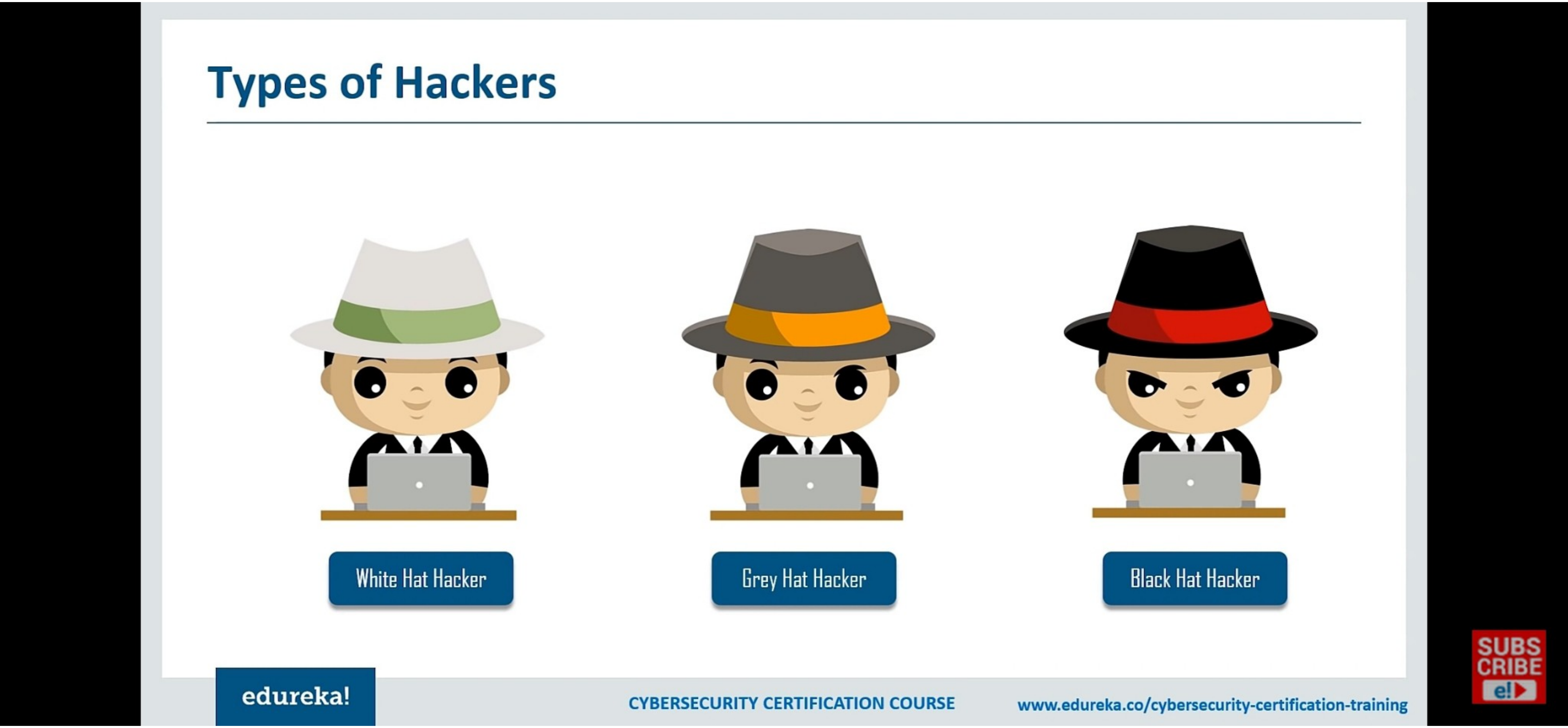
