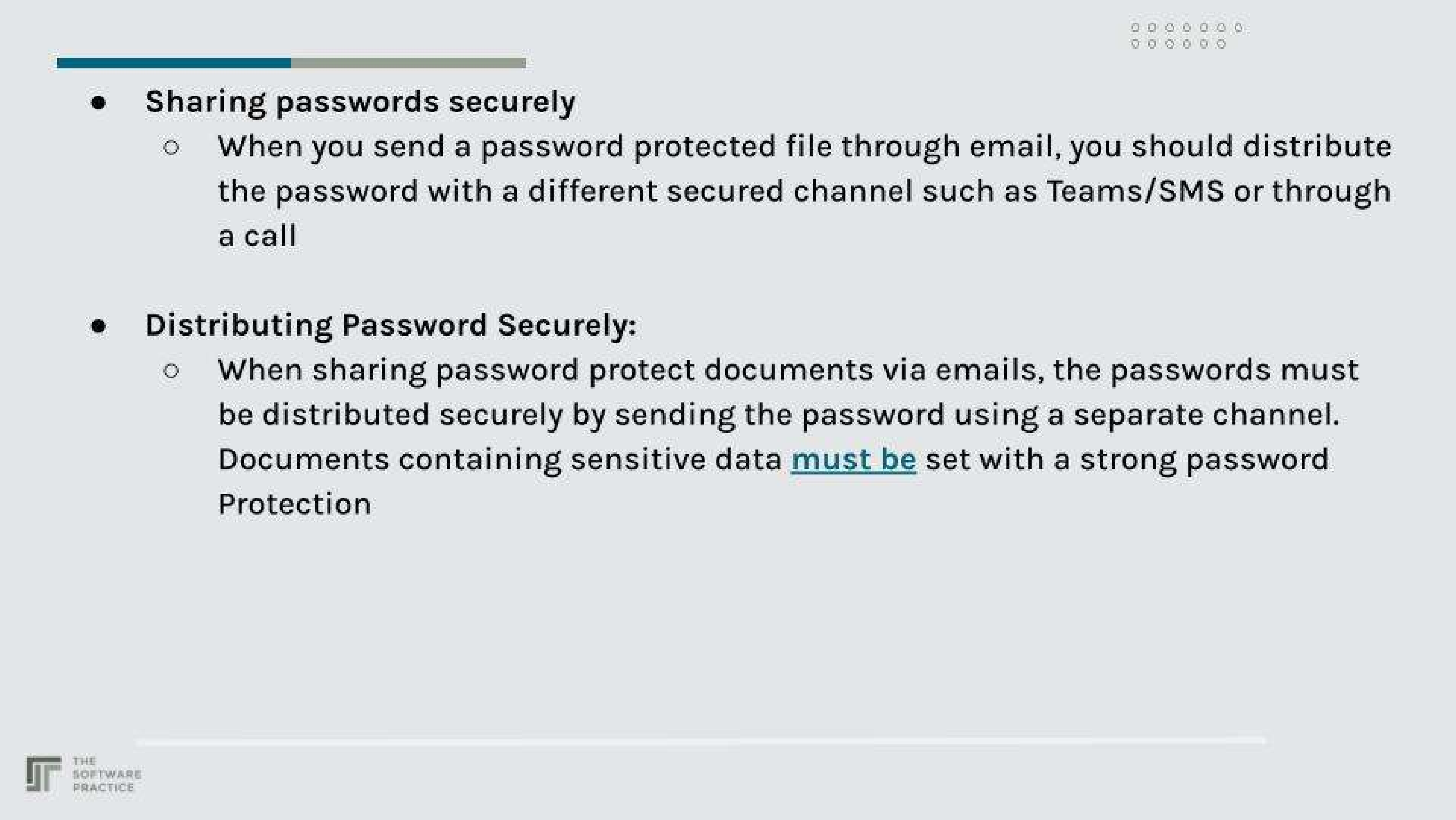
Signing as: localhost

Steps 3:

Input purpose for signing this document



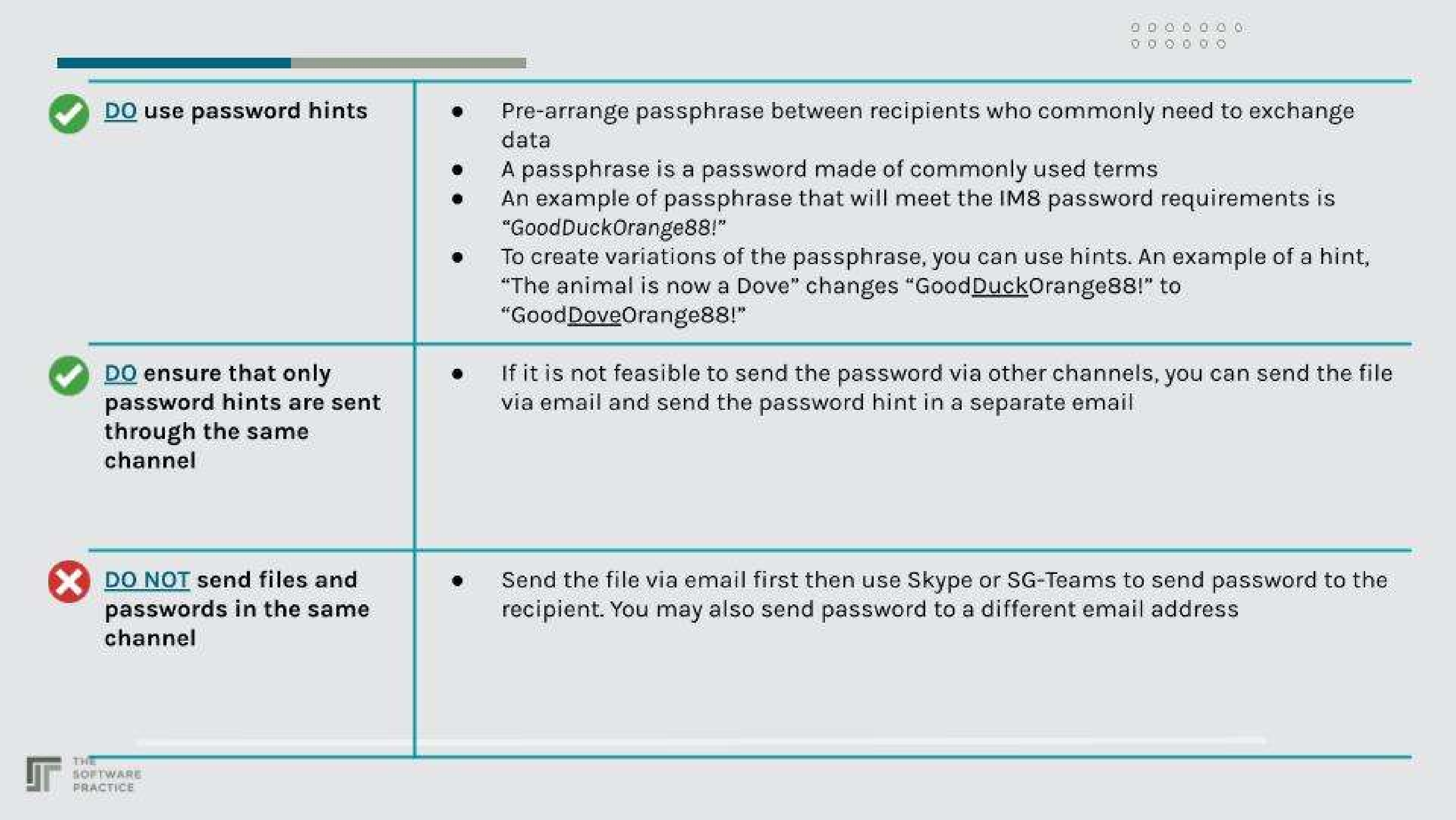
Secure Password Distribution



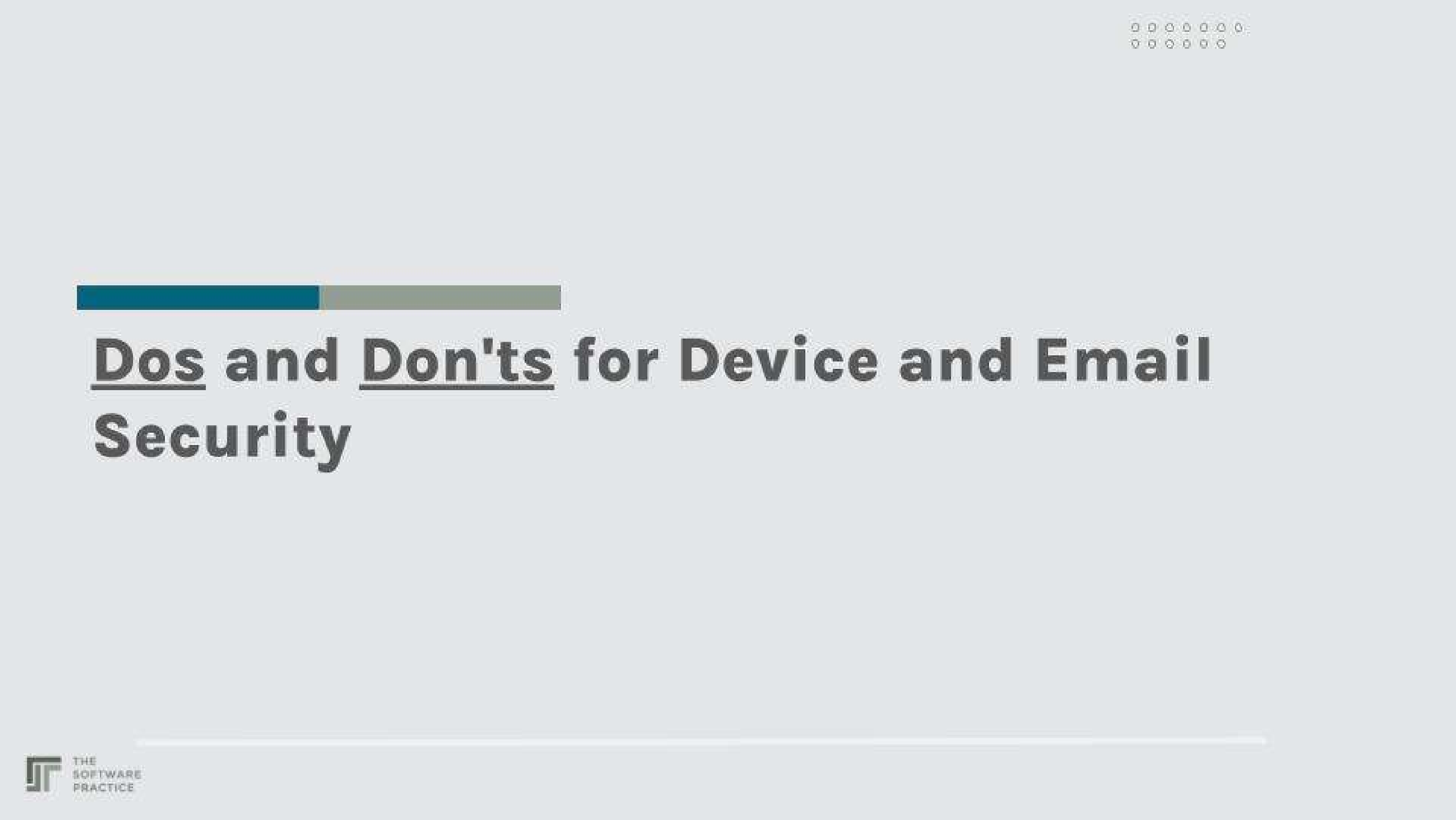
- **Sharing passwords securely**
  - When you send a password protected file through email, you should distribute the password with a different secured channel such as Teams/SMS or through a call

- **Distributing Password Securely:**
  - When sharing password protect documents via emails, the passwords must be distributed securely by sending the password using a separate channel. Documents containing sensitive data must be set with a strong password Protection

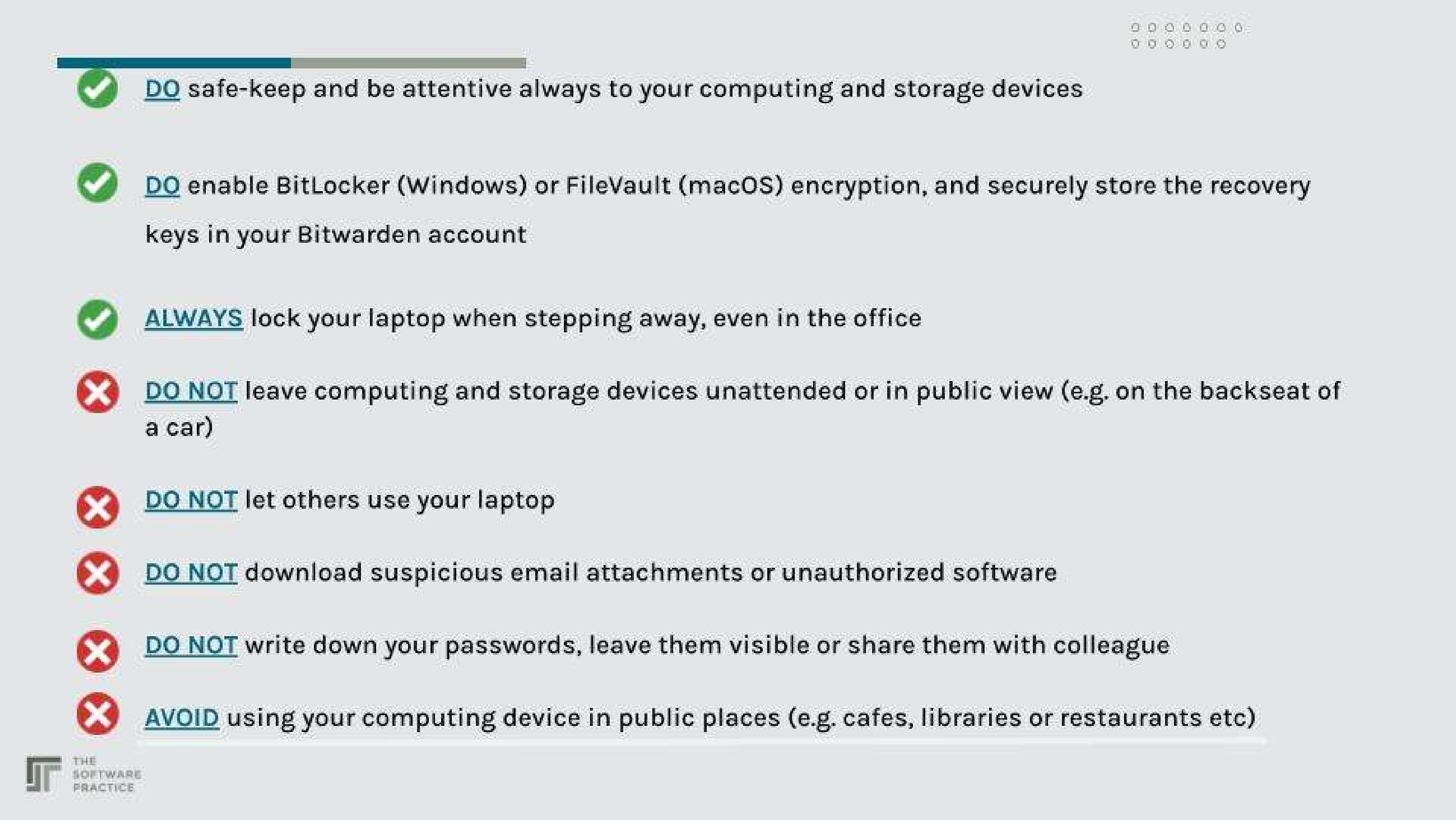
Leveraging Password Hints



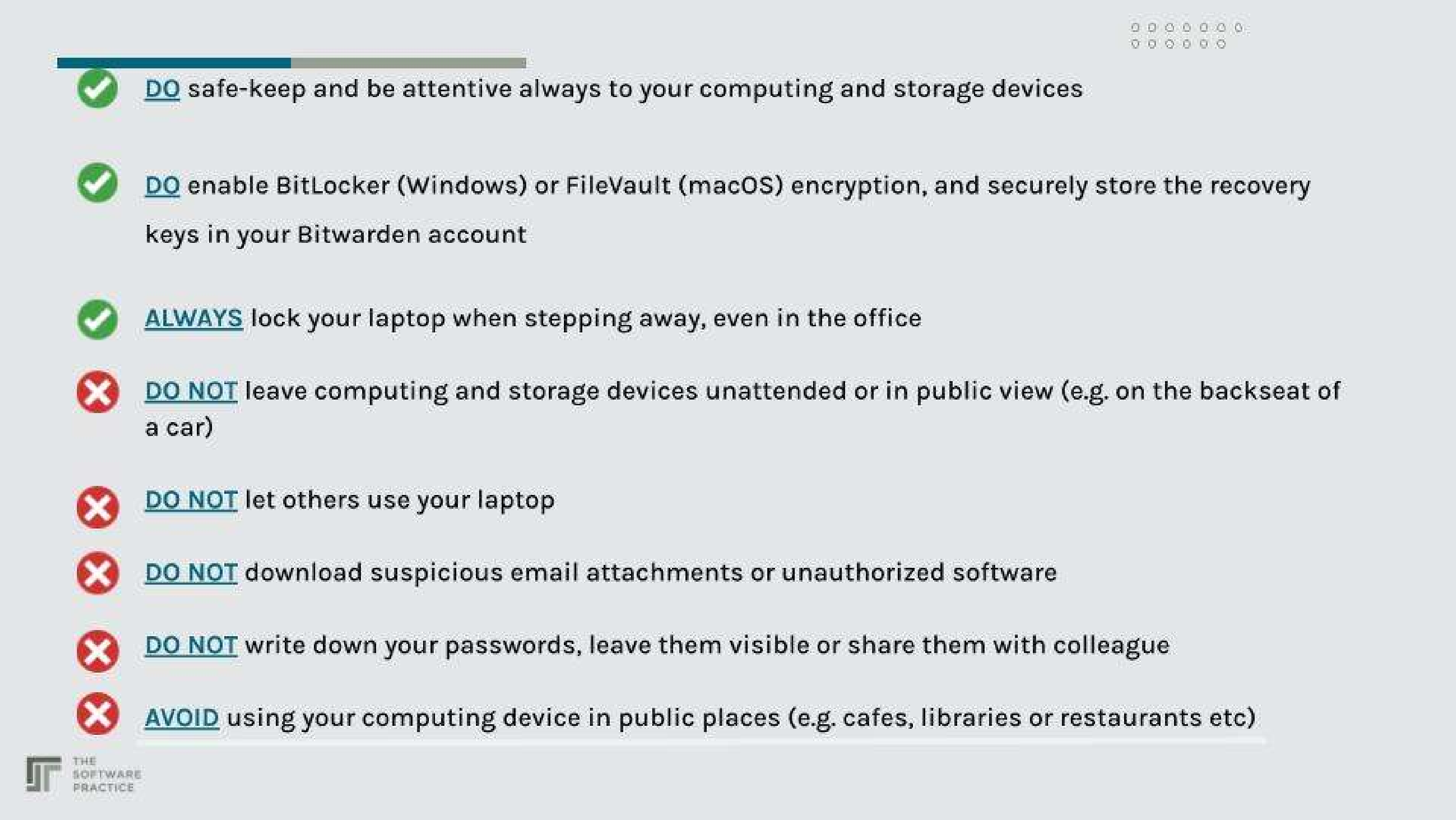
✓ **DO use password hints**	● Pre-arrange passphrase between recipients who commonly need to exchange data ● A passphrase is a password made of commonly used terms ● An example of passphrase that will meet the IM8 password requirements is *"GoodDuckOrange88!"* ● To create variations of the passphrase, you can use hints. An example of a hint, "The animal is now a Dove" changes "GoodDuckOrange88!" to "GoodDoveOrange88!"
✓ **DO ensure that only password hints are sent through the same channel**	● If it is not feasible to send the password via other channels, you can send the file via email and send the password hint in a separate email
✗ **DO NOT send files and passwords in the same channel**	● Send the file via email first then use Skype or SG-Teams to send password to the recipient. You may also send password to a different email address



