

# Building Trust in Digital World @COVID-19

Sameer Sharma  
Senior Advisor  
ITU Regional Office Asia-Pacific

For AIBD , Kuala Lumpur Malaysia  
6 May 2020



Digital transformation is key to accelerate our progress towards SDGs..

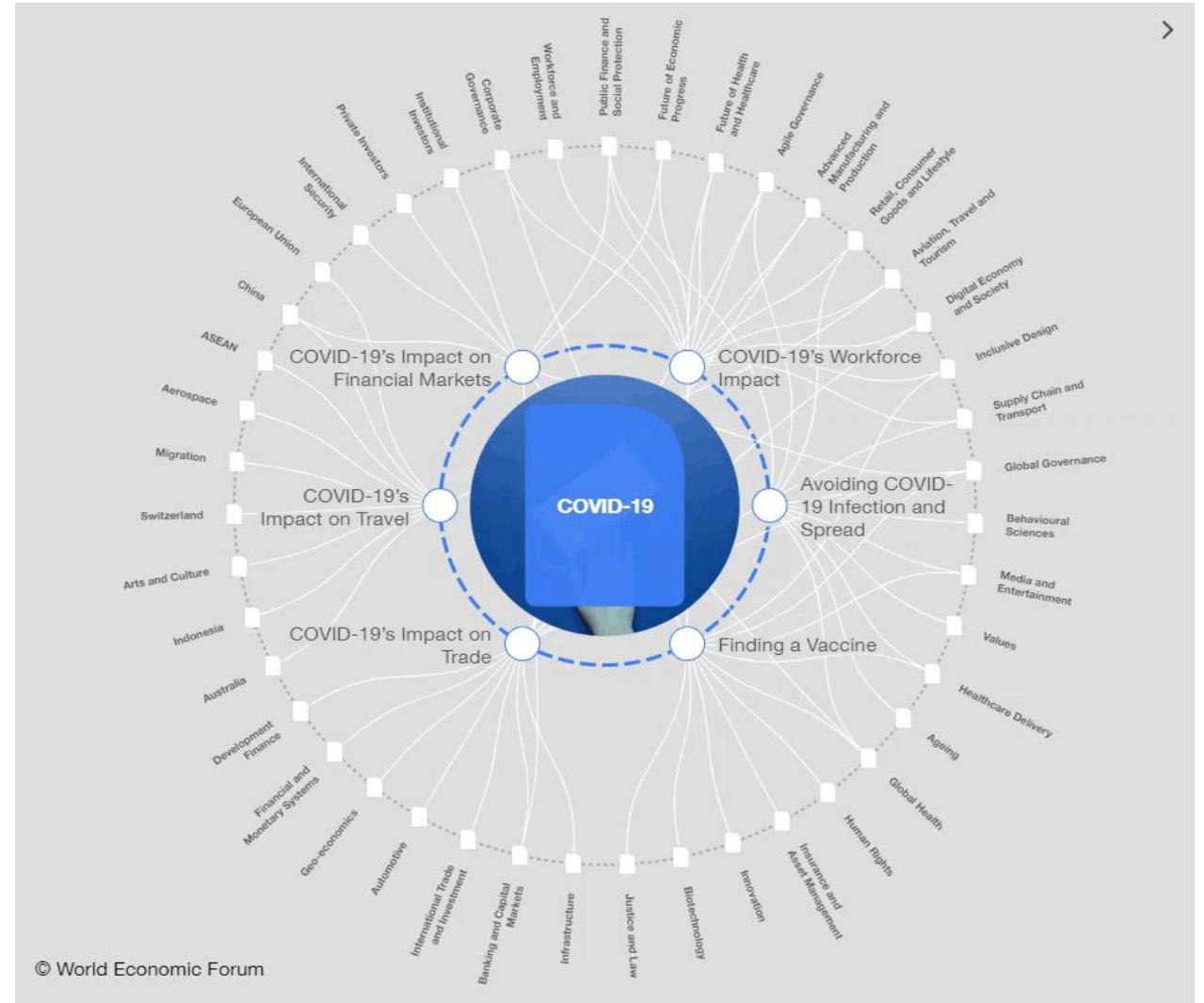
**17** Sustainable Development Goals

**169** Targets



# Impact of COVID-19

- The COVID-19 pandemic poses the risk of increased cyberattacks.
- Hackers are targeting people's increased dependence on digital tools.
- Strategies to maintain cybersecurity include maintaining good cyber hygiene, verifying sources and staying up-to-date on official updates.



# Impact of COVID-19

Here are three reasons robust cybersecurity measures matter more than ever.

## ***1. A heightened dependency on digital infrastructure raises the cost of failure.***

In a pandemic of this scale - with cases of coronavirus reported in more than 150 countries - dependency on digital communications multiplies. The Internet has almost instantly become the channel for effective human interaction and the primary way we work, contact and support one another.

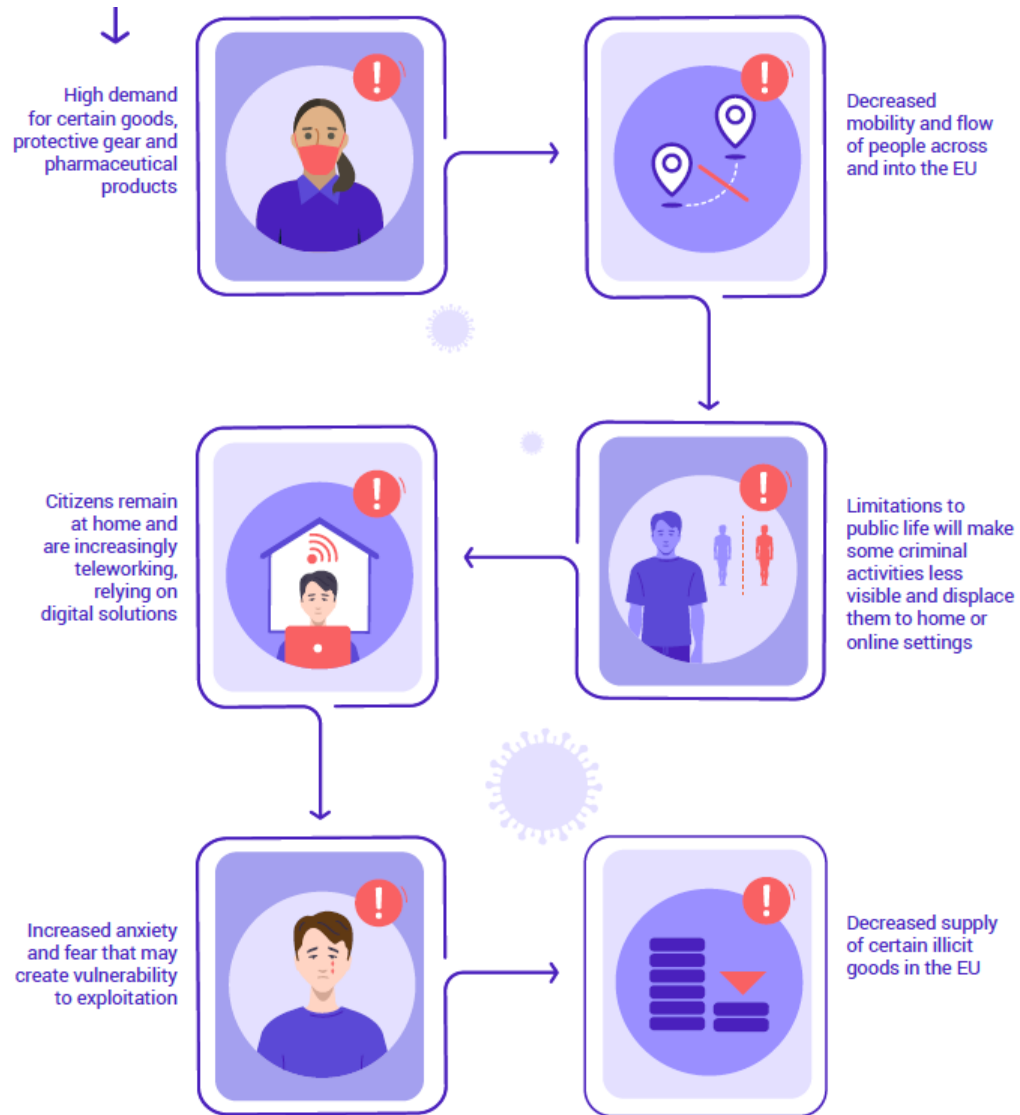
## ***2. Cybercrime exploits fear and uncertainty***

