**Lesson Plan**

Lesson 2.1.3 (Technology)

|  |  |  |
| --- | --- | --- |
| Lesson 2.1.3 (Technology) | | Duration: 150 minutes |
| **Resources Required:**   * PC/Laptop loaded with software versions compatible with the prepared materials * Projector and display screen. * Internet access (if available). * Student notepaper and pens. | | |
| **Session Aim:**  The aim of this session is to update delegates in relation to new crime types and threats delivered by new technology. Although some of the subjects were covered briefly on the introductory course, they are covered in more detail in this session | | |
| **Objectives:**  At the end of this session, delegates will be able to:   * Explain the different types of Business Email Compromise * Identify the threats offered by the Internet of Things (IOT) * Differentiate between the layers of the Internet * Explain how virtual currency transactions are conducted | | |
| **Trainer Guidance**  This session introduces the latest technologies that are impacting on criminal behaviour. The Internet Online Threat Assessment (IOCTA) 2017 was released in September 2017 and is used in some slides as it is the most up to date information available. Trainers will need to revisit this information as new reports and information becomes available. The videos used in this session are acknowledged and are available for free download and use. The trainer may wish to use demonstration as a teaching method, for example in the Darknet session, by using the TOR browser to show delegates how to access on line crime tools. | | |
| **Lesson Content** | | |
| **Slide Numbers** | **Content** | |
| 1 to 3 | The first slides lay out the structure and objectives of this session. Delegates will be given an opportunity to ask any preliminary questions that they may have regarding the structure and objectives of the session. | |
| 4 to 18 | These slides provide information about the influence of the Internet, on a global scale (slides 5 to 12) and specifically for the country that the course is being delivered (slides 13 to 18). The trainer should ensure that these slides are relevant to the country of delivery and use them to discuss the impact of the Internet in the country and in the global context. | |
| 19 to 30 | These slides provide information about recent crimes that impact at a significant level. The trainer should familiarise themselves with the crimes and introduce those that are relevant to the region of the training delivery. The trainer may wish to substitute cases from the country. | |
| 31 to 32 | Introduces information from IOCTA 2017 in relation to BEC. | |
| 33 | Trainer to ask the delegates the question in the slide. If there is no response, continue with the presentation. If there are some examples, give time for explanations from the delegates and use the information given to compare with the information in the presentation | |
| 34 to 42 | These slides and the videos are sourced from Trend Micro/Europol information and data and provide a very good explanation of the business Email Compromise methodologies and prevention measures. The final video introduces Business Process Compromise (BPC) as a variation of BEC. | |
| 43 to 44 | These are an introduction to the subject of Internet of Things (IOT). The trainer should invite the delegates to share any knowledge or experience they may have of IOT.  Please note that Slide 45 is a video that gives a very good example of how a motor vehicle may be connected to multiple services by IOT and how the services may be of great benefit to a customer. The trainer may also reflect on the availability of electronic evidence because of these connections. | |
| 45 | This video gives a very good example of how a motor vehicle may be connected to multiple services by IOT and how the services may be of great benefit to a customer. The trainer may also reflect on the availability of electronic evidence because of these connections. | |
| 46 | This slide provides an opportunity to introduce IP version 6 as the platform that enables IOT | |
| 47 | This slide gives the trainer the opportunity to discuss the issues of security of the IOT devices and the fact their producers are not security experts. IOT devices are a security time bomb. The trainer may wish to expand on the bullet points according to their own knowledge of the subject. | |
| 48 to 49 | These slides provide further up to date information from the IOCTA 2017 report. They support the issues raised in slide 20. | |
| 50 to 57 | These slides give information about IOT devices and some of the issues. Trainers are encouraged to use examples they are aware of and in particular if there are security issues with them, such as is the case with the iKettle. | |
| 58 to 60 | This is the beginning of the session on Dark net and services. These slides provide the context from IOCTA to set the subject in motion. | |
| 61 to 67 | These slides explain the Darknet, criminal use and services, as well as some successes in closing sites used for criminal activity. The trainer is encouraged to use live demonstrations of accessing the Darknet where appropriate and there is a suitable Internet connection. | |
| 68 to 77 | These slides are mostly a reminder of the issues raised in the introductory course, with additional video support and, as with other subjects, the most up to date information from the IOCTA 2017 report. | |
| 78 to 79 | The trainer should recap the session objectives with the delegates and give them the opportunity to ask any questions relating to the materials covered in this lesson. | |
| **Practical Exercises**  There are no compulsory practical exercises, although trainers are encouraged to give live demonstration of Darknet access where appropriate. | | |
| **Assessment/Knowledge Check**  No formal assessment has been prepared for this session. The delegates will be expected to participate actively. | | |