Dos and Don'ts for Device and Email Security

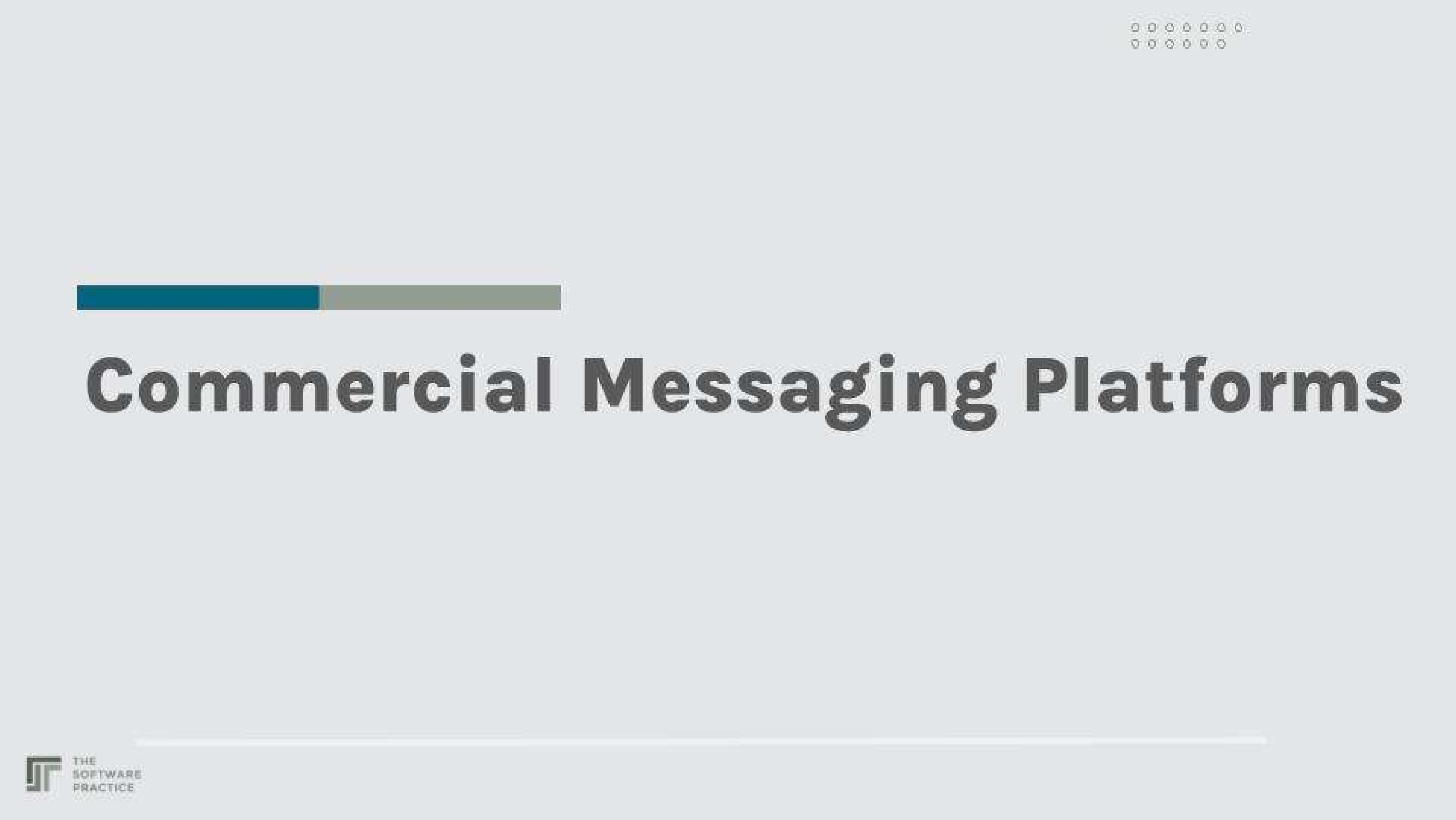


- ✓ DO safe-keep and be attentive always to your computing and storage devices
- ✓ DO enable BitLocker (Windows) or FileVault (macOS) encryption, and securely store the recovery keys in your Bitwarden account
- ✓ ALWAYS lock your laptop when stepping away, even in the office
- ✗ DO NOT leave computing and storage devices unattended or in public view (e.g. on the backseat of a car)
- ✗ DO NOT let others use your laptop
- ✗ DO NOT download suspicious email attachments or unauthorized software
- ✗ DO NOT write down your passwords, leave them visible or share them with colleague
- ✗ AVOID using your computing device in public places (e.g. cafes, libraries or restaurants etc)



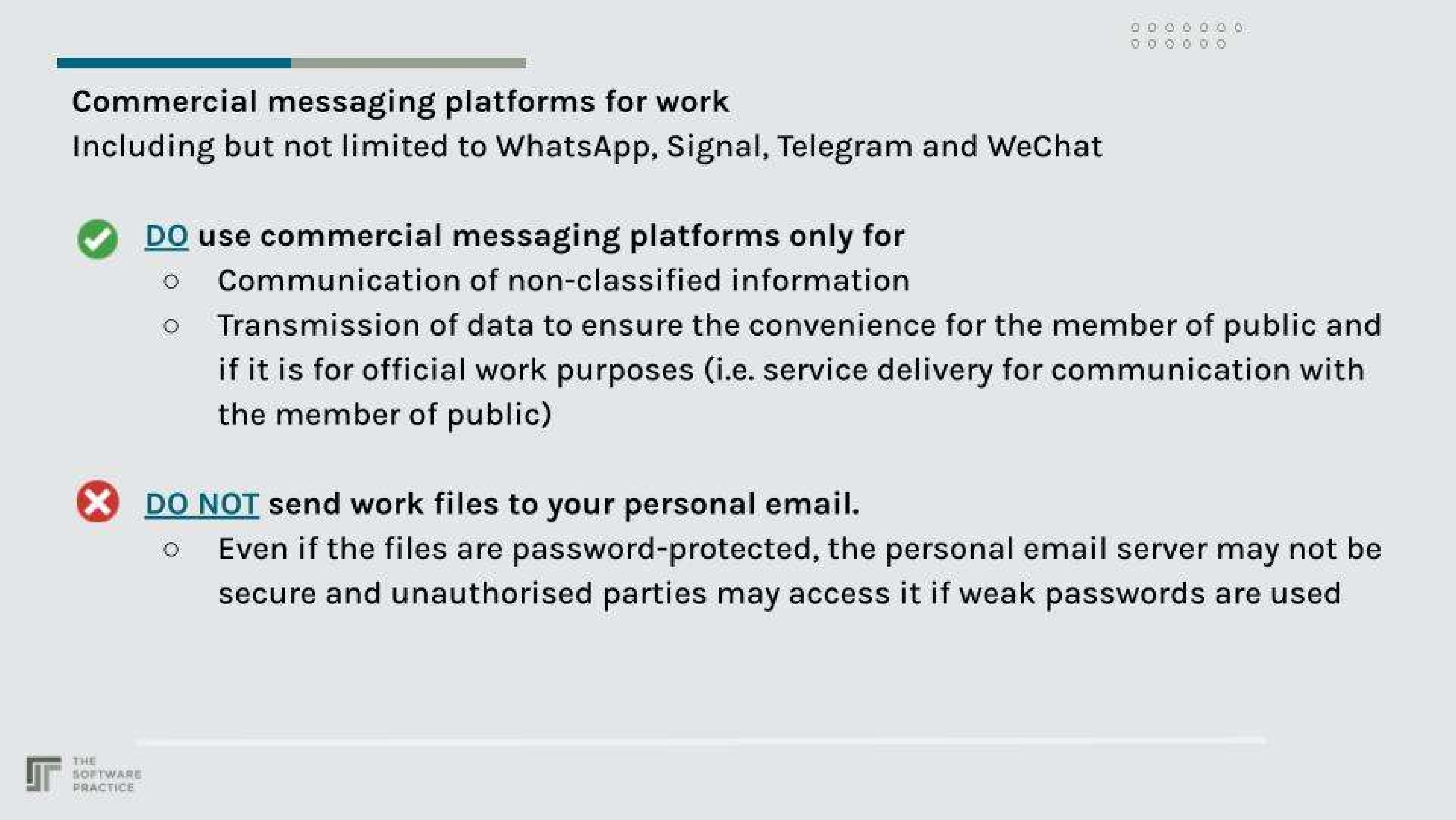
- ✓ DO safe-keep and be attentive always to your computing and storage devices
- ✓ DO enable BitLocker (Windows) or FileVault (macOS) encryption, and securely store the recovery keys in your Bitwarden account
- ✓ ALWAYS lock your laptop when stepping away, even in the office
- ✗ DO NOT leave computing and storage devices unattended or in public view (e.g. on the backseat of a car)
- ✗ DO NOT let others use your laptop
- ✗ DO NOT download suspicious email attachments or unauthorized software
- ✗ DO NOT write down your passwords, leave them visible or share them with colleague
- ✗ AVOID using your computing device in public places (e.g. cafes, libraries or restaurants etc)

THE SOFTWARE PRACTICE



Commercial Messaging Platforms

THE SOFTWARE PRACTICE



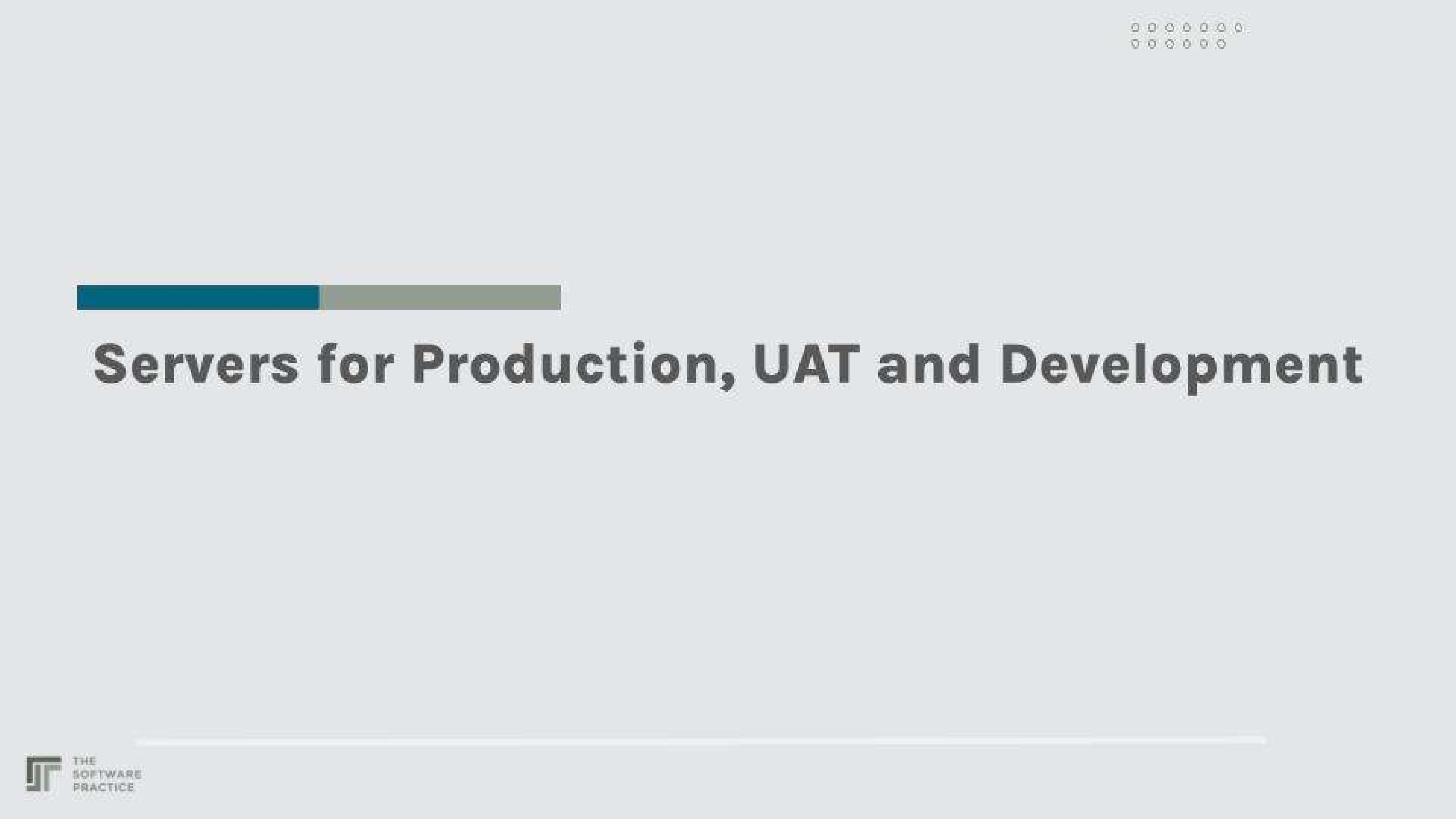
Commercial messaging platforms for work
Including but not limited to WhatsApp, Signal, Telegram and WeChat

✓ **DO use commercial messaging platforms only for**

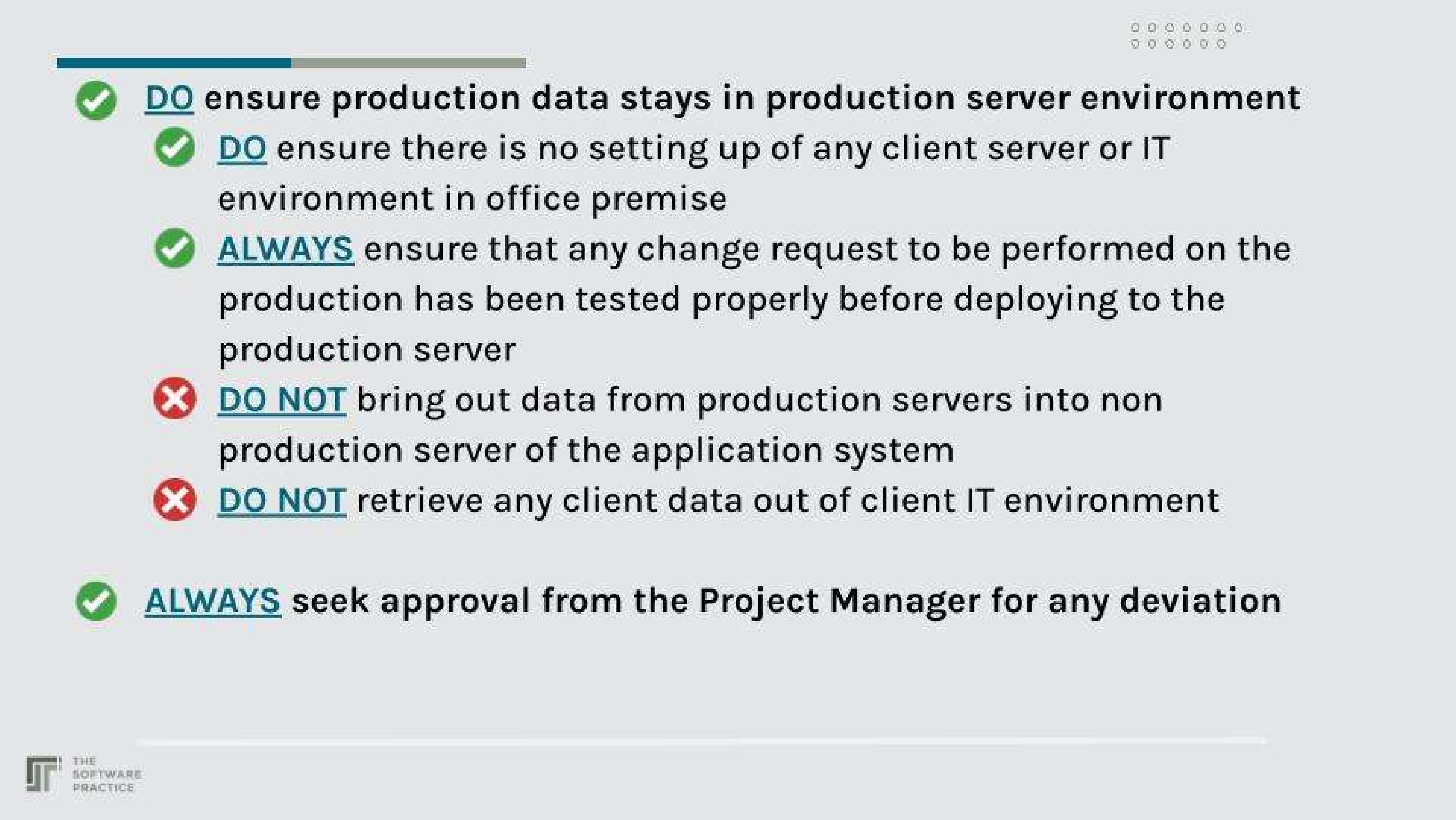
- Communication of non-classified information
- Transmission of data to ensure the convenience for the member of public and if it is for official work purposes (i.e. service delivery for communication with the member of public)

