7 Billion Impressions Without Paid Media: Fanta’s Halloween Strategy

Halloween is no longer just a seasonal celebration. For brands, it can become a powerful cultural platform for building relevance, generating engagement, and creating long-term brand assets.

In this episode of Adspeak by ADWEEK, Rebecca Stewart sits down with Ibrahim Khan, global vice president of marketing at Fanta, to explore how Fanta turned Halloween into a global brand moment and generated more than 7 billion impressions through fan-generated content without paid media spend.

The conversation explores how Fanta identified an opportunity to build ownership around Halloween, harnessed TikTok and community creativity, and partnered with Universal Pictures and Blumhouse to create collectible horror-themed cans.

Ibrahim also explains how product design can become a storytelling platform, how to balance brand authenticity with licensed IP, and why giving audiences creative freedom can drive deeper engagement.

He shares the long-term thinking behind turning a successful seasonal campaign into a recurring global franchise that builds anticipation and cultural relevance year after year.

[embedded content]

What you’ll learn:

- How to identify a “white space” holiday moment

competitors have left unclaimed and build ownership around it
- Why letting fans create content can generate more impressions than any paid campaign
- The “constructive tension” principle for balancing a licensor’s IP integrity with your own brand’s authenticity
- How to select characters or creative assets that flex across generations and 50+ global markets without losing relevance
- Why product design itself (not just advertising) can become the most scalable storytelling platform a brand has
- The long-game playbook for turning a single viral moment into a recurring, expectation-building annual tradition

About the guest:

Ibrahim Khan leads global strategy and marketing for Fanta, bringing more than a decade of experience at Coca-Cola across diverse markets. Previously, he served as senior marketing director for sparkling flavors in greater China and Mongolia, overseeing Fanta, Sprite, and Schweppes. His career also includes leading marketing for Sprite in its largest global market, managing sparkling portfolios across ASEAN, and driving brand strategy for Coca-Cola and Fanta across Thailand, Pakistan, and Afghanistan. Ibrahim specializes in global brand management, digital transformation, and creating consumer experiences that resonate across cultures.

Recommended videos
https://www.adweek.com/brand-marketing/7-billion-impressions-without-paid-media-fantas-halloween-strategy/

Apple to Tighten Full Disk Access Controls in macOS Amid AI Risks

Citing growing risks posed by more capable and autonomous AI agents, Apple will introduce additional controls.

The post Apple to Tighten Full Disk Access Controls in macOS Amid AI Risks appeared first on SecurityWeek.

https://www.securityweek.com/apple-to-tighten-full-disk-access-controls-in-macos-amid-ai-risks/

Cybersecurity M&A Roundup: 39 Deals Announced in September 2026

Significant cybersecurity M&A deals announced by Dragos, IBM, Palo Alto Networks, Kiteworks, and Upwind.

The post Cybersecurity M&A Roundup: 39 Deals Announced in September 2026 appeared first on SecurityWeek.

https://www.securityweek.com/cybersecurity-ma-roundup-39-deals-announced-in-september-2026/

Long-Running NPM Malware Campaign Accumulates 40,000 Downloads

Since August 2023, attackers have published eight malicious packages as part of the MALFEX supply chain campaign.

The post Long-Running NPM Malware Campaign Accumulates 40,000 Downloads appeared first on SecurityWeek.

https://www.securityweek.com/long-running-npm-malware-campaign-accumulates-40000-downloads/

8.8 Million Impacted by Data Breach at Denmark’s Central Person Register

Hackers abused a company’s lawful access to the CPR system to steal the personal information of registered citizens.

The post 8.8 Million Impacted by Data Breach at Denmark’s Central Person Register appeared first on SecurityWeek.

https://www.securityweek.com/8-8-million-impacted-by-data-breach-at-denmarks-central-person-register/

Social Engineering Detection Moves Into the Live Conversation

Companies are pouring time and dollars into security awareness training, but little evidence shows it actually works against social engineering.

The post Social Engineering Detection Moves Into the Live Conversation appeared first on SecurityWeek.

https://www.securityweek.com/social-engineering-detection-moves-into-the-live-conversation/

Sicurezza digitale e vulnerabilità al phishing: profilo demografico e abitudini

La sicurezza digitale rappresenta il punto di partenza di questo progetto di ricerca, che analizza la vulnerabilità al phishing in contesto aziendale attraverso lo studio di un caso reale: una survey di cybersecurity awareness somministrata a 65 dipendenti di un’azienda IT, tutti caduti in una simulazione di phishing condotta nel 2025 su un campione complessivo di 2.286 destinatari.

