اتحاد المصارف العربية
Union of Arab Banks

NAVIGATING NEW SECURITY CHALLENGES:

FROM PAGERS TO SMARTPHONES

ONLINE

28 - 30 OCTOBER 2024

FROM 11:00 TILL 14:00 (BEIRUT TIME GMT 3+)

NAVIGATING NEW SECURITY CHALLENGES:
FROM PAGERS TO SMARTPHONES

OVERVIEW: CYBERSECURITY'S MOBILE SAFETY

After the pager and VHF blasts in Lebanon, we saw a flood of false information spreading around the nation, inciting panic among smart device users.

This course will focus on the fundamental distinctions between smart devices and the outdated system pagers, as well as the risks associated to each of them. The pagers incident will serve as a wake-up call for all of us after exposing our smart phones to the internet and the impact of exploiting them by threat actors.

WORKSHOP OBJECTIVES

Raise Awareness: Inform people and organizations about the growing dangers that confront mobile devices and the significance of mobile security in the current digital environment.

Identify risks: Clearly explain the most frequent risks to mobile security, such as malware, phishing, and app-related vulnerabilities.

Encourage Best Practices: Provide advice and best practices for securing mobile devices, guaranteeing safe app usage, and preserving personal information.

Encourage Proactive Measures: Emphasize that in order to reduce risks, secure network procedures, robust authentication techniques, and frequent updates are essential.

Encourage a Culture of Cybersecurity: Create a culture of cybersecurity awareness in both personal and professional situations by instilling in users a sense of duty to stay watchful and informed about evolving threats.

AUDIENCE

Raise Awareness: Inform people and organizations Anyone interested in smart devices safe practices

NAVIGATING NEW SECURITY CHALLENGES:
FROM PAGERS TO SMARTPHONES

OUTLINE

I. Introduction

A. The personal and corporate Use of Mobile Devices in Daily Life

B. The Increase in Mobile Vulnerabilities and Threats

C. What is a Pager and how do VHF/UHF pagers work

D. Key difference between pagers and smart phones

II. Mobile cyber security Risks

A. Typical categories of mobile risks

1. Malware (ransomware, trojans, and viruses)
2. Attacks by phishers
3. Man-in-the-middle (or network) assaults
4. App flaws

B. Risks associated to pagers

C. Data on events involving mobile security

D. Instances of serious violations

III. Best Practices for Mobile Device Security

A. Use of complex and robust passwords

B. Strong authentication mechanisms

C. Software Updates for the operating system

D. Updates for apps

E. Setting up antivirus software

F. User awareness

G. Security Hardening checklists

IV. Safe App Usage

A. Downloading apps from trusted sources

B. Reviewing app permissions

C. Avoiding suspicious or unnecessary apps

V. Secure Network Practices

A. Avoiding public Wi-Fi for sensitive transactions

B. Using VPNs for enhanced security

C. Understanding secure vs. unsecured networks

VI. Data Protection and Privacy

A. Encrypting sensitive data

B. Backing up data regularly

C. Managing personal information shared on apps and social media

VII. Responding to Security Incidents

A. Identifying signs of a breach or malware

B. Steps to take if compromised

1. Reporting the incident
2. Restoring device security

VIII. Future Trends in Mobile Security

A. Advances in biometric security

B. AI and machine learning in threat detection

C. The impact of 5G technology on mobile security

NAVIGATING NEW SECURITY CHALLENGES:
FROM PAGERS TO SMARTPHONES

JEAN-MICHEL KAWKABANI
CISA
ARCSHIELDS, DIRECTOR

Jean-Michel is the former Head of Information Security Department at Byblos Bank Group.

He is a Certified Information Systems Auditor (CISA) from ISACA, a lecturer at University Saint Joseph-ESIB and Ecole Nationale D' Administration (ENA) Lebanon and a cyber security trainer and technical committee member in the Union of Arab Banks.

