COMPLETE

ANTIFRAUD

SOLUTION FOR ONLINE AND MOBILE BANKING

VIRTUAL COURSE

5 -7 OCT 2020

gce since 1985

ThreatMark

INTRODUCTION

A Threats and attacks aimed at digital payments and online banking services are growing in terms of frequency and volume. Majority of detected threats use specialized tools, at least at one stage of an attack. Alongside malware driven attacks, most frequent fraudulent schemes are based on: phishing, social engineering, attempts to misuse the application, bypass application business logic, and efforts to limit applications on all digital channels.

Within these sessions we will look under the hood of fraudulent applications and examine real-world examples of mobile & internet banking attacks.

These virtual sessions will answer questions such as: How can you protect your bank? How to recognize that a device has been compromised by malware? What are typical evasion techniques that malware uses to cover its activities? What are common strategies of anti-fraud solutions to detect malware & why they are failing?... and many others.

gce since 1985 ThreatMark

FULL COURSE OUTLINE

Complete antifraud solution for online and mobile banking

Brief overview:

This virtual course will arm attendees with knowledge about malware fundamentals and insights into fraudsters work including identification of the typical "point of entry" for fraud and malware. Additionally, the attendees will learn how to prevent the attacks & threats within a Layered Security methodology.

Delivery

The course will be delivered in 3 lessons, all containing presentations in PowerPoint, video live demo & showcases of malware types & relevant details.

1. **Mobile Malware Deep Dive**

- What are typical schemes bad actors use to steal funds through mobile banking
- How to recognize a device being compromised by a malware
- Typical steps for a malware attack
- Malware evasion techniques
- Mobile malware detection

FULL COURSE OUTLINE

2. Complex Phishing Techniques

- Typical phishing types (from simple to complex)
- Older strategies and why they worked
- Breakdown of complex phishing vectors (cross-channel, multi-step)
- Evasion techniques used by bad actors & how their work
- How to detect phishing sites

3. Introducing Layered Security

- Introduction to the concept of Layered Security
- Spotting the bad actor (what alerts are significant, how to "read" them)
- Methods to prove the identity of the legitimate user
- Type of data you might harvest from a user session
- What we have learned from previous client's deployments
- How to effectively prevent fraud

KEY TAKEAWAYS FROM THE PROGRAMME

- Understanding of terminology around cyber threats & malware
- Understanding of techniques used by bad actors to infect your device
- Ability to recognize malicious behavior on your device
- See a live simulation of a MiTB attack with bad actor tracing in real-time
- In-depth walkthrough with most common attack vectors
- Review real-life showcase of web injection & mobile malware
- Cunning malware evasion techniques and how malware is fighting against being detected

An invaluable workshop, packed with relevant, real-life examples supported with statistics & data from ThreatMark's Security Operation Center used by banks across four continents, protecting more than 20 million users, connected to millions of data points.

COURSE DETAILS

DATES	5-7 OCT 2020
TIMES	11.00 am - 2.00 pm
COST	450 JOD
LOCATION	This course will be delivered virtually

COURSE DIRECTOR

Lukáš Jakubíček

has more than 10-years of experience within IT and got strong security know-how by working with experts in cybersecurity in ThreatMark jointly building the next generation of anti-fraud solution for digital channels. Lukáš regularly trains banks' fraud analysts and is working closely with members of ThreatMark's Security Operation Center (SOC). This unique relationship provides him an excellent overview of the current threat's landscape and allows him to keep up with the current cyber threats & prevention methods.

FOR MORE INFORMATION AND TO REGISTER

PLEASE CONTACT:

Eng. Amer Al- Najjar

anajar@gce.com.jo

Mob:+962 77 739 7728

Tel : +962 6 551 38 79 – Ext. 350

Fax: +962 6 551 35 09