Il primo articolo della serie ha presentato il profilo demografico del campione e le sue abitudini di sicurezza

digitale, evidenziando un dato apparentemente paradossale: l’86% dei partecipanti possedeva già una formazione pregressa in cybersecurity, eppure il 100% è risultato vulnerabile alla simulazione. L’analisi ha messo in luce come fattori emotivi e cognitivi giochino un ruolo determinante nel determinare questa dissonanza tra conoscenza dichiarata e comportamento effettivo, mostrando inoltre differenze interessanti (e talvolta controintuitive) legate a genere ed età nella percezione del rischio e nelle esperienze pregresse con tentativi di phishing.

Caratteristiche del campione

Il campione analizzato è costituito dai dipendenti che hanno cliccato sul link della simulazione di *phishing*, effettuata nel corso del 2025, e che hanno aderito volontariamente alla *survey* in forma anonima. Come descritto nella sezione metodologica, la simulazione ha coinvolto complessivamente 2.286 dipendenti di un’azienda operante nel settore della tecnologia informatica.

Il questionario è stato compilato da 65 partecipanti, equamente distribuiti per genere (32 uomini, 32 donne, un partecipante non dichiarante). La fascia di età maggiormente rappresentata è quella compresa tra i 35 e i 44 anni (circa il 32%), seguita dalla fascia 45-54 anni (circa il 29%). Sono presenti anche partecipanti più giovani (18-24 anni, 5%) e *over* 55 (circa il 18%). Circa due terzi del campione possiede un titolo di studio universitario.

Un dato rilevante è rappresentato dall’elevata esposizione formativa: l’86% dei rispondenti dichiara di aver già partecipato a corsi di cybersecurity o di avere esperienza nel settore. Tuttavia, tutti i partecipanti sono risultati vulnerabili alla simulazione di *phishing*, evidenziando una possibile dissonanza tra formazione ricevuta e comportamento effettivo. Questo paradosso costituisce uno dei nodi centrali

dell’analisi che segue.

Differenze di genere nella suscettibilità al phishing

Il genere è un fattore ampiamente studiato in relazione alla vulnerabilità alle truffe online, in particolare agli attacchi di *phishing*, sebbene i risultati in letteratura siano spesso contrastanti.

Suscettibilità generale. Diversi studi hanno riscontrato che le donne tendono a essere più suscettibili al *phishing* rispetto agli uomini. Halevi et al. (2015) hanno rilevato che il 40% delle donne è caduto in uno schema di *phishing* a due fasi, rispetto al 27% degli uomini. Questa maggiore suscettibilità femminile potrebbe essere mediata da fattori quali una minore motivazione o opportunità di apprendere sugli attacchi informatici, una maggiore familiarità con la comunicazione digitale quotidiana, o una tendenza a seguire le istruzioni più prontamente. Tuttavia, altri studi non hanno riscontrato differenze significative tra i generi (Sheng et al., 2010), suggerendo che il contesto e la tipologia di attacco possano giocare un ruolo moderatore.

Tratti di personalità e genere. I tratti della personalità secondo il modello Big Five mostrano correlazioni diverse con la vulnerabilità in base al genere. Nelle donne, il nevroticismo è correlato positivamente alla suscettibilità: livelli elevati di ansia e instabilità emotiva possono portare a decisioni affrettate di fronte a messaggi che evocano urgenza o minaccia (Eftimie et al., 2022). L’amicalità, tratto mediamente più presente nelle donne secondo la letteratura psicologica (Costa & McCrae, 1992), è un forte predittore di suscettibilità poiché facilita la manipolazione attraverso la fiducia e la conformità sociale. Gli individui con elevata amicalità tendono infatti a dare il beneficio del dubbio e a rispondere positivamente alle richieste altrui,

caratteristiche che gli attaccanti sfruttano sistematicamente (Frauenstein & Flowerday, 2020).

Comportamenti online e competenze tecniche. Gli uomini tendono a comportamenti online più rischiosi in generale – come la visita di siti non sicuri o il download di software da fonti non verificate – mentre le donne, pur meno propense al rischio generico, risultano vulnerabili a esche specifiche come offerte di vantaggi immediati, coupon o promozioni (Halevi et al., 2013). Emerge inoltre un divario nelle competenze tecniche auto-percepite: le donne riportano mediamente una minore familiarità con gli aspetti tecnici della sicurezza informatica, e l'educazione anti-*phishing* non sempre si traduce in una riduzione effettiva della vittimizzazione per questo gruppo (Sheng et al., 2010). Questo suggerisce la necessità di approcci formativi differenziati che tengano conto delle diverse vulnerabilità.

