Subject: CFCA: Fall Education Collaboration 2020

Date: Wednesday, October 21, 2020 at 7:58:16 AM Eastern Daylight Time

From: Communications Fraud Control Association

To: IREIFEJ, PAUL

CFCA Fall Educational Online Event has begun, building on the hugely successful Summer of Education, it is full of interesting presentations and insights.

You can view all sessions, and register on the CFCA website: Fall KNOW Sessions.
New sessions are being added daily, so remember to check back regularly.

We are sending out emails weekly with information on upcoming sessions, as well as sharing all details on our social media.

It's another packed Educational Event of learning and collaboration opportunities, in addition there maybe topics that benefit others in your company so please share the details with other teams!

Please remember, for sessions noted as "Members Only" you must be logged into the website to see it and register for it.

From BEC to VEC - The Emergence of Vendor Email Compromise

Whilst BEC (Business Email Compromise) has been a familiar fraud risk facing businesses over the last few years, the emergence during 2019 of VEC (Vendor Email Compromise) has added a fresh challenge and many companies have incurred significant financial loss as a result. This presentation will address Vodafone's recent experience of VEC and the steps they are taking to mitigate the risk.

Date: 21 October 2020
Time: 11:00am Eastern/4.00pm GMT
Host: Morgan Ramsey, Vodafone Group

KNOWledge Network (Members Only)

The Knowledge Network is a forum for participants to discuss current issues and trends in communications fraud, to seek answers and/or to make contacts for future offline discussions.

Date: 22 October 2020
Time: 11:30am Eastern/4:30pm GMT
Host: Adam Panagia, AT&T/CFCA CFO

Real Time Machine Learning and AI Operations

We are utilizing big data, modern machine learning and other advanced analytics technologies to, directly and indirectly, enhance IT operations (monitoring, troubleshooting, and automation) functions with proactive and dynamic insight. It monitors all types of applications and systems for Flexible and Extensible real-time Remediations for Improved Mean Time to Resolution. The system has built-in forecasting, anomaly detections and predictive insights models as well as capabilities to integrate your own custom model. Using decision functions, analytics and monitoring data quality, this system is used to uniformly monitor our internal fraud detection systems with real-time mitigation response.

Date: 27 October 2020
Time: 11:00am Eastern/3:00pm GMT
Host: Paul Ireifej, AT&T and Heather Wighton, AT&T

2020 Cybercrime Survey Report

The presentation will go through the findings, trends and statistics from the latest cybercrime report in detail, to give audience members an insight to the latest threats and issues impacting our organisations in the market place and globally.

Date: 4 November 2020
Time: 11:00am Eastern/4:00pm GMT
Host: Jason Lane-Sellers, LexisNexisRisk/CFCA COO

Porting Panic! Gaming and Fraud Through Number Portability

In an ever-shrinking market of brand-new cellular customers, wireless providers are increasing port in incentives on devices and services in order to gain a competitive advantage. This has created opportunity for enterprising individuals who have discovered the ability to commodify phone numbers, allowing buyers to take advantage of port in offers. In this presentation, we will discuss the reasons demand in this new market has emerged, how phone numbers are acquired and sold, and the impacts to the wireless carriers.

Date: 5 November 2020
Time: 11:00am Eastern/4:00pm GMT
Host: Gary Barnhart, T-Mobile

Who's Calling? Characterizing Robocalls through Audio and Metadata Analysis

Unsolicited calls are one of the most prominent security issues facing individuals today. Despite wide-spread anecdotal discussion of the problem, many important questions remain unanswered. In this paper, we present the first large-scale, longitudinal analysis of unsolicited calls to a honeypot of up to 66,606 lines over 11 months. From call metadata we characterize the long-term trends of unsolicited calls, develop the first techniques to measure voicemail spam, wangiri attacks, and identify unexplained high-volume call incidences. Additionally, we mechanically answer a subset of the call attempts we receive to cluster related calls into operational campaigns, allowing us to characterize how these campaigns use telephone numbers. Critically, we find no evidence that answering unsolicited calls increases the amount of unsolicited calls received, overturning popular wisdom. We also find that we can reliably isolate individual call campaigns, in the process revealing the extent of two distinct Social Security scams while empirically demonstrating the majority of campaigns rarely reuse phone numbers. These analyses comprise powerful new tools and perspectives for researchers, investigators, and a beleaguered public.

Date: 10 November 2020
Time: 11:00am Eastern/4:00pm GMT
Host: Brad Reaves, North Carolina State University

Tackling Telecoms Subscription Fraud in a Digital World

Tackling Telecoms Subscription Fraud in a Digital World
The world is increasingly going digital and the COVID crisis is contributing to accelerating this reality across different industries and geos. According to FICO's 2020 Digital Consumer Survey, 74% of UK consumers would take out a mobile telephone contract digitally. This number is higher than the 70% who would open a credit card account online.
In the Telecoms fraud landscape, subscription fraud is the biggest focus, as reported by 91% of operators who responded to TM Forum's Report on Fraud in the Digital Experience Era. In addition, 48% say that digital identity theft has a major impact on fraud management and another 29% say it's increasing.

How are you dealing with this challenge? Learn how to:
- Uncover up to 50% more subscription fraud with powerful analytics
- Define the different subscription fraud types to apply the best action
- Apply Social Network Analytics (SNA) to help you quickly identify synthetic identities, subscription fraud, fraud rings and other sophisticated efforts to defraud your organisation

Deploy new biometric solutions that reduce consumer friction while preventing account takeover

Date: 12 November 2020
Time: 11:00am Eastern/4:00pm GMT
Host: Joerg Reuter, FICO

Register for KNOW sessions

#GoToKnow #HomeToKnow

Thank You 2020 Sponsors

Gold Sponsors

LexisNexis® RISK SOLUTIONS

NUANCE

Silver Sponsors

ENOVA DECISIONS
Data to Analytics to Action

FICO®

NetNumber

Bronze Sponsors

araxxe   mobileum

EQUINOX
Information Systems

TransNexus®   Neural Technologies