

RESORTS WORLD™ SENTOSA

Cybersecurity Awareness Training
网络安全意识培训

2025



Cyber Security Awareness Modules

			
DATA PROTECTION	SOCIAL ENGINEERING	INTERNET AND MOBILE SECURITY	CYBER SECURITY HYGIENE

网络安全意识模块

			
数据保护	社会工程学	互联网与移动设备安全	网络安全规范

DATA PROTECTION

Safeguarding our
organization



- **Data protection** ensures sensitive information is kept confidential, accurate, and accessible only to authorized users
- Protecting data helps organizations maintain trust, comply with regulations, and prevent breaches
- Examples include, but not limited to, market product strategies, company contracts, legal documents, files containing PII and account names with passwords
- Using company approved secure transfer system (RWS OneDrive) for transferring data
- Avoid viewing RWS confidential documents in public



数据保护

守护我们的组织



- **数据保护**旨在确保敏感信息的机密性、准确性，并仅限授权人员访问。
- 通过有效的数据保护措施，机构不仅能维护客户信任，还能遵守法规要求，并防范信息泄露事件。
- 敏感数据的示例包括但不限于：RWS 员工信息、市场产品策略、公司合同以及法律文件。
- 请使用公司批准的安全传输系统（如 RWS OneDrive）进行数据传输。
- 避免在公共场所查阅 RWS 机密文件，以降低泄露风险。



Data Protection (How To: Use GenAI Safely)



GenAI tools like Copilot Chat can boost productivity—but sharing sensitive data with them can lead to exposure or policy violations. Use AI responsibly and follow company guidelines to protect confidential information.

- Read and understand the **RWS Generative AI Usage Policy*** before using Copilot Chat
- Do not enter sensitive, confidential, or personal data (such as NRIC, Full Name, Address and etc) into generative AI tools
- Always use AI-generated content **responsibly** and verify its **accuracy**
- **Be mindful** of data classification when interacting with generative AI



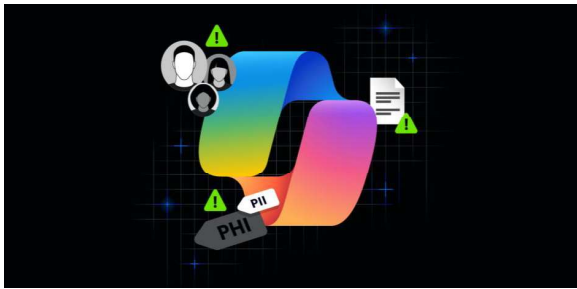
*<https://1rwsentosa.sharepoint.com/sites/ITTransformer/Policies%20Procedures/Forms/AllItems.aspx?id=/sites/ITTransformer/Policies%20Procedures/Generative%20AI%20Technology%20Usage%20Policy.pdf&parent=/sites/ITTransformer/Policies%20Procedures>

数据保护（如何：安全使用生成式AI）

生成式 AI 工具（如 RWS Copilot Chat）能够显著提升工作效率，但如果输入敏感数据，可能导致信息泄露或违反公司政策。

请务必遵守公司相关指南，以负责任的态度使用 AI 技术，切实保护机密信息。

- 使用 Copilot Chat 前，请务必阅读并理解 **RWS Generative AI Usage Policy***。
- 对 AI 生成的内容需验证其准确性，并承担使用责任。
- 与生成式 AI 互动时，应持续保持数据分类意识。
- 严禁向生成式 AI 工具输入 RWS 敏感信息、机密数据或个人资料（包括身份证号码、全名、住址等）。



*<https://1rwsentosa.sharepoint.com/sites/ITTransformer/Policies%20Procedures/Forms/AllItems.aspx?id=/sites/ITTransformer/Policies%20Procedures/Generative%20AI%20Technology%20Usage%20Policy.pdf&parent=/sites/ITTransformer/Policies%20Procedures>

Data Protection (Best Practices)



- Only transfer data via **company approved secure transfer system** (RWS OneDrive)
- Avoid viewing **RWS confidential documents** in public
- Read and understand the **RWS Generative AI Usage Policy**
- Never input sensitive, confidential or personal data into generative AI tools
- Verify the accuracy of any AI-generated content before use and ensure it is applied responsibly.