Età e vulnerabilità al phishing

L'età rappresenta un altro fattore demografico frequentemente indagato, con risultati che sfidano alcune assunzioni di senso comune.

Adulti più anziani. L'età è positivamente correlata ai tempi di risposta e alla cautela dichiarata. Gli adulti più anziani tendono a classificare le email più lentamente e con maggiore attenzione, e sono più propensi a ignorare o eliminare le email di *phishing* piuttosto che interagire con esse (Sarno et al., 2023). Questo comportamento più prudente potrebbe derivare da una minore pressione temporale percepita o da una maggiore diffidenza verso le comunicazioni digitali. Tuttavia, quando decidono di interagire, gli anziani possono essere più vulnerabili a causa di una minore familiarità con gli indicatori tecnici di frode (Gavett et al., 2017).

Giovani adulti. I giovani, al contrario, sono più propensi a seguire le richieste contenute nelle email di *phishing*. Questa

maggiore vulnerabilità può essere attribuita a diversi fattori: una maggiore velocità di elaborazione che si traduce in minore riflessione, un'esposizione più intensa al flusso di comunicazioni digitali che genera *habituation*, e una percezione di invulnerabilità tipica delle fasce d'età più giovani (Kumaraguru et al., 2009). I *millennial* e la Generazione Z, pur essendo "nativi digitali", non mostrano necessariamente una maggiore capacità di riconoscere le minacce – anzi, la familiarità con il mezzo può generare un falso senso di sicurezza.

Implicazioni per la formazione. Questi dati suggeriscono che gli interventi formativi dovrebbero essere calibrati sull'età dei destinatari: per i più giovani, enfatizzando l'importanza di rallentare e verificare; per i più anziani, fornendo strumenti pratici per riconoscere gli indicatori tecnici di *phishing*.

Abitudini di sicurezza digitale dichiarate

Per quanto riguarda le abitudini dichiarate nella gestione delle email, la maggioranza dei partecipanti riferisce di adottare comportamenti prudenti. Circa il 75% afferma di controllare spesso o sempre un'email inaspettata prima di agire, mentre oltre l'80% dichiara di verificare frequentemente l'indirizzo del mittente.

Tuttavia, un'analisi più approfondita rivela criticità significative. Solo una minoranza (30%) dichiara di adottare queste precauzioni in modo sistematico e costante, mentre la quota rimanente ammette comportamenti discontinui, condizionati dal contesto, dal carico di lavoro e dallo stato emotivo del momento. Questa variabilità suggerisce l'esistenza di "finestre di vulnerabilità" – momenti di riduzione dell'attenzione che possono essere sfruttati da attacchi di *phishing* ben progettati e tempestivamente orchestrati.

Gestione delle password. Un’area di particolare criticità emerge nella gestione delle credenziali. Quasi la metà dei partecipanti (49%) dichiara di aggiornare le password esclusivamente quando obbligato da *policy* aziendali o scadenze di sistema, mentre il 43% lo fa con cadenza trimestrale. L’uso sistematico di password uniche per ciascun servizio non risulta consolidato: il punteggio medio su una scala da 1 a 5 è pari a 3,4, e solo il 23% dichiara di adottare sempre credenziali differenti.

Questo aspetto riflette un *trend* generale osservato anche in contesti più ampi. Secondo l’indagine globale di Proofpoint (2024), il 71% degli utenti ammette di compiere azioni digitali rischiose pur essendo consapevole dei pericoli, spesso in nome della praticità, del sovraccarico cognitivo o di una percezione attenuata del rischio. La comodità, in altre parole, tende a prevalere sulla sicurezza quando quest’ultima richiede uno sforzo aggiuntivo.



Profilo emergente. Il quadro che emerge è quello di un campione mediamente istruito e formato, con una buona consapevolezza teorica dei rischi informatici, ma con comportamenti di sicurezza non sempre coerenti e sistematici. La presenza di abitudini discontinue, unite a un’elevata fiducia nelle proprie capacità, costituisce un contesto favorevole all’insorgenza di errori, specialmente in condizioni di pressione, urgenza o distrazione. È proprio in questi momenti che la formazione teorica mostra i suoi limiti e la vulnerabilità si manifesta.

