Get Safe Online Global24

Connect
Communicate
Collaborate

The role and importance of sharing in internet safety awareness

A White Paper by Get Safe Online

March 2022

COMMONWEALTH
UNITED KINGDOM CHAIR-IN-OFFICE

Foreign, Commonwealth & Development Office

"As the COVID-19 pandemic has rapidly accelerated digital transformation across the Commonwealth, it's more important than ever that the international community works together to ensure that people all over the world can use the internet safely, securely and with confidence. We've made great progress so far, but Get Safe Online's survey reveals there is much more to be done.

"That's why the FCDO is delighted to be partnering with Get Safe Online and supporting its Global24 event. With top cyber security tips shared across the 24-hour period and 24 Commonwealth countries brought together to share best practice, Global24 is a collective effort to make the online world a safer place for all."

William Middleton, Cyber Director, Foreign, Commonwealth & Development Office

"We are hugely grateful for the support of the Foreign, Commonwealth & Development Office and our country partners across the globe in helping us to exchange ideas, advice and best practice as to how to keep our communities safe and also effectively communicate good advice.

"The scams and tricks cybercriminals use have become increasingly sophisticated – particularly during the pandemic – and it is crucial that we are aware of the risks and protect ourselves from the ever-present threat."

Tony Neate, CEO, Get Safe Online

Introduction

It is an indisputable fact that collaboration is the most effective tool in making the internet a safer place. This paper – published as an adjunct to Get Safe Online's Global24 'Go Share' conference held on 10th March 2022 – aims to outline its benefits in the online safety space, supported by case studies and other examples.

In cybersecurity, there is much to be gained by working openly and collaboratively. It is accepted that there may be a multitude of commercial, political and security aspects to be considered when cooperating with other parties, but any intelligence, practices or data that can be shared for the common good of like-minded people, organisations and governments can surely only be regarded as a positive. Within the correct framework, individual parties' integrity, security and competitive and strategic advantage can all be maintained.

We could all work more effectively with the benefit of others' experiences – both positive and negative. We could be stronger by pooling resources to detect, identify and block threats whilst sharing knowledge and good advice. Doing so means that we can protect not only our own people, organisations and boundaries, but the economies and ecosystems of our neighbours, trading partners and cultural cousins, supporting the availability and openness of the internet for everyone in what has become a closely connected world.

An often-quoted example of this is ISACs (Information Sharing and Analysis Centres). These are not-for-profit organisations set up in many European countries that provide a central resource for gathering information on cyber threats (commonly to critical infrastructure) as well as facilitating two-way sharing of experience, knowledge and analysis between the private and public sectors about incidents, vulnerabilities and threats. Their success suggests an increasing acceptance of cooperation within the cybersecurity community.

The age-old expression "*Give a man a fish and you feed him for a day, teach a man to fish and you feed him for a lifetime*" has considerable relevance in the online safety context. Never before have so many around the world had so much need for online security education. This is simply because there are more people around the world, more cybercriminals, more opportunities for exploitation and more people with insufficient skills and knowledge owing to being obliged to take to the internet during the COVID-19 pandemic. For example, in research commissioned by Get Safe Online for the Global24 2022 event, 93% of the 5,200 adult respondents surveyed were unaware that email passwords are a prime target for cybercriminals, when of course email remains the principal attack vector for fraudsters and identity thieves.

We cannot sit behind every internet user, guiding them through cyberspace with impunity. But we can help them to acquire the tools they require for navigating it with more confidence and safety. In the online safety awareness and cybersecurity community, our primary task is to *empower*, whether that be by capacity building at a national level or giving citizens simple tips to improve and maintain the correct online behaviours.

We cannot hope to achieve this without collaboration.

Collaboration in the Commonwealth

In the Commonwealth, the British Government has taken a firm lead in facilitating a safer internet for the common good.

In April 2020, the CSSF (Conflict, Stability and Security Fund) established a new cyber portfolio – the Cyber and Technology Security Programme – drawing from the Cyber Maturity Model developed and delivered by Oxford University and evolving from the National Cyber Security Programme (2016-21), the CSSF Commonwealth Cyber Programme (2018-20), as well as the Prosperity Fund Digital Access Programme. The CSSF is a cross-government fund that finds creative solutions to meet complex national security challenges and promote international peace and stability. Its strategic direction is set by the UK's National Security Council (NSC), which is chaired by the Prime Minister and attended by senior cabinet ministers. Operating in over 80 countries and territories, it delivers more than 90 programmes and combines Official Development Assistance (ODA) with other, non-ODA funding sources.