Cybercriminals exploit human weakness to penetrate systemic defences. In a crisis situation, particularly if prolonged, people tend to make mistakes they would not have made otherwise. Online, making a mistake in terms of which link you click on or who you trust with your data can cost you dearly. The vast majority of cyberattacks - by some estimates, 98% - deploy social engineering methods.

## ***3. More time online could lead to riskier behaviour***

Inadvertently risky Internet behaviour increases with more time spent online. For example, users could fall for “free” access to obscure websites or pirated shows, opening the door to likely malware and attacks.

# Which Factors have an Impact on Crime?



The COVID-19 pandemic has forced national governments and the EU to enact various measures to limit the spread of the outbreak, to support public health systems, to safeguard the economy and to ensure public order and safety.

A number of these measures have a significant impact on the serious and organised crime landscape as well as the threat from violent extremists. To understand the impact of the COVID-19 pandemic on the internal security of the EU, it is crucial to identify the factors that prompt changes in crime and terrorism.



# Key Findings on Cyber Crime during COVID-19?

The global pandemic of COVID-19 is not only a serious health issue but also a cybersecurity risk. Criminals swiftly took advantage of the virus proliferation and are abusing the demand people have for information and supplies.

Criminals have used the COVID-19 crisis to carry out social engineering attacks, namely phishing emails through spam campaigns and more targeted attempts such as business email compromise (BEC).

There is a long list of cyber-attacks against organisations and individuals, including phishing campaigns that distribute malware via malicious links and attachments, and execute malware and ransomware attacks that aim to profit from the global health concern.

Information received from law enforcement partners strongly indicates increased online activity by those seeking child abuse material. This is consistent with postings in dedicated forums and boards by offenders welcoming opportunities to engage with children whom they expect to be more vulnerable due to isolation, less supervision and greater online exposure.

The pandemic has an impact on Darkweb operations. Certain illicit goods will become more expensive, as source materials become unavailable. Vendors on the Darkweb offer special corona goods (scam material) at discounts.



## Attack on critical health infrastructure

Cybercriminals carried out a cyber-attack on Brno University Hospital Brno, Czechia amid the COVID-19 outbreak in Europe. Since a state of emergency was declared in Czechia on 12 March 2020, the attack was considered an attack on a critical infrastructure.

The incident prompted the hospital to postpone urgent surgeries and reroute new acute patients to a nearby alternative hospital.

The hospital was forced to shut down its entire IT network during the incident and two of the hospital's other branches, the Children's Hospital and the Maternity Hospital, were also affected.<sup>1</sup>

These types of attack during a public health crisis such as the COVID-19 pandemic are particularly threatening and carry very real risks to human lives.

<sup>1</sup> ZDNet 2020, Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak, accessible at <https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/>

# Key Findings on Counterfeit & sub-standard goods during COVID-19?

The distribution of counterfeit and/or sub-standard goods has been a key area of criminal activity in relation to the COVID-19 pandemic.

The sale of counterfeit healthcare and sanitary products as well as personal protective equipment (PPE) and counterfeit pharmaceutical products has increased manifold since the outbreak of the crisis. The advertisement and sale of these items take place both on and offline.

Some developments, such as the distribution of fake corona home testing kits, are particularly worrying from a public health perspective.



## Criminals take advantage of the high demand in hygiene products driven by the COVID-19 outbreak<sup>1</sup>

Europol supported a global operation to target trafficking counterfeit medicines. Operation Pangea, coordinated by INTERPOL and involved 90 countries worldwide, took place between 3 and 10 March 2020.

The pandemic has opened up a business opportunity for predatory criminals. Authorities around the world seized nearly 34 000 counterfeit surgical masks, the most commonly sold medical product online. Law enforcement officers identified more than 2 000 links to products related to COVID-19.

The results of the operation reveal a worrying increase in unauthorised antiviral medications and the antimalarial chloroquine. Vitamin C, known for its immune-boosting properties, and other food supplements have been seized around the world. Painkillers and antibiotics also represented a significant portion of the seizures.

