Yes, we are protecting our communities not simply computers.

**KE-CIRT/CC detected 35.2million cyber threat events between July to September 2020, 152.9% increase from previous quarter**. This is accompanied by increase in malware and web applications attacks.

1. Attributed to uptake of eCommerce and Covid-19 pandemic.
2. Targeted remote working systems and tool plus eCommerce sites.
3. South Africa, Kenya, and Nigeria most affected.

Nigeria's Central Bank warned of spike in phishing attacks, malicious spams, and ransomware attacks - **messages from health organisations like Nigerian Centre for Disease Control (NCDC) or World Health Organization (WHO)**.

1. Using the coronavirus as bait to impersonate brands, circulating disinformation thereby misleading customers, and employees.
2. Register to collect government or aid agency relief packages.
3. Criminals collect victims' information e.g., account details under the guise of likely transfer relief funds.

**02 September 2020, Economic and Financial Crimes Commission (EFCC) operatives arrested 13 suspects** believed to be members of an organised cyber criminal syndicate who defraud unsuspecting victims of millions of Naira. The workings of the groups, as networks or connected individual hackers, remains largely unknown and is still being probed by security operatives.

Criminals impersonate bank staff and advise victims to download mobile apps ostensibly to ease their banking needs including loans during this period.

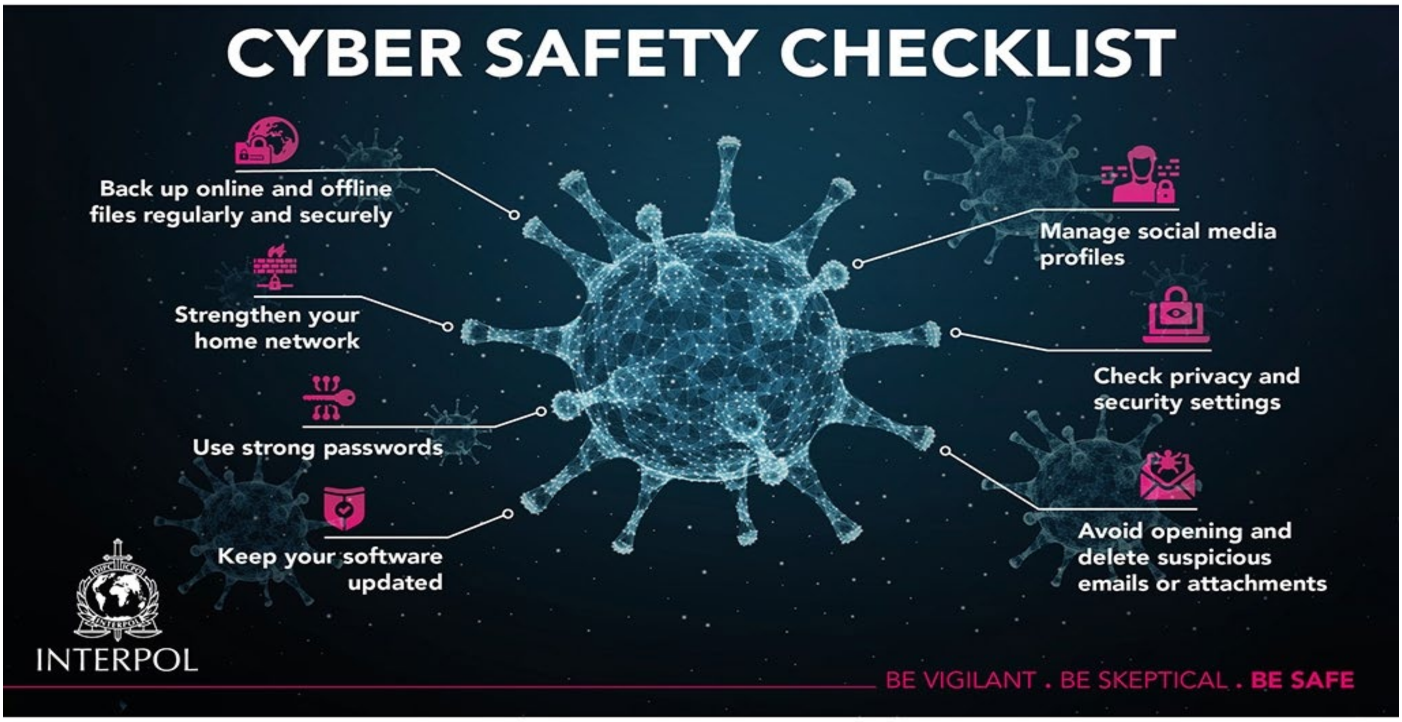
1. End users need to be careful and check emails or phone calls claiming to be from NCDC, WHO or Government agencies especially if the caller asks for Bank information or click any link or visit any website that collects information.
2. Avoid clicking on links or attachments in emails that claim they have information COVID-19 pandemic.
3. Do not download any mobile app that you are not sure of the source:
   a. Downloading ransomware.
   b. **Nigerian cybercrime group called SilverTerrier** that has targeted organisations and workers responding to COVID-19
   c. **Better more intuitive naming of apps by government e.g., "MWS" by NIMC or "Secure Fare" by NRC**?
4. Only collect relief packages from trust sources.
5. CBN says they continue to monitor criminal activities.
   a. Banks in Nigeria have taken extra measures, especially since the outbreak of COVID-19. Such as messages sent by phone and email to customers calling for caution in all online transactions and dealings.
   b. Government agencies and private corporate establishments have acted likewise.
   c. However, **many of the legitimate recipients are functionally illiterate thus the messaging media needs to be fully considered**.
6. We need **partnerships between government and private sector** to address problem.
   a. If **responses mechanisms are dominated by security agencies, concerns are likely to be raised about abuse, accountability, access to information as well as obligations** on the commercial sector to report attacks.
   b. This may cause a reluctance to report offences and a perpetuation of behaviour that increases vulnerability to cybercrimes.
7. Joint task forces to build confidence between the public and private sectors are preferable.

