Canva campaign aims to help drive digital learning in the Philippines

CANVA PHILIPPINES has launched a campaign that aims to boost digital transformation in the country's education system with the help of its tools and via teacher training, student workshops, and community initiatives.

Canva Eskwela 2026 is meant to help equip educators to bring creativity, efficiency, and AI-powered learning into everyday teaching, it said in a statement.

"Filipino educators are among the most dedicated in the world, yet they face real barriers, from connectivity challenges to time constraints, that limit what's possible in the classroom," said Ysa Delfin-Malinao, Education Marketing lead at Canva Philippines. "Canva Eskwela 2026 is our commitment to removing those barriers and ensuring every teacher has the tools to inspire the next generation of Filipino innovators and leaders."

This comes as a 2026 survey by Canva found that presentation creation is the most time-consuming back-to-school task for educators at 35%, followed by classroom visual preparation at 30% and lesson planning at 21%.

"While teachers are increasingly embracing digital learning, connectivity remains a major hurdle. The survey found that poor internet access was the biggest barrier to digital adoption, cited by 40% of respondents, followed by hesitation around using new technologies," it added. Meanwhile, 97% of teachers surveyed said they already use Canva, with 56% using it daily.

Through the campaign, Canva seeks to address hurdles to digital integration in the classroom via hands-on teacher training, student workshops, and experiential activations.

"(T)he campaign highlights Canva as a tool that enables more efficient, engaging and transformative learning experiences."

Canva's learning hub called Learn Grid has curriculum-mapped resources and AI-generated activities, while Canva Offline allows users to continue their work even without internet access, addressing connectivity issues.

"By streamlining resources, the platform makes daily instruction and classroom activities easier to manage with ready-to-use materials designed for all grade levels. With this approach, integrating digital tools enables learners to build the essential skills needed to thrive beyond the classroom," Canva said.

"These initiatives support the Department of Education's mission to strengthen 21st century skills among Filipino students. By easing administrative and preparation burdens, teachers can focus more on fostering critical thinking, creativity, and collaboration in the classroom."

Other initiatives under Canva Eskwela 2026 are device donations, school supplies distribution, and training programs for both students and educators. — **Bettina V. Roc**

Rising NFC-based attacks threaten contactless payments — Kaspersky

ATTACKS on Android smartphones based on near-field communication (NFC) to steal funds surged by 188% in the first four months of this year, posing risks to contactless payments, according to cybersecurity company Kaspersky.

Kaspersky said its cybersecurity solutions blocked 35,600 attacks coming from Android malware families that use NFC techniques, including SuperCard X, PhantomCard, NGate, and other malicious modifications of NFCGate tool. This was up from just over 12,300 attacks blocked in the same period a year ago.

Users in Russia see the most NFC relay mobile threats, it said.

It added that it expects attacks on NFC payments to continue growing as cybercriminals' schemes become more advanced.

"While previously attackers relied on 'direct NFC' scheme, now the 'reverse NFC' appears more common," comments Sergey Golovanov, chief security expert at Kaspersky. "The danger of a newer, more sophisticated scheme is that this type of fraud is harder to detect and fight against, because victims themselves transfer money to the attackers' accounts and such transactions are hard to distinguish from legitimate ones. We do not rule out that NFC relay malware itself continue to evolve and geography of attacks will expand. That's why this threat should be further closely monitored."

In direct NFC schemes, attackers contact victims via messaging apps pretending to do identity verification while tricking them into downloading malware that will lead them to tap their cards to an infected smartphone, leaking their card data.

Meanwhile, for reverse NFC schemes, fraudsters use social engineering techniques to trick victims into setting malicious applications as a primary contactless payment method on their compromised smartphones. These kinds of applications generate an NFC signal that ATMs recognize as the scammers' card.

"Victims are then persuaded to go to an ATM (automated teller machine) and deposit funds into a 'secure account' using their infected phone. In reality, the scammers receive the victims' money," Kaspersky said.

"The first publicly reported attacks that used a modified legitimate NFC tool occurred in late 2023. Those attacks were primarily detected in Europe. Then users from Russia and other regions faced similar mobile malware attacks. Later it became known that cybercriminals packaged NFC relay malware into malware-as-a-service offering, potentially simplifying access to malicious tools for other attackers. NFC relay campaigns demonstrate how threat actors adapt and reuse new methods to steal users' funds," Dmitry Kalinin, cybersecurity expert at Kaspersky, said.