Percezione del rischio ed esperienze pregresse

Esperienze passate con link sospetti

Le risposte relative alle esperienze pregresse mostrano una percezione eterogenea del rischio e della propria vulnerabilità. Il 46% dei rispondenti dichiara di non aver mai cliccato su link sospetti in passato, mentre il 38% ammette almeno un episodio precedente e il 15% si dichiara incerto.

Questa distribuzione merita attenzione. La quota di incerti (15%) e la possibile sottostima degli incidenti passati suggeriscono che molti *click* su contenuti malevoli potrebbero non essere stati riconosciuti come tali, oppure che meccanismi di rimozione o imbarazzo influenzino l'ammissione dell'errore. La vulnerabilità reale potrebbe quindi essere superiore a quella auto-riferita, un fenomeno noto in letteratura come *underreporting* (Wash & Cooper, 2018).

Differenze di genere nelle esperienze pregresse

L'analisi per genere evidenzia differenze interessanti e apparentemente controintuitive. Le donne riportano meno episodi pregressi di *click* su link sospetti rispetto agli uomini: solo il 31% delle partecipanti ha dichiarato "Sì, mi è capitato", contro il 44% degli uomini. Tuttavia, le donne si attribuiscono mediamente un livello di sicurezza inferiore nella capacità di riconoscere le minacce.

Questo dato suggerisce una possibile relazione inversa tra fiducia soggettiva e comportamento prudente: chi si percepisce meno competente potrebbe adottare maggiori precauzioni, mentre chi si sente sicuro tende a esporsi con maggiore disinvoltura. Una dinamica che richiama il fenomeno dell'*overconfidence*, approfondito nelle sezioni successive.

La letteratura sul tema mostra risultati contrastanti: alcuni studi trovano le donne più suscettibili al *phishing* (Halevi et al., 2015), altri non rilevano differenze significative tra

generi (Ribeiro et al., 2024). I risultati della presente *survey* si collocano in questa zona di ambiguità, confermando che il genere, di per sé, non è un predittore univoco della vulnerabilità.

Competenza percepita nel riconoscimento dello spoofing

Oltre metà del campione (57%) dichiara di saper distinguere un indirizzo email legittimo da uno falsificato (*spoofing*), mentre il restante 43% si dichiara incerto o incapace. Questo dato, apparentemente rassicurante, rivela però un paradosso centrale: anche i soggetti che si attribuiscono tale competenza sono caduti nella simulazione.

Il fenomeno evidenzia come la conoscenza tecnica, se non supportata da attenzione costante e consapevolezza situazionale, non sia di per sé sufficiente a prevenire l'errore. Sapere cosa cercare non garantisce che lo si cerchi effettivamente, soprattutto in condizioni di fretta, distrazione o *multitasking*.

Il paradosso dell'overconfidence

Questo fenomeno prende il nome di ***overconfidence*** ed è ben documentato nella letteratura sulla presa di decisione in condizioni di incertezza (Moore & Healy, 2008). L'eccessiva fiducia nelle proprie capacità riduce la propensione ad adottare comportamenti di verifica e attenzione, creando un falso senso di sicurezza che gli attaccanti possono sfruttare.

Nel contesto del *phishing*, l'*overconfidence* opera come un fattore di rischio paradossale: proprio chi si sente più preparato può abbassare la guardia, convinto di essere in grado di riconoscere qualsiasi minaccia. Come mostreremo nell'analisi delle correlazioni, tutti i partecipanti che si erano dichiarati "completamente sicuri" (5 su 5) della propria capacità di riconoscere link malevoli sono caduti nella

simulazione – un dato che rappresenta un monito inequivocabile sul pericolo di questa distorsione cognitiva.

Vishwanath et al. (2011) hanno dimostrato che la fiducia auto-riferita nella capacità di rilevare il *phishing* ha una correlazione negativa con l'effettiva capacità di rilevazione: in altre parole, chi si sente più sicuro tende a performare peggio nei test reali. Questo paradosso ha importanti implicazioni per la progettazione dei programmi formativi, che dovrebbero mirare non solo a trasmettere conoscenze, ma anche a calibrare realisticamente la percezione delle proprie competenze.

Il prossimo approfondimento sposterà l'attenzione dal piano descrittivo a quello interpretativo, introducendo il framework teorico che guiderà la lettura dei risultati empirici. Verranno presentati modelli psicologici, sociali e criminologici utili a comprendere perché individui formati e consapevoli continuino a cadere vittime di attacchi di social engineering ben congegnati.