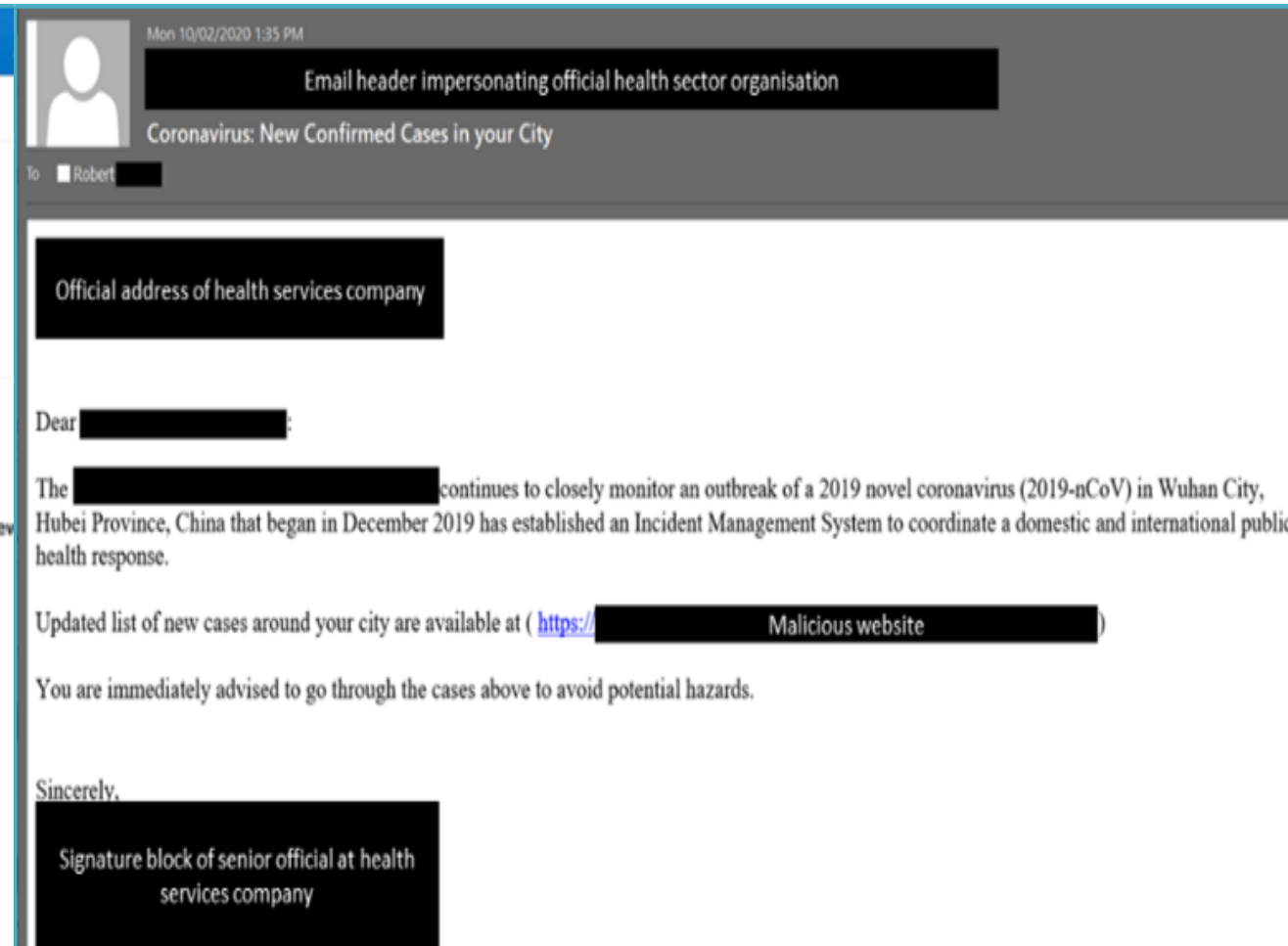
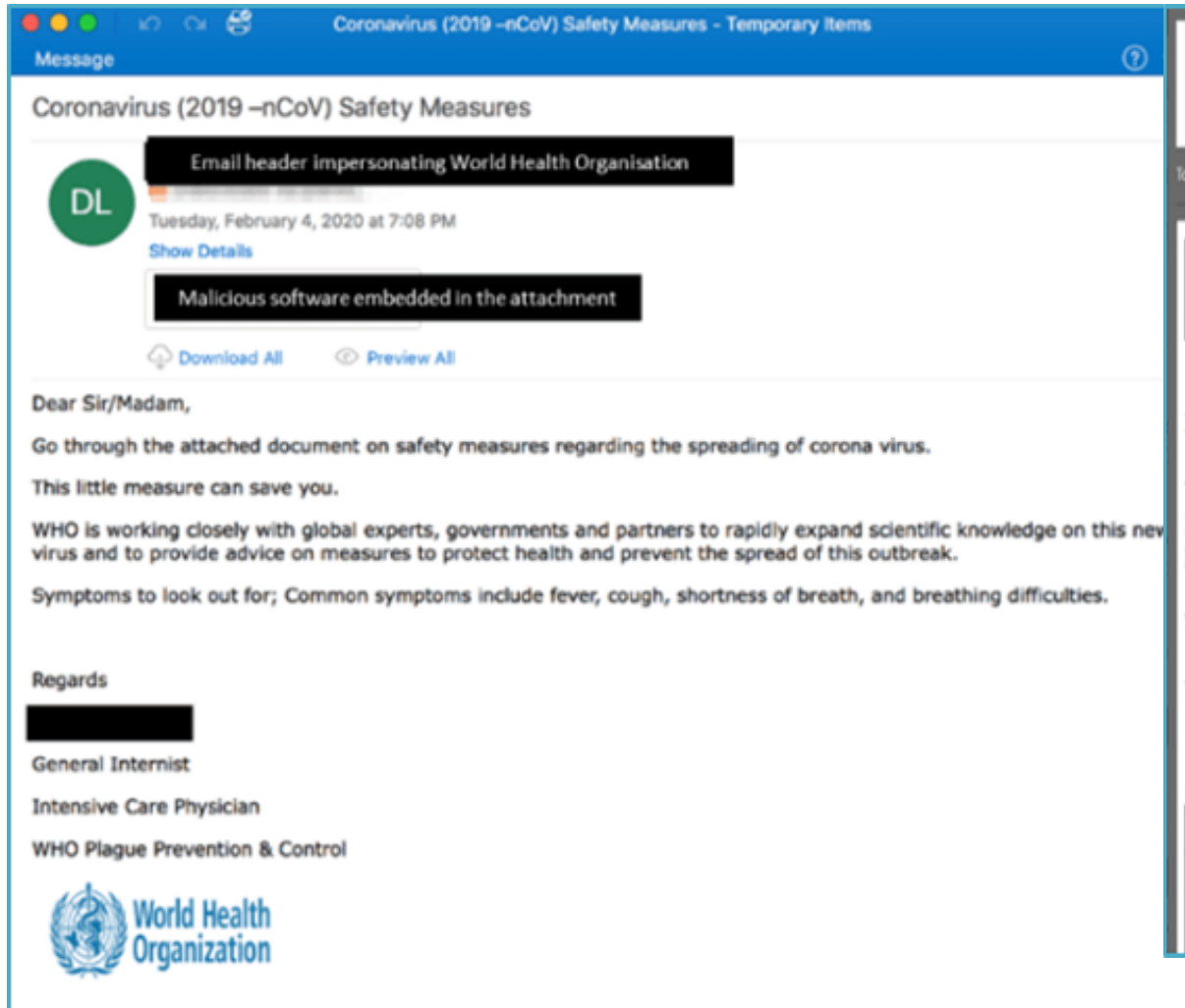
Europol supported the operation by facilitating information exchange and providing analytical support.

### The operation in numbers

- 121 arrests;
- €13 million in potentially dangerous pharmaceuticals seized;
- 326 00 packages inspected;
- 48 000 packages seized;
- 4.4 million units of illicit pharmaceuticals seized worldwide;
- 37 000 unauthorised and counterfeit medical devices seized (mostly surgical masks and self-testing kits for HIV and glucose monitoring);
- 2 500 links taken down (websites, social media, online marketplaces, adverts);
- 37 organised crime groups dismantled.