The company said users should protect themselves against NFC relay attacks and other mobile threats by not installing apps coming from unofficial sources, especially those sent via messaging apps, social media, or SMS.

Using security solutions on Android smartphones can also help flag and prevent visits to phishing sites and stop malware installation. — **Bettina V. Roc**

How AI can be the biggest accelerator for SMBs

By Alexey Navolokin

OPINION

TALKING about artificial intelligence (AI) in the context of small- and medium-sized businesses (SMBs) is no longer a discussion about the future, but about the present. In an environment where efficiency, speed and adaptability define business survival, AI is consolidating itself as a strategic ally for companies that need to do more with less and make better-informed decisions in less time.

The context could not be more demanding. SMBs operate in high-pressure environments: fewer resources, reduced teams, and the constant need to adapt to volatile markets. In this scenario, technology plays a key enabling role. Unlike large organizations, SMBs have a natural advantage: their agility to adopt new tools without lengthy purchasing processes or rigid structures. Today, that flexibility plays in its favor in the face of an AI that is no longer exclusive to large corporations and has become increasingly accessible.

One of the most relevant changes is the evolution of the PC as an intelligent productivity center. AI no longer lives solely in the cloud; It can now run directly on the device. This allows you to automate repetitive tasks, optimize workflows, and analyze real-time information to make faster, more informed decisions. Local processing offers concrete benefits: increased speed, operational continuity, even offline, and better data control, a critical aspect for companies that handle sensitive information.

But AI can only unleash its full potential if it has the right technological foundation. Hardware is no longer a secondary element and becomes the foundation on which daily productivity is built. Running AI models, automating processes, or analyzing information in real time requires teams that are prepared for those types of workloads. Otherwise, the promise of efficiency is quickly diluted.

At this point, the renewal of the PC must be understood as a strategic decision. Processors designed for enterprise environments, such as AMD Ryzen PRO processors with built-in AI capabilities, including AMD Ryzen AI PRO 300 and 400 processors, which enable SMBs to tackle AI workloads without sacrificing performance or power efficiency, while incorporating security features designed to protect business information. These characteristics are especially relevant in organizations where each team fulfills multiple functions and there is no room for interruptions.

The underlying question is no longer whether it is advisable to invest in technology, but how to do it with a business vision. Buying a PC should not only respond to operational urgency, but to clear criteria: AI capabilities, security, performance, and scalability. Each of these factors has a direct impact on the competitiveness and sustainability of the business.

AI is already helping SMEs to speed up processes and improve decision-making from the most everyday place: the PC work. Betting on AI-ready hardware not only generates immediate benefits but also prepares companies to grow with greater agility in an environment where adapting quickly makes a difference.

ALEXEY NAVOLOKIN is the general manager, APAC at AMD.

Chinese hackers pose biggest espionage threat to tech firms, CrowdStrike says

CHINA-LINKED HACKERS posed the biggest espionage threat to technology companies over the past year, CrowdStrike, a cybersecurity firm, said in a report published on Tuesday, amid surging investment in artificial intelligence (AI).

The hacking campaigns align with the Chinese government's strategic priorities and a sustained interest in technology development, intellectual property, and information with strategic and economic value, the firm said.

The technology sector was once again the most targeted industry by both foreign governments and cybercriminals, the report found. It focused on threats to companies that research, develop or distribute computer hardware and technology, IT services and consulting, semiconductors, and software overall.

CrowdStrike did not identify specific targeted companies.

The Chinese embassy in Washington dismissed the report.

The findings, which span April 1, 2025 to March 31, 2026, come amid frenzied valuations and investments in technology firms in and around the artificial intelligence space, which are among the high-value targets, said Adam Meyers, CrowdStrike's senior vice-president, head of counter adversary operations.

On April 23, the White House Office of Science and Technology Policy accused China-based entities of "deliberate, industrial-scale campaigns" to surreptitiously distill US-developed models for their own purposes, highlighting one recent example.

"There is an AI arms race occurring between the US and China, and China intends to achieve global dominance by 2030," Mr. Meyers said, noting the threat to major frontier labs along with smaller, domain-specific model developers.

