



## VICBHE Module 10 Newsletter **No. 4, May 5, 2025**

### Care for some fresh fish? Poisonous though

---

When growing up in Sapele, Delta State, we used to adventure at the bank of River Ethiope with our fishing lines attached with hooks baited with earthworms. A downward pull on the line signalled that some fish had swallowed the worm bait and got hooked. We pulled the fish out as “material” for pepper soup. This practice in the physical world has migrated to the virtual. While it is “fishing” in the physical, it is “phishing” in the virtual world. The term “phishing” comes from the idea of “fishing” for sensitive information, where attackers use deceptive tactics to lure victims into revealing personal data. The “ph” spelling is linked to early hackers known as “phreaks”, who explored and manipulated telecommunication systems.

The first recorded use of “phishing” appeared in 1995 in a hacking toolkit called AOHell, which was designed to exploit America Online (AOL) users. Hackers would send fraudulent messages pretending to be AOL employees, tricking users into providing their login credentials. Since then, phishing has evolved into a widespread cyber threat, targeting individuals and businesses through emails, fake websites, and social engineering tactics. In our warmup activity, about 80% of participants in Module 10 reported experience of being “phished”.

There are several types of phishing attacks. Email phishing is the most common. It involves deceptive emails that often look like they are from legitimate sources such as banks, friends, your institution or social networks, or well-known companies. Spear phishing is a more targeted form of phishing where attackers tailor their messages to specific individuals or organisations to increase the likelihood of success. Then you have whaling. This is a subtype of spear phishing aimed at high-profile individuals such as executives or public figures (you know the whale is a big aquatic mammal!). Also, in the list is vishing and smishing. These are phishing attempts that occur via phone calls or text messages, respectively. Clone phishing is another type. This creates near-perfect duplicates of real emails to deceive recipients.

How does phishing work? Phishing attacks generally work by leveraging fear, urgency, or curiosity to make victims act quickly without considering the consequences. A typical phishing scam might involve an email claiming that your bank account has been compromised and asking you to verify your details through a link. When you click the link, you are redirected to a fake website that mirrors the real one, and your login credentials are captured by the attacker.

There are several ways of recognising a phishing attempt. I will name four. First and as I stated earlier, is the deployment of urgency and fear tactics- threats like “your account will be suspended!”. Second is poor grammar and spelling – more likely than not, you will spot poor grammar, punctuation and errors in spelling. Legitimate companies do not send sloppy emails. Third is request for sensitive information – banks and official organisations never ask for passwords via email. Fourth is suspicious sender – emails from strange addresses or misspelled domains. Use slight misspellings in URLs (e.g., “paypa1.com” instead of “paypal.com”). Fifth is inclusion of malicious links or attachments.

Phishing scams are evolving, but awareness is your best defence. By staying vigilant and questioning unexpected requests, you can keep your personal and financial information safe. **Don't take the bait—outsmart the phishers!**

## Brilliant Performance in Weekly Test No. 1

---

Congratulations on the brilliant performance on the Weekly Test No. 1. We had 500/500 galore. Figure1 shows the distribution of the scores.