Il presente contributo introduce i principali risultati dell'analisi; per un approfondimento completo del disegno metodologico, dei modelli interpretativi adottati e delle evidenze empiriche, si rimanda alla lettura dell'Empirical Research Paper "**Phishing aziendale: perché i dipendenti formati cliccano comunque?",** a cura di Riccardo Laurenti, Veronica Vacchi e Ilenia Mercuri del team Cybersecurity di Dinova.

Fonti:

Articoli accademici:

- Costa, P. T., & McCrae, R. R. (1992). Revised NEO Personality Inventory (NEO-PI-R) and NEO Five-Factor Inventory (NEO-FFI) professional manual. *Psychological Assessment Resources*.
- Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A.,

Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLOS ONE*, 12(2), e0171620. https://doi.org/10.1371/journal.pone.0171620

- Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*, 1-12.
- Moore, D. A., & Healy, P. J. (2008). The trouble with overconfidence. *Psychological Review*, 115(2), 502-517. https://doi.org/10.1037/0033-295X.115.2.502
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373-382.
- Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3), 576-586. https://doi.org/10.1016/j.dss.2011.03.002
- Wash, R., & Cooper, M. M. (2018). Who provides phishing training? Facts, stories, and people like me. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1-12.

https://www.ictsecuritymagazine.com/articoli/vulnerabilita-al-phishing/

‘Io sono Giorgia Meloni’, la premier registra il copyright della sua voce

Oggi in primo piano la tutela del diritto d’immagine di una premier nell’era dell’AI, con la richiesta di tutelare i diritti sul suo timbro vocale.

*L’obiettivo di **Giorgia Meloni** è infatti è evitare il furto e l’uso distorto della sua voce in ottica anti fake e AI, in vista delle prossime elezioni politiche.*

*Negli Usa, l’AI va alla sbarra. La Città di New York chiama a testimoniare **Anthropic, OpenAI, Google** e **Meta** per esaminare i rischi degli agenti AI e nuove misure di tutela.*

*Infine, dallo Spazio **reattori nucleari sulla Luna**, e poi la sfida (in kilowatt) tra USA, Russia e Cina che partirà nel 2030.*

Per leggere tutte le news della dailyletter clicca qui.

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/io-sono-giorgia-meloni-la-premier-regis

tra-il-copyright-della-sua-voce/590447/

Google Narrows Open Source Bug Bounty Amid Wave of Invalid Automated Reports

Google has temporarily stopped accepting product vulnerability reports through its Open Source Software Vulnerability Reward Program (OSS VRP).

The post Google Narrows Open Source Bug Bounty Amid Wave of Invalid Automated Reports appeared first on SecurityWeek.

https://www.securityweek.com/google-narrows-open-source-bug-bounty-amid-wave-of-invalid-automated-reports/

“Dal Digital Innovation Forum al via a Como l’hub del Quantum”

Per conoscere le novità e i temi caldi della 4^ edizione del **Digital Innovation Forum – la Cernobbio del Digitale** – il principale appuntamento italiano ed europeo dedicato alle politiche per l’innovazione digitale, abbiamo intervistato **Antonio Franceschetti**, Presidente della **Fondazione Innovazione Digitale ETS**, promotrice del Forum, che si terrà dal 14 al 16

ottobre a Villa Erba, Cernobbio, sul Lago di Como. Key4Biz è media partner.

Key4Biz. ***Leggendo la presentazione e scoprendo l'agenda, con illustri speaker, della 4^ edizione del Digital Innovation Forum – la Cernobbio del Digitale – notiamo grandi cambiamenti e tante novità. Quali sono gli obiettivi di quest'anno?***

Antonio Franceschetti. Già il titolo dell'edizione è emblematico: "L'Europa del fare Innovazione tecnologica". L'obiettivo è fare sintesi, creare un momento di confronto ad alto livello, per fare il punto e mettere a fattor comune il contributo delle varie componenti e dei diversi rilevanti stakeholder dell'innovazione in Italia. E capire a che punto siamo.

Key4Biz. ***Qual è l'aspettativa?***

Antonio Franceschetti. Il tema è capire come *"non rimanere indietro",* stimolando una riflessione su cosa c'è da fare per stare al passo con gli Stati Uniti e la Cina. Dunque, al Forum sarà importante definire – con le visioni dei relatori e il dialogo tra i più qualificati rappresentanti delle istituzioni italiane ed europee, i CEO delle principali aziende tecnologiche, università, startup, venture capital e speaker internazionali – la Strategia per stringere il gap che ci separa da queste grandi potenze globali.