Jean Michel was respectively the Head of IT Audit, the Head of MIS and the Head of Information Security department at Byblos Bank Group. He was recently appointed as Director of ArcShields Cybersecurity company.

He graduated from the French engineering school Ecole Nationale de la Statistique et de L'Analyse de L 'Information (ENSAI) and holds a degree in Economics from Saint Joseph University.

Jean Michel has been an Information Systems professional for more than 20 years including 19 years of Information Security and IT Audit in the financial industry.

He is a certified vulnerability scanner, an expert in implementing an Enterprise Security Architecture, conducting risk assessment, CSIRT, Digital forensics, IT Auditing and Penetration testing and has been teaching & lecturing security standards & best practices in reputable universities & governmental agencies.

التعامل مع التحديات الأمنية الجديدة:
من الأجهزة إلى الهواتف الذكية

نظرة عامة: سلامة الأمن السيبراني للأجهزة المحمولة

بعد حوادث أجهزة الإرسال وأجهزة الـ VHF في لبنان، شهدنا انتشارًا كبيرًا للمعلومات الخاطئة التي أثارت الذعر بين مستخدمي الأجهزة الذكية.

ستركز هذا الدورة على الفروق الأساسية بين الأجهزة الذكية ونظام أجهزة الإرسال القديمة، بالإضافة إلى المخاطر المرتبطة بكل منها.

ستكون حادثة أجهزة الإرسال بمثابة جرس إنذار لنا جميعًا بعد أن كشفنا هواتفنا الذكية للإنترنت وتأثير استغلالها من قبل الفاعلين المهددين.

أهداف ورشة العمل

- **رفع الوعي**: إبلاغ الأفراد والمؤسسات بالمخاطر المتزايدة التي تواجه الأجهزة المحمولة وأهمية أمن الهواتف المحمولة في البيئة الرقمية الحالية.
- **تحديد المخاطر:** شرح المخاطر الأكثر شيوعًا لأمن الهواتف المحمولة، مثل البرمجيات الضارة، والتصيد الاحتيالي، والثغرات المتعلقة بالتطبيقات.
- **تشجيع الممارسات الجيدة:** تقديم نصائح وممارسات مثلى لتأمين الأجهزة المحمولة، وضمان استخدام التطبيقات بشكل آمن، والحفاظ على المعلومات الشخصية.
- **تشجيع التدابير الاستباقية:** التأكيد على أنه لتقليل المخاطر، فإن إجراءات تأمين الشبكة، وتقنيات المصادقة القوية، والتحديثات المتكررة هي أمر ضروري.
- **تشجيع ثقافة الأمن السيبراني**: خلق ثقافة وعي بالأمن السيبراني في كل من الأوضاع الشخصية والمهنية من خلال غرس إحساس بالمسؤولية لدى المستخدمين للبقاء يقظين ومطلعين على التهديدات المتطورة.

المشـــــاركـــــون

أي شخص مهتم بممارسات السلامة للأجهزة الذكية.

التعامل مع التحديات الأمنية الجديدة:
من الأجهزة إلى الهواتف الذكية

العناوين الرئيسية:

I. المقدمة

أ. الاستخدام الشخصي والتجاري للأجهزة المحمولة في الحياة اليومية

ب. زيادة الثغرات والتهديدات المحمولة

ت. ما هي أجهزة الإرسال وكيف تعمل أجهزة VHF/UH

ث. الفرق الرئيسي بين أجهزة الإرسال والهواتف الذكية

II. مخاطر الأمن السيبراني المحمول

أ. الفئات النموذجية للمخاطر المحمولة

- البرمجيات الضارة (برامج الفدية، والبرمجيات الخبيثة، والفيروسات)
- هجمات التصيد الاحتيالي
- هجمات الرجل في الوسط
- عيوب التطبيقات