The CSSF programme delivers the international elements of the National Cyber Security Strategy and the UK's cyber commitment to Commonwealth partners in its role as the Chair-in-Office. In 2020/21, it delivered assistance to help partner countries better protect Critical National Infrastructure (CNI) from cyberattacks. A new Commonwealth Cyber Security Incident Response Team (CSIRT) community platform is now being used by 30 African and Indo-Pacific countries, set up in partnership with not-for-profit cybersecurity organisation the Shadowserver Foundation. These countries receive free daily threat intelligence reports, facilitating their detection and response to the ever-changing threat landscape.

Another UK-based not-for-profit – Get Safe Online – has been working closely with the Foreign, Commonwealth & Development Office to engage with the populations of 22 Commonwealth countries in the Caribbean, Pacific and Africa regions to increase their awareness of online risks, equipping individuals and small to medium sized businesses with the behaviours necessary to use the internet with increased safety and confidence aligned with the UK's vision of a free, open, peaceful and secure cyberspace. The original programme was initiated in April 2019 with the launch of Get Safe Online websites in 12 Caribbean countries, extending to new websites in nine Pacific countries in October 2020 – seven of which feature translation into the countries' respective main local language – and a website in Rwanda, again bi-lingual.

The websites – which share simple, pragmatic advice on an exceptionally broad range of topics – are supported by locally targeted publicity and awareness campaigns which encompass, depending on the country concerned, press, radio and TV, social media and out of home advertising.

Get Safe Online has also recruited, trained and supported over 150 local online safety Ambassadors who cascade information and advice throughout their communities via face-to-face and virtual awareness sessions. They use their knowledge, enthusiasm and initiative to make a significant impact, largely in areas where levels of digital literacy – and indeed digital inclusion – can be relatively low. They also provide Get Safe Online with feedback which enables tailoring of information and messages in specific countries.

All of Get Safe Online's work described above is managed and delivered by virtue of funding made available through the offices of the FCDO.

With organisations such as ISACs working within the cybersecurity ecosystem, the CSSF working at governmental level and Get Safe Online delivering services at grass roots level – whilst working alongside governmental organisations, regulators and NGOs – the concept of collaboration works equally effectively across the spectrum of awareness.

COMMONWEALTH
UNITED KINGDOM CHAIR-IN-OFFICE

Effect of the COVID-19 pandemic

The effects of the COVID-19 pandemic cannot be ignored, and indeed since its onset we have witnessed a fortuitously ironic situation as regards online safety.

The restrictions we have witnessed almost everywhere in the world – particularly relating to personal contact, working and travel – have forced the rapid acceleration of digital transformation, with individuals, organisations and governments alike having to adapt to unprecedented change – both in technology and culture. Inevitably, this has been accompanied by an increase in online crime and other harms. Perpetrators have exploited not only the quantum increase in users and the volume and types of everyday tasks they perform, but also people's reduced concentration owing to concerns about their and their families' health, mental wellbeing, job security and financial stability.

At the same time, however, the same digital transformation has enabled unprecedented sharing of – and the *willingness and impetus* to share – information, intelligence, data, ideas and advice between individuals, businesses, law enforcement agencies, regulators and countries, with a substantial bundle of added benefits: ease, speed, efficiency, sustainability and economy. It is certainly an exciting time to be working in cybersecurity.

Case studies

In compiling this white paper, we have been very fortunate to speak to individuals in several Commonwealth countries whose initiative and proactivity exemplifies the concept of collaboration being vital to online safety awareness.

National Bank of Rwanda

The scenario

Part of the mandate of the National Bank of Rwanda is to ensure a sound financial system in the country, which is partially achieved by conducting regular reviews of banks and other financial institutions and helping them to ensure they adhere to approved inspection procedures and methodologies, in turn ensuring compliance with statutory requirements and regulations. A regulatory framework covers business continuity, outsourcing, provision of payment services and cybersecurity.