### Overall number of students achieving grade ranges

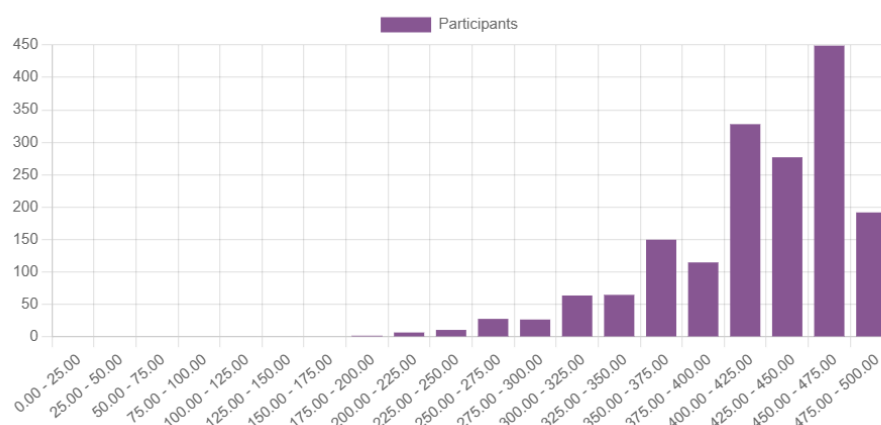


Figure 1: Distribution of scores for Weekly Test 2

It is our expectation that you will continue to present such negatively-skewed graphs in the coming weeks and in the end-of-module comprehensive examination.

## Practical 1 scores- Two-Day Map of Global Cyber Threat

---

Congratulations on your exceptionally brilliant performance in Practical 1. You are too much o! Kindly note that the scores are final. I repeat, FINAL. For me, the important thing is that you learned so much in the practical exercise as shown by your reports. For professional complainants on scores, we will start issuing cards- one yellow and then red. With a red, we will gently ease you out. It is not a do-or-die affair.

## Video Lesson No. 2- Introduction to the Internet and how it works by Peter A. Okebukola

---

This week's video lesson 2 is 37 minutes long, shorter than that of last week. It gives you insight into how the internet works. It provides definitions of a number of concepts and terminologies associated with the internet. Watch it [here](#).

## Practical No. 2- Measuring the strength of your internet service

---

Practical 2 is based on the contents of video lesson 2 on the internet and how it works. You are to measure the strength of the internet serving your computer. You will get the video guide

towards the end of video Lesson 2 (click [here](#)). You can submit on the VICBHE app whenever you finish, noting that the deadline for submission is Saturday at 6:00 p.m. This means you could start submitting from Wednesday if you selected Tuesday and Wednesday as data collection days. I provided the following steps for Practical 2 in Lesson 2 video:

1. Select any two days this week
2. Connect to the internet
3. Measurement on the first day selected should **be before 7:00 a.m.** On the second day, it should be **around 12 noon**
4. Go to **speedtest.net**
5. Click “Go” to start measuring the speed of your internet service
6. Wait until speedtest has completed its measurement.
7. Take the screenshot, paste in your report and record the details.
8. Discuss your results.

## Report Template

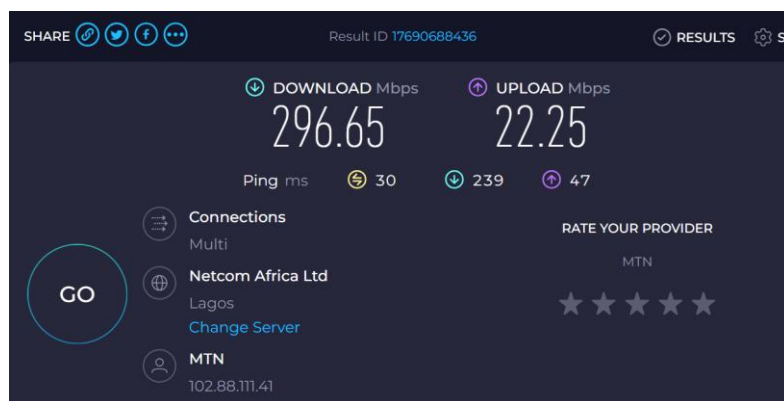
### Module 10-Practical 2- Strength of Internet Service