✗ **DO NOT send work files to your personal email.**

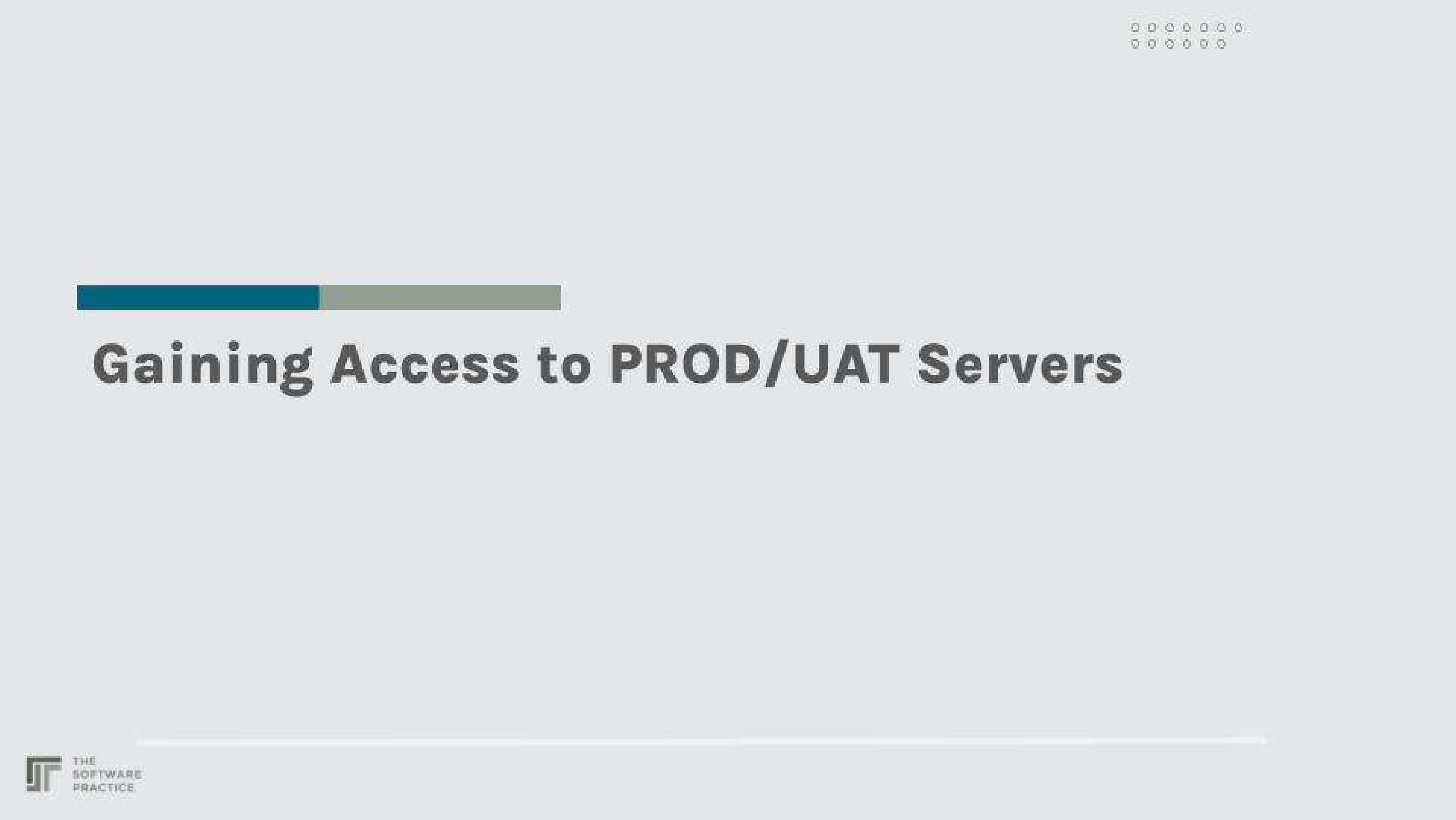
- Even if the files are password-protected, the personal email server may not be secure and unauthorised parties may access it if weak passwords are used



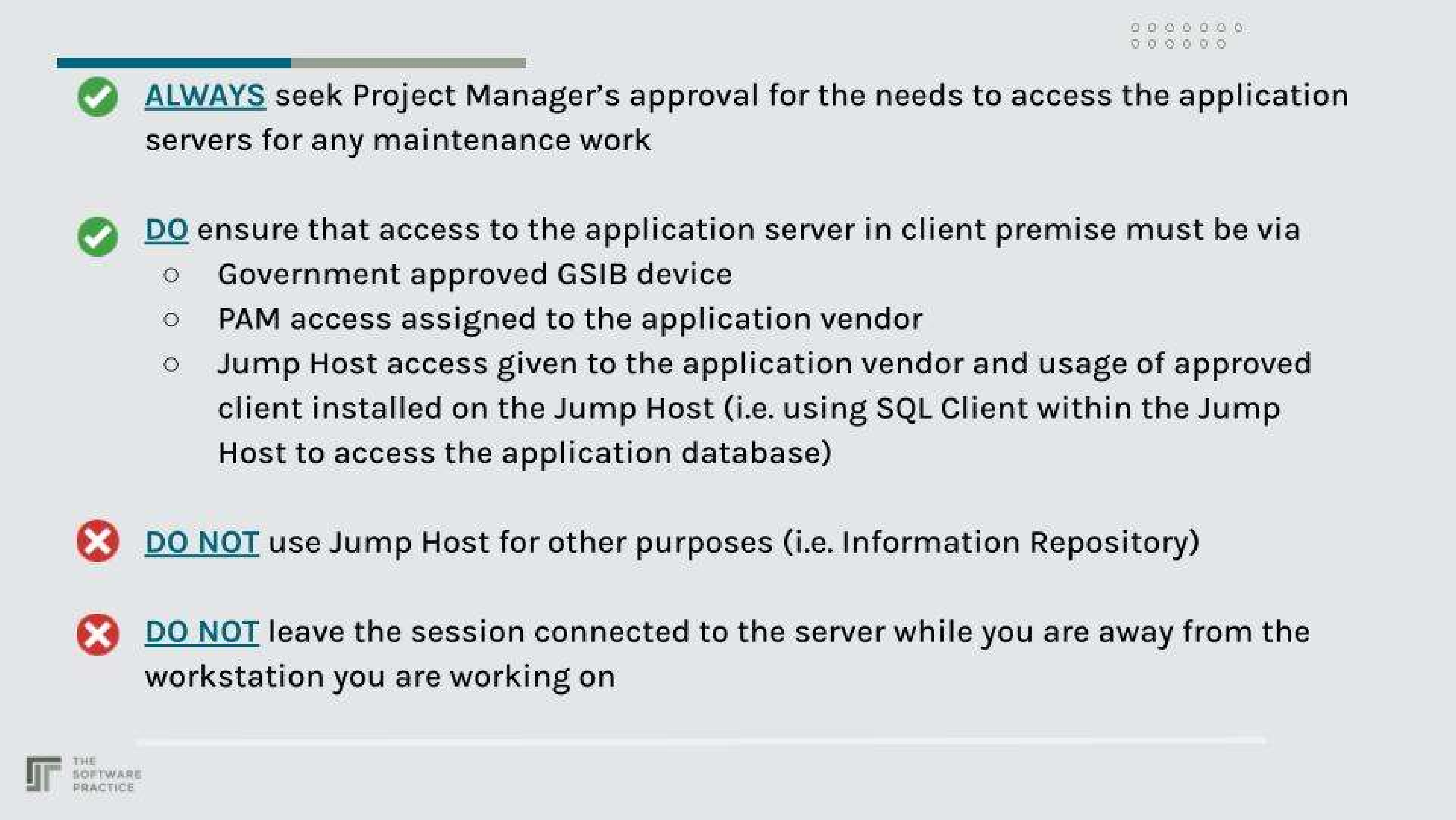
Servers for Production, UAT and Development



- ✓ DO ensure production data stays in production server environment
  - ✓ DO ensure there is no setting up of any client server or IT environment in office premise
  - ✓ ALWAYS ensure that any change request to be performed on the production has been tested properly before deploying to the production server
  - ✗ DO NOT bring out data from production servers into non production server of the application system
  - ✗ DO NOT retrieve any client data out of client IT environment
- ✓ ALWAYS seek approval from the Project Manager for any deviation



Gaining Access to PROD/UAT Servers



✅ ALWAYS seek Project Manager's approval for the needs to access the application servers for any maintenance work

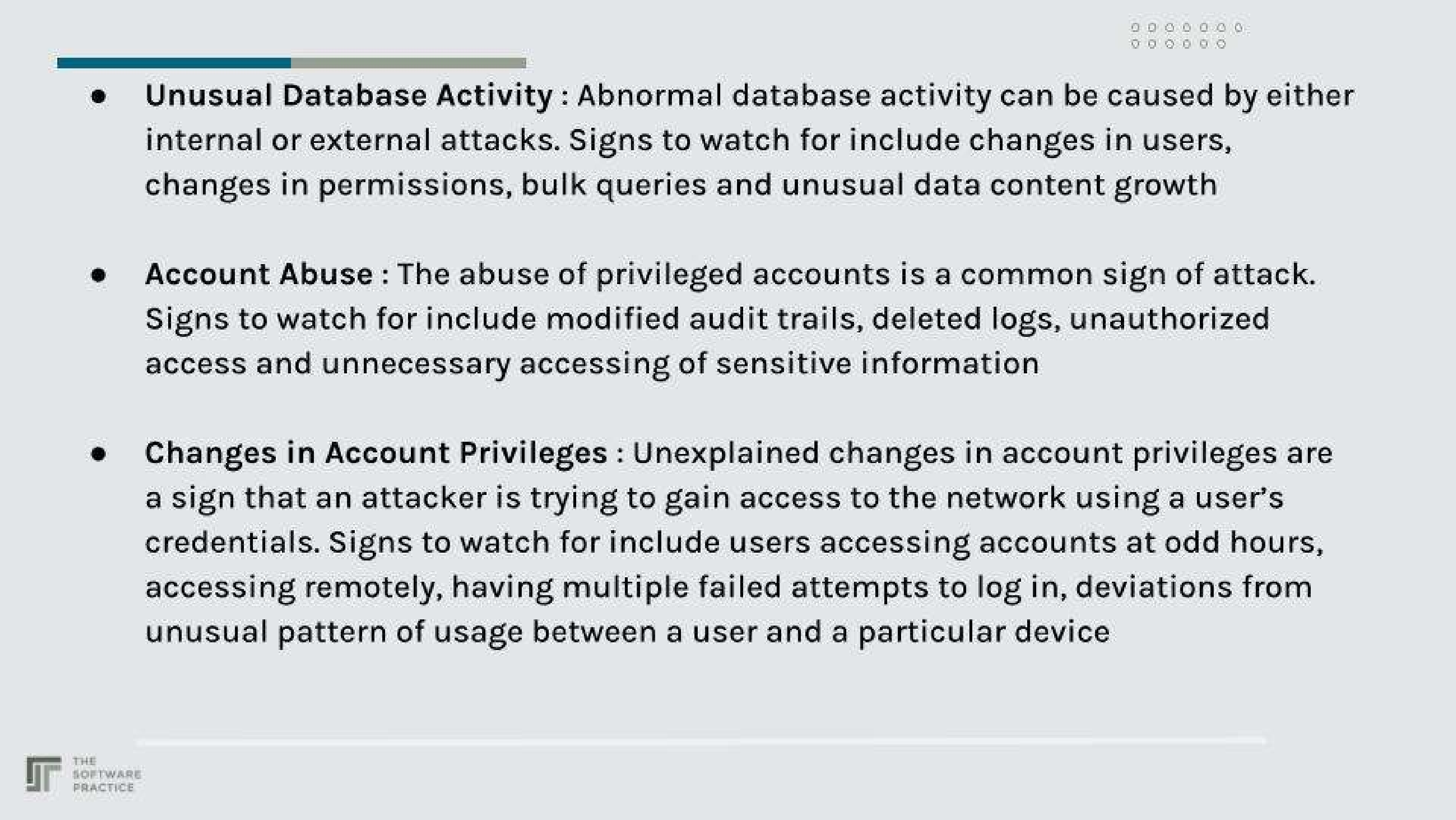
✅ DO ensure that access to the application server in client premise must be via

- Government approved GSIB device
- PAM access assigned to the application vendor
- Jump Host access given to the application vendor and usage of approved client installed on the Jump Host (i.e. using SQL Client within the Jump Host to access the application database)

❌ DO NOT use Jump Host for other purposes (i.e. Information Repository)

❌ DO NOT leave the session connected to the server while you are away from the workstation you are working on

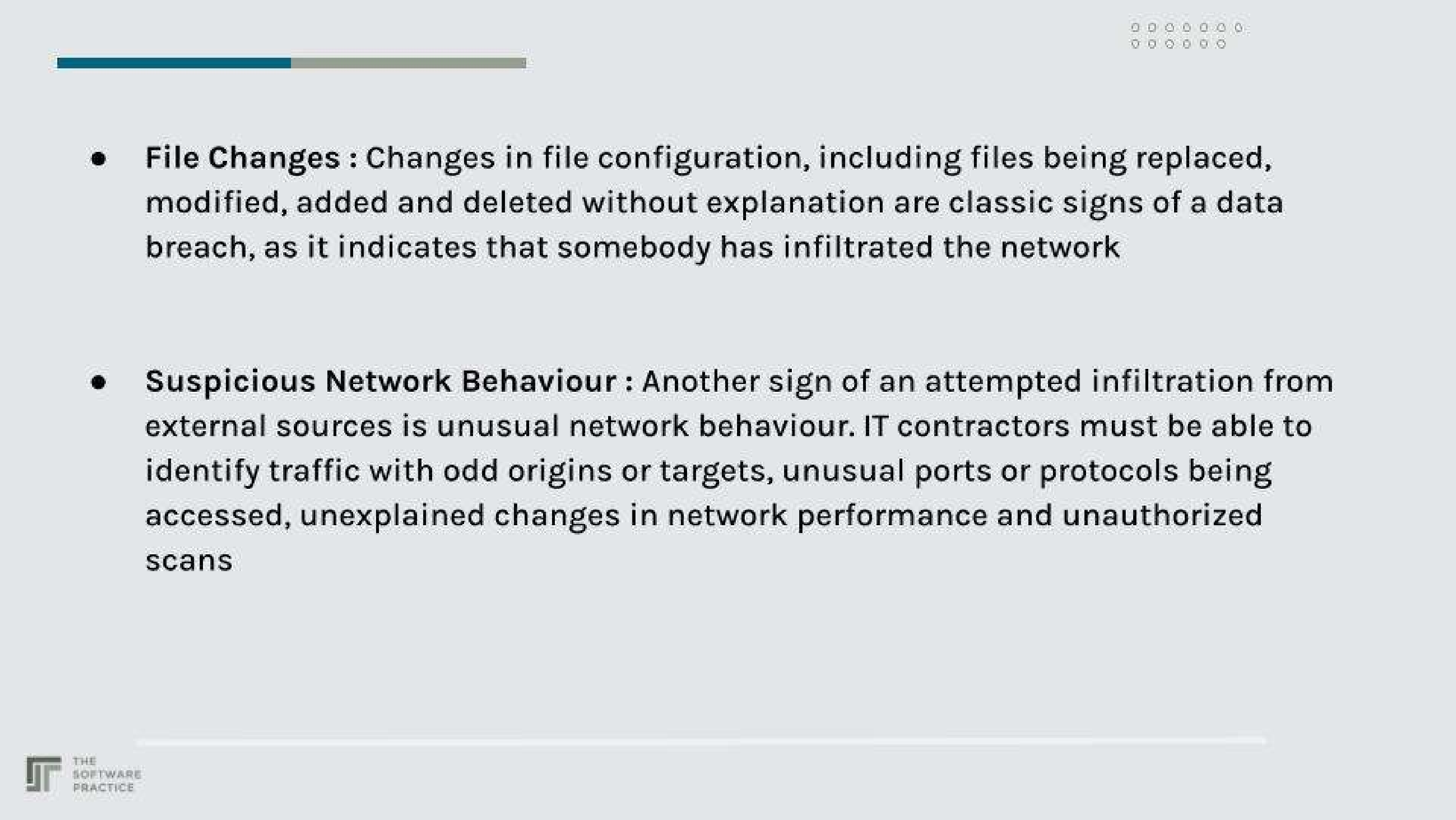
Indicators of Security Threats



- **Unusual Database Activity :** Abnormal database activity can be caused by either internal or external attacks. Signs to watch for include changes in users, changes in permissions, bulk queries and unusual data content growth