Against a background of increasing cybercrime and financial fraud and the organisation's mandate as a central bank to ensure a secure ecosystem at all levels, it was decided to embark on various initiatives to strengthen any weak links which, in common with any other country in the world, include the end users of financial systems. Deborah Uwera, Senior IT Inspector at the bank, explains:

> *"In developing countries, there is a huge lack of awareness of cybercrime so we're trying to increase financial literacy and inclusion."*

The initiative

Deborah's team – based in the Rwanda's capital, Kigali – adopted a multi-pronged approach to the project. In October 2021, designated National Cybersecurity Awareness Month, it partnered with the country's National Cybersecurity Authority to deploy a national campaign across television, radio and internet channels, designed to sensitise people on how to use digital financial services and equally importantly, do so securely.

Acknowledging, however, the substantial variation in digital literacy and indeed inclusion, the team also travelled into rural areas to meet communities face-to-face and impart the advice. Deborah recounts a widespread stigma attached to making payments or conducting any other financial transactions online, followed by an uneasy acceptance that it had been enforced owing to the physical restrictions resulting from the pandemic. This was accompanied by the admission that they did not know how act safely.

She recalls that there were concerns about two groups of people:

> *"One group wasn't aware that online financial services exist at all. Many of them don't even have access to a smartphone, with some just having a feature phone. They would do mobile payments, but there were so many cases of fraud, with scammers tricking people into giving away their PIN or password.*
>
> *"The other group was people who are already transacting online but either easily tricked or did things like using their children's names as passwords. We had to teach them to think like an attacker, and that when transacting online you're exposed to global threats, not just what's happening in your neighbourhood. I believe we have to keep doing this continuously. In the campaign we were trying to increase financial inclusion in the different areas of the country, educating on the ease of transacting online but at the same time, being prudent, reducing trust levels and using strong passwords etc."*

At the time of writing this paper, there are not yet any statistical outcomes available from the National Bank of Rwanda. However, it is witnessing an increase in online transactions and mobile money payments and, against a widening threat landscape an opening of people's mindsets, with Deborah's team welcoming a substantial number of questions on the best way to secure payments and other transactions.

> *"The next step is to determine any change in numbers of fraud cases and an assessment on whether people are being more prudent and changing their behaviour,"* she says.

In a further example of collaboration, another plan is to build a system that will link up all of the county's banks and other financial institutions to gain a 360°, real time view of what is happening on their networks. This will enable fast mitigation assistance to be provided in the event of a cyberattack and allow measures to be put in place across the entire financial services ecosystem to avoid a repeat incident.

> Deborah comments: *"We're very excited that this is going to strengthen our entire financial system and help us to help financial institutions better."*

CLICK TO WATCH INTERVIEW

Jervis Dabreo, Grenada

The scenario

Working within Grenada's Ministry of ICT, Jervis Dabreo is tasked with raising awareness and helping citizens to become both comfortable and safe online, supporting the country's overall cybersecurity effort. As a former classroom teacher in one of the country's larger secondary schools for 13 years, he is also passionate about passing on the benefit of his knowledge.

The initiative

As a teacher in ICT, Jervis had constantly received requests to help resolve issues and provide advice. In 2012 he launched a blog with the intention of helping its readers to help themselves. Both the content and audience steadily grew, then in early 2020 the COVID-19 pandemic hit.

Jervis recalls:

> *"When that happened, I started to see a lot of misinformation and as a result I began doing some fact checking and created a WhatsApp group specifically for that purpose, which has now grown to 150 people. After a while I thought it made sense to not only share facts with the group but have actual conversations, so I started arranging free awareness sessions, first on misinformation but soon branching out into online safety."*

The sessions are aimed mainly at secondary school students, but he also addresses parents with a tailored version of the advice.

Part of Jervis's day job involves reaching students and teachers, but the steep increase in people's reliance on the internet and advent of virtual home schooling forced by COVID restrictions made him realise that he could personally do more.

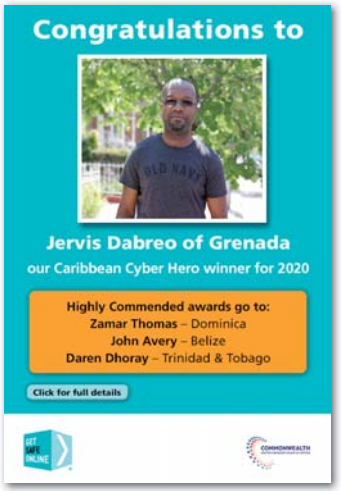
Part of this was re-packaging his slides, taking content from Get Safe Online and other sources. However, he then decided that more impetus was called for and launched daily tips around online safety, digital citizenship and associated topics. His initial objective was to reach 100 tips, but at the time of writing, the list has grown to 370, ranging from charity and romance scams to screen brightness and the hazards of earbuds to small children, internet usage laws to digital literacy and digital wellbeing. Constantly monitoring the media and other sources for new scams and other threats that could pose a serious threat to Grenadian people, he includes them in his tips but also obtains interviews on radio and TV for maximum impact, always accompanied by protection advice.

