UNIVERSITÀ DEGLI STUDI DI MILANO

Avviso di sicurezza del 17.2.2020

Gentilissimi utenti,
Vi inviamo questa mail per informarvi su un tentativo di frode attraverso social engineering diretto verso invited speaker a conferenze. La pericolosità di tale truffa risiede nella estrema verosimiglianza nelle comunicazioni oggetto della truffa che viene perpetrata anche attraverso comunicazioni via telefono.

Truffa verso congressisti invited-speaker

La truffa di cui siamo venuti a conoscenza è diretta verso congressisti invited speaker o altri soggetti destinatari di rimborsi per la partecipazione ad eventi accademici. Lo scopo finale è carpire dati personali, principalmente i dati della carta di credito.
La truffa comincia con una chiamata via telefono, probabilmente in inglese ma può essere anche in italiano o altra lingua coerente con il tentativo di impersonificazione, in cui un sedicente organizzatore (di seguito indicato come attaccante) del congresso in cui è invitato l'invited speaker, target della truffa. L'attaccante informa il Professore invited speaker che gli verrà inviato un modulo da compilare per la prenotazione alberghiera connessa al congresso. La comunicazione può continuare con frasi di circostanza tipo frasi sull'eventuale rimborso, preferenze varie o simili. Lo scopo della chiamata è create fudicia sulla mail che verrà inviata alla vittima.
Il modulo viene quindi inviato al Professore attraverso un servizio legittimo di invio certificato di documenti mimando le credenziali di un hotel effettivamente esistente (in fondo al documento in Fig.1 trovate una snapshot della mail).

Come reagire

Nel caso riceviate mail o chiamate simili, Vi invitiamo a verificare presso l'organizzazione dell'evento a cui siete invitati sulla bontà di tali comunicazioni, recuperando i contatti dell'organizzazione non dalla mail sospetta ma da altre fonti come il sito del congresso stesso o, se possibile, attraverso contatti di cui avete già la fiducia per precedenti interazioni.
Nel caso abbiate il sospetto o la certezza di essere stati oggetto di un tale tentativo di truffa, Vi preghiamo di darcene riscontro a sicurezza@unimi.it.

Cordialmente

Ufficio Cybersecurity, Protezione Dati e Conformità -Direzione Generale
Universita' degli Studi di Milano
Via Giuseppe Colombo n. 46 - 20133 Milano
Info: https://work.unimi.it/servizi/security_gdpr/118546.htm

Fig1: Email con link di rimando al modulo fraudolento

From: **"EHotel Services.org via DocuSign"** <dse_NA3@docusign.net>
Date: Jan 13, 2020 3:20:29 PM
Subject: Please DocuSign: Online_Booking_Form.pdf
To: [redacted]@unimi.it>