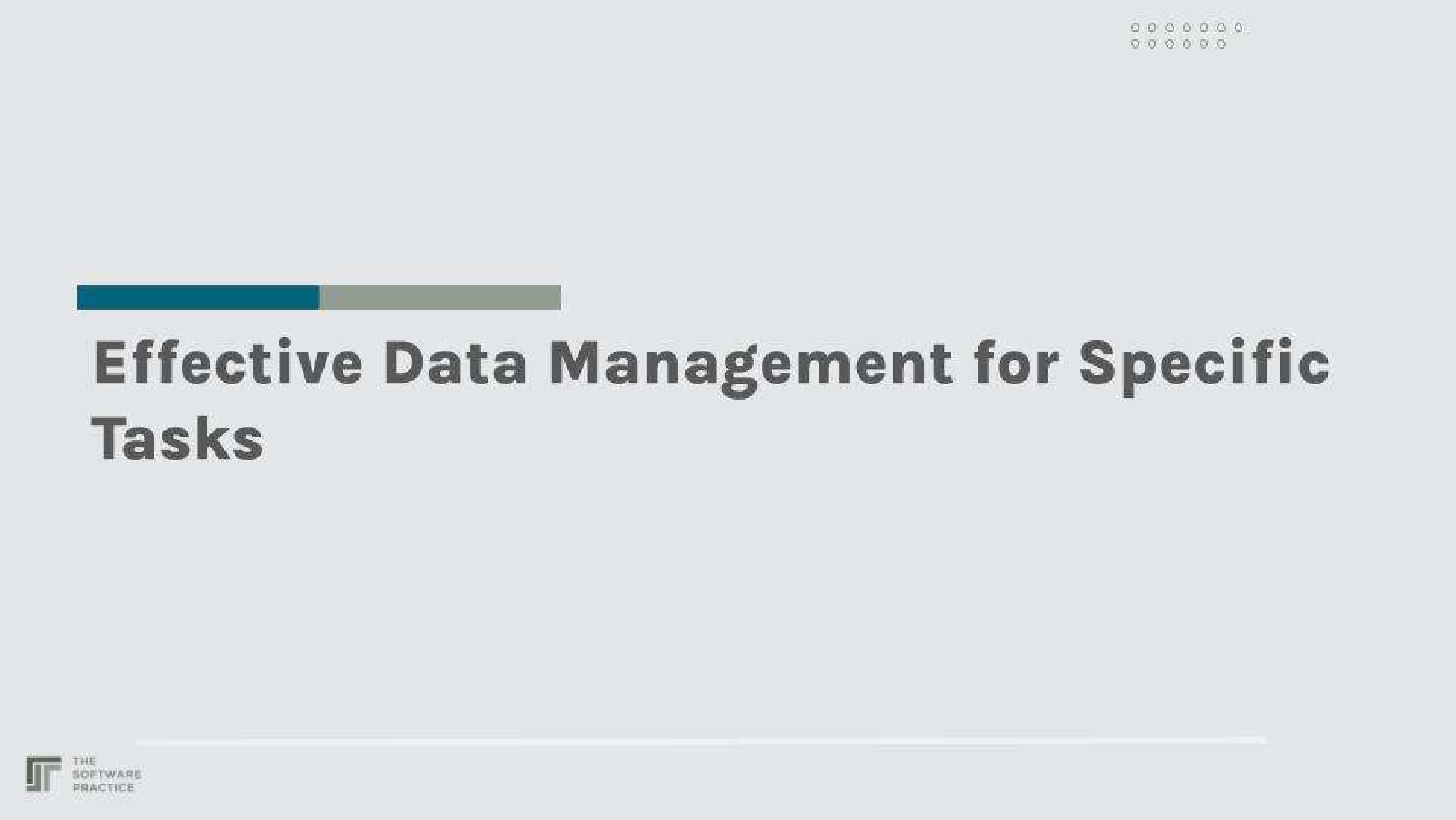
- **Account Abuse :** The abuse of privileged accounts is a common sign of attack. Signs to watch for include modified audit trails, deleted logs, unauthorized access and unnecessary accessing of sensitive information

- **Changes in Account Privileges :** Unexplained changes in account privileges are a sign that an attacker is trying to gain access to the network using a user’s credentials. Signs to watch for include users accessing accounts at odd hours, accessing remotely, having multiple failed attempts to log in, deviations from unusual pattern of usage between a user and a particular device

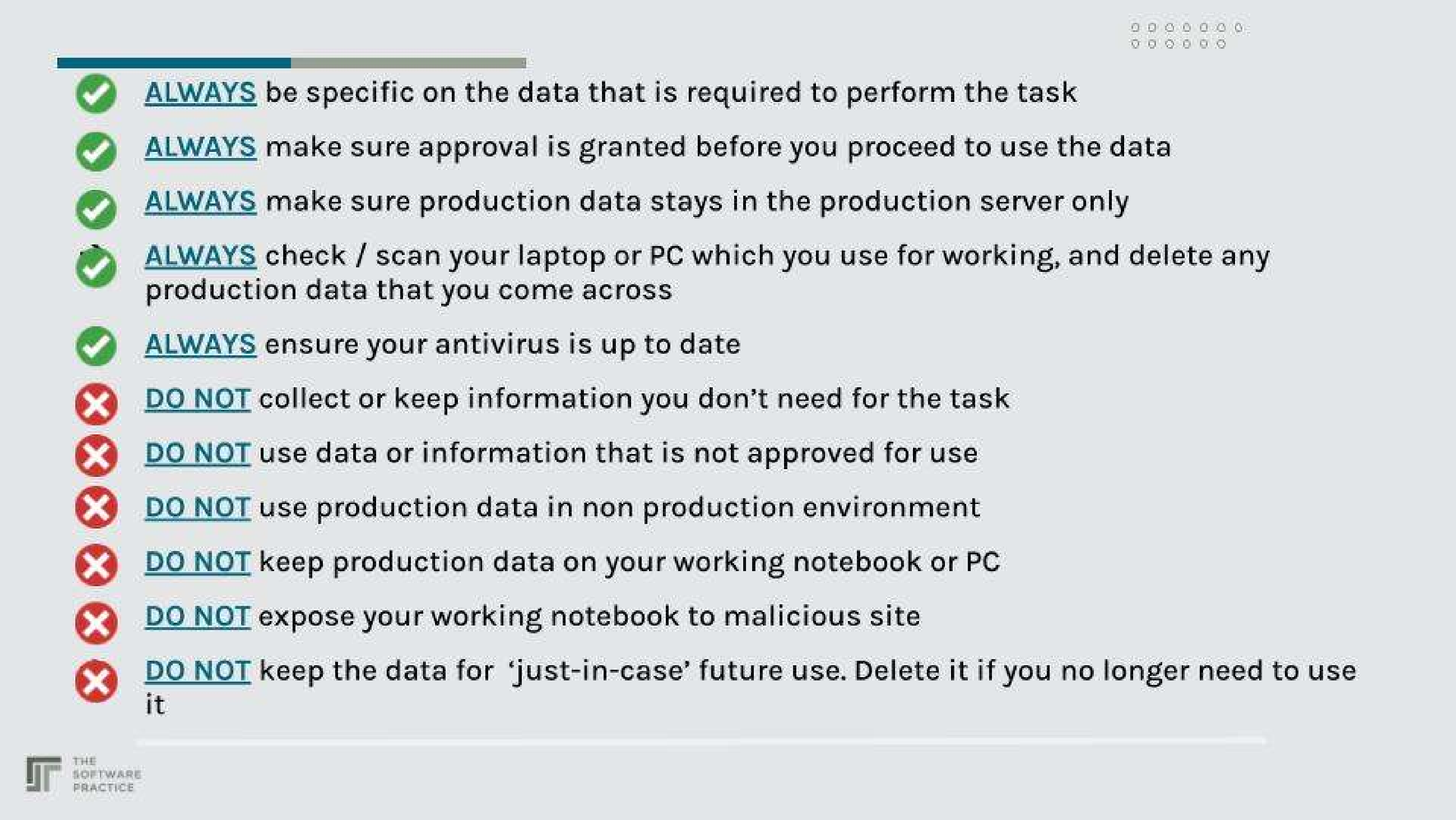


- **File Changes :** Changes in file configuration, including files being replaced, modified, added and deleted without explanation are classic signs of a data breach, as it indicates that somebody has infiltrated the network

- **Suspicious Network Behaviour :** Another sign of an attempted infiltration from external sources is unusual network behaviour. IT contractors must be able to identify traffic with odd origins or targets, unusual ports or protocols being accessed, unexplained changes in network performance and unauthorized scans



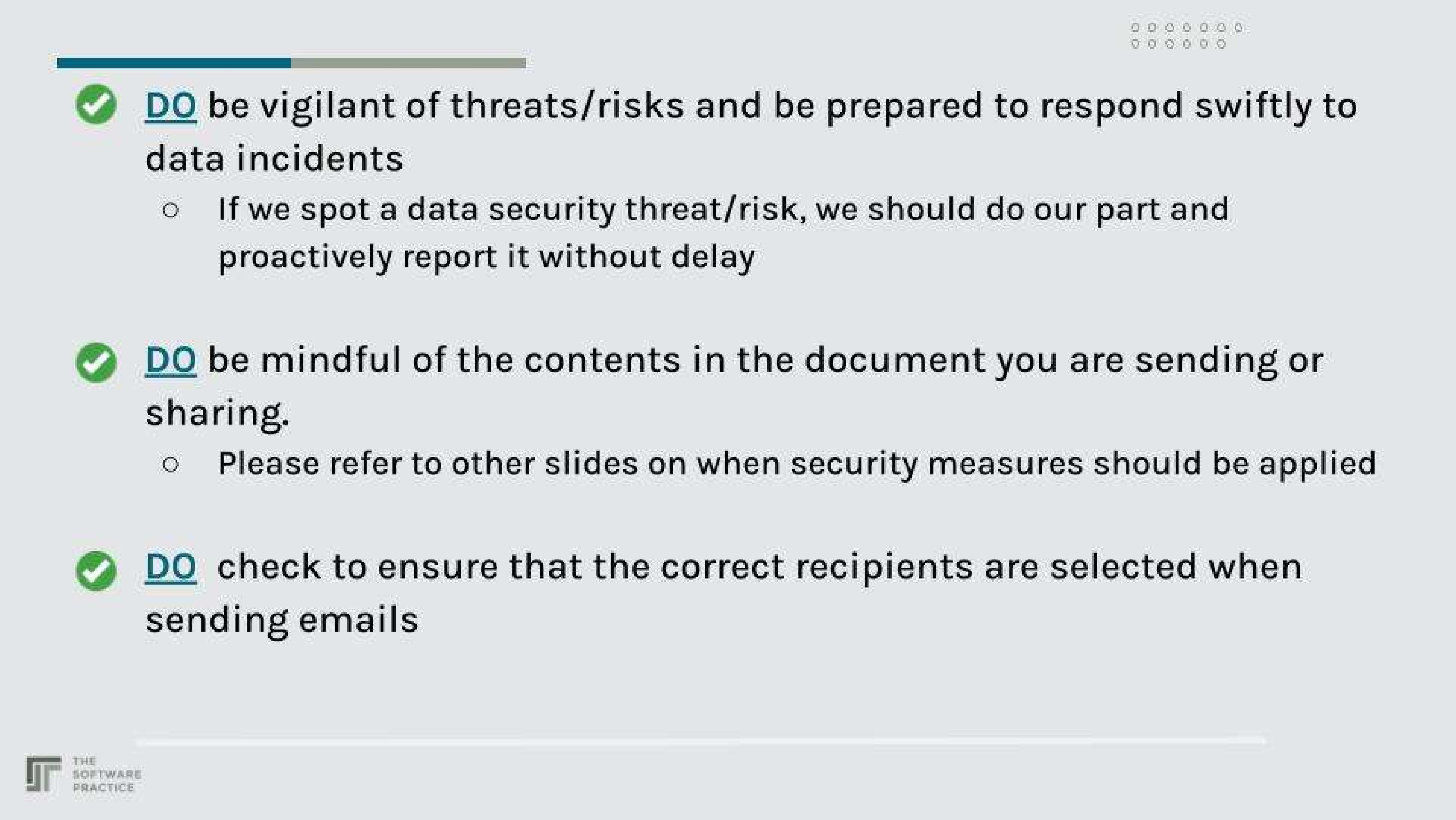
Effective Data Management for Specific Tasks



- ✓ ALWAYS be specific on the data that is required to perform the task
- ✓ ALWAYS make sure approval is granted before you proceed to use the data
- ✓ ALWAYS make sure production data stays in the production server only
- ✓ ALWAYS check / scan your laptop or PC which you use for working, and delete any production data that you come across
- ✓ ALWAYS ensure your antivirus is up to date
- ✗ DO NOT collect or keep information you don’t need for the task
- ✗ DO NOT use data or information that is not approved for use
- ✗ DO NOT use production data in non production environment
- ✗ DO NOT keep production data on your working notebook or PC
- ✗ DO NOT expose your working notebook to malicious site
- ✗ DO NOT keep the data for ‘just-in-case’ future use. Delete it if you no longer need to use it

THE SOFTWARE PRACTICE

Data Incident Management Standard Operating Procedures



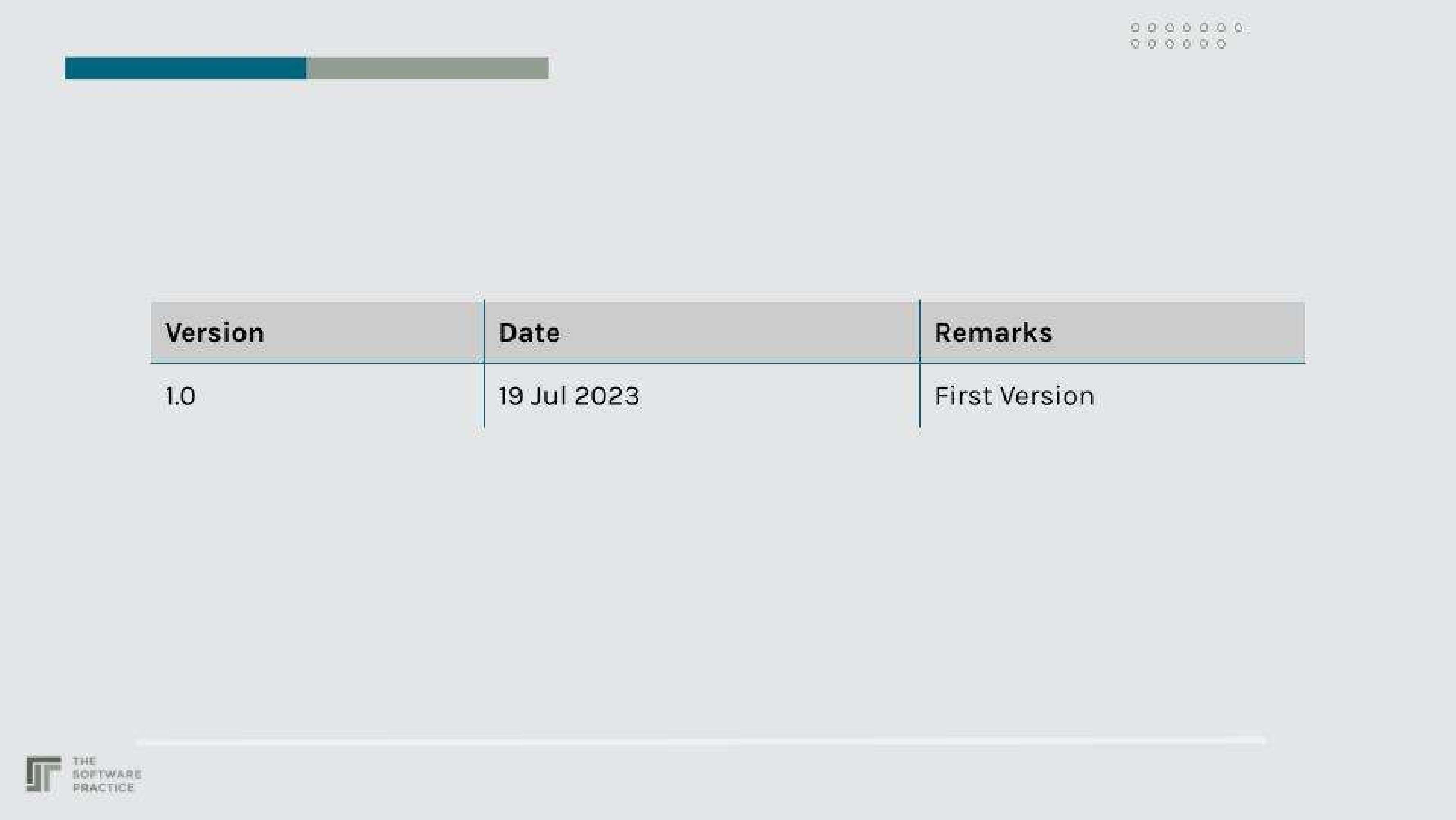
- ✓ DO be vigilant of threats/risks and be prepared to respond swiftly to data incidents
  - If we spot a data security threat/risk, we should do our part and proactively report it without delay
- ✓ DO be mindful of the contents in the document you are sending or sharing.
  - Please refer to other slides on when security measures should be applied
- ✓ DO check to ensure that the correct recipients are selected when sending emails

Thank you for Taking Cyber Security Seriously.