Jervis says:

> *"Based on the impact of what I have seen, there are many people who have benefited. They tell me that before, they hadn't been sure what to do, but now they know what to look out for and what to do about it.*
>
> *"I get a great amount of joy from helping people. I'm not active in the classroom any more, but will always be a 'teacher' and part of that is helping others. Those who know should help those who are willing to learn, and the strong have an obligation to protect the weak."*

Jervis's vision and enthusiasm has prompted the Grenadian Ministry of ICT to launch a CCERT, for which he is co-ordinator. Plans are also afoot to set up a cybersecurity agency for the first time in the country's history.

Jervis achieved further recognition with the award of overall winner in Get Safe Online's Caribbean Cyber Heroes Awards against tough competition in December 2020.



CLICK TO WATCH INTERVIEW

Broadcasting Commission of Jamaica

The scenario

For almost ten years, the Broadcasting Commission of Jamaica has been prioritising digital literacy as one of its most effective responses to the digital age.
Senior Director of Public Education & Communications Don Dobson explains:

> *"We're in a new media environment where content flows seamlessly across platforms and devices. Viewers and listeners are not just viewers and listeners any more, they are content creators in their own right, with the ability to inform, educate and entertain but also cause harm, distress and other problems."*

In common with other countries around the Commonwealth and worldwide, Jamaica's citizens were using the internet largely without the necessary skills and knowledge, putting them at risk. Against this background, the Broadcasting Commission decided to intervene with the appropriate guidance in the knowledge that digitally literate citizens are the first line of defence against online scams, harmful content and other commonly encountered harms.

> *"We already have one divide where access to the internet and digital resources are concerned, certainly we didn't want another in terms of user capability. We had to find creative means to engage our citizens young and old with opportunities and challenges in a digital space,"* recounts Don Dobson.
>
> *"We want people to go on the internet, use smart devices, explore and be innovative, but we also want them to be aware of the risks they may encounter, not least children with grooming, cyberbullying, sexting, fake news, exposure to self-harm, hate speech and other forms of problematic content. How do they navigate this space safely?"*

The initiative

The Broadcasting Commission's response was to develop a schools' outreach programme to engage young people by means of a dynamic and frequently updated presentation comprising creative video content.

Working in collaboration with a creative agency, the Commission developed two short videos using the musical genres of dance hall and hip hop to ensure that they were catchy and resonated with the students. Music is regarded as a major passion point for Jamaicans and, of course, universally popular with young people. The theme, common to both videos, was the question 'What if?' … for example 'what if I'd shared that message?', 'what if I'd put out some fake news?', 'what if I'd used my device for a particular purpose?'

Don Dobson explains:

> *"Music invites you to sing along: you start to sing the message and develop your own associations. We wanted that message of responsible and thoughtful media use to be in the heads of young people and have it repeated and repeated to the extent that it influenced intention and, ultimately, behaviour."*

The public's response to the Broadcasting Commission's presentations and advertisements has been positive. A survey conducted in October 2018 revealed that (82%) of Jamaicans said they wanted the Broadcasting Commission to educate the public on how to protect themselves and their families online. They agreed that protection against malicious and harmful online content was important and necessary, especially for young people who are increasingly able to access unrestricted content.

A more recent survey found that 98% of the public was aware of the 'What If?' campaign and revealed that over 90% of youth, somewhat or strongly agreed that the 'What if?' ads made them think carefully about their media use.

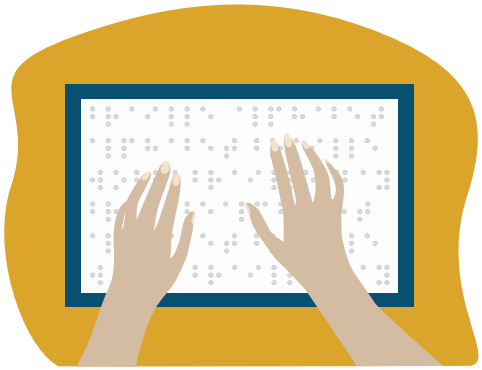
At the time of writing, The Broadcasting Commission is also investigating the application of artificial intelligence to assist with the monitoring of content across platforms and devices, as the volume of work has increased exponentially and now far exceeds human processing capacity. The Commission is also in the final stages of developing a Digital Media and Information Literacy Skills Framework for Jamaica. The outputs will include tools for assessing and eventually certifying Digital Literacy, and recommendations for the creation of a national digital literacy policy which will include setting and monitoring targets in relation to education, training, employment, digital safety and media literacy.

