NTRC ICT NEWSLETTER

NATIONAL TELECOMMUNICATIONS REGULATORY COMMISSION

OCTOBER 2018 | ISSUE 103

23 teams advance to the Finals of the NTRC's 2018 I Squared Competition

A total of twenty-three (23) teams have advanced to the finals of the NTRC's 2018 I Squared Competition following the preliminaries which were held from October 9—11, 2018 at the NIS Conference Room.

During the preliminary events, all teams were required to present their ideas or mobile apps to a panel of judges for no more than 7 minutes followed by a 5 minute round of questioning.

The judging of the preliminary events resulted in eight (8) teams from open category; seven (7) teams from the Secondary Mobile app category and; eight (8) teams from the Secondary idea category advancing to the finals. The Grand Finale and Prize Giving Ceremony will be held at the Kingstown Methodist Church Hall on Wednesday November 14, 2018 from 9:00am - 5:00pm.

There will be an exhibition for the Open Category entrants where the public can interact with the teams about their apps. The public will also be given the opportunity to cast a vote for their best app or idea in each category of the competition via the NTRC's Facebook page.

Source: NTRC

SPONSORS OF THE NTRC'S 2018 I SQUARED COMPETITION

gogetta · SEARCHLIGHT · KDLT · TUSI · FLOW · Internet Society Saint Vincent and the Grenadines · VITA MALT · NRG Radio · 104.3 TREME FM · EDS EXPRESS DATA SYSTEMS · King Computer · Digicel · SUGBO · RIGHT STUFF · NTRC

How to Stay Safe on Public Wifi

With various public Wi-Fi hotspots, it's a convenient way to check your emails, catch up on social networking or surf the web when you're out and about. However, cybercriminals will often spy on public Wi-Fi networks and intercept data that is transferred across the link. In this way, the criminal can access users' banking credentials, account passwords and other valuable information.

Here are some useful tips from Kaspersky Lab's team of Internet security experts:

Use a VPN (virtual private network)

By using a VPN when you connect to a public Wi-Fi network, you'll effectively be using a 'private tunnel' that encrypts all of your data that passes through the network. This can help to prevent cybercriminals — that are lurking on the network — from intercepting your data.

Avoid using specific types of website

It's a good idea to avoid logging into websites where there's a chance that cybercriminals could capture your identity, passwords or personal information — such as social networking sites, online banking services or any websites that store your credit card information.

Protect your device against cyberattacks

Make sure all of your devices are protected by a rigorous anti-malware and security solution — and ensure that it's updated as regularly as possible.

Source: Kaspersky

SVG to introduce e-bus system early next year

Minister of of Finance, Economic Planning, Sustainable Development and Information Technology—Hon. Camillo Gonsalves

An e-bus system which will let commuters know how long they will have to wait for their bus will be introduced here in St. Vincent early next year.

The initiative involves equipping participating buses with electronic devices which would transmit certain information to specialized bus stops to be installed across the country. Each bus stop would have a digital display which would let commuters know the whereabouts of participating buses and how long they will take to get to the bus stop.

The bus stops will be equipped with free wi-fi and commuters will also be able to access bus information using a mobile phone app.

Minister of of Finance, Economic Planning, Sustainable Development and Information Technology Camillo Gonsalves, speaking at a press briefing on Monday, October 1st 2018 said bus drivers will be given incentives to participate in the e-bus program.

The initiative will also allow for monitoring of certain minibus behaviors.

"We will be able to monitor the information and we know there are some stories about van drivers who drive in a less than safe manner and the devices in their vehicles will allow us to track their speed and various other information about their routes," Gonsalves explained.

He said discussions have already been held with the National Omnibus Association (NOBA) to sensitize drivers about the program. The pilot project will focus on 20 to 30 buses in the first phase and Gonsalves is hoping that the program can be expanded as the benefits manifest themselves and the usage and ridership of the buses involved go up.

Another initiative, which will be coupled with e-bus program, is a security measure involving CCTV cameras. These programs will be implemented with the help of the Government of Taiwan under the Systems and Technology Cooperation agreement and the International Cooperation and Development Fund.

Gonsalves explained that during his recent visit to Taiwan, meetings were held with both entities who agreed to help install the CCTV cameras around the country.

"The CCTV cameras will be placed in Kingstown at all bus stops and other high traffic areas. They will be networkable and monitored from the Central Police Station; a development which is expected to act as a crime deterrent and assist with solving crime.

Gonsalves said the cameras will also have a disaster preparedness element and Taiwan has promised to expedite the CCTV element of the program.

Source: Searchlight

Flow's country manager, Wayne Hull, right, and a technician

FLOW upgrades broadband network in SVG

Telecommunications provider FLOW has announced its latest network upgrade, the Arris E6000 CMTS, which it says aims to improve the capacity of the core Hybrid Fiber & Coaxial (HFC) broadband network by 50 per cent.

Welcoming the upgrade, which commenced since February of this year, FLOW's country manager, Wayne Hull, said he is thrilled that the new upgrade has been able to extend the network capacity so that the company can better serve the customers, who will be able to get more broadband speed and even more value for their money.

Hull said that the FLOW team is on a journey of allowing its customers to have a better experience and be satisfied with the services they are paying for.

He added that it is extremely important that the company stand true to the commitment made to Vincentians: to transform the quality of their services, invest heavily in the network and offer a world class telecommunication service to the nation.

Source: iWitness News SVG

Flow doubles internet speeds in Saint Lucia

Flow Saint Lucia Country Manager—Chris Williams

Customers of Saint Lucia and the Caribbean's leading telecommunications provider are once again reaping benefits from significant investment in infrastructure and technological assets.