**Name:** Surname first

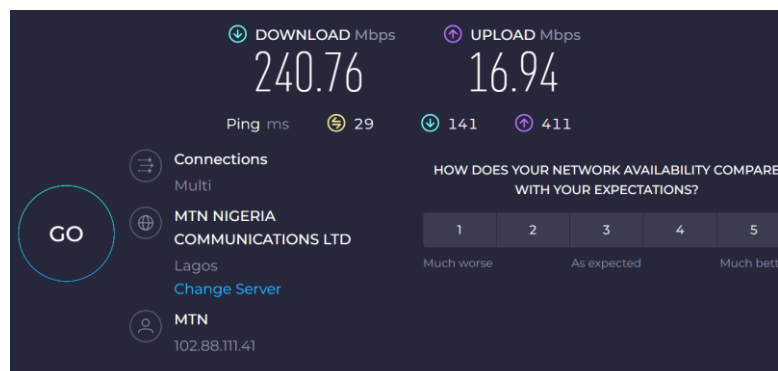
**Institution**

**Registration No:**

**Tuesday, May 6, 2025- before 7:00 a.m.**



**Wednesday, May 7, 2025 at 12 noon**



### Summary table

	Reading No. 1	Reading No. 2
Date	May 5, 2025	
Time	7:06 a.m.	
Result ID	17690688436	
Download speed	496.65 Mbps	
Upload speed	22.25 Mbps	
Idle latency	30	
Download latency	239	
Upload latency	47	
IP Address	102:88:111:41	

### Discussion of results and Conclusion

## Module 10 Prizes

---

Participants are invited to note the following prizes and work hard towards “carrying some home”.

S/No.	Winner	Prize
1.	Best Overall	Malam Adamu Adamu
2.	Best Head of Institution (VC, Rector, Provost)	Professor Abubakar Adamu Rasheed
3.	First Position in Intergroup Debate	Professor Emeritus Nimi Briggs
4.	Best Female Participant <ul style="list-style-type: none"><li>Universities</li><li>Polytechnics</li><li>Colleges of Education</li></ul>	Professor Ruqayyatu Ahmed Rufa'i
5.	Best in Project	Peter A. Okebukola
6.	Best in Practicals in Cyber Security <ul style="list-style-type: none"><li>Universities</li><li>Polytechnics</li><li>Colleges of Education</li></ul>	Buba Marwa
7.	Best in Discussion Forum <ul style="list-style-type: none"><li>Universities</li><li>Polytechnics</li><li>Colleges of Education</li></ul>	Professor Olufemi Peters
8.	Best Participant in Friday Tests <ul style="list-style-type: none"><li>Universities</li><li>Polytechnics</li><li>Colleges of Education</li></ul>	Professor Eytape Ogunbodede
9.	Best Male Participant <ul style="list-style-type: none"><li>Universities</li><li>Polytechnics</li><li>Colleges of Education</li></ul>	Arc Sonny Echono
10.	Best Participant from Other African Countries	Dr. Cynthia Jackson-Hammond
11.	Most Consistent Participant	Professor Olusola Oyewole

## Locating other participants from your institution

We have sorted the registered participants' list by institution. This will allow you share thoughts with your colleagues as the course progresses. Click [here](#) for the list.

## Module 10 Virtual Library

Two weeks ago, our Institute Librarian Dr. Adetola Akanbiemu, produced the virtual library resources for Module 10. You will find this on the VICBHE website. It is a one-stop electronic resource for all you need for the training. Click [here](#) for your personal download.