CLICK TO WATCH INTERVIEW

Sight Scotland & Sight Scotland Veterans

The scenario

Founded in 1793, Sight Scotland is the world's oldest visual impairment charity that caters for all ages. Its Braille press began production in 1891, initially focusing on production of religious and educational materials but over the years broadening its scope to corporate and other publications.



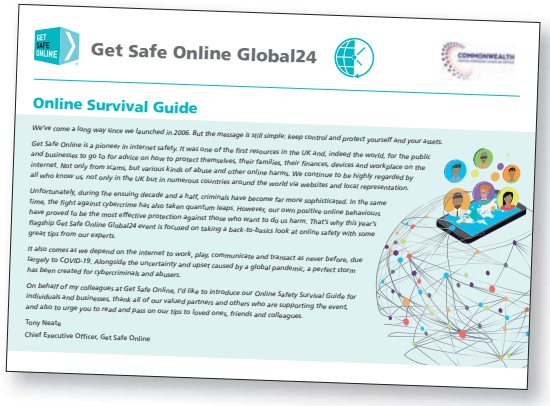
It has been long known that many visually impaired people have serious difficulty in using the internet and also accessing online security messages, making this a vulnerable group. IT Manager Kevin Burns recalls:

"The charity was involved years ago when we helped the Scottish Government build a cyber resilience strategy for the country's third sector. Not only that, but our Braille press handles a lot of information for banks and building societies, so security is very high on our agenda."

The charity is also certified to ISO 27001 – the international standard that lays out the specifications for implementing an information security management system – and holds the UK Cyber Essentials and PCI DSS standards.

The initiative

When Get Safe Online produced an Online Survival Guide as part of its inaugural Global24 Commonwealth event in 2020, it was approached by Kevin Burns to determine whether the charity could produce a Braille version.



"We produce Braille versions of all kinds of printed material day-in, day-out for businesses and other organisations, so I thought it would be a great way to offer our services, as a charity, to those with a vision impairment," says Kevin.

Feedback from the charity's outreach services that work in the community is that the Braille version of the Online Survival Guide has been very useful for visually impaired people who have used it, as it has enabled them to keep safe when using the internet.

CLICK TO WATCH INTERVIEW

Online Safety Commission, Fiji

The scenario

In Fiji, there has been a digital literacy programme for schools in place since 2015, but like every other country around the world, internet use has massively increased over the COVID-19 pandemic, as has online crime, abuse and other harms. The Online Safety Commission is finding that many young citizens have the knowledge and skills to protect themselves, but older people do not, resulting in their becoming victims of online harms or reluctance to use the internet at all.

The initiative

Tajeshwari (Taj) Devi, an executive at Fiji's Online Safety Commission and also a Get Safe Online Ambassador since 2020, devised an initiative to conduct awareness sessions in the community. She explains:

> *"In Fiji culture, people believe more in face-to-face than virtual. When we invited them to come online for an awareness session, they were a bit hesitant, whereas when we let them know we were coming to their communities, more than 200 people were there waiting for us for the first session, which was three and a half hours from Suva."*

Buoyed by the success of the initial session and further funding, Taj embarked on conducting further sessions in the Western Division. Continuously going out into communities at weekends, her team reached in excess of 1,000 people. Taj says:

> *"In Fiji, most people refer to 'online' as meaning social media. One of the first questions people ask is about securing their social media platforms, then about how to make purchases safely to avoid fraud. We also get a number of business-related queries."*

Anticipating how the need for, and popularity of, sessions would grow, Taj next devised a five-week Community Awareness Raisers Programme in which volunteers from different communities were hand-picked, trained, equipped with materials and tasked to present

one-hour sessions. This enabled presentations to take place in more remote regions of Fiji without requiring the physical resources of the Online Safety Commission team and also empowered the presenters to provide valuable help to their communities.