A spokesperson for the Chinese Embassy in Washington said "China opposes hacking activities and fights such activities in accordance with the law," and that it rejects "vilification and smears under the pretext of cybersecurity." The spokesperson added that China and the US need to work together on AI development and governance, and that during President Donald J. Trump's recent visit "the two heads of state had constructive exchanges on AI and agreed to launch government-to-government dialogue on AI."

North Korean hacking campaigns "posed a major threat," the report said, particularly through a scheme in which North Korean operatives use fake identities to secure remote IT jobs at technology companies. The workers' salaries are largely funneled back to the Pyongyang government, and their positions inside the companies provide footholds for intelligence collection.

Russian and Iran-linked hacking groups also heavily target the US and other nations' technology sectors for intelligence collection and, at times, destructive malware attacks.

The report also highlighted an increase in hacking activity from financially motivated cybercriminal groups targeting technology firms over the same time period, including a 30% increase in advertisements from hackers selling access to various targets. — ***Reuters***

First Gen defends Prime Infra hydro deal amid dispute with Lopez family

FIRST GEN CORP. defended the structure of its hydropower investment with Prime Infrastructure Capital, Inc., (Prime Infra) rejecting allegations from the Lopez family majority that the company had agreed to a "scandalous" P50-billion premium in the transaction.

In a clarification submitted to the Philippine Stock Exchange on Wednesday, the Lopez-led power producer said the premium attached to the deal reflects investments already made by Prime Infra in developing its hydropower assets.

The clarification came after the Lopez family majority questioned the structure of the original P75-billion agreement involving Prime Infra's pumped storage hydro portfolio, claiming that First Gen Corp. Chairman Federico "Piki" Lopez had agreed to pay P50 billion as transaction premium and P25 billion as construction equity.

"Note that the premium paid is a standard consideration in M&A (mergers and acquisitions) transactions, and one that is incorporated in the acquisition cost," First Gen said.

It added that it is "not free, superfluous money" but in consideration of Prime Infra's own investments and costs poured in over many years that brought

FIRSTGEN.COM.PH

the projects to its de-risked state at the time of First Gen's acquisition.

First Gen earlier sought to acquire a 40% stake in Prime Infra's pumped storage hydro projects, including the Wawa and Pakil facilities, for P75 billion. The company later reduced the planned acquisition to 33% for P62 billion.

The company also rejected allegations that the reduced stake meant surrendering strategic minority protections and giving Prime Infra absolute control over the projects.

First Gen said the decision to trim its stake was made after considering funding requirements for other projects in its pipeline.

"Since First Gen has a significant number of high-potential assets in the pipeline, management thought it best to scale back the hydro investment to make sure that First Gen would have the liquidity to fund all its projects," the company said.

"These significant financial considerations outflank any rights that are provided to a 40% shareholder," it added.

The dispute forms part of a broader conflict within the Lopez family that resurfaced after the majority bloc of Lopez, Inc. withdrew a Feb. 27 board resolution removing Mr. Lopez as president and chief executive officer.

The Lopez majority earlier cited loss of trust and confidence tied to the company's P125-billion hydropower and gas transactions, which they alleged were entered into without their knowledge. — **Sheldeen Joy Talavera**

NICKELASIA.COM

Nickel Asia unit signs agreement to operate mining area in Zambales

NICKEL ASIA CORP. said its unit Samar Nickel Mining Resources Corp. has signed an operating agreement with San Juanico Resources Corp. covering nickel mining claims in Zambales.

In a disclosure to the Securities and Exchange Commission on Tuesday, Nickel Asia said the deal gives Samar Nickel the right to operate San Juanico's mineral claim holdings under a mineral production sharing agreement.

The mining area covers about 3,432 hectares located in the municipalities of Candelaria and Sta. Cruz, Zambales province.

"The areas covered are believed to contain nickel ore and other associated minerals that can be extracted under the mineral production sharing agreement," Nickel Asia said.

The operating agreement will be submitted to the Mines and Geosciences Bureau for approval and will take effect once cleared by the agency.

The company did not disclose the financial terms of the agreement or the planned production timeline.

Nickel ore is a key raw material used in stainless steel production and electric vehicle battery manufacturing.

Nickel Asia is among the country's biggest nickel ore producers and exporters, supplying customers in China and Japan while expanding investments in battery material and renewable energy projects.

Shares of Nickel Asia fell 9 centavos to close at P4.49 each on the Philippine Stock Exchange. — **MJFM**