<sup>1</sup> Europol 2020. Criminals take advantage of the high demand in hygiene products driven by the COVID-19 outbreak, accessible at <https://www.europol.europa.eu/newsroom/news/rise-of-fake-%E2%80%98corona-cures%E2%80%99-revealed-in-global-counterfeit-medicine-operation>

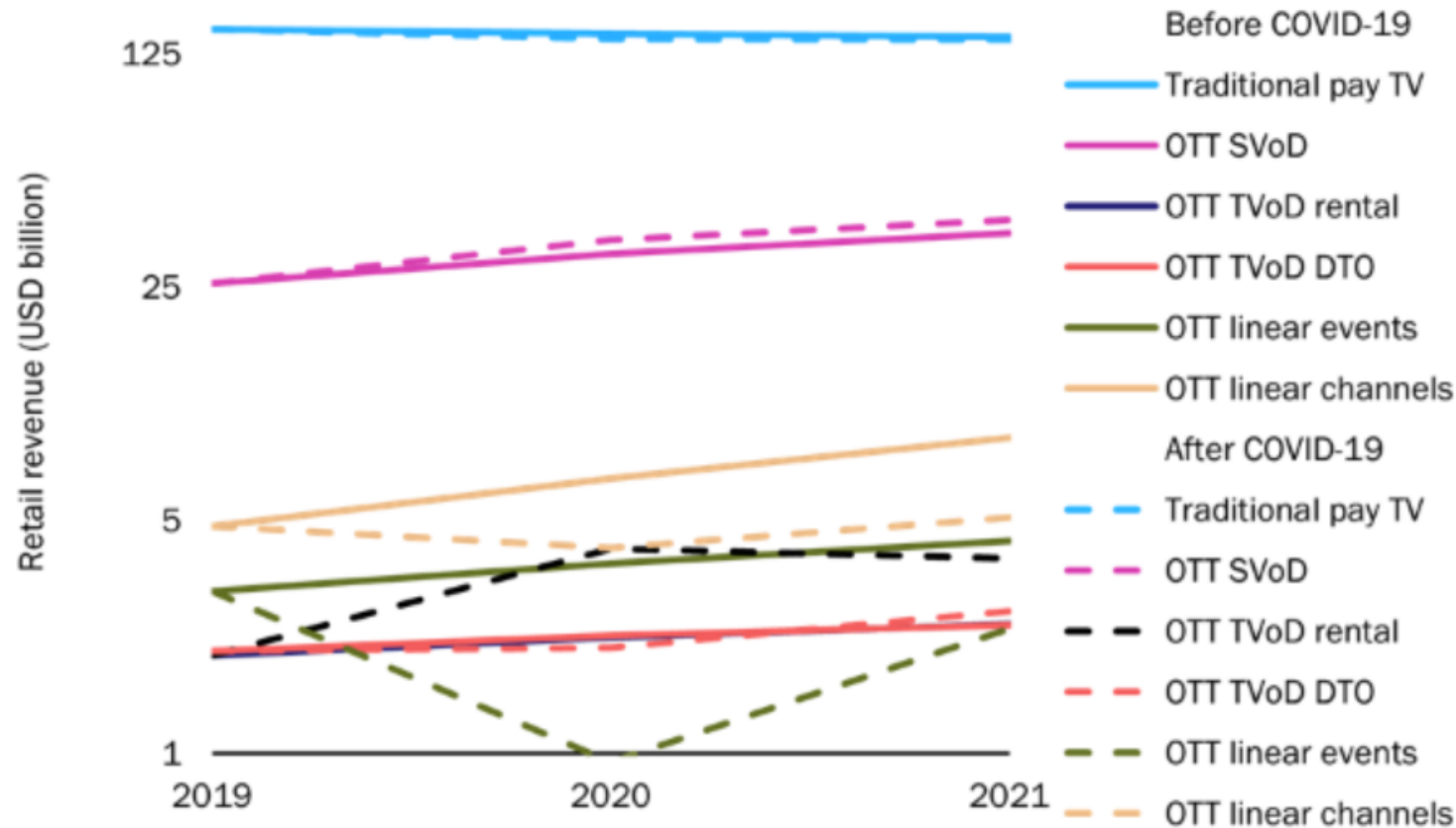
# Examples of Cybersecurity Scams/ Risks @COVID-19





# Impact of COVID-19 on Broadcasting Industry

**Figure 1:** Pay-TV and OTT video retail revenue in a selection of countries, before and after the impact of COVID-19, 2019–2021

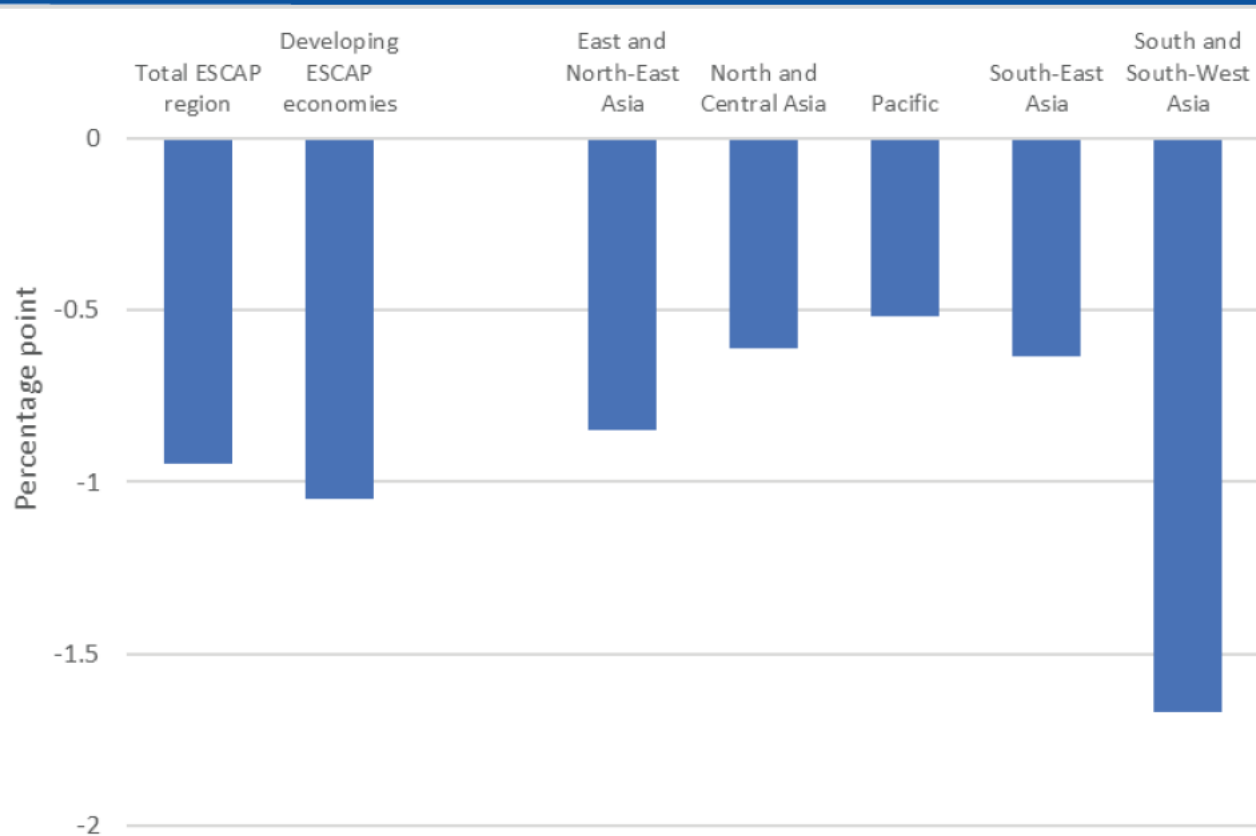


The pandemic will reduce the total pay-TV retail revenue by 3.4% in 2020 despite strong gains for SVoD and TVoD

