logo Image not found or type unknown

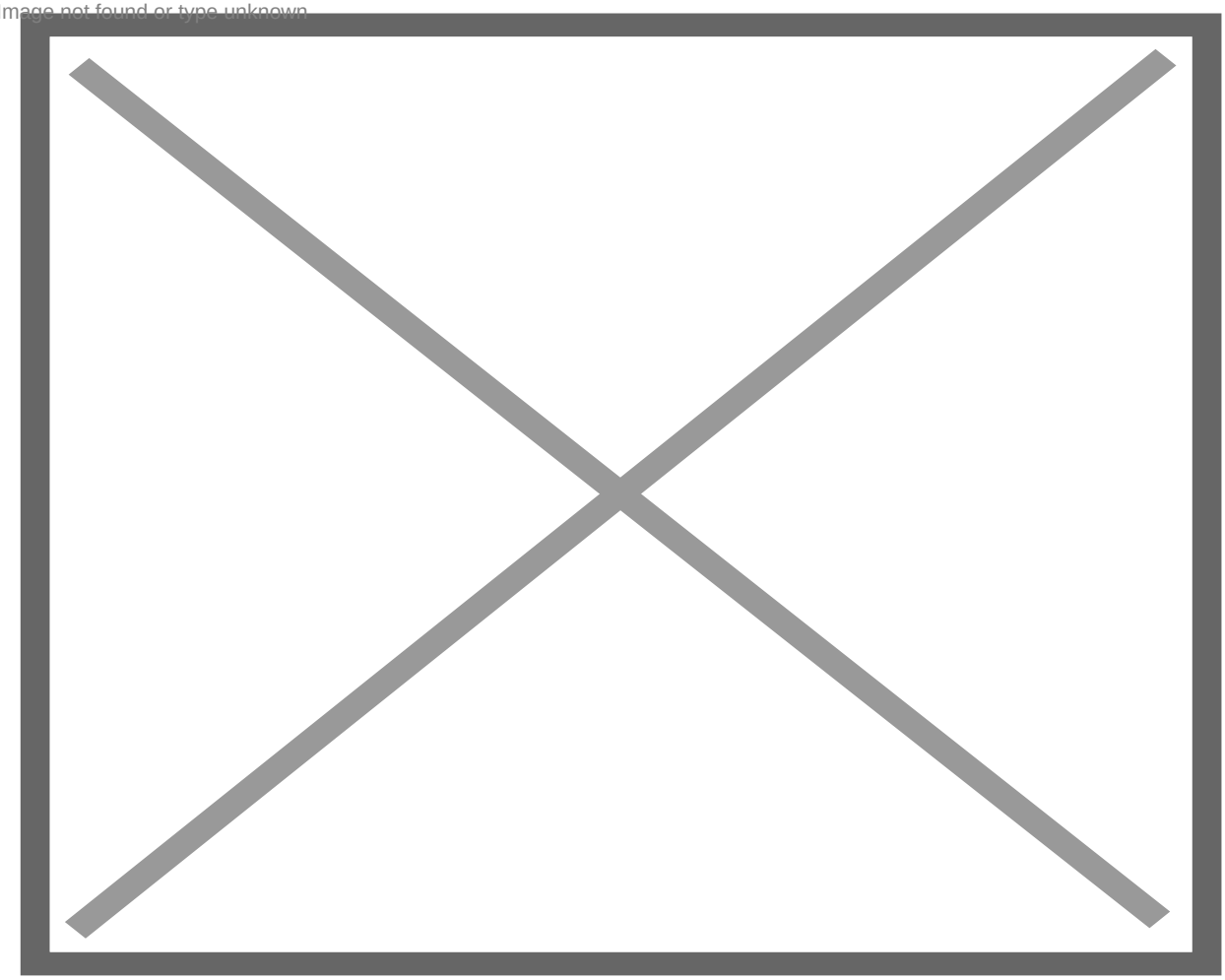
Human Error Is Biggest Threat to Virgin Islands Digital Future, Experts Warn at Summit

After breaches at hospitals and the VI Lottery, experts said software and firewalls are not enough. Panelists urged ongoing training, phishing tests, and cybersecurity education for students and small businesses to reduce vulnerabilities.

