FREQUENTLY ASKED QUESTIONS FROM NEW MEDIA AND INFORMATION SECURITY DEPARTMENT, NCC

1. **What can people do to increase the chance of recovering a mobile phone?**

   - Record your phone's IMEI number and keep it in a safe place in case your phone is lost or stolen. It will be easier to identify and locate your phone if you can provide the IMEI number to police and your service provider.
   - Use the security features on your phone. The PIN number and code locks the mobile phone making it more likely to be recovered.
   - Record your handset serial number and keep it in a safe place.
   - Engraving your initials on your phone (If possible).
   - If your phone is stolen notify the police and your service provider immediately.

2. **What is an IMEI number?**
   The International Mobile Equipment Identity (IMEI) number is an international identity number used to uniquely identify a mobile phone. The 15-digit IMEI number is an electronic fingerprint transmitted every time a phone is used, which reveals the identity of the mobile handset. They are independent of phone numbers and are usually stamped beneath the battery on the back of the handset.

3. **How can I find out my IMEI number?**
   IMEI numbers are independent of the phone number and are usually written underneath the battery or on the back of the handset. Mobile phone users can also check their 15 digit IMEI number by **dialling *#06#** on their mobile handset. Mobile phone owners should make a note of their IMEI number and keep the details in a safe place.

4. **When can I expect updates for my phone?**
   When a software update is available for you to download, a notice will appear on your phone, telling you of the software download availability.

5. **What do you mean by Mobile Device Security?**
   "Mobile Device Security" refers to enabling a set of basic security settings to protect data residing on a smartphone or tablet in the event that the device is lost or stolen.

6. **How can I modify my phones security settings?**
   Other than setting a password, do not alter security settings for convenience. Tampering with your phone's factory settings, jailbreaking, or rooting your phone undermines the built-in security features offered by your wireless service and smartphone, while making it more susceptible to an attack

7. **Can I jailbreak my mobile device?**
   It is advisable not too. Devices that are "jailbroken" or "rooted" will not be allowed to access secure data from the device manufacturer and operating system provider since these devices become highly insecure.

8. **How do I prevent unauthorized access to my phone?**
   To prevent unauthorized access to your phone, set a password or Personal Identification Number (PIN) on your phone's home screen as a first line of defence in case your phone is lost or stolen. When possible, use a different password for each of your important log-ins (email, banking, personal sites, etc.). You should configure your phone to automatically lock after five minutes or less when your phone is idle, as well as use the SIM password capability available on most smartphones. If you own an iPhone, you can also use the Touch ID feature to securely and conveniently unlock your iPhone.

9. **Should I backup my data? If so how do I do that?**
   You should backup all of the data stored on your phone – such as your contacts, documents, and photos. These files can also be stored on your computer, on a removal storage card, or in the cloud. This will allow you to conveniently restore the information to your phone should it be lost, stolen, or otherwise erased.

10. **Are Free Wi-Fi networks secure?**
    When you access a Wi-Fi network that is open to the public, your phone can be an easy target of cybercriminals. You should limit your use of public hotspots and instead use protected Wi-Fi from a network operator you trust or mobile wireless connection to reduce your risk of exposure, especially when accessing personal or sensitive information. Always be aware when clicking web links and be particularly cautious if you are asked to enter account or log-in information.

11. **What is ADAPTI?**
    ADAPTI means Advanced Digital Appreciation Programme for Tertiary Institution (ADAPTI), sponsored by Nigerian Communications Commission (NCC) and coordinated by the Digital Bridge Institute (DBI). It is a 'train-the-trainer programme which aims at bridging the ICT gaps in Nigerian Tertiary institutions.

12. **How can my school benefit from the ADAPTI programme?**
    The Digital Bridge Institute (DBI) writes letters to all tertiary institutions in Nigeria requesting them to indicate interest for the training of their staff on the programme every January of the succeeding year. Furthermore, same information is disseminated through regulatory bodies of the various institutions. Your school should therefore lookout for the advert and indicate interest.

13. **How can I protect my phone from cybercrime?**
    Avoid downloading unnecessary attachments from websites, e-mail etc. Do not click on suspicious links sent through social media on your phone. Install and update anti-virus from known vendors.

14. **If I am scammed through my mobile line, how will I report the fraud?**
    Report the fraud via https://www.cert.gov.ng/report-an-incident by filling the complaint form, send email to incident@cert.gov.ng, or a message to +234 (0) 7044642378. Also you

can report to the nearest police station, call your mobile provider for assistance or report to NCC via its Toll Free Number: 622.

15. **I have received this scam messages severally that my BVN needs to be re-activated; I should call a particular number what do I do?**
    Never respond to messages about BVN. Instead walk in to your bank and confirm if uncertain, because your bank would not ask you to activate BVN

Compiled by:
New Media and Information Security Department
Nigerian Communications Commission (NCC)