- Disruption from COVID-19 is changing the value of transactional, advertising and subscription revenue.
- These countries currently account for around 75% of the worldwide pay-TV and OTT video revenue.
- The total retail revenue for pay-TV and OTT video services in these countries will be USD6.5 billion (3.4%) lower in 2020 than predicted in our pre-COVID-19 forecasts.
- Retail revenue for 2021 will be USD3.5 billion (1.8%) lower.

# Impact and Policy Responses for COVID-19

Figure 3. GDP Growth decline in Asia and the Pacific Region due to COVID-19



### COVID-19 IMPACT ON WOMEN

In Asia and the Pacific

WOMEN WILL CONTINUE TO SHOULDER A DISPROPORTIONATE AND INCREASING BURDEN OF CARE

WOMEN ARE AT INCREASED RISK OF GENDER-BASED VIOLENCE

WOMEN IN VULNERABLE EMPLOYMENT MAY FALL BACK INTO POVERTY

ACCESS TO HEALTH SERVICES FOR WOMEN MAY DWINDLE

### POLICY MEASURES

In Asia and the Pacific

SUPPORT WOMEN ON THE FRONT LINES

PROMOTE FLEXIBLE WORK ARRANGEMENTS

PROVIDE TAILORED ADVICE TO CARE TAKERS

PROVIDE PSYCHO-SOCIAL SUPPORT

BUILD RESILIENCE TO FUTURE SHOCKS

ANALYSE SEX-DISAGGREGATED DATA

TARGET ECONOMIC RECOVERY EFFORTS TO WOMEN

STRENGTHEN ESSENTIAL HEALTH SERVICES

PROMOTE UNIVERSAL HEALTH CARE

UNITED NATIONS ESCAP

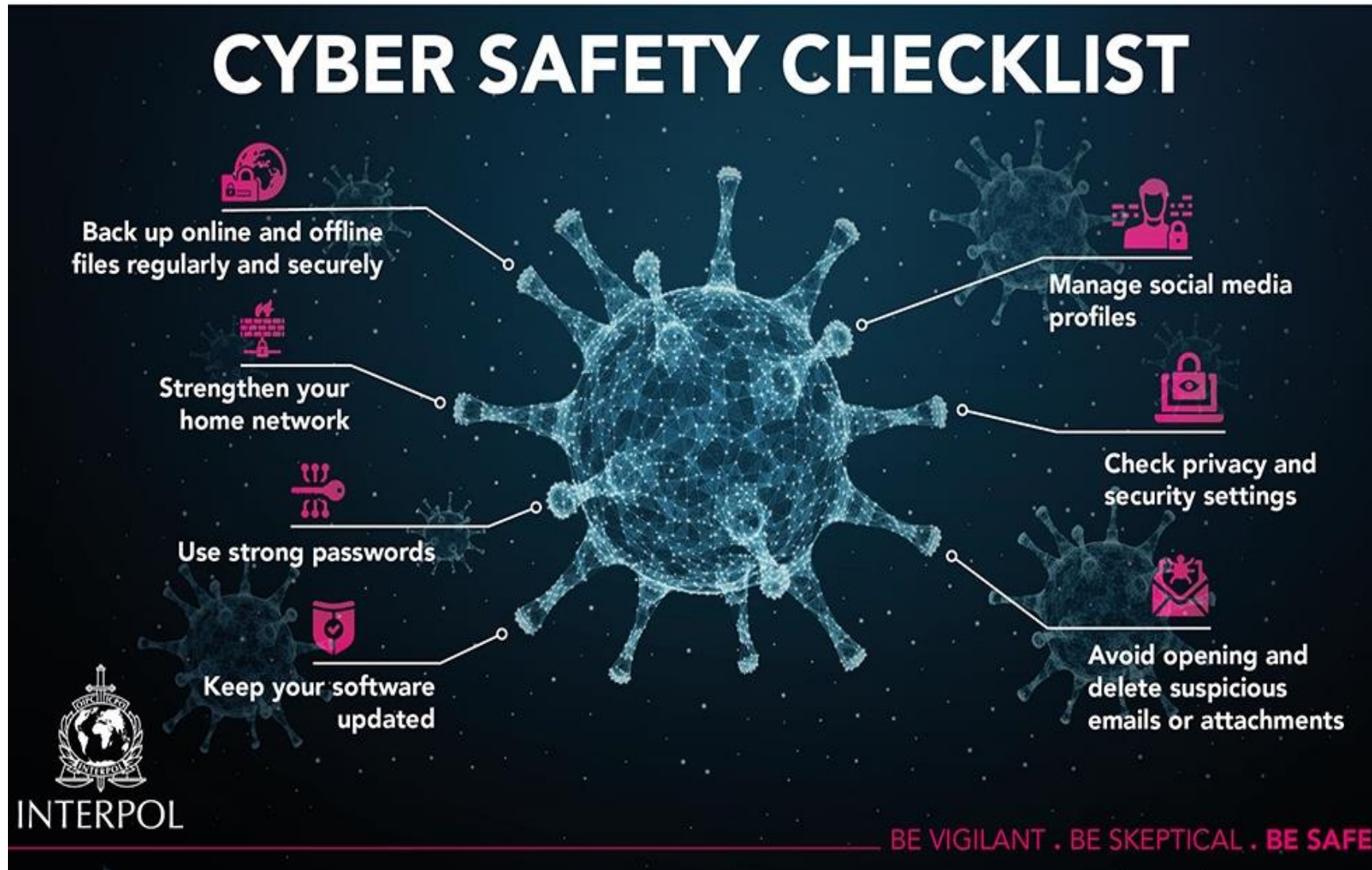
5th DECADE OF ACTION

## Messages:

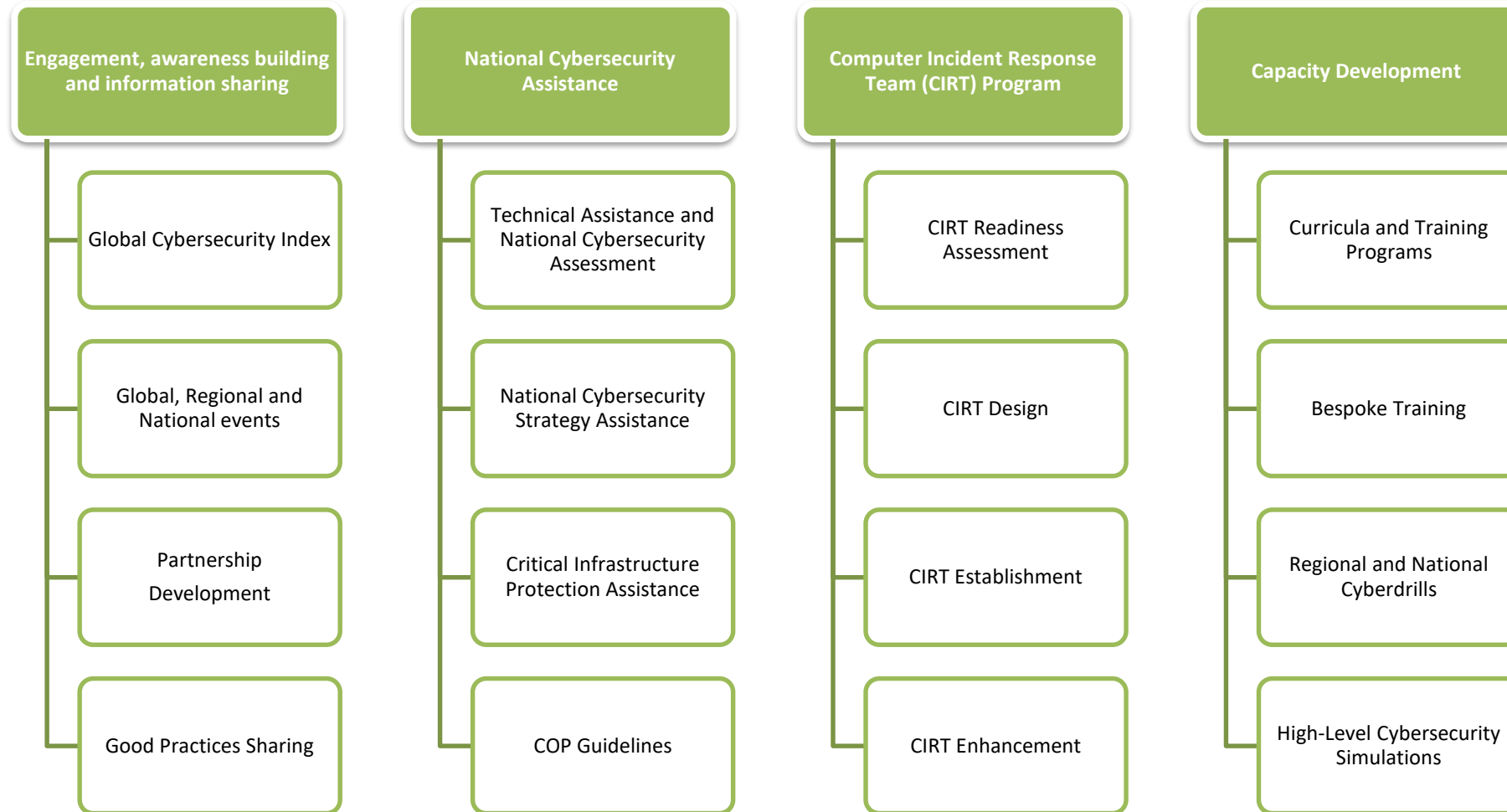
- Countries with established universal health care and universal social protection systems are better positioned to address the pandemic.
- Vulnerable population groups must be placed at the centre of all social policy reform packages in the short- and medium-term.
- In long term, countries should invest to enhance emergency preparedness and strengthen social protection in order to enhance resilience of economies and minimize impact of potential health emergencies in future.
