ITU Centres of Excellence Network for Arab Region
Smart Tunisian Technoparks
(S2T)

Face-to-Face Training on
"Cybercrime Management: A Proactive Approach"
Tunis - Tunisia, 16 - 20 September 2019

COURSE OUTLINE

COURSE DESCRIPTION

Title	Cybercrime Management: A Proactive Approach
Objectives	This course is designed to introduce the participant to the cybercrime prevention, detection and incident management processes, policies, procedures and cybercrime governance activities. It therefore focus on cybercrime management standards, guidelines and procedures as well as the implementation and governance of these activities. In addition, the present course provides participants with an understanding of the new and advanced digital investigation techniques for machines, systems and networks since new technologies are opening today the door to new criminal approaches.
Dates	16 - 20 September 2019
Duration	5 Days
Registration deadline	6 September 2019
Training fees	500 USD
Course code	**19WS24250ARB-E**

LEARNING OUTCOMES

This training aims to build knowledge in the current methods and technologies used across cyber crime and provide the participants with extensive insights and practices about Cybercrime Management: A proactive approach.

The training will cover the following topics:

- ✓ Present and discuss the cybercrime statistics and case studies;
- ✓ Explain the cybercrime prevention and detection;
- ✓ Describe in detail the cybercrimes processes, policies and procedures;
- ✓ Provide a detailed understanding of the cybercrime governance activities;
- ✓ Explain the investigation process and basics of a digital investigation mission;
- ✓ Provide support and guidance in the identification and handling of the electronic evidences.

TARGET POPULATION

This training is designed to ICT and Telecoms professionals with an interest in cyber-security and cyber-criminality.

TUTORS/INSTRUCTORS

NAME OF TUTOR(S)/INSTRUCTOR(S)	CONTACT DETAILS
Nizar Ben Neji is a Professor and a researcher at the University of Carthage in Tunisia and former Fulbright visiting scholar at the Massachusetts University of Amherst in USA. He worked also as PKI engineer then project manager at the Tunisian Government Certification Authority (ANCE) of the Ministry of ICT and Digital Economy in Tunisia from 2005 to 2013 and was member of several National Steering committees and working groups in charge of supervising and conducting National IT and e-Government projects such as TUNEPS (Tunisian Online E-Procurement System) and the National committee in charge of revising the cybersecurity and cybercriminality law in Tunisia and many others. To date, Dr. Nizar Ben Neji is delivering seminars in wide variety of subjects related to computer and network security at an international level with CTO (Commonwealth Telecommunications Organization) and ITU (International Telecommunication Union) and AICTO (Arab Information and Communication Technology Organization).	nizar.benneji@fsb.rnu.tn nizar.benneji@gmail.com

EVALUATION

I. Post Test.
II. Case Study.
III. Design Project.

TRAINING SCHEDULE AND CONTENTS / AGENDA

Date for 1st day	Time; Start time	Topics/Activities
16/09/2019	08:00 - 8:30	Registration
	09:00 - 12:00	**Introduction** **Statistics and annual reports about cybercrimes** – In the world – In Africa – In Tunisia
	12:00 - 14:00	Lunch time
	14:00 - 17:00	**Legal and institutional frameworks needed for cybersecurity and cybercriminality** – Stack of regulation texts – Stack of security policies – Entities needed to implement security strategies, rules and policies – Protection of personal data
Date for 2nd day	**Time; Start time**	**Topics/Activities**
17/09/2019	09:00 - 12:00	**Digital security** – Evolution of security – Security objects and objectives – Vulnerability, Threat and Risk
	12:00 - 14:00	Lunch time
	14:00 - 17:00	**Cyber crimes** – Non-payment/non-delivery/advanced fee for goods and services – Personal data breach – Phishing / Vishing / Smishing / Pharming – Credit card fraud – Cyber extortion – Identity theft and government Impersonation – Cyber harassment – BEC (Business Email Compromise) and EAC (Email Account Compromise) – Tech support fraud and misrepresentation

		– Malware dissemination (Virus, Worm, Scareware, Ransomware, Trojan, Backdoor, …) – Large scale attack (Cyberterrosim, hacktivism,…) – Denial of Service (DoS or DDoS) – Cybervandalism – Software piracy and counterfeiting of programs – Data leak
Date for 3rd day	**Time; Start time**	**Topics/Activities**
18/09/2019	09:00 - 12:00	**Security Objectives and Techniques of Protection** – Authentication (Multifactor authentication, SSO, OTP, ...) – Confidentiality and privacy (Encryption, Anonymization, ...) – Data integrity over its entire life-cycle (Hashing, Digital signature, Time Stamping, ...) – Non-repudiation of creating, approving, sending and receiving documents – High availability (Data replication, Failover, Load balancing, ...) – Traceability and history of electronic acts and actors
	12:00 - 14:00	Lunch time
	14:00 - 17:00	**Digital Proofs and Building Trust in the Digital World** – Cryptographic solutions – Role of PKI systems and the electronic identification: eID, e-Passport, e-Health Card, e-Driving License, – Digital signature mechanisms and standards – Time stamping service
Date for 4th day	**Time; Start time**	**Topics/Activities**
19/09/2019	09:00 - 12:00	**Forensics Overview** – Computer Forensics Fundamentals – Benefits of Computer Forensics – Computer Crimes – Computer Forensics Evidence and the Courts **Cyber Forensics:** – Computer forensics – Network forensics – Forensics tools
	12:00 - 14:00	Lunch time
	14:00 - 17:00	**Forensics Process and Evidence**