Annex B

THE SOFTWARE PRACTICE

Understanding Cyber Threats



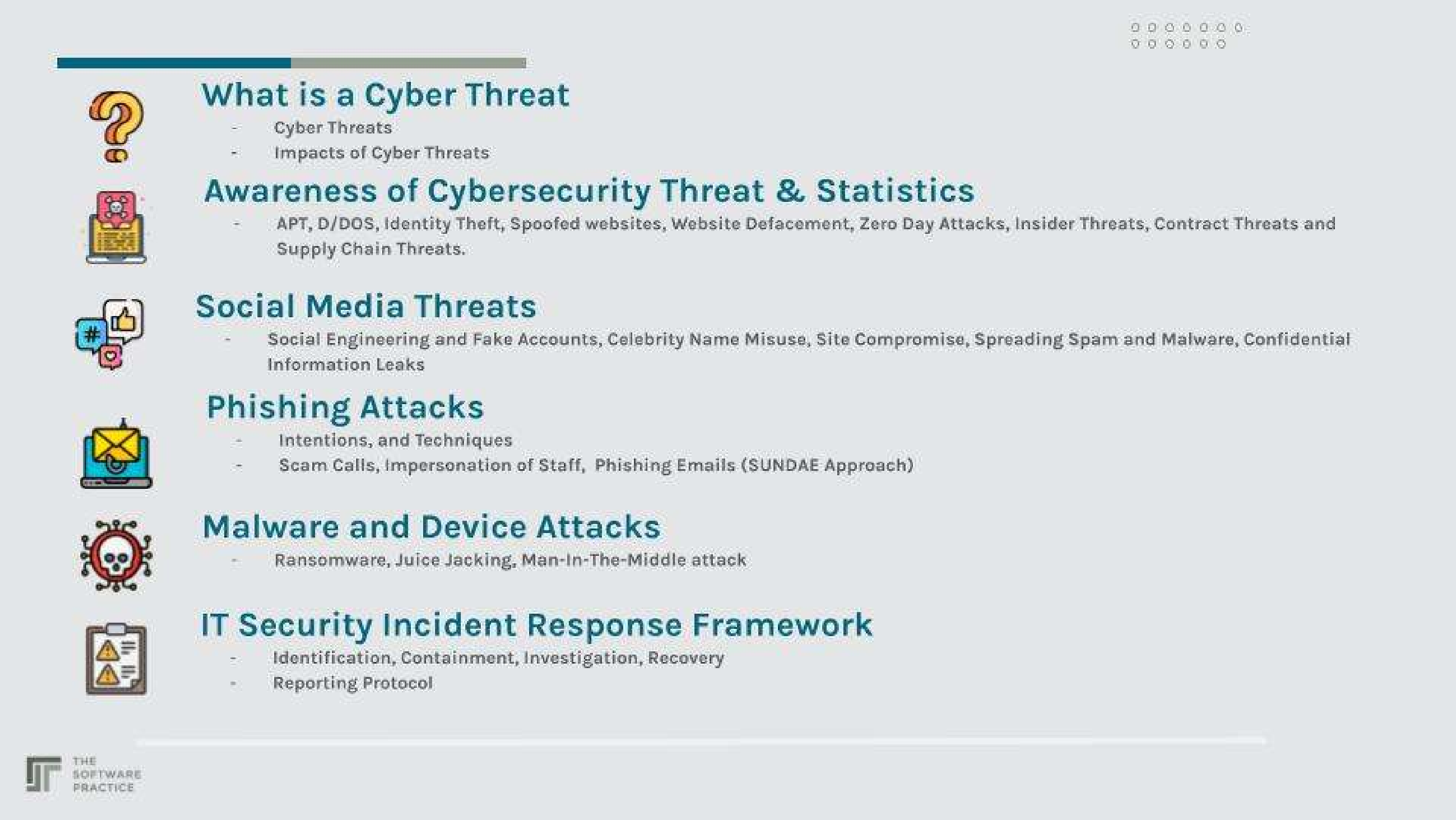
Version	Date	Remarks
1.0	19 Jul 2023	First Version

THE SOFTWARE PRACTICE

Understanding Cyber Threats

In a Nutshell

THE SOFTWARE PRACTICE



What is a Cyber Threat

- Cyber Threats
- Impacts of Cyber Threats

Awareness of Cybersecurity Threat & Statistics

- APT, D/DOS, Identity Theft, Spoofed websites, Website Defacement, Zero Day Attacks, Insider Threats, Contract Threats and Supply Chain Threats.

Social Media Threats

- Social Engineering and Fake Accounts, Celebrity Name Misuse, Site Compromise, Spreading Spam and Malware, Confidential Information Leaks

Phishing Attacks

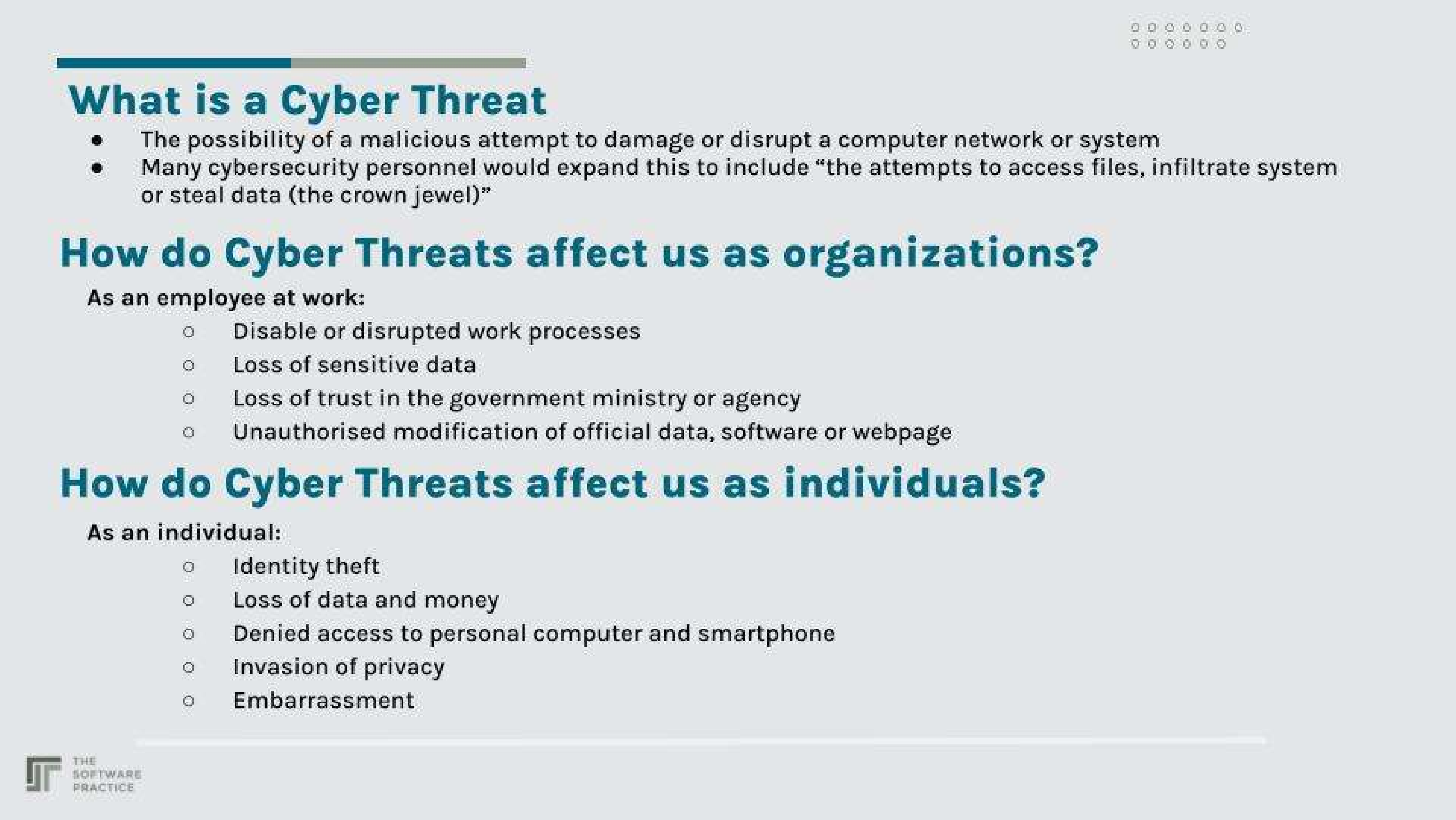
- Intentions, and Techniques
- Scam Calls, Impersonation of Staff, Phishing Emails (SUNDAE Approach)

Malware and Device Attacks

- Ransomware, Juice Jacking, Man-In-The-Middle attack

IT Security Incident Response Framework

- Identification, Containment, Investigation, Recovery
- Reporting Protocol



What is a Cyber Threat

- The possibility of a malicious attempt to damage or disrupt a computer network or system
- Many cybersecurity personnel would expand this to include “the attempts to access files, infiltrate system or steal data (the crown jewel)”

How do Cyber Threats affect us as organizations?

As an employee at work:

- ○ Disable or disrupted work processes
- ○ Loss of sensitive data
- ○ Loss of trust in the government ministry or agency
- ○ Unauthorised modification of official data, software or webpage

How do Cyber Threats affect us as individuals?

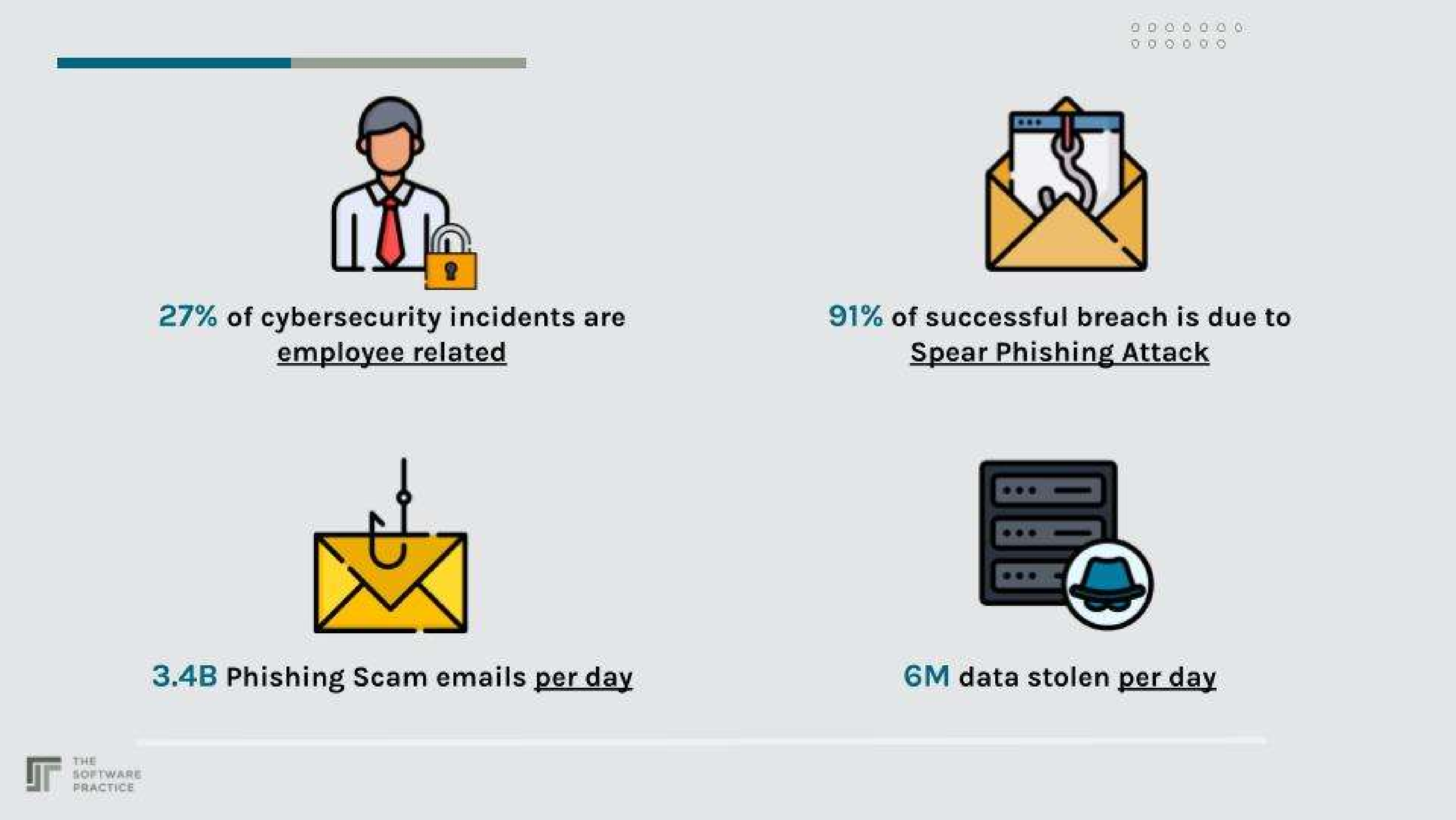
As an individual:

- ○ Identity theft
- ○ Loss of data and money
- ○ Denied access to personal computer and smartphone
- ○ Invasion of privacy
- ○ Embarrassment

THE SOFTWARE PRACTICE

Awareness of Cybersecurity Threat & Statistics

THE SOFTWARE PRACTICE



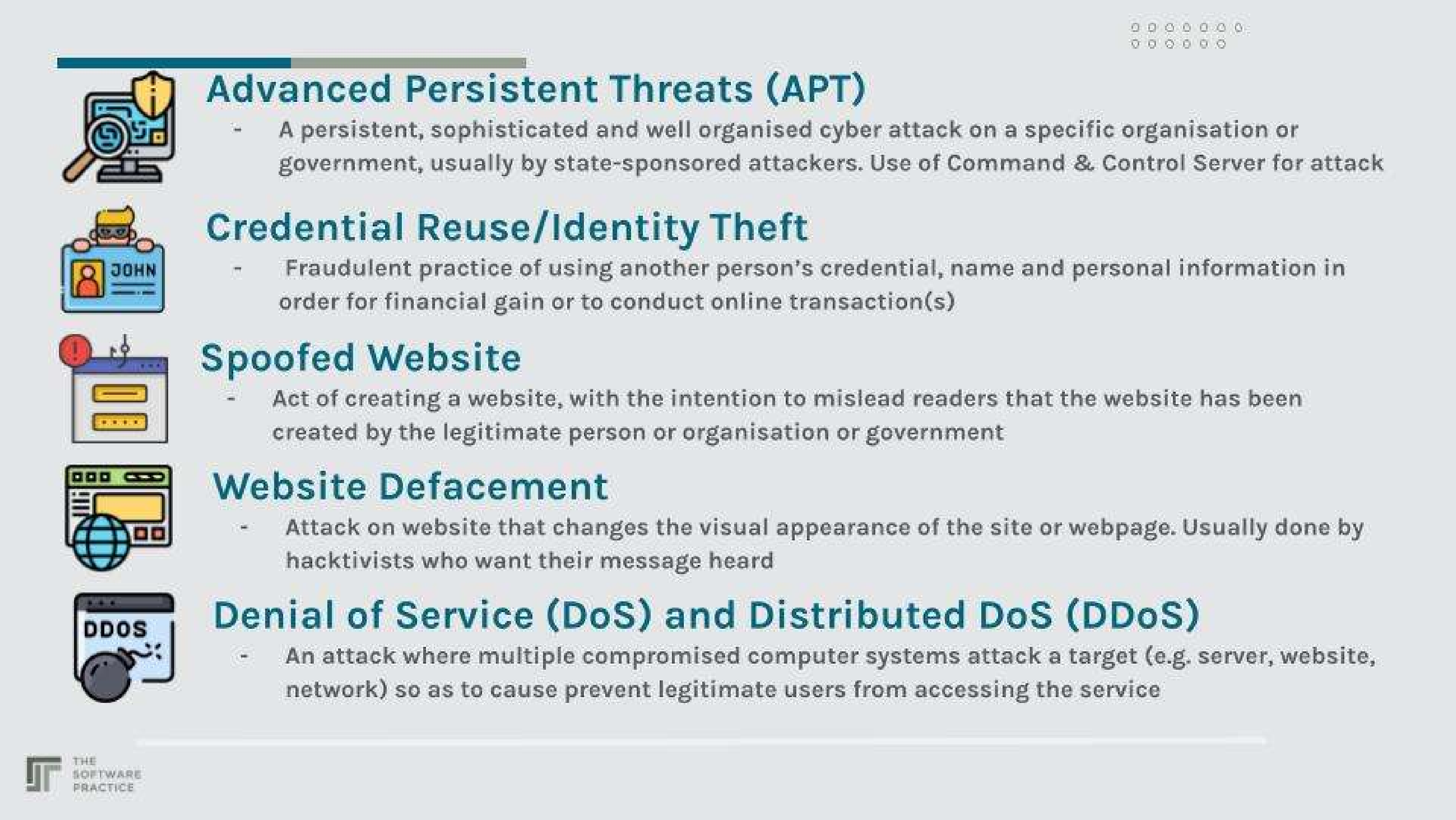
27% of cybersecurity incidents are employee related

91% of successful breach is due to Spear Phishing Attack

3.4B Phishing Scam emails per day

6M data stolen per day

THE SOFTWARE PRACTICE



Advanced Persistent Threats (APT)

- A persistent, sophisticated and well organised cyber attack on a specific organisation or government, usually by state-sponsored attackers. Use of Command & Control Server for attack

Credential Reuse/Identity Theft

- Fraudulent practice of using another person's credential, name and personal information in order for financial gain or to conduct online transaction(s)