ب. المخاطر المرتبطة بأجهزة الإرسال

ت. بيانات حول الحوادث المتعلقة بأمن الهواتف المحمولة

ث. حالات انتهاكات خطيرة

III. الممارسات الجيدة لأمن الأجهزة المحمولة

أ. استخدام كلمات مرور معقدة وقوية

ب. آليات مصادقة قوية

ت. تحديثات البرمجيات لنظام التشغيل

ث. تحديثات للتطبيقات

ج. إعداد برامج مكافحة الفيروسات

ح. وعي المستخدم

خ. قوائم فحص تعزيز الأمان

IV. استخدام التطبيقات بشكل آمن

أ. تحميل التطبيقات من مصادر موثوقة

ب. مراجعة أذونات التطبيقات

ت. تجنب التطبيقات المشبوهة أو غير الضرورية

V. ممارسات الشبكات الآمنة

أ. تجنب الشبكات العامة للمعاملات الحساسة

ت. استخدام الشبكات الافتراضية الخاصة (VPN) لتعزيز الأمان

ث. فهم الشبكات الآمنة مقابل غير الآمنة

VI. حماية البيانات والخصوصية

أ. تشفير البيانات الحساسة

ب. عمل نسخ احتياطية للبيانات بانتظام

ت. إدارة المعلومات الشخصية المشتركة على التطبيقات ووسائل التواصل الاجتماعي

VII. الاستجابة لحوادث الأمان

أ. تحديد علامات الاختراق أو البرمجيات الضارة

ب. خطوات يجب اتخاذها في حال التعرض للاختراق

ت. الإبلاغ عن الحادث

ث. استعادة أمان الجهاز

VIII. الاتجاهات المستقبلية في أمان الهواتف المحمولة

أ. التقدم في الأمان البيومتري

ب. الذكاء الاصطناعي والتعلم الآلي في اكتشاف التهديدات

ت. تأثير تقنية 5G على أمان الهواتف المحمولة

التعامل مع التحديات الأمنية الجديدة:
من الأجهزة إلى الهواتف الذكية

المحاضر:
الأستاذ جان ميشال كوكباني
مدير ArcShields

شغل جان ميشال رئيس قسم أمن المعلومات في مجموعة بنك بيبلوس.

وهو مدقق معتمد في نظم المعلومات (CISA) من ISACA، ومحاضر في جامعة سان جوزيف - ESIB، ومدرسة الإدارة الوطنية (ENA) في لبنان، ومدرب في مجال الأمن السيبراني وعضو في اللجنة الفنية في اتحاد المصارف العربية.