The next step was a 'Be Cyber Safe' one-day workshop, inspired by a similar event held by the UN and attended by Taj. The concept was trialled at Lautoka, Fiji's second city and attracted 35 people who had been invited from different communities. Most had poor knowledge of issues that can be encountered online and how to deal with them. Apart from learning the skills necessary to protect themselves, the delegates went out into their respective communities to cascade the online safety messages, supported by Get Safe Online materials. Many also took these messages back to the banks, universities and other organisations they worked for in order to initiate increased awareness and structure. Delegate feedback provided on the day was highly positive, with many requesting more workshops so that they could, in turn, invite more people. An event is planned in the capital Suva, home to the majority of businesses in Fiji. Taj says that from the modest beginnings of the workshop and community awareness sessions, it is hoped to reach out to more than 10,000 people.

On the importance of sharing and helping others, she says:

> *"We let young adults know that whilst everybody may be on social media, it's more elderly people who are starting to get accounts and don't know how to protect themselves. We ask them to offer help to the older generation but also teach their friends about things like two-factor authentication, passwords and not saving credit card details in the browser."*

In a further initiative to increase digital literacy, the Online Safety Commission has launched an online safety booklet in collaboration with the Australian eSafety Commission. The booklet is published in two versions – one for adults and one for children. More than 28,000 copies have been printed, many of which Taj's team is distributing in the community.

CLICK TO WATCH INTERVIEW

CERT, Vanuatu

The scenario

Since CERT Vanuatu's launch in 2018, the organisation had been concerned about the country's very low digital literacy rates. Under Vanuatu's National Cyber Security Strategy, and having carried out local assessments and research in other countries, it was decided that a cybersecurity awareness campaign should be launched.

The initiative

CERT Acting Manager Kensley Joses explains:

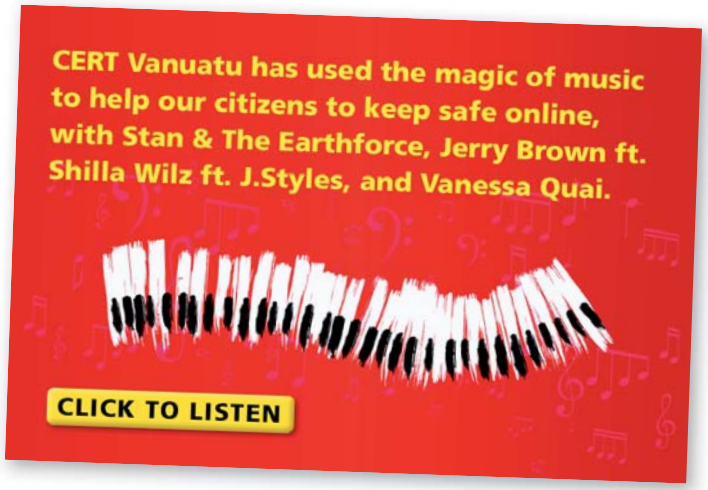
> *"We wanted to find an option where we could engage citizens with something that was common to all and everyone could participate in. After considering a few options, we decided on music. Everyone listens to music and we knew it would prove a highly effective medium."*

The CERT picked artistes who command a large following in Vanuatu and whose songs can regularly be heard on the country's popular radio stations. Kensley Joses recalls:

> *"We invited them in for a meeting at the CERT office and briefed them on the topic and key messages, which reflected the main type of activity we've seen in Vanuatu: misinformation – especially during the pandemic – cyberbullying and online respect."*

After the writing process and a short period of liaison and adjustment to lyrics, the three songs were ready for release:

- **'Watch What You're Doing'** by Stan & The Earthforce (about misinformation)
- **'Tingting Smart'** by Jerry Brown ft. Shilla Wilz ft. J.Styles (about online respect)
- **'Cyberbullying'** by Vanessa Quai (about cyberbullying)



All three songs are played regularly on the local radio station in capital Port Vila, and they can be heard being played in cars and people's mobile phones on the country's different islands. People have also been contacting the CERT referring to the initiative's effectiveness. "*We know the messages are getting across,*", says Kensley Jones. The songs can also be found on the CERT's website.

Discussions are already taking place with local collaboration partners and aid donors about producing more songs, and the CERT is getting local schools involved in writing songs about specific online safety topics.