Spoofed Website

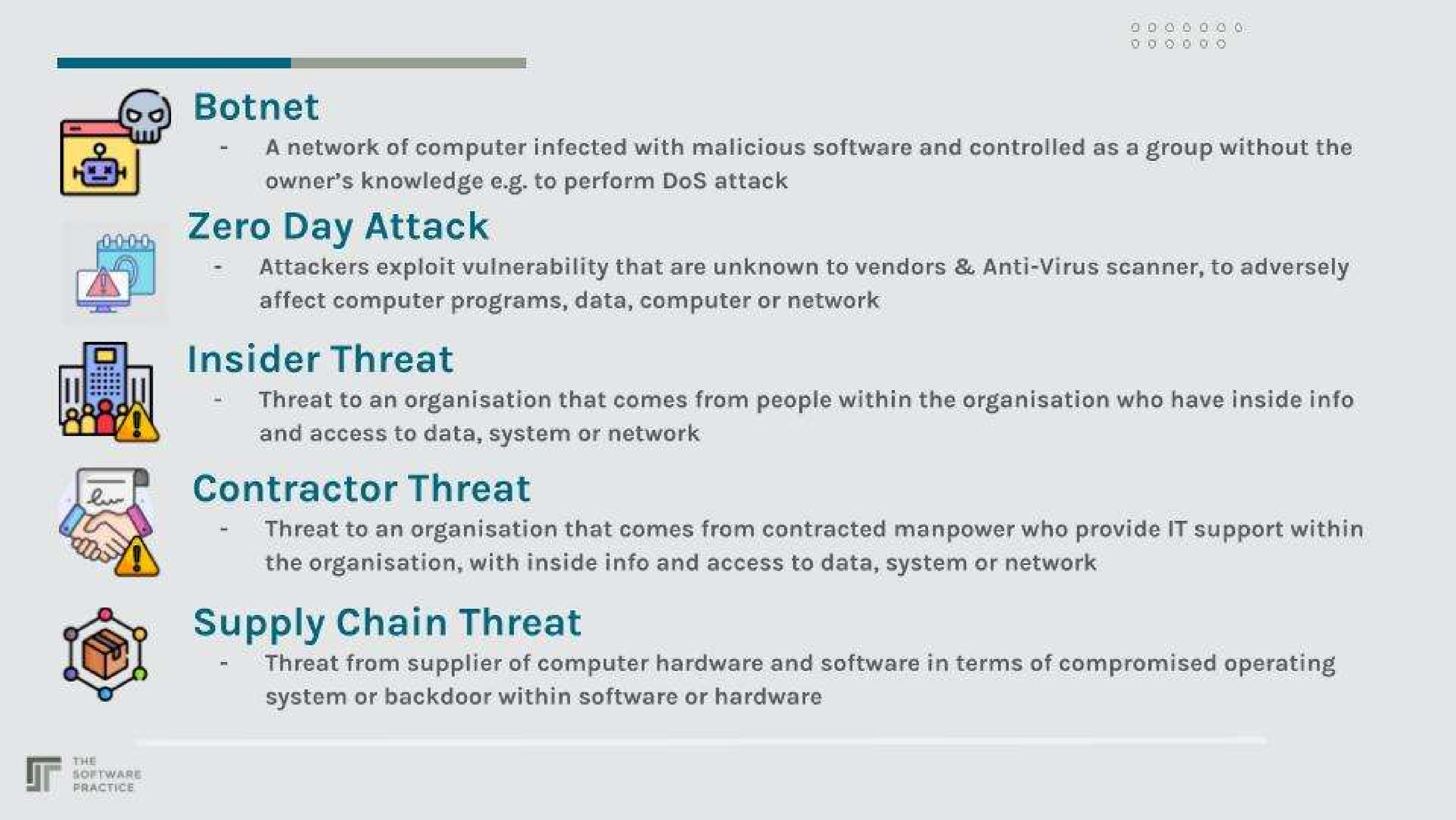
- Act of creating a website, with the intention to mislead readers that the website has been created by the legitimate person or organisation or government

Website Defacement

- Attack on website that changes the visual appearance of the site or webpage. Usually done by hacktivists who want their message heard

Denial of Service (DoS) and Distributed DoS (DDoS)

- An attack where multiple compromised computer systems attack a target (e.g. server, website, network) so as to cause prevent legitimate users from accessing the service



Botnet

- A network of computer infected with malicious software and controlled as a group without the owner's knowledge e.g. to perform DoS attack

Zero Day Attack

- Attackers exploit vulnerability that are unknown to vendors & Anti-Virus scanner, to adversely affect computer programs, data, computer or network

Insider Threat

- Threat to an organisation that comes from people within the organisation who have inside info and access to data, system or network

Contractor Threat

- Threat to an organisation that comes from contracted manpower who provide IT support within the organisation, with inside info and access to data, system or network

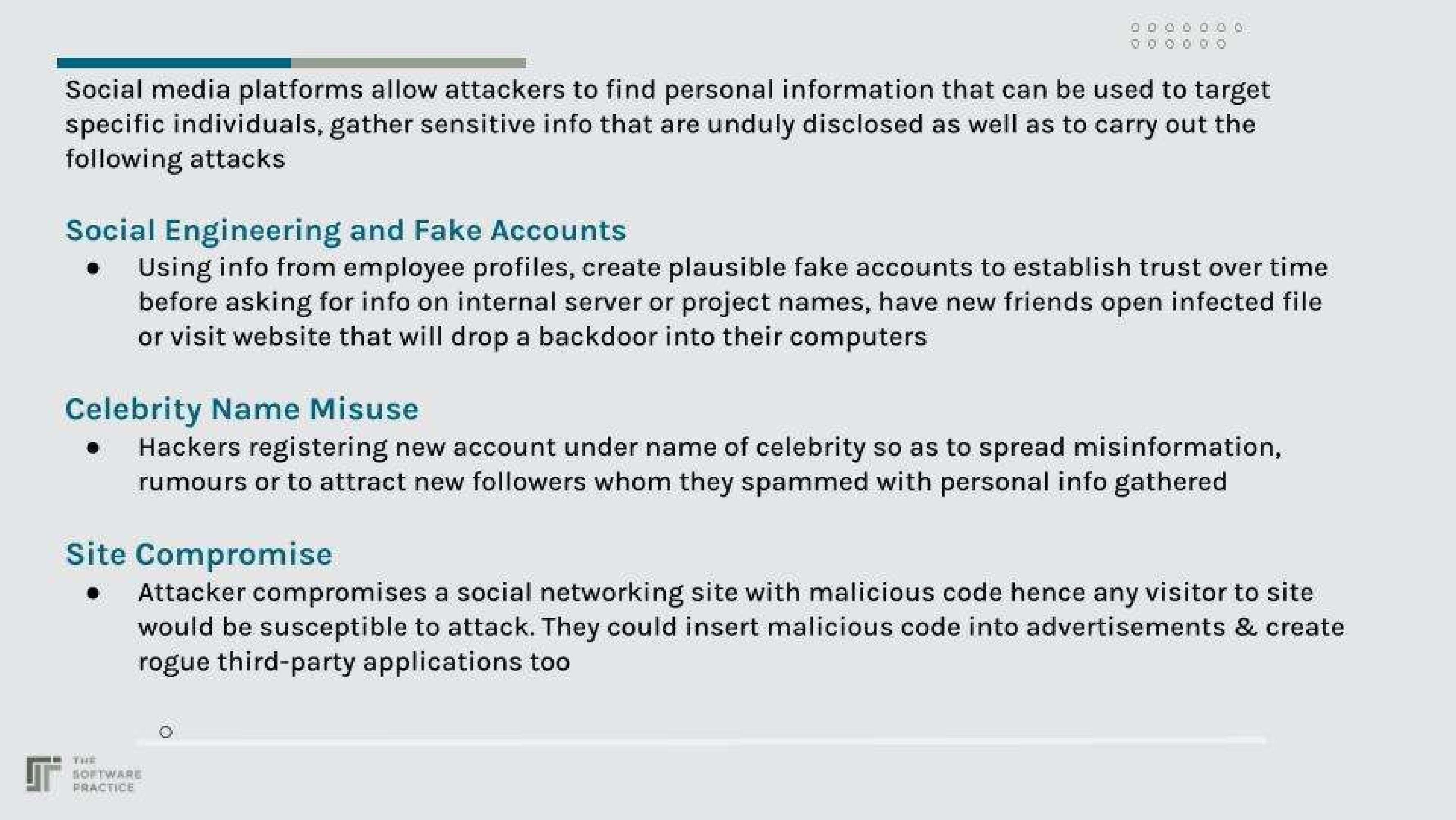
Supply Chain Threat

- Threat from supplier of computer hardware and software in terms of compromised operating system or backdoor within software or hardware

THE SOFTWARE PRACTICE

Social Media Threats

THE SOFTWARE PRACTICE



Social media platforms allow attackers to find personal information that can be used to target specific individuals, gather sensitive info that are unduly disclosed as well as to carry out the following attacks

Social Engineering and Fake Accounts

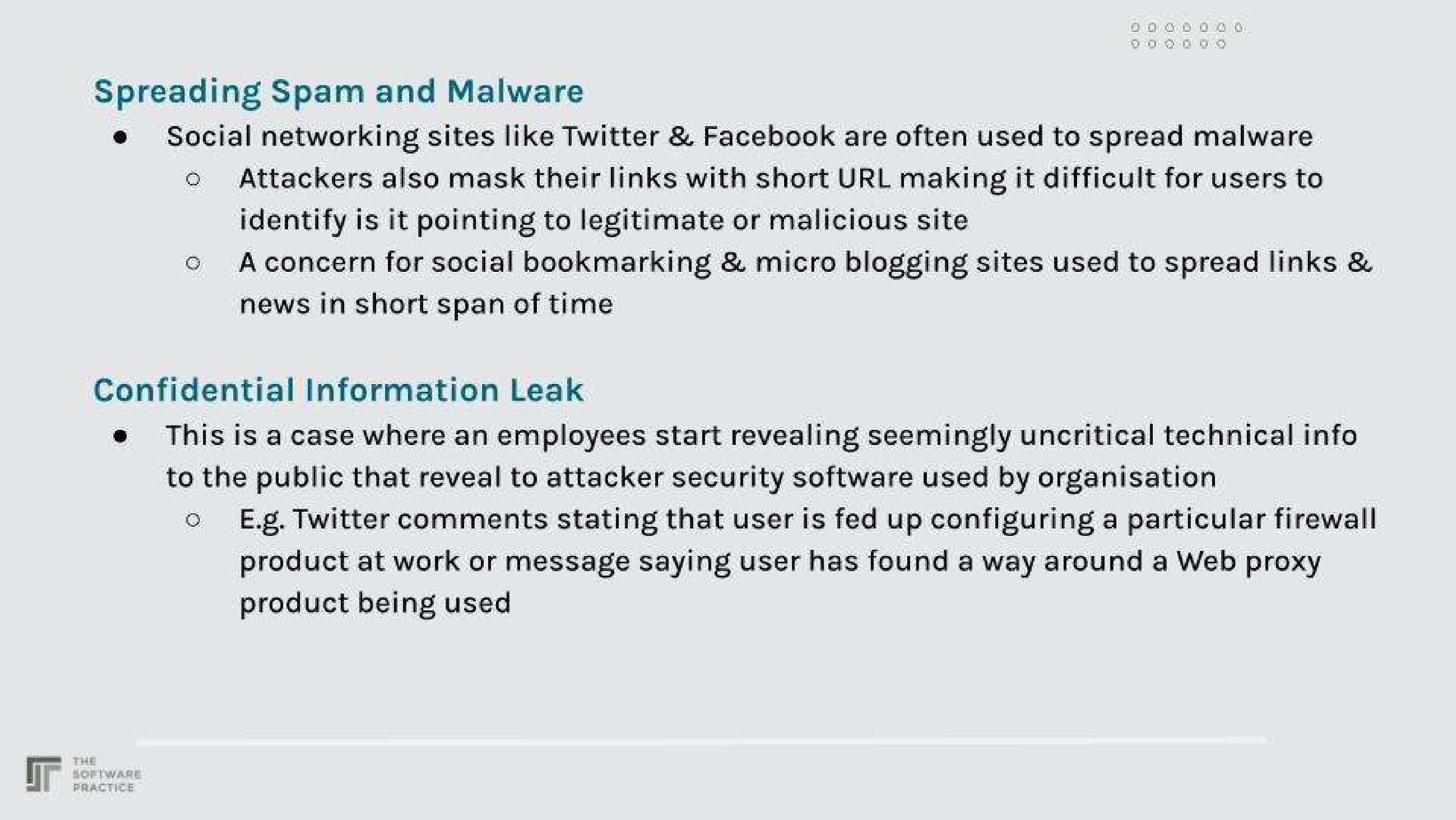
- Using info from employee profiles, create plausible fake accounts to establish trust over time before asking for info on internal server or project names, have new friends open infected file or visit website that will drop a backdoor into their computers

Celebrity Name Misuse

- Hackers registering new account under name of celebrity so as to spread misinformation, rumours or to attract new followers whom they spammed with personal info gathered

Site Compromise

- Attacker compromises a social networking site with malicious code hence any visitor to site would be susceptible to attack. They could insert malicious code into advertisements & create rogue third-party applications too



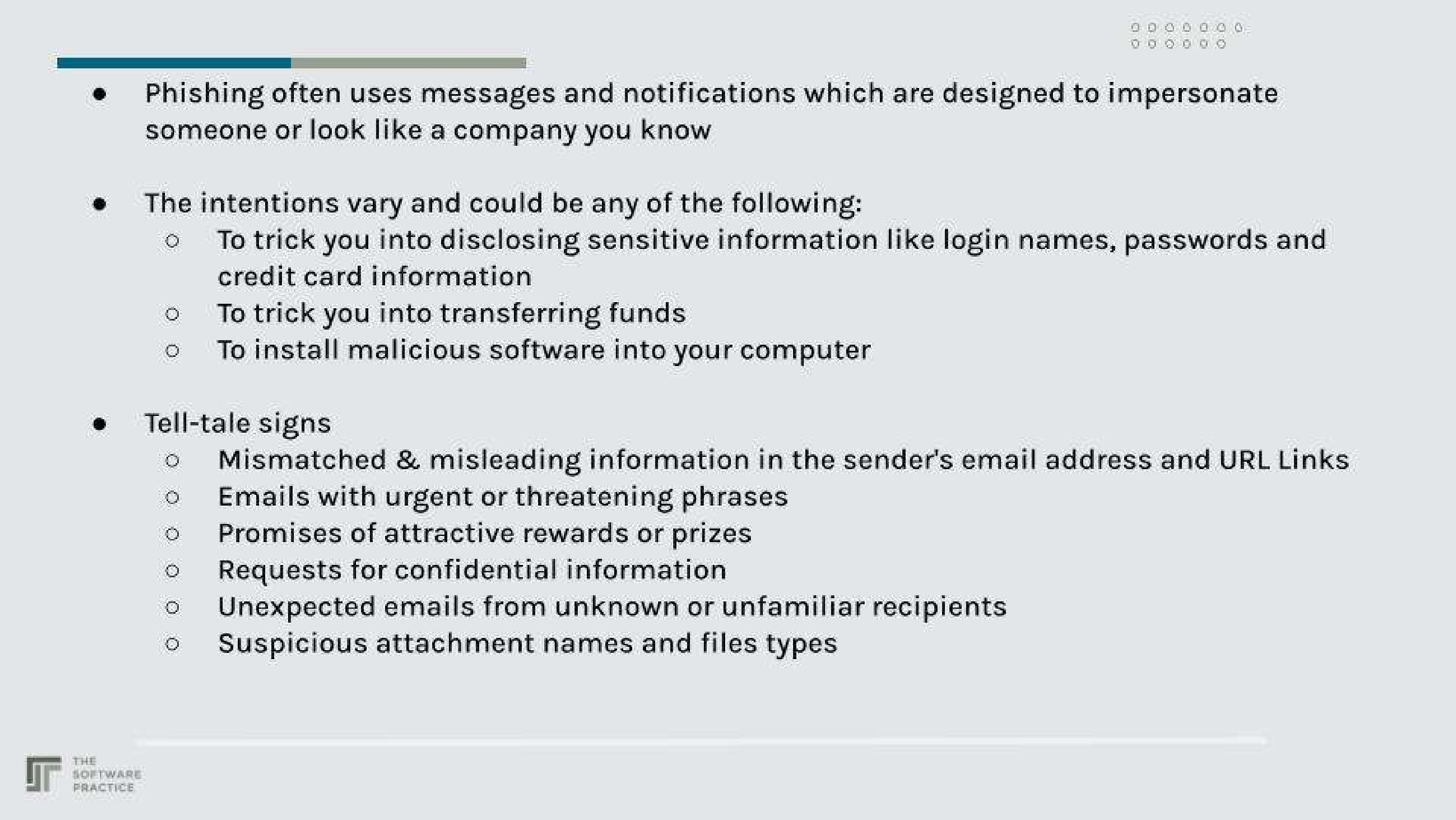
Spreading Spam and Malware

- Social networking sites like Twitter & Facebook are often used to spread malware
  - Attackers also mask their links with short URL making it difficult for users to identify is it pointing to legitimate or malicious site
  - A concern for social bookmarking & micro blogging sites used to spread links & news in short span of time

Confidential Information Leak

- This is a case where an employees start revealing seemingly uncritical technical info to the public that reveal to attacker security software used by organisation
  - E.g. Twitter comments stating that user is fed up configuring a particular firewall product at work or message saying user has found a way around a Web proxy product being used

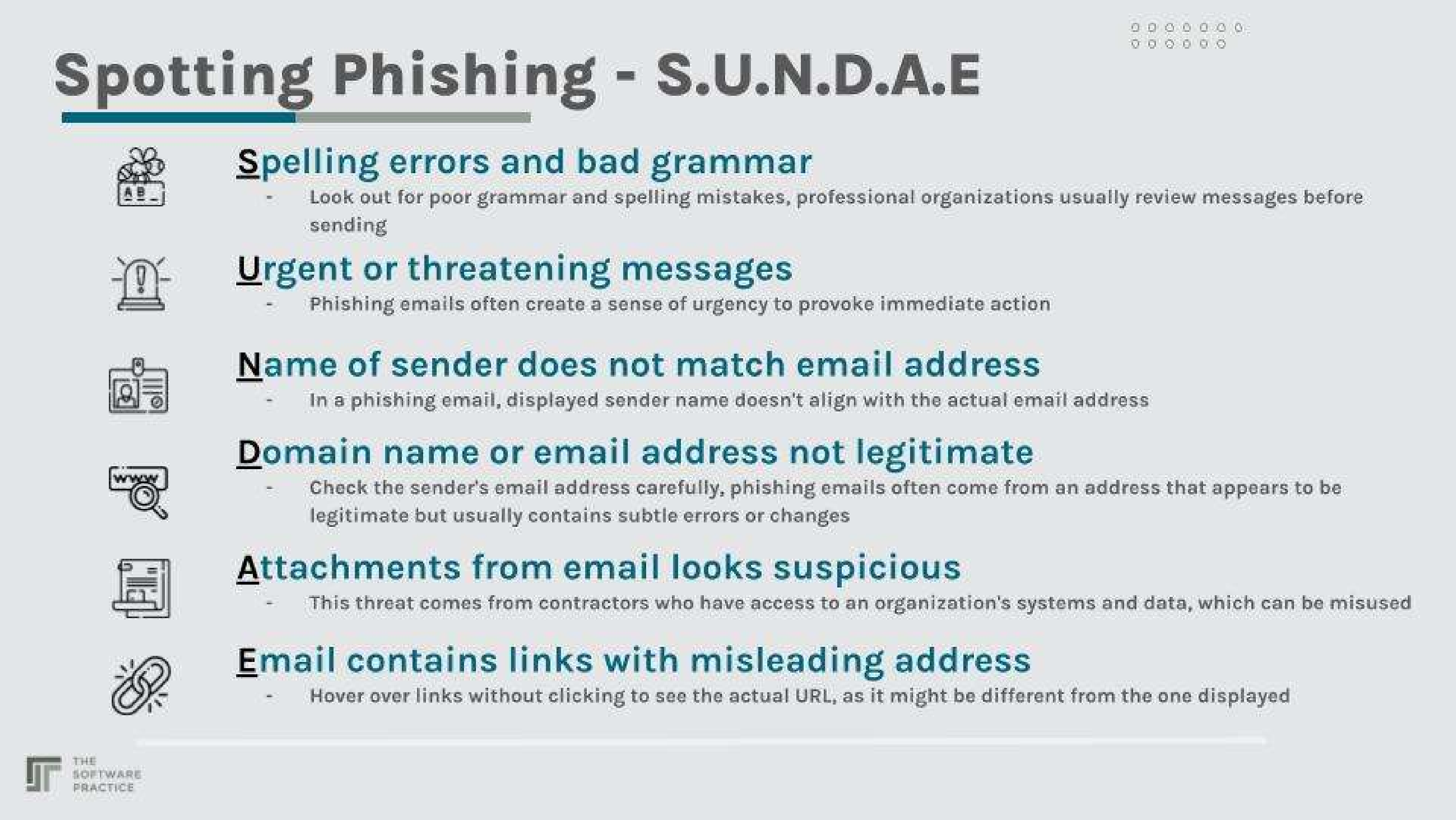
Phishing Attacks



- Phishing often uses messages and notifications which are designed to impersonate someone or look like a company you know

