ICDL

Arabia

Cyber Safety

Syllabus Version 2.0

Module Goals

Cyber Safety provides Candidates with the skills and knowledge required to operate safely with computers and a range of mobile devices and to be aware of online threats. Candidates will recognise the need to safeguard personal information on computers and mobile devices and will recognise the threats posed by Internet criminals and scams.

Candidates will understand the threats posed by viruses and will know the importance of using anti-virus software and Firewalls. Candidates will know about back-up procedures and good password practices as well as knowing how to filter email for spam and the importance of scanning email attachments before opening them.

Candidates will be aware of the information contained in smart devices and how it is shared online. Candidates will know how to set appropriate security features for smart devices to guard against security threats and prevent unauthorised access to the device and the data it contains.

Candidates will recognise the risks in everyday use of the Internet and know how to protect themselves when shopping online. Candidates will be aware of the implications of putting personal information on social networking sites and be aware of privacy issues. Candidates will be aware of the range of devices that can be used to share information and how photo and video features may be used to record and post inappropriate information.

Candidates will be aware of some of the dangers associated with social networking, including inappropriate content, age verification issues, access to profiles and the potential for predators. Candidates will understand the threats posed by social engineering attacks and the cyber threats posed to children by the use of false identities on social media.

Candidates will learn responsible behaviour practices when engaging in online activity: the importance of not circulating material that would be hurtful to others, knowing how to decline or block strangers and unwanted contacts, using webcam with only people you know, treating others online with respect.

Candidates will learn how to set parental controls in order to protect their children's online activities as well as selecting and using filtering and monitoring software. Candidates will understand the concept of online addiction and how to recognise the symptoms of the same as well as how to deal with the problem. Candidates will recognise and understand what Cyberbullying is and understand the mediums through which it can occur. Candidates will recognise the warning signs of Cyberbullying and know how to counter it. Candidates will understand why organizations develop and adopt Acceptable Usage Policies (AUP's) and recognise the components of effective policies.

CATEGORY	SKILL SET	REF.	TASK ITEM
2.1 PROTECT	2.1.1 Identity	2.1.1.1	Recognise that personal information contained on your computer needs to be safeguarded.
		2.1.1.2	Recognise the serious threats posed by Internet criminals and Internet scams.
		2.1.1.3	Understand what identity theft means, and what the risks are.
		2.1.1.4	Be aware of scams and frauds such as: Phishing, Pharming & Hacking.
	2.1.2 Authenticate	2.1.2.1	Understand the concept of user authentication.
		2.1.2.2	Know how to develop good password practices; password length, mix of alpha numeric characters, change frequency.
		2.1.2.3	Understand 'two-factor' authentication: tokens, smart cards, biometric.
	2.1.3 Anti-Virus	2.1.3.1	Understand the term virus and distinguish between different kinds of virus such as worms, Trojan Horses.
		2.1.3.2	Understand the purpose of anti-virus software.
		2.1.3.3	Understand the need to keep anti-virus software up-to-date.
		2.1.3.4	Understand what a Firewall does and why it is necessary.

CATEGORY	SKILL SET	REF.	TASK ITEM
	2.1.4 Anti-Spyware	2.1.4.1	Understand the term Spyware, and the risks associated with Spyware.
		2.1.4.2	Know how to run anti-Spyware software, and how to remove Spyware from your computer.
		2.1.4.3	Recognise the warning signs that Spyware may be on your computer.
2.2 SECURE	2.2.1 Backup	2.2.1.1	Understand what the term back up means, and why a regular backup routine is important.
		2.2.1.2	Recognise common backup devices: CD's, DVD's USB Drives, External Hard Drives, and be aware of different capacities.
		2.2.1.3	Understand what cloud-based back-up entails.
		2.2.1.4	Use backup features on your computer, and understand what it means to 'restore' a backup.
	2.2.2 Email	2.2.2.1	Understand the concept of junk / Spam email and the need to filter email. Know how to scan email attachments before opening them.
		2.2.2.2	Turn on the Spam filter in your email.
		2.2.2.3	Set Spam filter rules.
	2.2.3 Wireless	2.2.3.1	Understand what a wireless or 'Wi-Fi' network is.
		2.2.3.2	Recognise the advantages and risks associated with using public Wi-Fi hotspots.