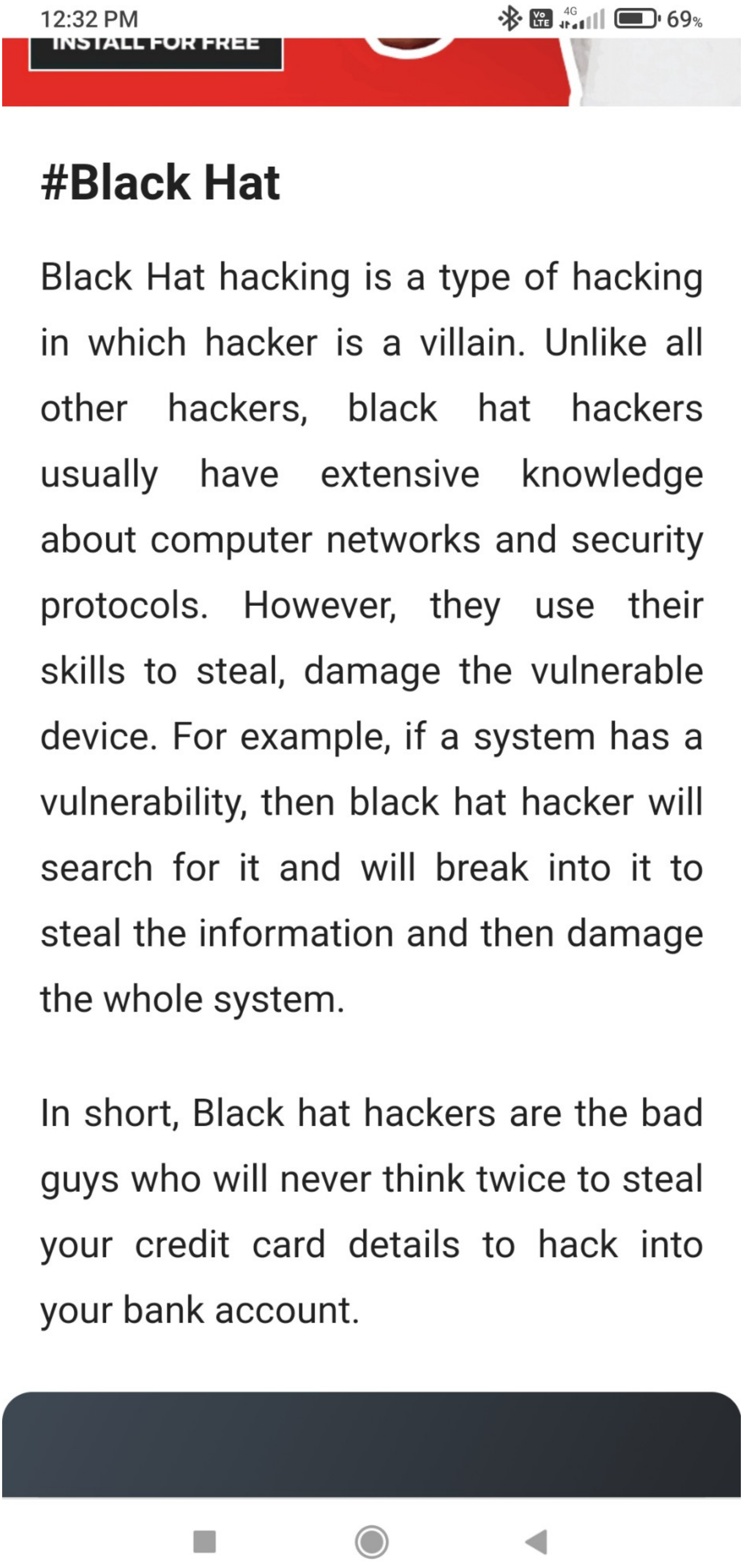