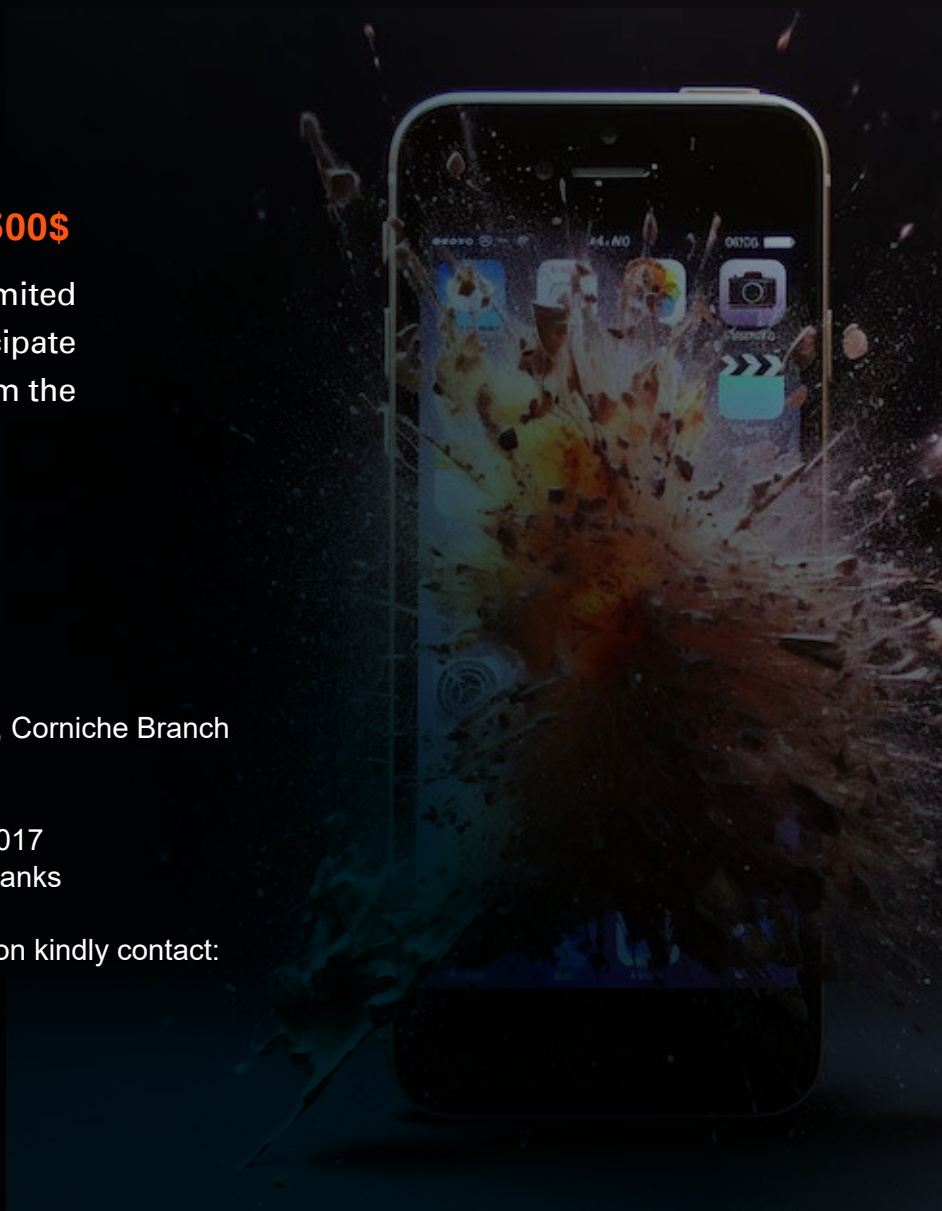
شغل جان ميشال سابقًا مناصب رئيس تدقيق تكنولوجيا المعلومات، ورئيس نظم المعلومات الإدارية، ورئيس قسم أمن المعلومات في مجموعة بنك جبيل. وقد تم تعيينه مؤخرًا كمدير لشركة ArcShields للأمن السيبراني.

تخرج من المدرسة الفرنسية للهندسة (Ecole Nationale de la Statistique et de L›Analyse de L›Information (ENSAI ويحمل درجة في الاقتصاد من جامعة سان جوزيف.

يمتلك جان ميشال أكثر من ٢٠ عامًا من الخبرة المهنية في نظم المعلومات، بما في ذلك ١٩ عامًا في مجال أمن المعلومات وتدقيق تكنولوجيا المعلومات في الصناعة المالية.
وهو مدقق معتمد للثغرات، وخبير في تنفيذ بنية الأمان المؤسسية، وإجراء تقييمات المخاطر، ومركز استجابة الحوادث السيبرانية (CSIRT)، والطب الشرعي الرقمي، وتدقيق تكنولوجيا المعلومات، واختبار الاختراق، وقد قام بالتدريس والمحاضرة حول معايير الأمن وأفضل الممارسات في جامعات مرموقة والوكالات الحكومية.

NAVIGATING NEW SECURITY CHALLENGES:

FROM PAGERS TO SMARTPHONES



PARTICIPATION FEES: 500$

Banks wishing to nominate unlimited number of attendees to participate in this webinar ,Can benefit from the special offer of 5000 $ only

MEANS OF PAYMENT

FAB - USD : First Abu Dhabi Bank, Corniche Branch
Swift code : NBADAEAA
Account no : 1411203132414017
Iban no: AE91 0351411203132414017
Beneficiary name : Union of Arab Banks

For more information and registration kindly contact:
training@uabonline.org