Key4Biz. ***Quanto è importante questo confronto ad alto livello della Cernobbio del Digitale per contribuire a definire le policy e ad accelerare l'innovazione tecnologica in Italia?***

Antonio Franceschetti. È fondamentale, perché la riflessione critica e il confronto serve anche per tenere fermi alcuni valori tipici e imprescindibili della nostra Europa, ma ora è necessario avere da parte dell'UE una normativa che non ostacoli più l'innovazione tecnologica – come è emerso dal Rapporto Draghi – ma che sia, invece, una leva per il progresso tecnologico, in base alle necessità di noi europei.

Antonio Franceschetti, Presidente della Fondazione Innovazione Digitale ETS

Key4Biz. ***Qual è il nostro comportamento errato in quanto europei?***

Antonio Franceschetti. Il nostro comportamento microeconomico di fatto è assolutamente legittimo, finalizzato a far rendere i nostri risparmi. Ma questo comportamento legittimo si trasforma in un disastro macroeconomico, perché l'Europa non investe con costanza e lungimiranza nel settore tecnologico, causando una forte dipendenza dalle tecnologie extra Ue, con tutti i rischi geopolitici, tra l'altro già emersi ultimamente.

Key4Biz. ***Al termine dei lavori del Digital Innovation Forum, si terrà, presso Villa Saporiti – e in collegamento con Villa***

Erba – l'inaugurazione del primo quantum annealer (un tipo di computer quantistico specializzato in problemi di ottimizzazione) industriale d'Italia, in occasione delle celebrazioni del bicentenario della morte di Alessandro Volta. Quale impatto avrà sul territorio e per il nostro Paese in generale?

Antonio Franceschetti. Sarà un importante evento nell'evento. Si tratta della installazione del computer quantistico più potente d'Europa con 4.000 qubit che è l'evoluzione di un accordo nato lo scorso anno sempre al Digital Innovation Forum con la **Q-Alliance**. La presenza di questa opportunità nel nostro territorio con la possibilità per ricercatori università e aziende di avere accesso favorisce la ricerca, la formazione, la professionalità. In sostanza, stimolerà un indotto che mi piacerebbe che nascesse in Italia per trasformare questi luoghi in una nuova "Silicon Valley".

Key4Biz. ***Il Digital Innovation Awards 2026 celebra anche le migliori esperienze di innovazione tecnologica sviluppate da imprese, startup, pubbliche amministrazioni, università, centri di ricerca e organizzazioni che contribuiscono alla crescita dell'ecosistema digitale europeo. Quanto è significativa questa apertura del Forum verso le idee e i progetti innovativi?***

Antonio Franceschetti. Dall'Italia sono nate le basi di tutto il progresso di innovazione tecnologica che si è sviluppato poi a livello globale. Dalla corrente elettrica, alle comunicazioni elettroniche, passando poi al resto d'Europa con la fisica, la fisica quantistica. Abbiamo dei centri di assoluta eccellenza e, se lei si guarda, vede che a capo delle aziende anche estere spesso ci sono italiani. Qualcosa vorrà dire? È un retaggio storico, che resta nel nostro DNA.

E l'apertura a progetti innovativi sta proprio in questo senso e sta anche nel cercare un avvicinamento al mondo dei finanziatori. Le ricordo che per le startup come partner

tecnico oltre a **COMONExT** abbiamo **CDP Venture Capital**: quindi, cerchiamo di avvicinare i due mondi.

Key4Biz. ***Infine, nella ricca agenda è prevista, in plenaria, anche una sessione dedicata alle Università e agli studenti: un Forum che affronta le future sfide tecnologiche non può permettersi di essere autoreferenziale.***

Antonio Franceschetti. No, assolutamente. Gli studenti che studiano ICT e gli universitari che fanno ricerca sulla cybersecurity e le TLC saranno una rappresentanza importante dei partecipanti della prossima edizione. Lo scopo è ascoltare le startup e i progetti universitari grazie ai quali potremmo plasmare il nostro futuro progresso tecnologico.

RICHIEDI DI PARTECIPARE AL DIGTAL INNOVATION FORUM – LA CERNOBBIO DEL DIGITALE

Lavori della Pubblica Amministrazione o sei un imprenditore oppure un manager e vuoi partecipare al Digital Innovation Forum – la Cernobbio del Digitale?

Compila il form per richiedere la partecipazione

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/dal-digital-innovation-forum-al-via-a-c

omo-lhub-del-quantum/590418/