CATEGORY	SKILL SET	REF.	TASK ITEM
		2.2.3.2	Recognise the advantages and risks associated with using public Wi-Fi hotspots.
		2.2.3.3	Recognise the security advantages of using the latest WEP or WPA wireless protocols.
	2.2.4 Physical	2.2.4.1	Recognise physical security considerations around laptop, tablet usage.
		2.2.4.2	Know how to minimize risk associated with theft or loss: keep device in view, use security cable (if appropriate), password protect, note serial number, use security pen marker.
		2.2.4.3	Recognise security issues around disposal of computers and the importance of data removal before disposal.
	2.2.5 Smart Devices	2.2.5.1	Recognise what information your device contains and shares online and how it could be misused.
		2.2.5.2	Be aware of basic security features: password protect device, set automatic locking facility, install security software, install operating system updates, mobile tracking.
		2.2.5.3	Know how using encryption on your smartphone can help prevent data theft.
		2.2.5.4	Be aware of security issues with apps. Only download apps from approved sources, check apps permissions.

CATEGORY	SKILL SET	REF.	TASK ITEM
		2.2.5.5	Be aware of viruses on mobile operating systems and mobile malware
		2.2.5.6	Be aware of security threats arising from unsolicited email or text messages. Recognise symptoms of malicious software infection: unusual data charges on bill, unexplained changes in user interface.
		2.2.5.7	Know how to turn off automatic Wi-Fi and Bluetooth functions to prevent unauthorized access to your device and data.
		2.2.5.8	Know how to delete all personal information when disposing of device.
		2.2.5.9	Know how to enable and disable location settings. Understand the advantages and risks of enabling location settings.
		2.2.5.10	Only share your mobile number with people you know and trust. Keep a record of your IMEI number in case your phone is lost or stolen.
		2.2.5.11	Know how to switch on the Internet filter to block inappropriate Internet content.
2.3 BEWARE	2.3.1 Online Risks	2.3.1.1	Recognise the risks in everyday use of the Internet: email, web browsing, online banking, online shopping, social networking etc.

CATEGORY	SKILL SET	REF.	TASK ITEM
		2.3.1.2	Recognise how pervasive inappropriate material is on the Internet.
		2.3.1.3	Be aware of common threats: recognise suspicious email requests, potentially malicious web sites.
	2.3.2 Shopping Online	1.3.7.1	Know how to protect yourself before shopping online: use most recent version of browser, ensure anti-virus software is up-to-date etc.
		2.3.2.1	Know how to identify a secure web site: padlock icon on browser status bar, an‘s’ added after the http protocol in the URL.
		2.3.2.3	Know about privacy policies.
		2.3.2.4	Be aware of the information being collected to complete the transaction and determine if it is appropriate.
	2.3.3 Paying Online	2.3.3.1	Be aware of safe payment options: credit card, debit card etc.
		2.3.3.2	Recognise when to use and when to turn off Auto-Complete tools.
		2.3.3.3	Recognise different security measures around payment: using pop-up blockers, turning off Auto-Complete tools, browser security and filtering settings.
2.4 THINK FIRST	2.4.1 Personal Identity	2.4.1.1	Understand the concept of online identity and what social networking means.

CATEGORY	SKILL SET	REF.	TASK ITEM
		2.4.1.2	Be aware of the implications of putting personal information online.
		2.4.1.3	Consider who can access your personal information: friends, work colleagues, employers, criminals, predators.
		2.4.1.4	Know about social networking privacy options, and why they are important.
	2.4.2 Sharing Devices	2.4.2.1	Be aware of the range of devices that can be used to share information: mobile phones, Smart Phones, MP3 players, iPods, Tablets etc.
		2.4.2.2	Beware how photo and video features may be used to record and post inappropriate content online.
		2.4.2.3	Be careful when posting pictures or movie clips online with your mobile phone. Ask permission of others before you post photos or video clips of them with your mobile phone.
	2.4.3 Social Networking	2.4.3.1	Recognise different social networking sites used by young people such as: Facebook, Google +, Friendster, Twitter, hi5, MySpace.
		2.4.3.2	Know how to create a social network profile and how to set your profile to private or public view.