Residential subscribers to Flow's fixed broadband service have been enjoying a drastic improvement in their web experience, thanks to the company's recent decision to increase internet download speeds islandwide at no additional cost.

Thanks to the latest system upgrade, Flow customers across Saint Lucia are now able to get much more bandwidth for work, study, or play. Once the user restarts his or her modem, a speed test will confirm the increased download speed.

This development comes at a time when more citizens are desirous of participating in the technological revolution and expansive growth of ecommerce opportunities, both as a source of employment and as a proven catalyst of economic growth.

Flow Saint Lucia Country Manager, Chris Williams, said:

"This added value is more than just increasing the utility of our service; it is Flow leading the charge and spurring growth in the Information and Communications Technology (ICT) sector, whilst expanding the possibilities for our customers to tap into new and emerging markets."

Earlier this year, Flow increased upload speeds on residential broadband, with the TV platform also experiencing an upgrade to a new firmware and interface that clears the way for exciting features such as Video On Demand.

Flow Saint Lucia home internet download speeds are up to 100 MBps, with unlimited browsing, messaging, emailing, online shopping, and downloading.

Source: St Lucia News Online

Local Number Portability (LNP) services to be launched in ECTEL member states

The Eastern Caribbean Telecommunications Authority (ECTEL) is pleased to announce that Local Number Portability (LNP) services will be launched in all ECTEL Member States on Monday, 19th November 2018.

This date was agreed upon at a meeting of the ECTEL LNP Working Group which was held on 11th and 12th September 2018 in St. George's Grenada.

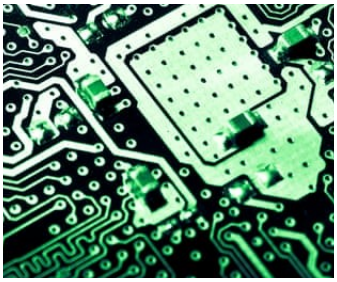
Local number portability is a service which allows subscribers of fixed and mobile networks to move their voice services to another provider within the same ECTEL member state while retaining their current number. This means that a person or company who changes their provider and decides to keep their phone numbers will not have the trouble of informing their family, friends, colleagues, customers and clients that their number has changed.

ECTEL is confident that the launch of local number portability across the ECTEL region will give consumers the flexibility to move their fixed and mobile voice services to the provider that best meets their needs. Consumers can focus on issues such as quality of service and price to help them to choose a provider. The availability of local number portability will therefore enhance competition across the fixed and mobile sectors across the ECTEL region.

The ECTEL LNP Working Group comprises representatives from ECTEL, the National Telecommunications Regulatory Commissions (NTRCs) of the five ECTEL Member States and service providers – Aislecom, Digicel and Flow. The ECTEL Member States are Dominica, Grenada, St. Kitts and Nevis, Saint Lucia and St. Vincent and the Grenadines.

Source: ECTEL

China planted chips in Apple and Amazon servers, report claims



A Chinese military unit has been inserting tiny microchips into computer servers used by companies including Apple and Amazon that give China unprecedented backdoor access to computers and data, according to a new Bloomberg report.

The tiny chips, as small as the tip of a sharpened pencil and designed to be undetectable without specialist equipment, were implanted on to the motherboards of servers on the production line in China, the report in Bloomberg Businessweek said.

The chips were reportedly developed by a specialised computer hardware attack unit in the People's Liberation Army, and gave hackers unfettered access to anything the server did, allowing them to potentially manipulate the server to steal data, contact other servers and alter operations.

The allegedly compromised hardware, sold by Super Micro Computer, which is based in San Jose, California and described as "the Microsoft of the hardware world", found its way into the data centres and operations of 30 companies, including Apple and Amazon as well as banks, hedge funds and government contractors, according to the report.

The attack was reportedly discovered in 2015 by the US intelligence services, as well as by Apple and Amazon as the companies purchased servers made by Super Micro Computer. The report claims Amazon became aware of the attack during moves by its subsidiary Amazon Web Services (AWS) to purchase streaming video compression firm Elemental Technologies in 2015. Apple had reportedly bought around 7,000 Super Micro servers when its security teams discovered the chips.

The report cited 17 unnamed intelligence and company sources as saying that Chinese spies had placed computer chips inside equipment used by around 30 companies, as well as multiple US government agencies, which would give Beijing secret access to internal networks.

Source: The Guardian

Facebook hack affects 90 Million Users

Facebook announced a major security breach on Friday, September 28, 2018 and information has been trickling out ever since.

While the public waits for a full accounting of what happened and who was affected, here's a quick overview of what we know so far. Facebook says attackers were able to get into and take control of about 50 million accounts, as if they were the users in charge of those accounts. But the company has not said yet if any of the accounts were actually taken over and used, and if so, for what purpose.

The incident also could have affected third-party accounts, like Instagram, that let users log in with their Facebook accounts, the company has acknowledged .

Facebook automatically logged the 90 million compromised or at-risk users out of their accounts, then asked them to log back in. That patched the vulnerabilities for those users. Those 90 million represent only about 4 percent of the company's user base as of the second quarter.

Source: The Verge

Contact Us

National Telecommunications Regulatory Commission
2nd Floor NIS Building, Upper Bay Street Kingstown
St. Vincent
Tel: 784-457-2279 | Fax: 784-457-2834 | Email: ntrc@ntrc.vc

ntrc svg *www.ntrc.vc*