数据保护（最佳实践）

- 仅通过**公司批准的安全传输系统**（如 RWS OneDrive）进行数据传输。
- 避免在公共场所查阅 **RWS 机密文件**。
- 仔细阅读并理解 **RWS Generative AI Usage Policy**。
- 严禁向生成式 AI 工具输入 RWS 敏感信息、机密数据或个人资料（包括身份证号码、全名、住址等）。
- 在使用前务必验证 AI 生成内容的准确性，并确保其得到负责任的应用。



SOCIAL ENGINEERING

Protecting yourself and
the organization



- **Social engineering** is the act of tricking people into giving away confidential information or performing actions that compromise security.
- Attackers often **impersonate** as legitimate individual or organization via emails, messaging apps, phone calls or social media.
- Malicious intention to fraudulently **obtain** and **steal** personal or sensitive information through impersonation and scam.



社会工程学

保护个人与组织的安全



- **社会工程学**是指攻击者通过欺骗手段，诱导人们泄露机密信息或执行危害安全的行为。
- 常见攻击方式包括通过电子邮件、即时通讯应用程序、电话或社交媒体等渠道，**冒充合法个人或组织**。
- 其恶意目的在于利用身份冒充和诈骗手段，**窃取**个人或敏感信息。

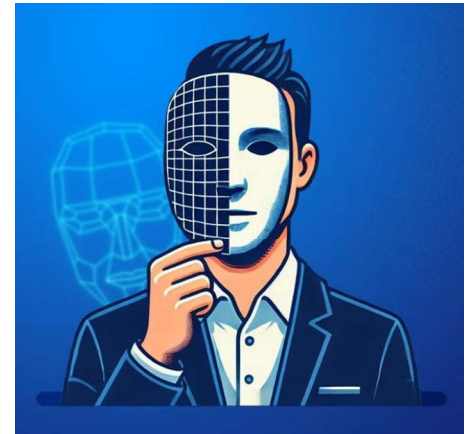


Social Engineering (How To: React To Deepfake)



Deepfake : A digitally altered video or image created using AI to imitate real people and makes someone appear to say or do things they never did—often used to mislead or spread false information.

- Always **check source** of story, video, or images. Specially if it is sensational listing. When in doubt, confirm the authenticity of the media via different sources.
- If you receive call from unknown sources, **verify. Call back** via a trusted number, before you act.
- **Limit the personal details you share online** to reduce the risk of your likeness being used in deepfakes. Be mindful of sharing preferences or professional info.

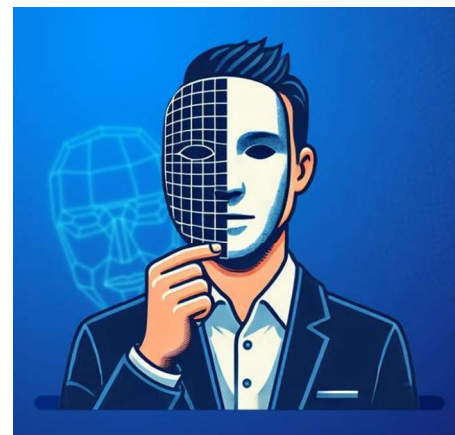


社会工程学（如何：应对“深度伪造”技术）

“深度伪造”技术（Deepfake）

深度伪造是一种利用人工智能技术篡改视频或图像，通过模拟真人形象，使其呈现未曾说过的内容或未曾实施的行为。此类技术常被用于误导公众或传播虚假信息，具有较高的安全风险。

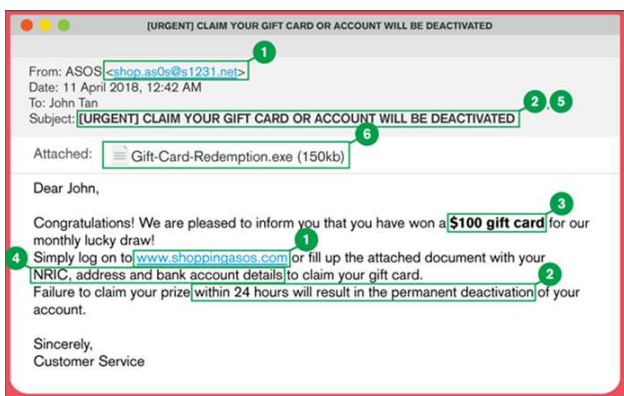
- **务必核查新闻、视频或图像的来源**，尤其是具有煽动性的内容，更应提高警惕。若有疑虑，请通过多个可信信源核实媒体资料的真实性。
- 接到陌生来电时保持警觉，在采取任何行动前，应通过可信渠道回拨确认对方身份。
- **减少在网上分享个人信息**，以降低肖像被用于“深度伪造”技术（Deepfake）的风险。同时避免过度公开个人偏好与职业资料。



Social Engineering (How To: Spot Email Phishing)



Email Phishing : A scam where attackers send fake emails to trick you into sharing sensitive information or clicking malicious links.