CATEGORY	SKILL SET	REF.	TASK ITEM
		2.4.3.3	Know that that anyone may be able to view your online profile, search by criteria and access information about you.
		2.4.3.4	Recognise some of the dangers of social networking: inappropriate content, age verification issues, access to profiles, the potential for predators.
	2.4.4 Spamming and Phishing on Social Networking Platforms.	2.4.4.1	Recognise that spamming and phishing are also prevalent on social networking sites.
		2.4.4.2	Be aware of suspicious links to online ads, status updates, tweets and other posts.
		2.4.4.3	Understand the term ‘Social Engineering’ and be aware of the threats posed by social engineering attacks.
		2.4.4.4	Recognise how easy it is to create a profile on social networking sites and how criminals can use this as an opportunity to pass themselves off as someone else.
	2.4.5 False Identities on Social Media	2.4.5.1	Be aware of the cyber threats posed to children by the use of false identities: grooming, child exploitation.
		2.4.5.2	Be aware of the cyber threats posed to adults by the use of false identities: access to personal information, identity theft.

CATEGORY	SKILL SET	REF.	TASK ITEM
2.5 VIRTUAL WORLD	2.5.1 IM / Chat Rooms	2.5.1.1	Understand what Instant Messaging (IM) is, and what Chat rooms are.
		2.5.1.2	Know how to create a generic IM profile.
		2.5.1.3	Set options to only allow contacts from Buddy list only, and block unwanted contacts
		2.5.1.4	Know how to disable web cam.
	2.5.2 Video, Blogs	2.5.2.1	Recognise the ability of the Internet to share videos: YouTube, Myspace TV, etc.
		2.5.2.2	Understand what blogs and micro-blogs are, and how they integrate with social networking.
		2.5.2.3	Recognise the risks associated with releasing personal information, or slander or gossip in a blog.
		2.5.2.4	Understand how file sharing web sites work, and the potential for viruses and malware from using file sharing sites.
	2.5.3 Online Games	2.5.3.1	Be aware of online Role Playing Games (RPG's) and related risks: unknown players, addictive quality.
	2.5.4 Be Responsible	2.5.4.1	Do not circulate messages, pictures, or other material that can be hurtful. Share images only with people you know and trust

CATEGORY	SKILL SET	REF.	TASK ITEM
		2.5.4.2	Know how to decline or block strangers and unwanted contacts. Be careful about planning to meet people you don't really know, even if they have become your 'online friends'.
		2.5.4.3	Use a webcam only with people you know – disconnect or disable it when not using it.
		2.5.4.4	Be aware that downloading music, films, pictures, computer programs and games from the Internet may be against the law, unless it clearly says on the site you are using.
		2.5.4.5	Always treat others online as you would like or expect to be treated yourself.
2.6 LEARN TOGETHER	2.6.1 Discuss	2.6.1.1	Learn together; discuss your computer use with friends and family.
		2.6.1.2	Accept that it is best to keep home computers in central and open locations.
		2.6.1.3	Know about filtering and monitoring software to: filter explicit images, log online activities, set online timers, block personal information from being posted or emailed.
	2.6.2 Parental Controls	2.6.1.1	Recognise that parental controls are available on a range of media devices: digital TV, computer & video games, mobile phones, iPods, tablets and computer software.

CATEGORY	SKILL SET	REF.	TASK ITEM
		2.6.2.2	Set parental controls on operating software.
		2.6.2.3	Know how to install or download parental monitoring software: www.theparentalcontrolbar.org
		2.6.2.4	Know how to install or download parental monitoring software: Know why it may be appropriate to create different user accounts with different access and privileges for each account.
		2.6.2.5	Know why you would set-up a child email account, direct incoming emails to parental inbox for review.
		2.6.2.6	Be aware of the criteria to consider when choosing parental filtering software: •Does it work on non-English content? •How customizable is it? •Does it only filter websites, or does it also include e-mail, instant messaging, file-sharing programs and social media? How applicable is it to different types of devices, such as smart phones, or gaming consoles?
		2.6.2.7	Be aware of how young people might hide online activity.
		2.6.2.8	Know ways to protect against young people hiding online activity.
		2.6.2.9	Be aware that filtering software is not a substitute for proper parental supervision and open discussion with children and teens.