		– Forensics Process – Forensics Investigation Process – Securing the Evidence and Crime Scene – Chain of Custody – Law Enforcement Methodologies – Forensic Evidence – Evidence Sources – Evidence Duplication, Preservation, Handling, and Security – Forensics Soundness – Order of Volatility of Evidence – Collection of Evidence on a Live System – Court Admissibility of Volatile Evidence
Date for 5th day	**Time; Start time**	**Topics/Activities**
20/09/2019	09:00 - 12:00	**Recommendation on the protection of the cyberspace** – For the Government – For the Businesses – For the Individuals
	12:00 - 14:00	Lunch time
	14:00 - 16:00	**Evaluation of the seminar, handing-over of the training certificates and closing of the workshop.**

METHODOLOGY

The course's methodology is based on the following types of sessions:

- Theory sessions: Part deal with both basic and advanced concepts, those are directly applicable to professional practices.
- Practical sessions. In these sessions, a set of practical labs will be done to experiment and be familiar with the theoretical concepts.
- This training for maximum 15 people will be held mainly in laboratory as practical training, to ensure trainer availability and ease access to handling materials in optimal conditions (course material included).

COURSE COORDINATION

Training Coordinator:	**ITU Coordinator:**
Mrs. Houda Jarraya Focal Point S2T Tel: + 216 70 834 870 Mobile: +216 28 300 878 – +216 97 879 228 Fax: +216 71 857 803 Email : houda.jarraya@s2t.tn houda.jarraya@gmail.com	**Eng. Mustafa Al Mahdi** Programme Administrator Arab Regional Office-ITU Tel: +202 3537 1777 Mobile: +201141177573 Fax : +202 3537 1888 Email : mustafa-ahmed.al-mahdi@itu.int

REGISTRATION AND PAYMENT

ITU Academy portal account

Registration and payment should be made online at the ITU Academy portal.

To be able to register for the course you MUST first create an account in the ITU Academy portal at the following address:

https://academy.itu.int/index.php/user/register

Training registration

When you have an existing account or created a new account, you can register for the course online at the following link: https://academy.itu.int/index.php/training-courses/full-catalogue/cybercrime-management-proactive-approach

You can also register by finding your desired course in our training catalogue https://academy.itu.int/index.php/training-courses/full-catalogue

Payment

1. On-line payment

A training fee of USD 500 per participant is applied for this training. Payments should be made via the online system using the link mentioned above for training registration at https://academy.itu.int/index.php/training-courses/full-catalogue/cybercrime-management-proactive-approach

2. Payment by bank transfer

Where it is not possible to make payment via the online system, select the option for offline payment to generate an invoice using the same link as above. Download the invoice to make a bank transfer to the ITU bank account shown below. Then send the proof of payment/copy of bank transfer slip and the invoice copy to Hcbmail@itu.int and copy the course coordinator. All bank transaction fees must be borne by the payer.

Failure to submit the above documents may result in the applicant not being registered for the training.

3. Group payment

Institutional Contacts are users that represent an organization. Any student can request to be an institutional contact or to belong to any existing organization.

To do this, head to your profile page by clicking on the **"My account"** button in the user menu. At the bottom of this page you should see two buttons:

a. If you want to **become an institutional contact**, click on the "**Apply to be an Institutional Contact"** button. This will redirect you to a small form that will ask for the organization name. After you fill the name of the organization you want to represent, click on **"continue"** and a request will be created. An ITU Academy manager will manually review this request and accept or deny it accordingly.

b. If you want to **belong to an existing organization**, click on the **"Request to belong to an Institutional Contact"** button. This will redirect you to a small form that will ask you to select the organization you want to join from an organization list. After you select the correct organization, click on **"continue"**, a request will then be created. The Institutional Contact that represents that organization will manually accept or deny your request to join the organization.

ITU BANK ACCOUNT DETAILS:	
Name and Address of Bank:	UBS Switzerland AG Case postale 2600 CH 1211 Geneva 2 Switzerland
Beneficiary:	Union Internationale des Télécommunications
Account number:	240-C8108252.2 (USD)
Swift:	UBSWCHZH80A
IBAN	CH54 0024 0240 C810 8252 2
Amount:	USD 500
Payment Reference:	CoE-ARB [24250]-[WBS No. P.40592.1.03]

4. Other method of payment

If due to national regulations, there are restrictions that do not allow the payment to be made using options 1 & 2 above, please contact the ITU Coordinator for further assistance.