CLICK TO WATCH INTERVIEW

Tongan Women in ICT

The scenario

Tongan Women in ICT was established with the aim of improving participation of women and girls in ICT and as a hub providing a voice in this male-dominated area. In the ten years that the group's President, Seluvaia (Selu) Kauvaka, has been working in the field, she has been the only female in every team of which she has been a member. Tongan Women in ICT has recently gained formal recognition from the Tongan government as an NGO.

Selu comments:

> *"We want to get more females in the group, encouraging women to take up technology. I've noticed that girls go overseas to study ICT and come back with degrees, only to become administrators and secretaries and not making good use of their qualification."*

This is despite the Ministry of Education actively encouraging girls to study STEM subjects at school.

The initiative

With online safety a major concern in Tonga, the group considered that one of the best ways it could help was to increase awareness. Selu says:

> *"We couldn't really do much technically as we have Tonga CERT doing that, so we asked them if they needed us to support awareness, for example in villages and schools. One of our biggest issues in Tonga is the misuse of social media, with misinformation, abuse, bullying, fraud and fake pages."*

Tongan Women in ICT has around ten active members, of whom only two or three have an interest in cybersecurity. When asked what they need in order to be effective, they invariably request more training to equip them with the knowledge and skills to carry out more awareness activity than they do currently. The group has stated that it would like to support any future Pacific-based programmes designed to encourage girls into careers in the cybersecurity field. However, its connection with Get Safe Online does enable it to seek available ways to receive training from experts.

With the CERT having only three members, resources are limited, so Tongan Women in ICT members deliver online safety awareness training on its behalf, equipped with CERT-supplied tools and scripts enabling them to present and answer any questions that may be asked. Feedback is requested via attendee surveys, with data supplied to the CERT for analysis.

They conduct awareness sessions in schools and villages and also provide information via social media. This complements CERT's own activity which includes TV slots and email bulletin distribution.

Selu claims that awareness raising activity has gone more online because of the pandemic, even though COVID-19 did not actually reach the country until after the volcanic eruption and ensuing tsunami in mid-January.

> *"Cyber has changed, everything is more online, but not everyone is online. There's always more to be done."*

CLICK TO WATCH INTERVIEW

Ministry of Innovation, Science and Smart Technology (MIST), Barbados

The scenario

Technology, as is the case with many aspects of life, brings a multitude of benefits, but also issues which if not addressed, can result in untold turmoil in a matter of seconds.

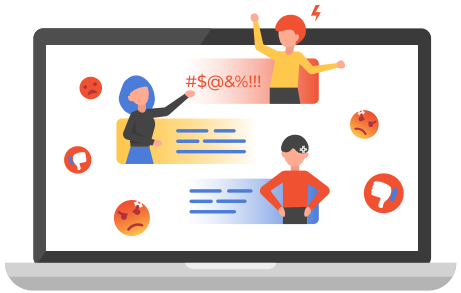
For example, the onset of the COVID-19 pandemic forced schools to conduct most learning and exchanges over the internet, rather than face-to-face. Based on evidence provided and research done, it is generally accepted that children and the younger generation use technology on a larger scale than the older generation and in doing so, tend to be able to navigate technological devices more smoothly, accessing online capabilities which until recently, would have been impossible.

Unfortunately, however, this makes the younger generation an attractive target for not only cyber attackers but also perpetrators of abuse, including bullying. This is especially true of those who are not fully aware of the dangers that can be encountered when using technology, or who consider themselves immune.

The initiative

In Barbados, the Digital Ambassadors Acceleration Program was originally launched in 2019 by the Ministry of Innovation, Science and Smart Technology (MIST), to not only assist university students fulfil their required stipulation of giveback hours to attain their degree but also support technological advancement in the country.

Against the background of increased cyberbullying, the Digital Ambassadors created a campaign to educate children on the implications of bullying or being bullied over the internet, particularly on social media platforms.



The campaign also included information on ways children could protect themselves and their families from cyberattacks and how to deal with an attack in the case of victimisation.

Having obtained permission from the Ministry of Sport, Youth and Culture and the Ministry of People and Elders Affairs, the Digital Ambassadors conducted informative and impactful drop-in sessions at several summer camps. The sessions focused mainly on cyberbullying under the catchphrase 'Cyberbullying is NOT OK!' – but also advised on what to do in the event of a cyberattack, whether a hack or adware infection. Phishing was also covered, being a common attack vector. Information was also shared with regards to phishing and how to avoid becoming a victim of phishing.