## This Week at VICBHE

Sunday May 04	FREE	
Monday May 05	<p><b>Live Lectures No. 2:</b> Time: 2:00 to 3:00 p.m.</p> <p><b>Zoom link:</b> Click <a href="#">here</a></p> <p><b>Host: Professor Joy Eyisi-</b> VICBHE Management</p> <p><b>Chairman:</b> Professor Stephen Abah, VC, Federal University of Health Sciences, Otuokpo</p> <p><b>Co-Chairman:</b> Professor Felix Akinwumi, Adekunle Ajasin University, Akungba Akoko</p> <ul style="list-style-type: none"><li>• <b>Topic 1:</b> Keeping individuals cyber secure. (20 minutes)</li><li>• <b>Speaker:</b> Professor Boniface Kayode Alese, Federal University of Technology, Akure</li><li>-----</li><li>• <b>Topic 2:</b> Building a Culture of Cyber Security (20 minutes)</li><li>• <b>Speaker:</b> Dr. Felicia Nkrumah, Association of African Universities, Accra</li></ul> <p><b>Plenary Discussion: 15 minutes</b></p>	<p><b>Unit 2: How the Internet Works</b> by Peter A. Okebukola</p> <p>Click <a href="#">here</a> for the video</p>
Tuesday May 06	FREE	
Wednesday May 07	<p><b>Discussion Forum No. 2</b></p> <p>Opens 8:00 a.m. Closes at 10:00 a.m. <b>Submit to VICBHE app.</b></p> <p><b>Topic: <i>Cultivating a culture of cyber security is the panacea for sustainable safety online.</i></b></p> <p><b>Discuss any four points.</b></p> <p>(<b>Maximum 250 words</b>). Any word in excess will be penalised by deduction of 20 marks. <b>Marking scheme:</b> Listing of the four points and expatiation of the four. Ensure you list the points first and then expatiate. Each correct point listed 5 marks 5 X 4 = 20; Each point expatiated 20 marks 20 X 4=80 <b>Total=100.</b></p>	

Thursday May 08	<b>Live Debate No.1: Time:</b> 2:00 – 3:00 p.m. <b>Zoom link:</b> Please click <a href="#">here</a> <b>Host:</b> Professor Ibiyinka Fuwape- VICBHE Management <b>Coordinator:</b> Professor Olubiyi Adewale ( <b>To select debaters</b> ) <b>Moderator:</b> Professor Maryam Aminu, Dean, Ahmadu Bello University, Zaria <b>Topic:</b> Individuals rather than their institutions should bear responsibility for their cyber security. <b>For:</b> Universities <b>Against:</b> Polytechnics	
Friday May 09	Weekly test No. 2 (30 minutes) <b>5:00-5:40 p.m.</b>	
Saturday May 10	FREE	Deadline for the submission of practical 2 (6:00 p.m.) <b>Submit to VICBHE app</b>

## Test for this Week (Friday, May 9, 2025)

---

**Time:** 5:00 to 5:40 p.m.

**Number of items**=50 multiple-choice

**Time allowed:** 35 minutes

**Content covered:** Video Lesson 2, Live Lectures 2; and Debate No. 1

**Link to the examination room:** Click [here](#)

## Cyber security tips for the week: Protect Yourself from Phishing

---

- Verify the source: Always double-check the sender's email address or phone number and be cautious about unexpected messages from unknown sources.
- Do not click links directly: Instead of clicking on links in emails, type the website address into your browser manually.
- Never share sensitive information through email, SMS, or phone calls.
- Verify requests: Contact your bank or the organization directly using official numbers or websites.
- Use strong, unique passwords and change them regularly.
- Enable two-factor authentication (2FA) where possible.
- Delete the message immediately.

## Helpdesk/Technical Officers

---

If you need help, send an email/ SMS to your Group helpdesk/technical support officer.

**PLEA:** Emails should NOT be sent to me directly but to the HelpDesk/Technical Officers who are trained to process requests/feedback and escalate when necessary.

Serial number on the admission list	Name of Technical Support Staff	Telephone number	Email address	NB: Please copy all emails to
1-900	Buhari Segun	08059570507	sbuhari@noun.edu.ng	pokebukola@yahoo.com <a href="mailto:waalsadesina@gmail.com">waalsadesina@gmail.com</a> lordaikins@gmail.com
901-1800	Gazalli Muhammad Nuraddeen	07035375751	mgazali@noun.edu.ng	
1801-2700	Emmanuel Jatau	07034667166	ejatau@noun.edu.ng	
2701-3600	Abdulkadir Hauwa	08038889935	habdulkadir@noun.edu.ng	
3600-4653	Gbenga Atteh	08030441024	gatteh@noun.edu.ng	

Have a great week and God bless.

**Peter A. Okebukola**, OFR  
Director/Facilitator-General