Business / **Published On October 03, 2025 06:19 AM /**

Nelcia Charlemagne October 03, 2025

Image not found or type unknown



If the discussion on cybersecurity during Thursday's Workforce Development Summit could be distilled down into three words, they might be “people are fallible.” In the wake of debilitating cyberattacks on several entities in the territory, including both hospitals and the VI Lottery in the past year, panelists discussed the increasingly relevant issue of protecting digital resources across the Virgin Islands.

“These cybersecurity attacks often have a way of impacting our economy, revenue, [and] services to our citizens,” noted Kevin Williams, Governor Albert Bryan Jr.'s chief of staff and panel moderator. “While everybody loves technology, there's also a threat there that can disrupt our lives as we become ever more reliant on these efficient systems.” There must be a focus on protecting computer systems from unwanted incursion, despite the understanding that there is no foolproof method for doing so, he said.

Philip Corey is the head of business solutions in the USVI for Brava Solutions, a business communications company associated with One Communication. He stated that while you can “do a lot” on the software and hardware side of things, it ultimately boils down to the human element – the biggest vulnerability, he believes.

Several of the panelists agreed that individual awareness should be the main priority. “Everybody in the room should have a basic, fundamental education on cybersecurity. We're clicking on links, we're accepting calls, all those kinds of things are just basic cybersecurity hygiene,” said Horace Jones, president of CyberPoint International. “The better we equip ourselves with just basic knowledge, the less we'll have people being able to get into our systems,” he said.

viNGN’s Jaughna Neilsen-Bobbitt, who made the “people are fallible” statement, doubled down by noting that “businesses are still run by people. So until the robots take it over, that's still our biggest point of failure as far as cybersecurity.” She concurred with the other panelists that training is the key.

“They just need to be aware of how to use the technology. That's all. They don't have to be experts,” Mr. Jones added.

Mr. Corey emphasized that training should be “ongoing.” He expressed his support for internal phishing tests, where IT departments gauge staff awareness of potential risks.

“It takes one person to click on that link [that] gets the hacker in. They compromise your entire network,” noted Mr. Williams. He was also a strong proponent of external testing.

“What a wonderful world that would be if people were just a little more vigilant across the board…If we could all just be just a little more cognizant of the power that we hold here, even beyond just access to our bank accounts, what a wonderful world that would be,” Ms. Nielsen-Bobbitt said.

“You don't have to reinvent the wheel,” she added. She explained that viNGN’s technical team issues a “two-minute training” every quarter with a “little quiz at the end.” It’s something that other entities can adopt.

Small businesses, too, must also take particular care to protect themselves. While the government may have the resources to provide regular training, small businesses with only a few employees may not enjoy that luxury. Robbery, said Mr. Williams, has “evolved from somebody walking in trying to steal your cash to ransomware.”

Mr. Corey suggested entrepreneurs prepare a “written policy for your business” governing things like employee passwords, for example.

There is also a growing need to ensure that today's students, who are growing up in a much more technologically advanced world than previous generations, are able to keep themselves safe online.

Mr. Jones believes that these concepts should be introduced at the elementary level. There should be concerted efforts to teach them that devices are “not just a toy.” When students move to high school, “you can start talking about cybersecurity and AI and all the kinds of things that are a little more complex,” he suggested.

The Virgin Islands is making steady strides to become digitized. From the availability of online payment platforms to digital forms and hospital billing, technological advancement is a clear priority. Given the major breaches that have slowed down business and caused major revenue shortfalls in government entities, it is clear that the level of security needed to protect physical assets is negligible compared to the resources to protect digital data.