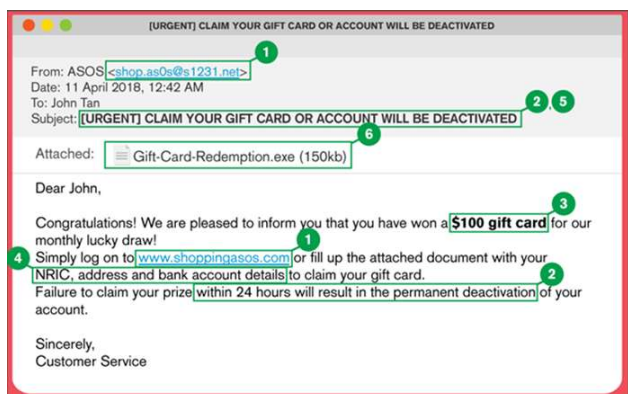


1. **Mismatched** or **misleading** information in email address or content (Hover mouse over the link to verify the real URL before clicking)
2. Use of **urgent** or **threatening** language such as fine, account lock or service disruption
3. Promise of **attractive offers**
4. **Persuasion** to open, preview attachments or click on URL links or provide confidential information
5. **Unfamiliar** or **unexpected** email sender
6. **Suspicious attachment** names and file types

社会工程学（如何：识别钓鱼邮件）



钓鱼邮件：一种网络骗局，攻击者通过发送伪造电子邮件，诱骗您分享敏感信息或点击恶意链接。



1. 发件人为未知或非预期的电子邮件。
2. 电子邮件地址或内容中存在不一致或误导性信息（点击前请将鼠标悬停在链接上以验证真实网址）。
3. 承诺诱人的优惠或奖励。
4. 诱导打开附件、点击链接或提供机密信息。
5. 使用紧急或威胁性话术（如罚款、账户锁定、服务中断等）。
6. 可疑的附件名称和文件类型。

Social Engineering (Best Practices)



How To: React To Deepfake

- Always **check source** of story, video, or images. Specially if it is sensational listing.
- Be cautious of **unexpected communications**. Verify unknown calls or emails before responding—especially if they request personal or financial information. When in doubt, consult your supervisor.

How To: Spot Email Phishing

- **Verify before you click or open** – Always hover your mouse over links to check the real URL, and confirm attachments are from trusted sources before opening
- Be cautious with **attachments and links**. Think before you click.



社会工程学（最佳实践）

如何：应对“深度伪造”技术（Deepfake）

- 务必**核查新闻、视频或图像的来源**，尤其是具有煽动性的内容，更应提高警惕。
- 对**意外收到的信息**保持警觉，在回复任何陌生来电或邮件前，务必先核实对方身份，特别是当对方索要个人资料或财务信息时。
- 若遇到任何疑虑，请立即向主管请示。

如何：识别钓鱼邮件

- **点击前先验证**—再点击链接之前将鼠标悬停在链接上查验真实网址，并在打开附件前确认其来源可信。
- 谨慎处理**附件与链接**，三思而后点击。



INTERNET AND MOBILE SECURITY

Protecting your online identity



- Mobile devices and internet access are essential but **can expose personal and company data** to cyber threats.
- **Risks** include phishing, malware, fake apps, and unsafe public Wi-Fi networks.
- Unsecured devices or apps from **unofficial sources** increase the chance of data compromise.
- Practicing **safe browsing** and **device habits** helps protect your identity and sensitive information.



互联网与移动设备安全

保护您的网络身份



- 互联网与移动设备虽不可或缺，却可能使**个人与公司数据**暴露于网络威胁之下。
- 常见风险包括：钓鱼攻击、恶意软件、仿冒应用及不安全的公共无线网络。
- 使用未受保护的设备或从**非官方来源**下载的应用程序，将显著增加数据泄露的风险。
- 培养**安全浏览与设备使用习惯**，有助于保护您的网络身份与敏感信息。



Internet Security (How To: Surf Internet Safely)

- Watch for **unexpected pop-ups or redirects** while browsing—these may indicate malicious activity
- Check for **HTTPS and padlock icon** in the URL before entering any personal or company data on a website
- Keep your browser and security software up to date to protect against known vulnerabilities and malware.