   a. Effective collaboration between financial institutions, corporates and the Cybercrime Advisory Council would be a practical step.
   b. Ensure a **balance between the protection of privacy and law enforcement**.

8. In address the challenge of the management of remote workforces during pandemic by:
   a. Nobody had anticipated the pandemic would live and continue to live with us for so long
   b. Initiation of a hybrid approach.
   c. The challenge of managing on-premsis systems remotely.
   d. Ensuring Mobile Device Management (MDM) has Two-factor authentication (2FA) access in place.
   e. Having distributed denial-of-service (DDoS) solutions in pl.ace
   f. Using managed service providers to increase resource capabilities and incident response.
   g. Adoption of cloud-based options requiring wholesale change i.e., Extended detection and response (XDR) becomes important as updates are pushed from cloud

9. Corporate CISO Lessons:
   a. **There is no patch for human error and foolishness** – We must build capabilities with this mindset whether the threat stems from intentional, accidental or part of a larger conspiracy.
   b. Cyber Incident Management (CIM) demands continuous improvement based on the monitoring important (crown jewels) data.
   c. Remote worker systems are important and plays a critical role, however they are only 1 component of the wider eco-system.
   d. **Cyber Criminals look at the effort vs. gain and look for the cheaper way to exploit**.
   e. Threat Intelligence and collaboration is key – We must continue to share to increase visibility and develop capabilities.
   f. Remote worker environment will vary in different locations.
   g. Remote worker environment is a ‘tug and war’ which requires options to mitigate threats without hampering productivity

10. Institutions should continue raising awareness among their customers on information security outside the office space.
    a. They need to **build institutional capacity** to deal with cybercrime and keep abreast of the innovations and technology.
    b. **Enhance existing consumer awareness** and financial enlightenment initiatives.
    c. **Seek ways to protect the endpoints i.e., customers** regardless of their status or level of enlightenment.



# CYBER SAFETY CHECKLIST

- Back up online and offline files regularly and securely
- Strengthen your home network
- Use strong passwords
- Keep your software updated
- Manage social media profiles
- Check privacy and security settings
- Avoid opening and delete suspicious emails or attachments

INTERPOL

BE VIGILANT . BE SKEPTICAL . **BE SAFE**