- Digital connectivity is making social distancing possible without social isolation. Investments need to be stepped up to reduce the digital divide.
- Regional Cooperation can promote enhanced collaboration on health care related R&D so that vaccines and medicines can be developed quickly and made available for the benefit of all countries in the region



# Cyber Safety Check List



# Cybersecurity Output Areas





# ITU Global Cybersecurity Index

GCI is a composite index combining 25 indicators into one benchmark measure to monitor and compare the level of ITU Member States' **cybersecurity commitment** with regard to the five pillars identified by the High-Level Experts and endorsed by the GCA.

“GCI is a capacity building tool, to support countries to improve their national cybersecurity”

Rank	Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
1	United Kingdom	0.931	0.200	0.191	0.200	0.189	0.151
2	United States of America	0.926	0.200	0.184	0.200	0.191	0.151
3	France	0.918	0.200	0.193	0.200	0.186	0.139
4	Lithuania	0.908	0.200	0.168	0.200	0.185	0.155
5	Estonia	0.905	0.200	0.195	0.186	0.170	0.153
6	Singapore	0.898	0.200	0.186	0.192	0.195	0.125
7	Spain	0.896	0.200	0.180	0.200	0.168	0.148
8	Malaysia	0.893	0.179	0.196	0.200	0.198	0.120
9	Norway	0.892	0.191	0.196	0.177	0.185	0.143
10	Canada	0.892	0.195	0.189	0.200	0.172	0.137
11	Australia	0.890	0.200	0.174	0.200	0.176	0.139

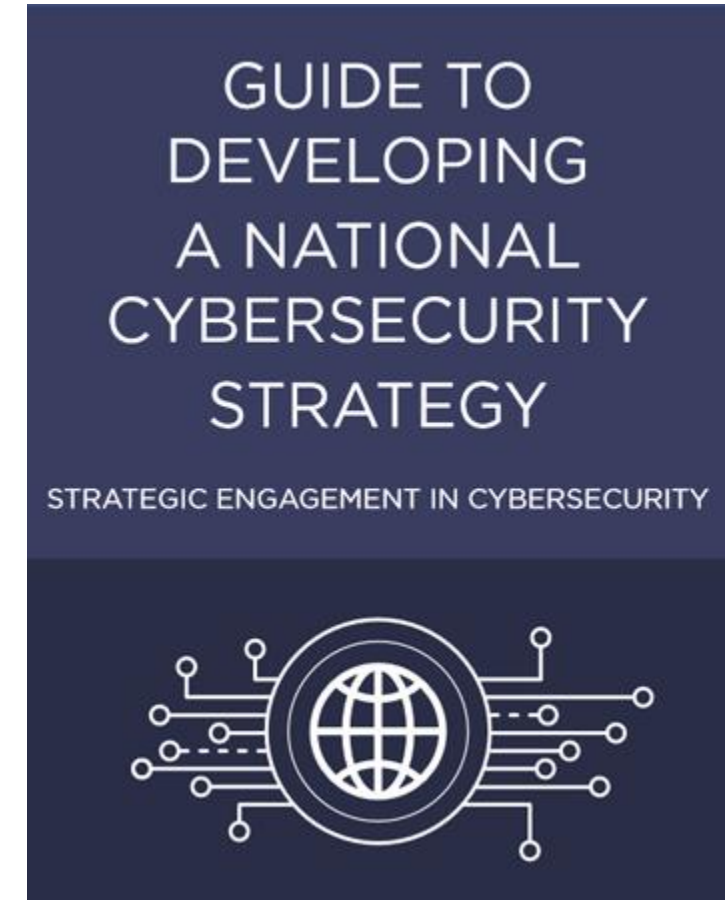
# National Cybersecurity Strategy (NCS)

The reference guide represents a comprehensive one-stop resource for countries to gain a clear understanding of the purpose and content of a national cybersecurity strategy, as well as actionable guidance for how to develop a strategy of their own. The reference guide further lays out existing practices, relevant models and resources, as well as offers an overview of available assistance from other organizations. An accompanying support tool assists evaluation of the strategy.