网络安全（如何：安全上网）

- 浏览网页时，警惕意外弹窗与页面跳转——这些可能是网络恶意活动的征兆。
- 在网站输入任何个人或公司数据前，请检查网址栏是否显示 **HTTPS** 及锁形图标。
- 保持浏览器与安全软件及时更新，以有效防范已知漏洞和恶意软件的攻击。



Mobile Security (How To: Protect Yourself on Public Networks)



Public Wi-Fi networks are often unsecured, making it easy for attackers to intercept data or launch cyberattacks. Using mobile devices on these networks can expose personal and company information.

- Be careful when connecting to Wi-Fi networks, including those in cafés, hotels, shared workspaces (e.g., WeWork), or even at home.
- Avoid using Wi-Fi networks that are unsecured, unfamiliar, or seem suspicious or fake.
- Only enable Bluetooth when needed, as these connections can be exploited.
- Be caution when using GPS, as your location information could be used by attackers to track you.



移动设备安全（如何：在公共网络中保护自己）



公共无线网络通常缺乏安全防护，使攻击者能够轻易窃取数据或发动网络攻击。在此类网络中使用移动设备，可能导致个人及公司信息泄露。

- 连接商场、酒店或共享办公区等公共无线网络时，务必保持警惕。
- 避免使用不安全、来源不明或可疑的无线网络。
- 仅在需要时开启蓝牙功能，以防此类连接被恶意利用。
- 谨慎使用 GPS 定位服务，防止行踪轨迹被攻击者追踪



Internet and Mobile Security (Best Practices)



How To: Surf Internet Safely

- Make sure the website uses **HTTPS** and shows a **padlock icon** before submitting any personal information.
- Keep your browser and security software up to date

How To: Protect Yourself on Public Networks

- Avoid using **free or unsecured Wi-Fi**, especially in public places (e.g shopping mall, hotel and shared workspaces)
- Enable Bluetooth and GPS only when necessary to reduce tracking and potential exposure.



互联网与移动设备安全（最佳实践）

如何：安全上网

- 在提交任何个人信息前，请确认网站使用**HTTPS**协议并显示**锁形图标**。
- 保持浏览器与安全软件更新至最新版本。

如何：在公共网络中保护自己

- 避免连接陌生的无线网络，尤其是在商场、酒店、共享办公区等公共场所。
- 仅在必要时开启蓝牙和GPS功能，以降低被追踪和数据泄露的风险。



CYBER SECURITY HYGIENE

Practicing good habits
to reduce cyber security
risks



- Practicing good cyber security hygiene helps protect your devices, accounts, and data from cyber threats and unauthorized access.
- Stay alert and avoid clicking on suspicious links or downloading unknown attachments that could contain malware.
- Each TM is responsible for having good **IT and cyber security etiquette** when using company resources like laptops, PCs, and applications
- Regularly back up important files to safeguard against data loss caused by system errors, cyberattacks, or accidental deletion.



网络安全规范

养成良好习惯以降低网络安全风险



- 养成良好的网络安全习惯，能有效保护您的设备、账户和数据免受网络威胁及未经授权的访问。
- 保持警惕，避免点击可疑链接或下载可能含有恶意软件的未知附件。
- 每位公司成员在使用电脑及应用程序等公司资源时，均有责任遵守良好的 **IT 与网络安全规范**。
- 定期备份重要文件，以防因系统故障、网络攻击或意外删除导致的数据丢失。

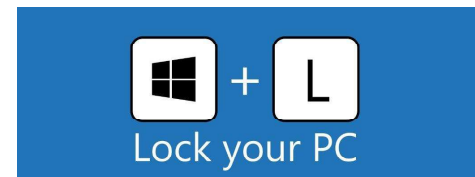


Cyber Security Hygiene (How To: Secure Your Password)

Having a strong and unique password habits are essential to protect personal and company data. Poor practices like sharing, reusing, or exposing passwords can lead to unauthorized access and data breaches.