CATEGORY	SKILL SET	REF.	TASK ITEM
		2.6.2.10	Know how to create an Internet User Agreement for parents and children
	2.6.3 Online Addiction	2.6.3.1	Understand how Internet use can interfere with daily life, work and relationships
		2.6.3.2	Recognise the concept of Internet Addiction Disorder (IAD) and the different types of addiction problems: inappropriate content, chat rooms, online gaming, and compulsive web surfing.
		2.6.3.3	Recognise some of the symptoms of IAD: losing track of time online, isolation from family and friends, defensive about Internet use, trouble completing other tasks, sleep disturbances.
		2.6.3.4	Know how to help a child with Internet addiction: encourage other interests and social activities, monitor computer use and set clear limits, use apps to limit child's smartphone use, discuss underlying issues with the child, get professional help.
		2.6.3.5	Online Addiction Quiz.
2.7 VIRTUAL BEHAVIOUR	2.7.1 Communicating	2.7.1.1	Understand what 'Netiquette' means.
		2.7.1.2	Understand the concept of no 'take backs' once information is posted.
		2.7.1.3	Know why 'smart' online user names that reveal only limited personal information are used.

CATEGORY	SKILL SET	REF.	TASK ITEM
		2.7.1.4	Recognise why protecting personal information, and maintaining privacy is always important.
		2.7.1.5	Beware of adding strangers to buddy/friend lists, and the risks.
	2.7.2 Cyber Bullying	2.7.2.1	Recognise and understand what Cyberbullying is.
		2.7.2.2	Understand the mediums through which Cyberbullying can occur.
		2.7.2.3	Understand the speed with which information / pictures can spread and the impact of Cyberbullying.
		2.7.2.4	Understand the consequences of cyber bullying. Understand the motives for bullying online, such as anonymity, bully feels they can 'get away with it'. Understand that online bullying can also be a two way process.
		2.7.2.5	Recognise the warning signs of Cyberbullying. A child may be experiencing cyber bullying if he or she: •appears sad, moody, or anxious •avoids school •withdraws from or shows a lack of interest in social activities •experiences a drop in grades or decline in academic performance •appears upset after using the computer or being online
		2.7.2.6	Know how to counter Cyberbullying, how to record it and report Cyberbullying concerns to the appropriate authorities.

CATEGORY	SKILL SET	REF.	TASK ITEM
		2.7.2.7	What if your child is the bully? Tips for parents (and teachers) on how to deal with children who bully others online.
		2.7.2.8	Recognise that adults can also suffer from Cyberbullying: inappropriate comments in messages, emails, on public forums and social network sites, inappropriate texting, Cyber Stalking. Understand the difference between Cyber Stalking and Social Engineering.
2.8 POLICY	2.8.1 Usage	2.8.1.1	Understand what an Acceptable Usage Policy (AUP) is and why it is important in organizations.
		2.8.1.2	Know the components of a good AUP: educate parents & students, minimize risk, encourage Netiquette & appropriate social & ethical behaviour, protect vulnerable children, personal identity, password protection.
		2.8.1.3	Understand mobile operator moderation policies with regard to access to chat rooms or games and control of spam.
	2.8.2 Copyright	2.8.2.1	Be aware of copyright laws and their impact for illegal downloads using file sharing services.
		2.8.2.2	Recognise that pirating of music, movies and software is illegal the implications of this.

Appendix to Cyber Safety book:

1. Online Safety Tips for Parents.
2. Online Safety Policy Guidelines for Schools and Advice for Teachers.
3. Online Safety Tips for Young Internet Users (Teens and Preteens).