Reference Guide and evaluation tool were drafted in a democratic process among partnering organizations.

The [National Cybersecurity Strategies repository](#) is a collection of strategic national policies, action plans and other relevant elements which relate to cybersecurity. This list or repository is populated and frequently updated with documents either acquired through research of primary and secondary sources, or provided directly by the respective governments.

*Access the repository via [National Cybersecurity Strategies repository](#).*



# Regional Cyber Drills



**Date :** 23-27 September 2019,  
Kuala Lumpur, Malaysia

**Hosted by**



MINISTRY OF COMMUNICATIONS  
AND MULTIMEDIA MALAYSIA



The National Cyber  
Security Agency Malaysia

1	Enhancing cybersecurity capacity and capabilities through regional collaborations and cooperation;
2	Enhancing the awareness and the capability of countries to participate and to contribute to the development and deployment of a strategy of defeating a cyber threat;
3	Strengthening international cooperation between Member States to ensure continued collective efforts against cyber threats;
4	Enhancing Member States' and incident response capabilities and communication;
5	Assisting Member States to develop and implement operational procedures to respond better to various cyber incidents, identify improvements for future planning CIRT processes and operational procedures

# Child Online Protection (COP) Initiative

The COVID-19 global pandemic saw a huge surge in the number of children joining the online world for the first time, to support their studies and maintain social interaction. The constraints caused by the virus also meant that many younger children began interacting online much earlier than their parents might have planned.

The pandemic has shown even more how urgent and necessary it is to act jointly to respond to risks and harms for children online since children are also often less supervised while online and more self-generated content has been produced that could become harmful for children and young people as child sexual abuse material.

The ICT industry is uniquely placed to prevent and mitigate violence against children online starting with education about the services they provide. Further Industry need to do more to support the principle of safety-by-design, to be proactive in developing strong age-verification systems, and in detecting, blocking and removing illegal and harmful material on their platforms, and to report promptly and collaborate fully with law enforcement agencies and hotlines.

Children and young people will no doubt face a new different reality after the crisis and their future seems uncertain, therefore they will have to be part of the solution.

It is vital that governments across regions provide opportunities for children's views to be heard and taken into account in decision-making processes on the pandemic, through consultation and dialogue.

# Technical Note: COVID-19 and its implications for protecting children online

- ITU together with UNICEF, GPEVAC, UNESCO, UNODC, WePROTECT Global Alliance, WHO and World Childhood Foundation USA released a [Technical note on COVID-19 and its implications for protecting children online](#), which aims to help governments, ICT companies, educators and parents protect children in lockdown.
- The note states:

**Increased online activity supports children's learning, socialization and play, but also puts them at heightened risk.** This includes higher risk for **sexual exploitation, bullying, online risk-taking behavior**, which may expose children to risks of extortion, harassment and humiliation, **potentially harmful content, inappropriate collection, use and sharing of data and limited child safeguarding online during distance learning.**

- **Recommendations for policymakers, parents, educators, industry & children themselves:**
  1. Empower children online
  2. Support parents and caregivers to help children stay safe online
  3. Provide a safe online learning experience for students
  4. Make online platforms safe and accessible for children
  5. Strengthening national prevention, response and support services.



- Following the Secretary General's policy brief on the impact of COVID-19 on children, the UN Inter-Agency Working Group on Violence against Children has put together an Agenda for Action. The Agenda for Action is based on the different mandates of the entities involved and provides a child rights and multi-sectoral framework for action.
- The Agenda aims to mobilize Governments and other stakeholders around the world in defense of social services for children. A global crisis calls for a global response. Solidarity, multi-stakeholder cooperation and multilateralism are needed now more than ever.
- The Agenda calls for strong mobilization of governments, bilateral/multilateral donors, civil society and private sector to:
  - safeguard social protection, health, education and protection of children services;
  - ensure children are duly protected and have the possibility to thrive and reach their full potential, when this crisis will be over;
  - achieve the Goals and Targets of the Sustainable Development Agenda.

# COVID-19: 7 Key Ways to Keep Children Safe Online at home

S. N	Key Ways for to keep children Safe	Explanatory Notes
1	Set up parental controls	All leading browsers (Google, Safari, Firefox, Bing, Duck Duck Go) include a parental control mode; make sure you turn it on, and also check the individual privacy settings on apps and games. Some internet service providers and mobile operators provide additional parental control tools, which block or restrict access to certain types of content, as well as limiting the amount of time spent on devices.
2	Talk with your children	Talk with your children about online safety and be aware of the online and mobile services they are using. Help them understand the importance of managing personal information in the correct way.
3	Help your children be tech ready	Common Sense Media provides advice for age-appropriate apps, games and other platforms. Help children set up a strict privacy setting with the e-Safety Guide and check if they know how to report inappropriate content.
4	Stay aware of the online and mobile services used by your children	Spend time with your children online. Better Internet for Kids recommends that parents check on their children's technology use regularly – find out about what they are doing online, what new tools and apps they might be using.
5	Know how to report problems and seek help	When playing online games or using apps children can be exposed to serious risks like cyberbullying and grooming.
6	Create a culture of support so that children and young people feel comfortable seeking help	Open dialogue and discussion are crucial. Research has shown that many young people are reluctant to speak to an adult about a negative online experience for fear of the consequences.
7	Manage children's screen time	It is important to set boundaries and limits for online activities where possible. Build safe online habits and find a balance between online time and other activities.

# ITU- WHO –UNICEF Efforts to defeat COVID-19

Health Topics ▾

Countries ▾

Newsroom ▾

Emergencies ▾

## ITU-WHO Joint Statement: Unleashing information technology to defeat COVID-19

20 April 2020 | Statement | Geneva

The World Health Organization, the International Telecommunication Union (ITU) with support from UNICEF are set to work with telecommunication companies to text people directly on their mobile phones with vital health messaging to help protect them from COVID-19. These text messages will reach billions of people that aren't able to connect to the internet for information.

Now more than ever, technology must ensure that everyone can access the information they need. The collaboration will start in the Asia Pacific region and then roll out globally. The goal is to reach everyone with vital health messages, whatever their connectivity level. An estimated 3.6 billion people remain offline, with most people who are unconnected living in low-income countries, where an average of just two out of every ten people are online.

ITU and WHO call on all telecommunication companies worldwide to join this initiative to help unleash the power of communication technology to save lives from COVID-19. This initiative builds on current efforts to disseminate health messages through the joint WHO-ITU BeHealthy BeMobile initiative.

Coronavirus disease (COVID-19) is the first pandemic in human history where technology and social media are being used on a massive scale to keep people safe, productive and connected while being physically apart.