- Set strong password by using a mix of uppercase, lowercase, numbers and special characters
- Do not **write down** or **share** your passwords to anyone
- Never enter passwords when others can observe what you are typing
- **Logout** of applications when finished
- **Lock** computer before walking away from your desk
- Change your password **immediately** if you suspect someone knows your password or account has been accessed without authorization

Is+HiS@\$Tr0nGP@55w0rd
?

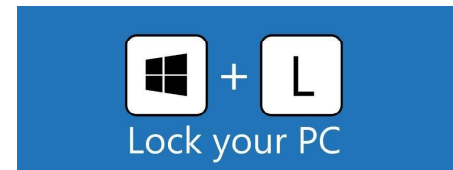


网络安全规范（如何：保障密码安全）

培养使用高强度且独特的密码习惯，是保护个人与公司数据的重要防线。密码共享、重复使用或泄露等不当行为，可能导致未经授权的访问及数据泄露事件。

- 设置高强度密码需混合使用大写字母、小写字母、数字及特殊符号。
- 严禁记录或向他人透露密码。
- 避免在他人可窥视的环境下输入密码。
- 使用完应用程序后及时退出登录以及离开座位前将电脑上锁 (按键 “Win+L”) 以防止未经授权访问。
- 若怀疑密码已被泄露，请立即更改密码。

Is+HiS@\$Tr0nGP@55w0rd?



Cyber Security Hygiene (Best Practices)



- **Use strong, unique passwords** – Include a mix of uppercase, lowercase, numbers, and special characters, and avoid reusing passwords
- **Protect your passwords** – Do not write them down or share them with anyone and avoid typing them where others can see
- **Secure your devices and applications** – Logout of applications when finished and lock your computer when stepping away
- **Respond to suspected compromise** – If you suspect someone knows your password, change password immediately



网络安全规范（最佳实践）

- **使用高强度且独特的密码**—混合使用大写字母、小写字母、数字和特殊符号，且不得重复使用相同密码。
- **保护密码安全**—禁止以任何形式记录或向他人透露密码，避免在他人可视范围内输入密码。
- **落实设备与应用程序防护**—使用完毕后立即退出应用程序，离开工位前务必将电脑上锁以防未经授权访问。
- **应对疑似泄露情况**—若怀疑密码已被泄露，请立即更改密码。



Key Takeaways

 DATA PROTECTION	Data Protection • Only use approved secure platforms (RWS OneDrive) for data transfer • Never enter sensitive or confidential information into generative AI tools
 SOCIAL ENGINEERING	Social Engineering • Always verify sender identity before clicking links or opening attachments • Being wary of unexpected communications even if they seems legitimate
 INTERNET AND MOBILE SECURITY	Internet & Mobile Security • Avoid using unsecured public Wi-Fi networks • Download apps only from official stores (iOS App Store/Google Play Store)
 CYBER SECURITY HYGIENE	Cyber Security Hygiene • Always set strong, unique passwords and never share them with anyone • Lock your devices and logout of applications when not in use



关键点

 数据保护	数据保护 - 使用公司批准的安全传输系统（RWS OneDrive）进行数据传递。 - 严禁向生成式AI工具输入RWS敏感或机密信息。
 社会工程学	社会工程学 - 点击链接或打开附件前务必核实发件人的身份。 - 对意外收到的信息保持警惕，即使内容看似合理。
 互联网与移动设备安全	互联网与移动设备安全 - 保持浏览器与安全软件更新至最新版本。 - 避免连接陌生的无线网络，在公共场所尤需注意。
 网络安全规范	网络安全规范 - 设置高强度且独特的密码，并不向任何人共享。 - 使用完应用程序后立即退出登录，离开座位前将电脑上锁。

The End

Please contact us at it-security@rwsentosa.com if you have any further questions



Acknowledgement

I hereby acknowledge that I have read information mentioned in Cyber Security Training. I further understand and agree that any breach or neglect of this policy may render me liable to prosecution.

Signature :	
Name : (Name as in Passport/NRIC)	
Passport/FIN/NRIC Number (Last 4 characters)	
Designation :	
Company Name :	
Date :	

Note: All fields are mandatory.

By signing this form, I understand and agree to provide my personal information to the Group for the purpose of conducting IT related services at the Group's premise. I will be required to produce my passport or NRIC for verification.

The Group recognizes the importance of a person's privacy and is mindful of the value of any information that a person may share with us.