- The intentions vary and could be any of the following:
  - To trick you into disclosing sensitive information like login names, passwords and credit card information
  - To trick you into transferring funds
  - To install malicious software into your computer

- Tell-tale signs
  - Mismatched & misleading information in the sender's email address and URL Links
  - Emails with urgent or threatening phrases
  - Promises of attractive rewards or prizes
  - Requests for confidential information
  - Unexpected emails from unknown or unfamiliar recipients
  - Suspicious attachment names and files types



Spotting Phishing - S.U.N.D.A.E

Spelling errors and bad grammar

- Look out for poor grammar and spelling mistakes, professional organizations usually review messages before sending

Urgent or threatening messages

- Phishing emails often create a sense of urgency to provoke immediate action

Name of sender does not match email address

- In a phishing email, displayed sender name doesn't align with the actual email address

Domain name or email address not legitimate

- Check the sender's email address carefully, phishing emails often come from an address that appears to be legitimate but usually contains subtle errors or changes

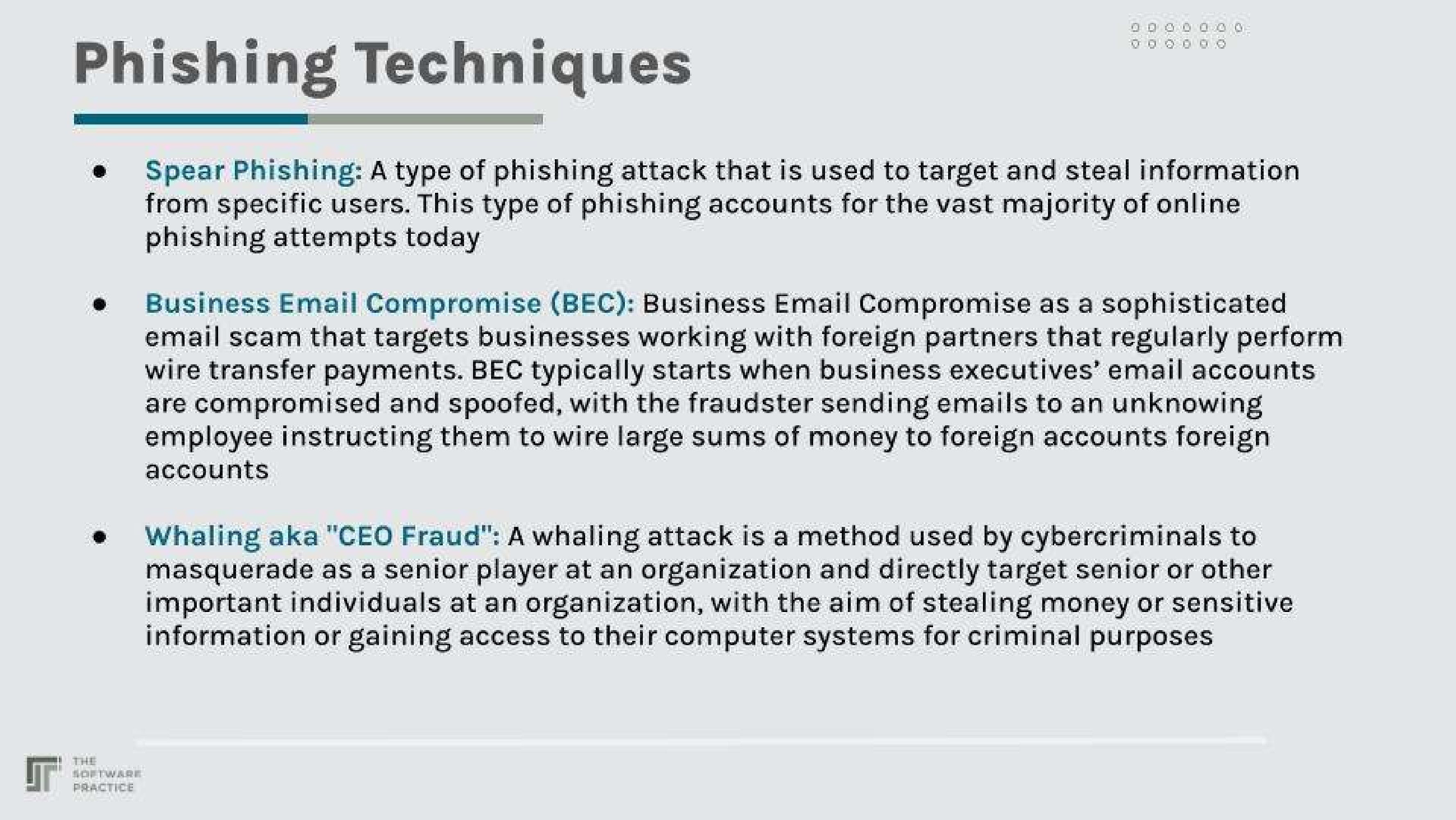
Attachments from email looks suspicious

- This threat comes from contractors who have access to an organization's systems and data, which can be misused

Email contains links with misleading address

- Hover over links without clicking to see the actual URL, as it might be different from the one displayed

THE SOFTWARE PRACTICE



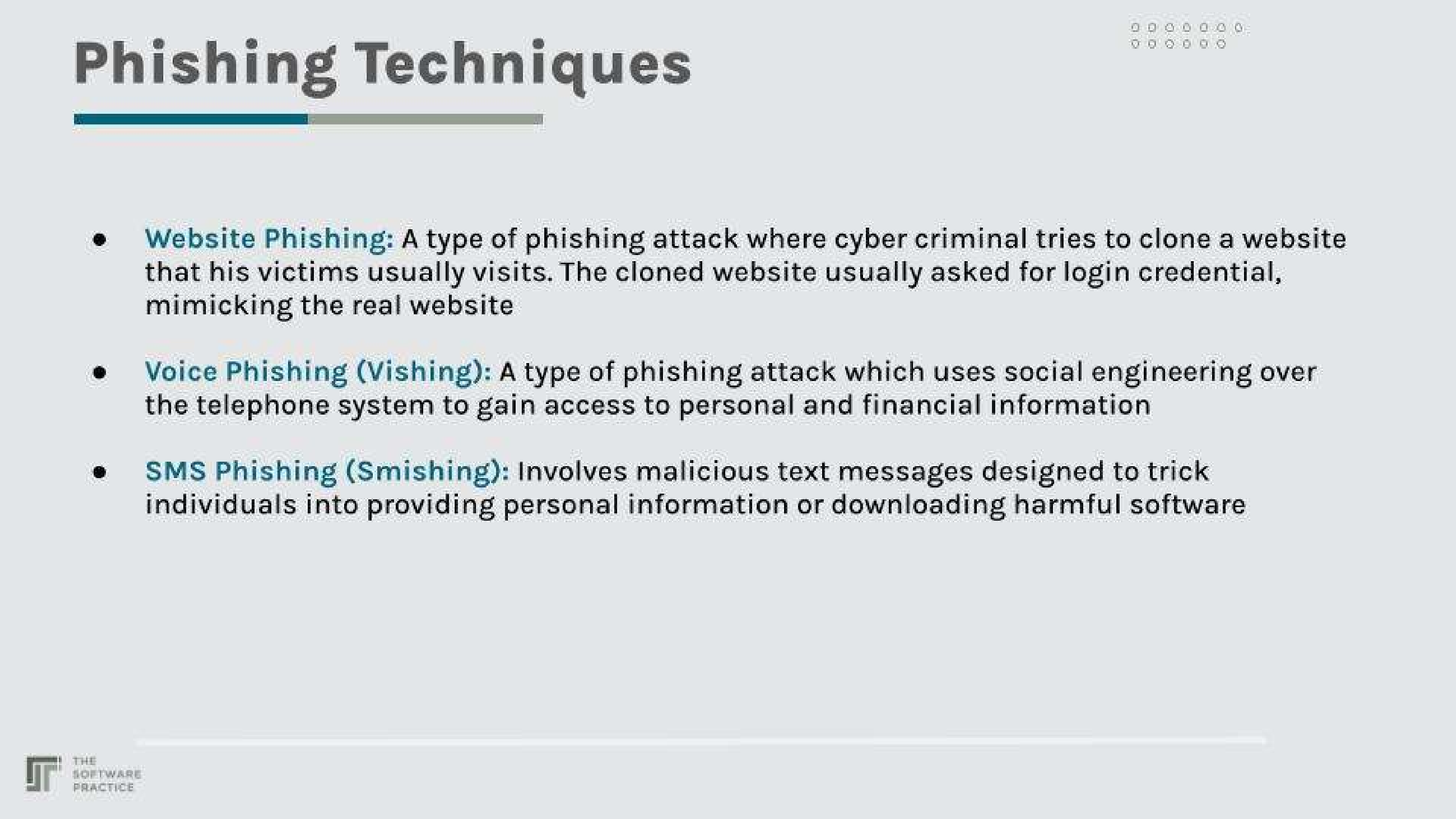
Phishing Techniques

- **Spear Phishing:** A type of phishing attack that is used to target and steal information from specific users. This type of phishing accounts for the vast majority of online phishing attempts today

- **Business Email Compromise (BEC):** Business Email Compromise as a sophisticated email scam that targets businesses working with foreign partners that regularly perform wire transfer payments. BEC typically starts when business executives' email accounts are compromised and spoofed, with the fraudster sending emails to an unknowing employee instructing them to wire large sums of money to foreign accounts foreign accounts

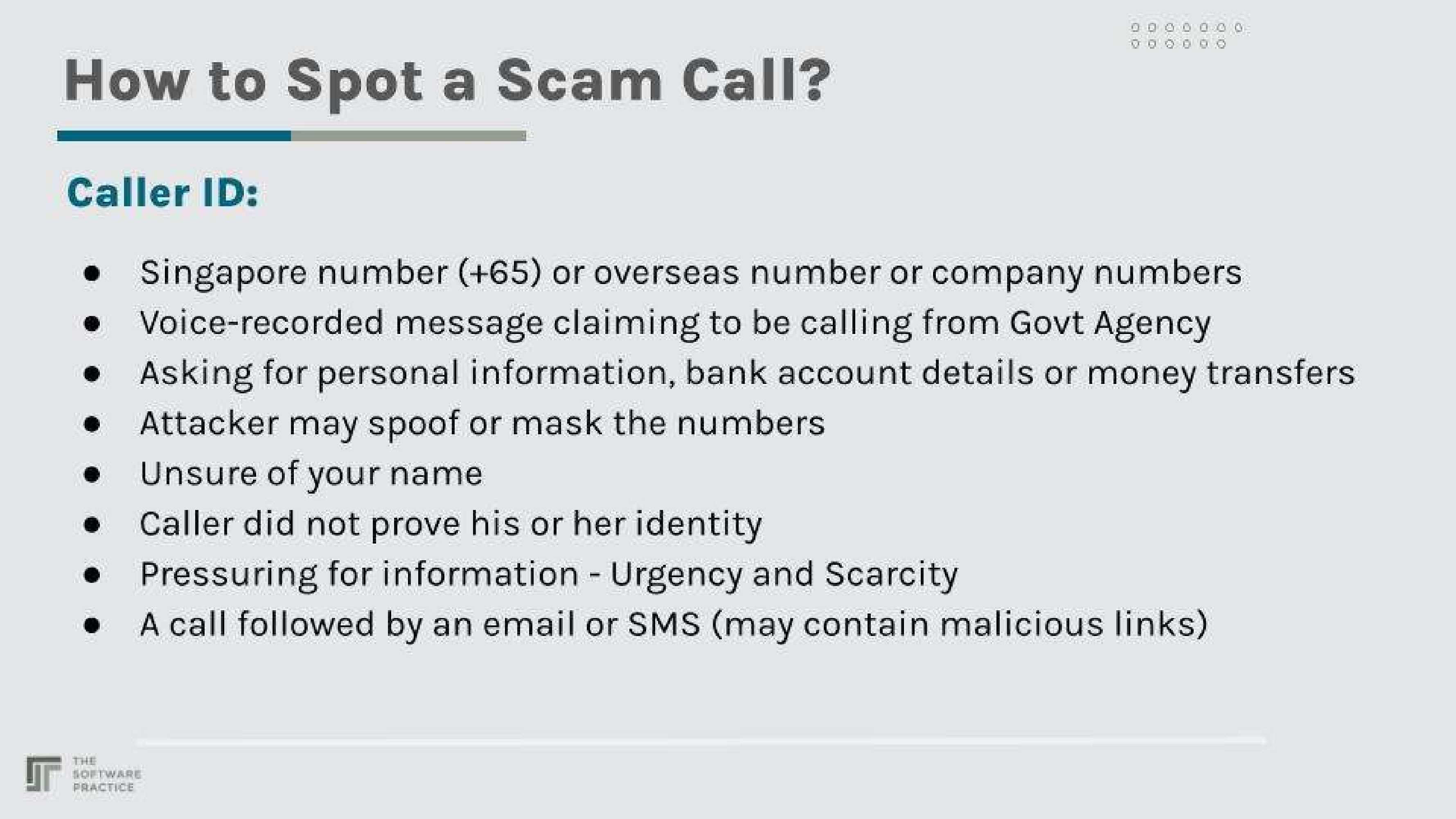
- **Whaling aka "CEO Fraud":** A whaling attack is a method used by cybercriminals to masquerade as a senior player at an organization and directly target senior or other important individuals at an organization, with the aim of stealing money or sensitive information or gaining access to their computer systems for criminal purposes

THE SOFTWARE PRACTICE



Phishing Techniques

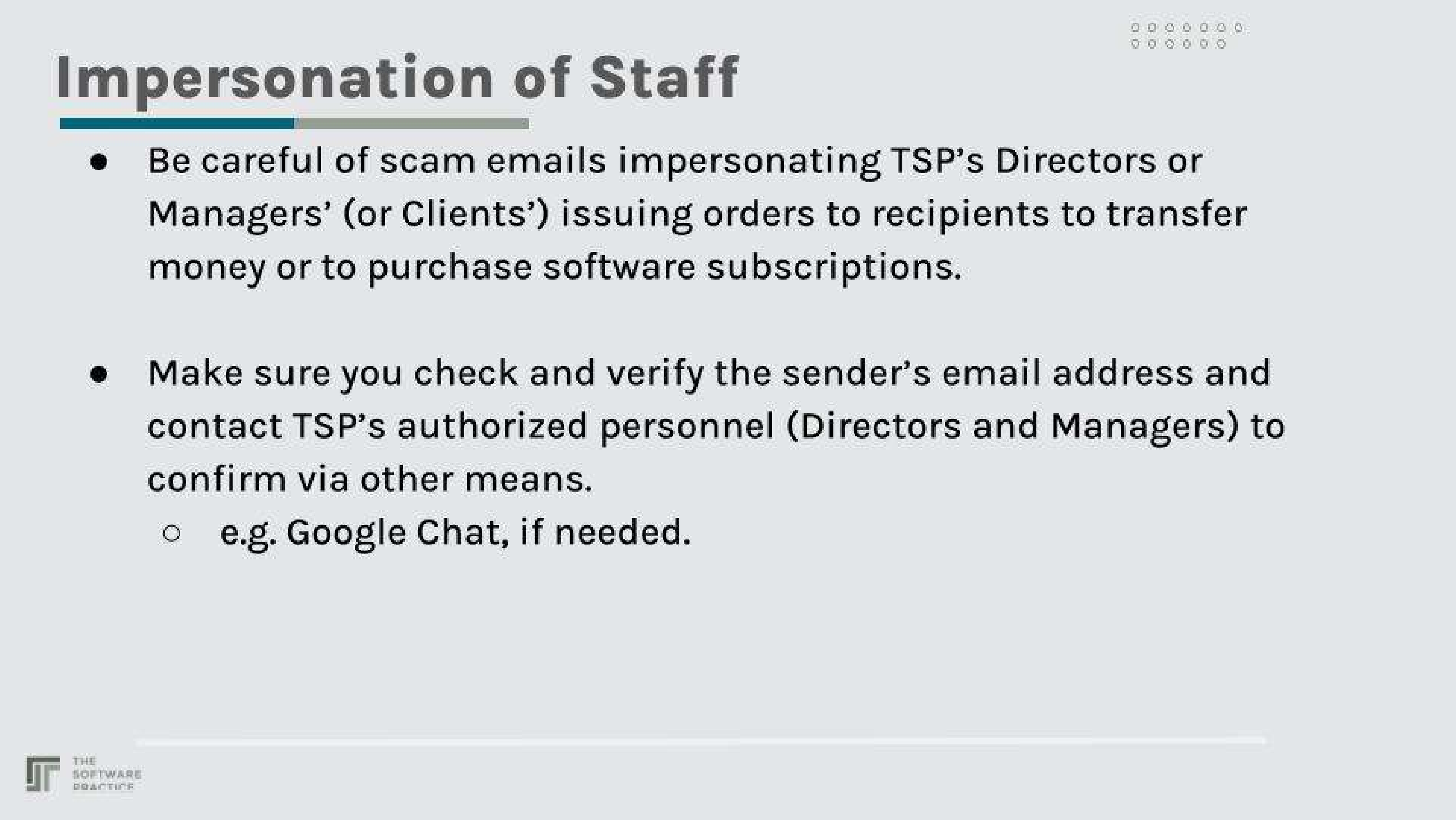
- **Website Phishing:** A type of phishing attack where cyber criminal tries to clone a website that his victims usually visits. The cloned website usually asked for login credential, mimicking the real website
- **Voice Phishing (Vishing):** A type of phishing attack which uses social engineering over the telephone system to gain access to personal and financial information
- **SMS Phishing (Smishing):** Involves malicious text messages designed to trick individuals into providing personal information or downloading harmful software



How to Spot a Scam Call?

