Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Employee	Awareness and Tra	aining: Social Engineering
Train employe	ees on possible social engineering t	techniques and how to combat them
Area of Risk	Attack Technique	Train Employee or Help Desk on:
Phone	Impersonation	Not providing any confidential information
		Not throwing sensitive documents in the thrash
Dumpsters	Dumpster Diving	Shredding document before throwing out
		e Erasing magnetic data before throwing out
	Phishing or Malicious Attachments	Differentiating between legitimate emails and a
Email		targeted phishing email
		Not downloading malicious attachments
		Il if information is considered confidential or not Train Employee or Help Desk on How to classify and mark document-based classification levels and keep sensitive document in a secure place
Typical Informet Top Secret Confidential Restricted Official Unclassified Clearance	Attack Technique Stealing sensitive information nation classification levels:	Il if information is considered confidential or not Train Employee or Help Desk on How to classify and mark document-based classification
Organization sh Area of Risk office Typical Inform Typical Inform Top Secret (TS) Secret Confidential Restricted Official Unclassified	Attack Technique Stealing sensitive information nation classification levels:	Train Employee or Help Desk on How to classify and mark document-based classification levels and keep sensitive document in a secure place Security labels are used to mark the security-level requirements for information assets and controls access to it Organizations use security labels to manage access dearance to their information assets
Organization sh Area of Risk office Typical Inform Top Secret (TS) Secret Confidential Restricted Official Unclassified Clearance Compartmente	Attack Technique Stealing sensitive information nation classification levels:	Il if information is considered confidential or not Train Employee or Help Desk on How to classify and mark document-based classification levels and keep sensitive document in a secure place Security labels are used to mark the security-level requirements for information assets and controls access to it Organizations use security labels to manage access
Organization sh Area of Risk office Typical Inform Top Secret (TS) Secret Confidential Restricted Official Unclassified Clearance Compartmente	Attack Technique Stealing sensitive information nation classification levels:	Train Employee or Help Desk on How to classify and mark document-based classification levels and keep sensitive document in a secure place Security labels are used to mark the security-level requirements for information assets and controls access to it Organizations use security labels to manage access dearance to their information assets
Organization sh Area of Risk office Typical Inform Top Secret (TS) Secret Confidential Restricted Official Unclassified Clearance Compartmente	Attack Technique Stealing sensitive information nation classification levels:	Train Employee or Help Desk on How to classify and mark document-based classification levels and keep sensitive document in a secure place Security labels are used to mark the security-level requirements for information assets and controls access to it Organizations use security labels to manage access dearance to their information assets
Typical Inform Top Secret (TS) Secret Confidential Restricted Official Unclassified Clearance Compartmente	Attack Technique Stealing sensitive information nation classification levels:	Train Employee or Help Desk on How to classify and mark document-based classification levels and keep sensitive document in a secure place Security labels are used to mark the security-level requirements for information assets and controls access to it Organizations use security labels to manage access dearance to their information assets
Typical Informet Top Secret Confidential Restricted Official Unclassified Clearance	Attack Technique Stealing sensitive information nation classification levels:	Train Employee or Help Desk on How to classify and mark document-based classification levels and keep sensitive document in a secure place Security labels are used to mark the security-level requirements for information assets and controls access to it Organizations use security labels to manage access dearance to their information assets

Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Separation of Duties (SoD) and Principle of Least Privileges (POLP)



Separation of Duties (SoD)

- Conflicting responsibilities create unwanted risks such as security breaches, information theft, and circumvention of security controls
- A successful security breach sometimes requires the collusion of two or more parties. In such cases, separation of duties woks well to reduce the likelihood of crime
- Regulations such as GDPR insist on paying attention to the roles and duties of your security team

Principle of Least Privileges (POLP)

- Believes in providing employees with the minimum necessary access they need, no more, no less
- Helps the organization protect against from malicious behavior, and achieve better system stability and system security



powiete © by RC-Council, All Rights Reserved, Reproduction is Strictly Prohibited.

Information Security Controls







Physical Security Controls



Technical Security Controls

Copyright $\, \mathfrak{S} \,$ by \mathfrak{W} -Cosscil. All Rights Reserved. Reproduction is Strictly Problemed.

Notes:

Appendix B Page 3696

Ethical Hacking and Countermeasures Copyright © by **EC-Council**All Rights Reserved. Reproduction is Strictly Prohibited.