Health workers are utilizing telemedicine to diagnose patients and hospitals rely on being connected to coordinate and triage them. Resilient and trustworthy telecommunication networks and services are essential, as more countries, companies and individuals turn to digital technologies to respond to and cope with the impact of COVID-19.

- ITU- WHO Issued Joint Statement to join forces to defeat COVID-19 to help unleash the power of communication technology to save lives from COVID-19.
- This initiative builds on current efforts to disseminate health messages through the joint WHO-ITU BeHealthy BeMobile initiative.
- ITU-WHO-UNICEF-GSMA reaching out to 25 countries in Asia- Pacific region using digital platforms SMS/ IVR/USSD etc. for reaching out to most vulnerable communities who may not have access to Internet but to mobile phone
- ITU reached out to Member States / Regulators and Mobile operators to facilitate access of digital platforms to reach out to vulnerable communities

# ITU- WEF-WB-GSMA COVID-19 Crisis Response: Digital Development Joint Action Plan and Call for Action



COVID-19 Crisis Response:

Digital Development Joint Action Plan and Call for Action

In this unprecedented fight against COVID-19, digital technologies offer the only opportunity for governments, individuals and businesses to cope with social distancing, ensure business continuity, and prevent service interruptions.

Immediate action is needed especially to leverage digital to respond to challenges presented by COVID-19, from governments and regulators around the world, supported by the private sector and the digital development community. Fostering knowledge-sharing, notably through the ITU's [Global Network Resiliency Platform](#) (#REG4COVID) and WEF's [COVID Action Platform](#) (the [COVID Digital Response Network](#) and the [Digital Transformation for Post-COVID World group](#)), the Broadband Commission for Sustainable Development's [Agenda for Action](#), and other platforms and forums, this call for action has been developed as part of a fast-tracked collaboration initiated by the World Bank, the International Telecommunication Union (ITU), GSMA and the World Economic Forum.


Our high dependency on digital infrastructure and increased reliance on secure online services have never been greater. However, many of those who remain unconnected to digital services risk being left further behind in these times and beyond:

- Today there are 3.9 billion internet users globally, leaving almost 50% of the world's population still excluded from digital technologies. In addition, there is also a "usage gap" with 3.3 billion people covered by mobile broadband networks but who are not using mobile internet services. Of the 25 least connected countries in the world, 21 are in Africa.
- African countries and Fragile, Conflict and Violence-affected States with relatively high prices for mobile broadband connectivity, high voice and data taxes, and limited penetration will be most affected by the digital divide.
- Socially marginalized groups, including rural communities, persons with disabilities young people and children, and women and girls who are often excluded from digital development opportunities, will be disproportionately affected.
- Since the start of COVID-19,
  - Over one billion students are now out of school and in need of online/distance learning and safe environments to learn and communicate.
  - Voice calls have almost tripled in some countries while the use of some communications apps has more than doubled, causing increased congestion and the need to support network resilience.
  - Data traffic has increased by at least 20 percent and cyberattacks on the health sector infrastructure and mobile networks have increased by 150 percent in the last two months.


- Objective 1: Increasing bandwidth, strengthening resilience and security of networks, and managing congestion
- Objective 2: Connecting vital services and ensuring the continuity of public services to safeguard the welfare of populations
- Objective 3: Powering FinTech and digital business models to support the most impacted businesses and communities
- Objective 4: Promoting trust, security and safety online
- Objective 5: Leveraging the power of mobile big data



# ITU Initiatives on Addressing COVID-19



Committed to connecting the world

What would you like to search for? 

[Home](#) [ITU](#) [General Secretariat](#) [Radiocommunication](#) [Standardization](#) [Development](#)

[About ITU-D](#) [Partners](#) [Projects](#) [TDAG](#) [WTDC](#) [Study Groups](#) [Regional Presence](#)

## REG4COVID Platform

YOU ARE HERE [HOME](#) > [ITU-D](#) > [REGULATORY & MARKET ENVIRONMENT](#) > [REG4COVID PLATFORM](#)

## Policy and Regulatory experiences and best practices that can improve COVID-19 responses

### FROM TELECOM/ICT POLICY MAKERS AND REGULATORS

- **Ministerio de Transportes y Telecomunicaciones (MTT) of Chile** activates solidarity plan to guarantee connectivity during the COVID-19 outbreak. Telecommunications companies in Chile join the request of **SUBTEL** to establish measures in favor of users to address the COVID-19 contingencies.
- **ComReg Ireland** to release more radio spectrum to boost mobile phone & broadband capacity due to the COVID-19 crisis.
- **Ofcom UK** agrees measures with telecoms companies to support vulnerable consumers through COVID-19.
- **Ministerio de Asuntos Económicos y Transformación Digital de España:** the Government and the telecommunications operators sign an agreement to extend the measures to guarantee the connectivity of people and companies.
- **Instituto Federal de Telecomunicaciones México** regulatory actions being implemented together with

### CYBERSECURITY RESOURCES FOR COVID-19

Resource	Target Audience	Organization
<b>Why cybersecurity matters more than ever during the coronavirus pandemic.</b> This resource outlines the risks of cyberattacks that prey on the current increased reliance on digital tools, and provides for cyber hygiene standards to be adopted.	Public Sector Private Sector End users	World Economic Forum
<b>Pandemic Profiteering: How Criminals Exploit The COVID-19 Crisis.</b> The report provides an overview of how criminals adapt their misdeeds to the COVID-19 pandemic. It is based on information Europol receives from the EU Member States on a 24/7 basis and intends to support Member States' law enforcement authorities in their work.	Public sector Private sector End users	Europol
<b>Coronavirus crisis: A digital policy overview</b> This resource has mapped out the coronavirus outbreak with digital policy issues as per the GIP Digital Watch taxonomy.	Public Sector Private Sector End users	Geneva Internet Platform, Digital Watch Observatory
<b>COVID-19 Cybersecurity Response Package</b> This package compiles rapid response initiatives / tools / services from the European cybersecurity community which includes ECSO members, ECSO partners, and other stakeholders.	Public Sector Private Sector End users	European Cyber Security Organization
<b>Resource Guide for Cybersecurity during the COVID-19 Pandemic</b> This resource guide provides information about common cyber-attacks that are currently being reported. It also provides resources for improving cyber hygiene to enhance cyber defenses, both for organizations and their employees.	Public Sector Private Sector End users	Center for Internet Security
<b>COVID-19 Resources</b> These free resources offer insights into how telecoms	Public Sector Private Sector	Analysys Mason



# ITU and UN Secretary General Partnership on Online Safety

Joint webinar series

## Digital cooperation during COVID-19 and beyond

*Webinar #4 Theme:*

*“Online Safety  
and Security during  
Covid-19”*

6 May Wednesday,  
09:00-10:30 New York/15:00-16:30 Geneva

Co-organizers

An ITU event, in partnership with the Office of the UN Secretary-General's  
Special Advisor, working on Digital Cooperation



# Stay Connected - Stay Safe & Healthy