Caller ID:

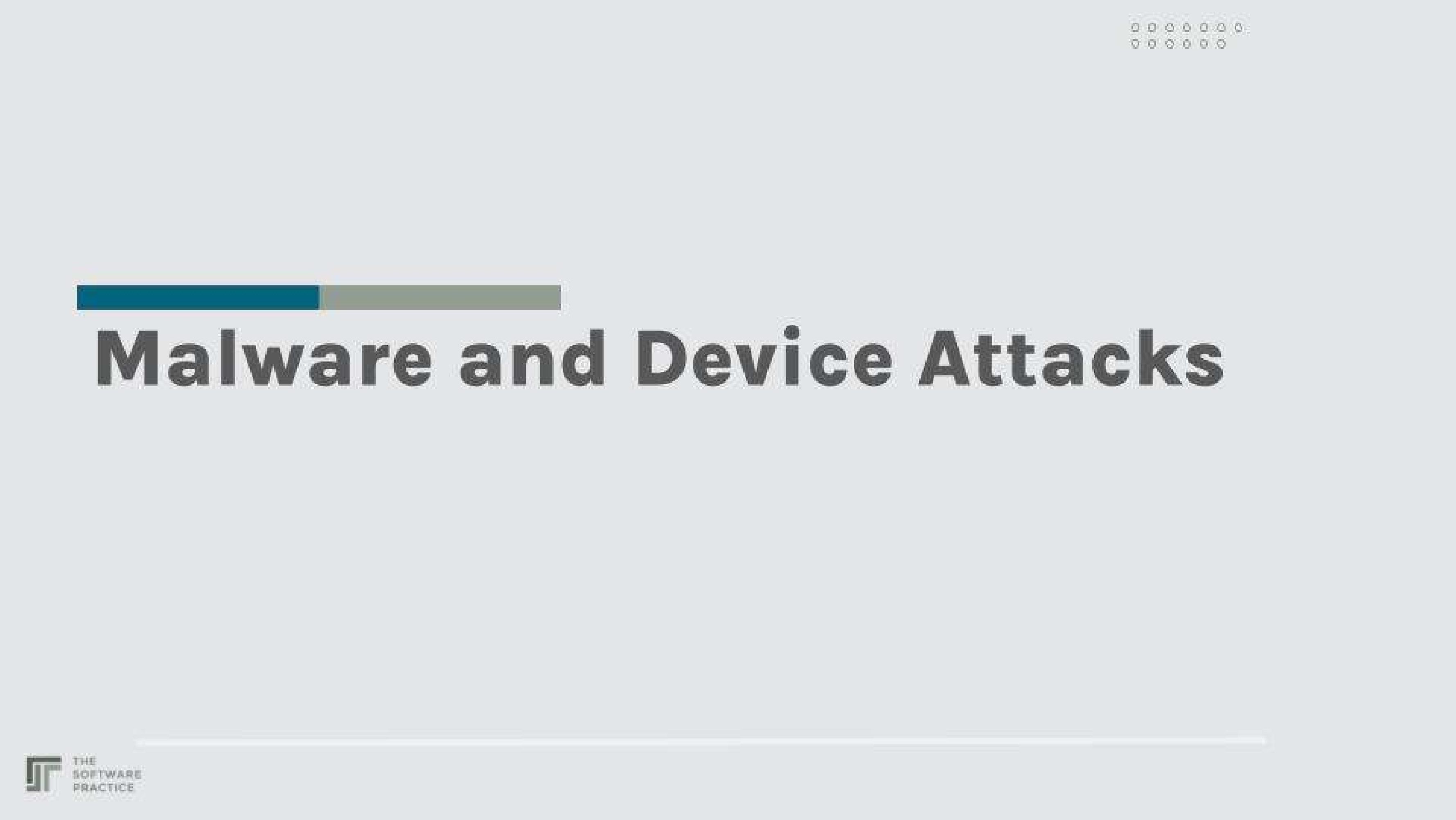
- Singapore number (+65) or overseas number or company numbers
- Voice-recorded message claiming to be calling from Govt Agency
- Asking for personal information, bank account details or money transfers
- Attacker may spoof or mask the numbers
- Unsure of your name
- Caller did not prove his or her identity
- Pressuring for information - Urgency and Scarcity
- A call followed by an email or SMS (may contain malicious links)



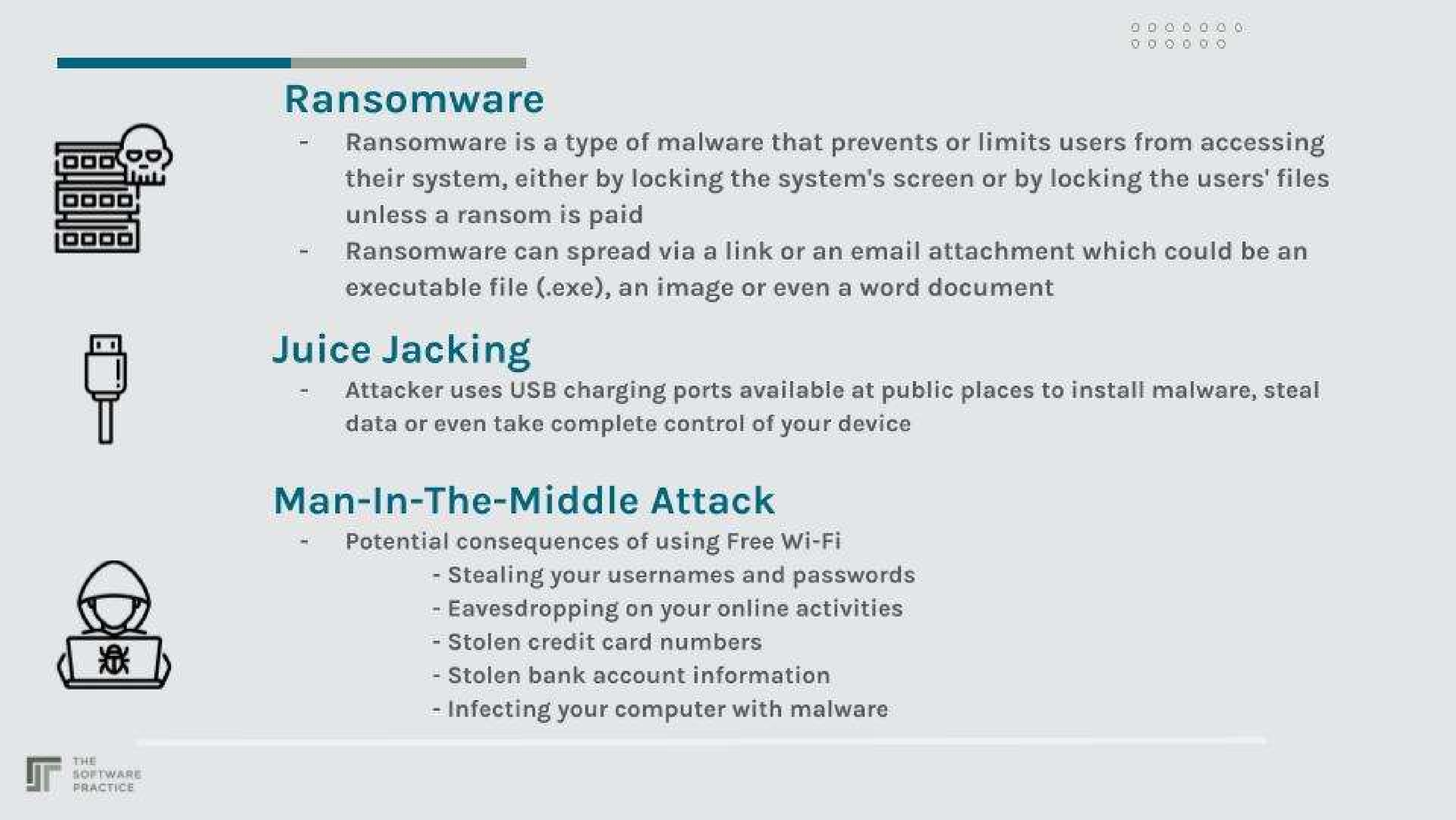
Impersonation of Staff

- Be careful of scam emails impersonating TSP’s Directors or Managers’ (or Clients’) issuing orders to recipients to transfer money or to purchase software subscriptions.

- Make sure you check and verify the sender’s email address and contact TSP’s authorized personnel (Directors and Managers) to confirm via other means.
  - e.g. Google Chat, if needed.



Malware and Device Attacks



Ransomware

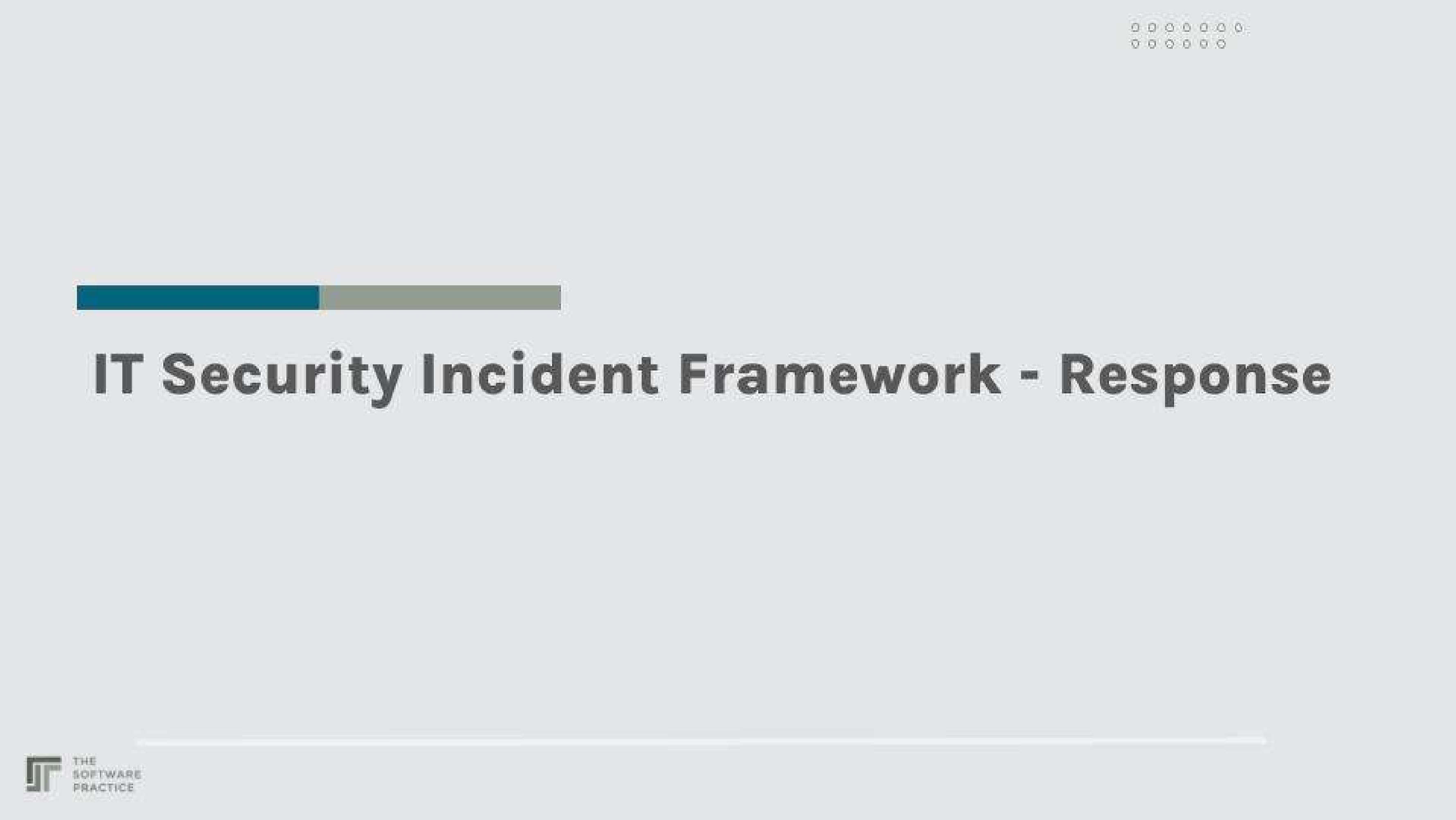
- Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid
- Ransomware can spread via a link or an email attachment which could be an executable file (.exe), an image or even a word document

Juice Jacking

- Attacker uses USB charging ports available at public places to install malware, steal data or even take complete control of your device

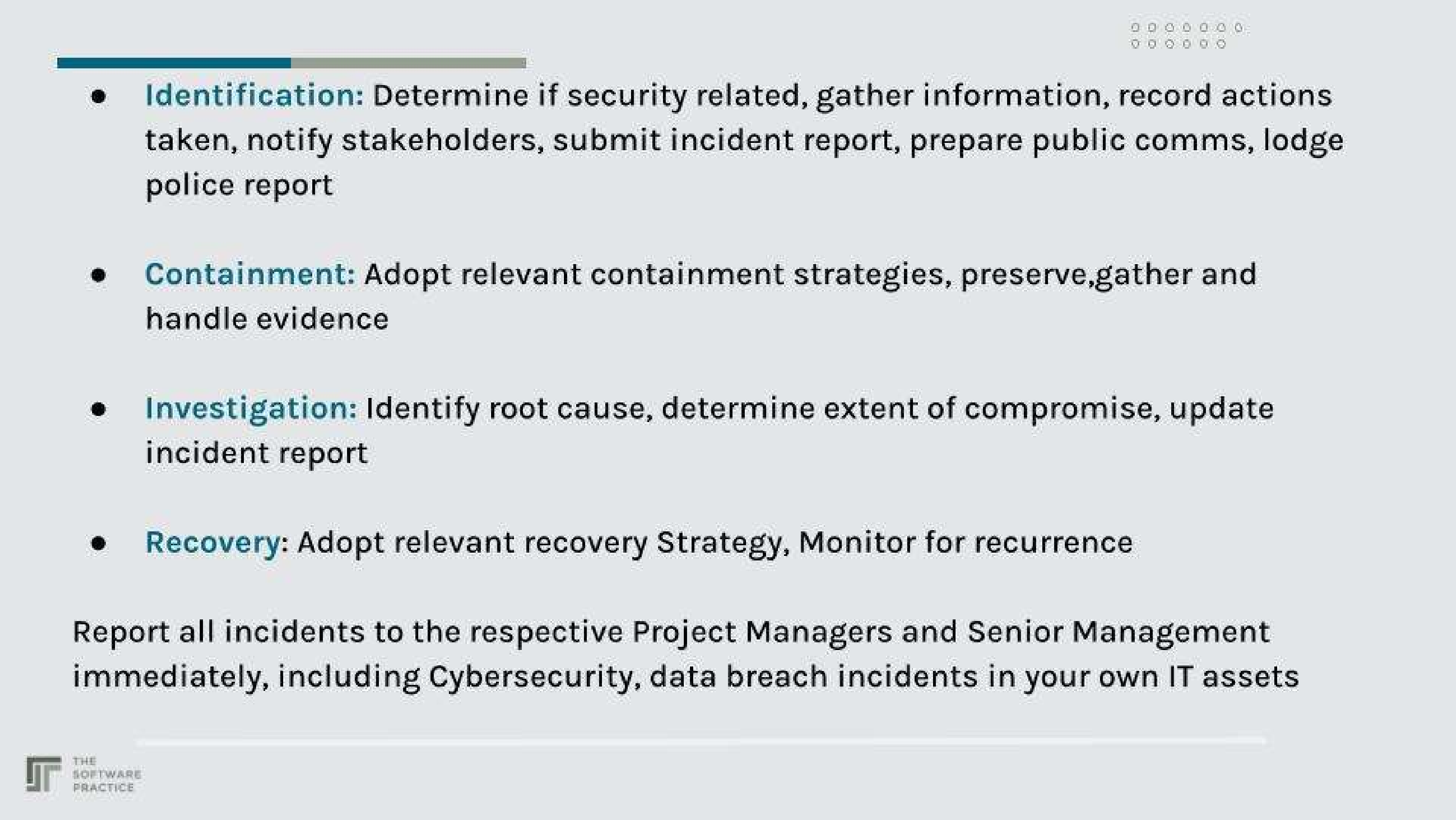
Man-In-The-Middle Attack

- Potential consequences of using Free Wi-Fi
  - Stealing your usernames and passwords
  - Eavesdropping on your online activities
  - Stolen credit card numbers
  - Stolen bank account information
  - Infecting your computer with malware



IT Security Incident Framework - Response

THE SOFTWARE PRACTICE



- **Identification:** Determine if security related, gather information, record actions taken, notify stakeholders, submit incident report, prepare public comms, lodge police report
- **Containment:** Adopt relevant containment strategies, preserve,gather and handle evidence
- **Investigation:** Identify root cause, determine extent of compromise, update incident report
- **Recovery**: Adopt relevant recovery Strategy, Monitor for recurrence

Report all incidents to the respective Project Managers and Senior Management immediately, including Cybersecurity, data breach incidents in your own IT assets

Thank you for Taking Cyber Security Seriously.