The cyberbullying catchphrase was constantly repeated throughout presentations by the Digital Ambassadors and also by soca artist Michael "Mikey" Mercer, who is a MIST Ambassador. Soca music is a combination of West Indian and East Indian rhythmic traditions. Being a well-known and respected public figure, Mercer appealed to the audience to not cyberbully anyone, but instead be respectable, law-abiding citizens, not only for the sake of themselves and their families but also for him and the wider Barbadian population.

The 45-minute sessions, which adopted a 'youth supporting youth' approach, were attended by some 250 young people in total. A segment entitled "Social Media and Me" focused on both the positive and negative aspects of social media as part of the "We 'gine' Digital, Think it through, Tech Chat Series."

As well as feeling strongly that the summer camp sessions had made a difference, the Digital Ambassadors enjoyed the programme and were grateful to MIST for creating the opportunity to make a positive difference to the lives of Barbadians.

Global24 Conference 2020: 'Go Share'

The Get Safe Online Global24 Conference took place on March 10th 2022 to showcase some of the excellent initiatives which have been taking place around the Commonwealth since the inaugural Global24 event in October 2020.

The event celebrated the concept of collaboration as being the most effective tactic in making the internet a safer place and focused on two main themes:

- Breaking down silos and raising awareness
- Digital literacy and building capacity

Highly respected journalist and strategic communications specialist Dafydd Rees moderated the two-hour virtual conference which provided a forum for delegates to present and share case studies from different regions resulting in positive, constructive and information sharing discussions.

Agenda

- Introduction from Dafydd Rees
- Interview with Tony Neate, CEO, Get Safe Online
- Endorsement from The Rt Hon James Cleverly, Minster Of State, UK Foreign, Commonwealth & Development Office
- Endorsement from Omar Daair, British High Commissioner to Rwanda
- Case study 1: Jamaica Broadcasting Commission
- Discussion with Don Dobson, Jamaica Broadcasting Commission and Muriana McPherson, National Data Management Authority, Guyana
- Interview with Dr Dustin Fraser, Cybersecurity Risk Manager
- Case study 2: National Bank of Rwanda
- Discussion with Colonel David Kanamugire, National Cyber Security Authority, Rwanda
- Video on romance fraud: 'Sai's Story' from Fiji
- Case study 3: CERT Vanuatu
- Discussion with Tajeshwari Devi, Online Safety Commission, Fiji and Suetena Loia, Ministry of Communications and Information Technology, Samoa
- Interview with Anju Mangal, World Wide Web Foundation

"We want to promote 'one voice and one Pacific' highlighting cyber safety for everyone in our region. Pacific countries need to have a strong and unified approach and ensure that inputs from Civil society, private and public sector, governments, academic institutions and marginalised groups are taken into consideration to tackle complex cyber safety and cyber security issues."

Anju Mangal, Head of Asia Pacific, Alliance for Affordable Internet, World Wide Web Foundation

"We are pleased to take part in the important discussions that will take place at the Global24 strategic conference, and welcome the partnership of the UK's Foreign, Commonwealth & Development Office (FCDO) and Get Safe Online, in raising online safety awareness and preventing cybercrime amongst our citizens. Ensuring online safety requires significant commitment in global partnership and collaboration among all stakeholders. In this regard, NCSA has the opportunity of working closely with Get Safe Online. Get Safe Online campaigns have been impactful in raising Cyber Security awareness among the Rwandan population."

Colonel David Kanamugire, CEO, National Cyber Security Authority, Rwanda

Get Safe Online is grateful for all of the contributions made during the event and thankful for the support of both the panellists and audience who enabled such an open and collaborative discussion. We hope it will inspire more people to help Get the Commonwealth Safe Online and we look forward to future collaborative events as we collectively progress with our efforts.

CLICK TO WATCH THE 'GO SHARE' CONFERENCE

Get Safe Online operates in the following countries:

Click on your country in the list to visit your Get Safe Online website.

Antigua and Barbuda
Bahamas
Barbados
Belize
Cook Islands
Dominica
England
Fiji
Grenada
Guyana
Indonesia
Jamaica
Kiribati
Nauru
Northern Ireland
Papua New Guinea
Rwanda
Samoa
Scotland
Solomon Islands
St Kitts and Nevis
St Lucia
St Vincent and the Grenadines
Tonga
Trinidad and Tobago
Tuvalu
Vanuatu
Wales