Types of Hackers

White Hat Hacker

Grey Hat Hacker

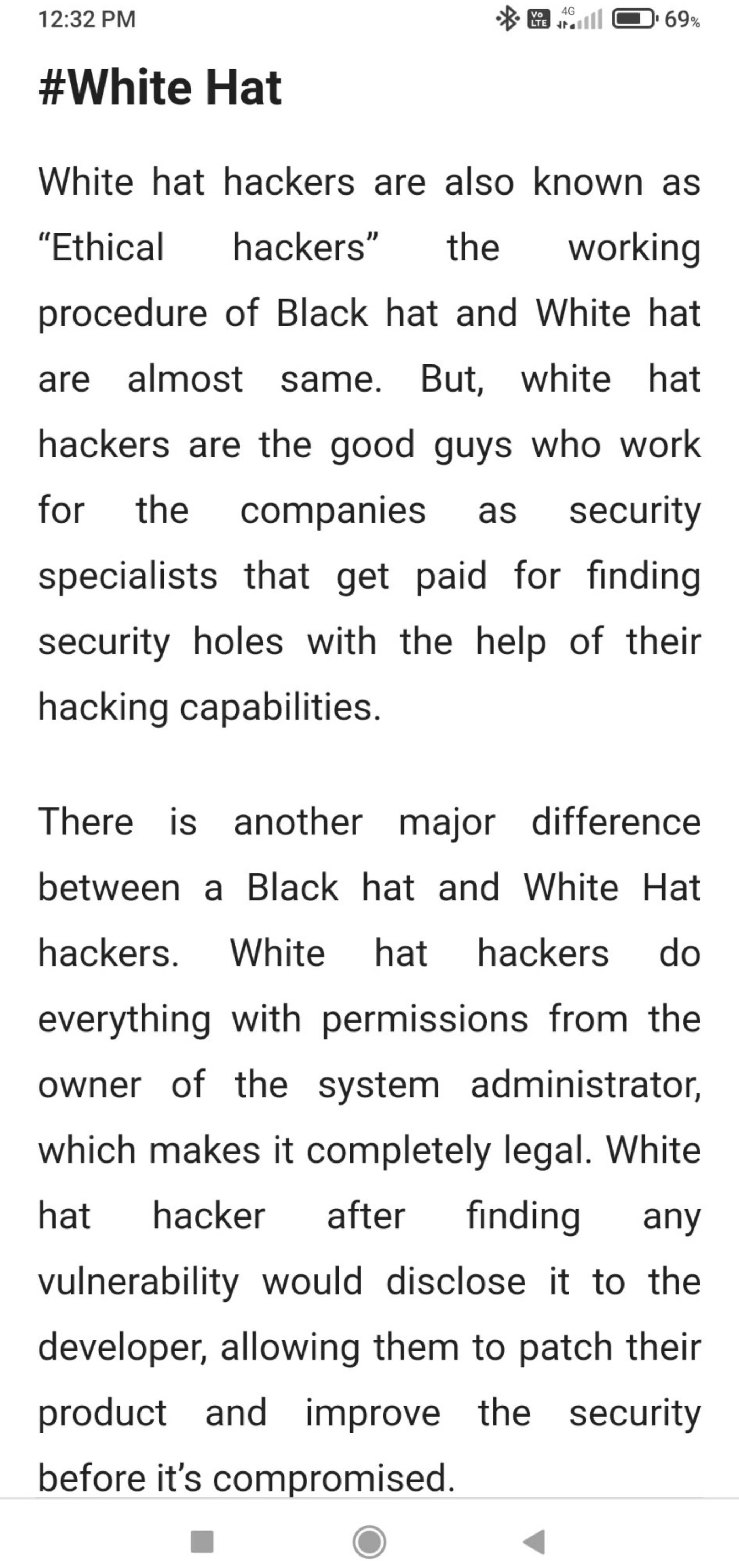
Black Hat Hacker



#Black Hat

Black Hat hacking is a type of hacking in which hacker is a villain. Unlike all other hackers, black hat hackers usually have extensive knowledge about computer networks and security protocols. However, they use their skills to steal, damage the vulnerable device. For example, if a system has a vulnerability, then black hat hacker will search for it and will break into it to steal the information and then damage the whole system.

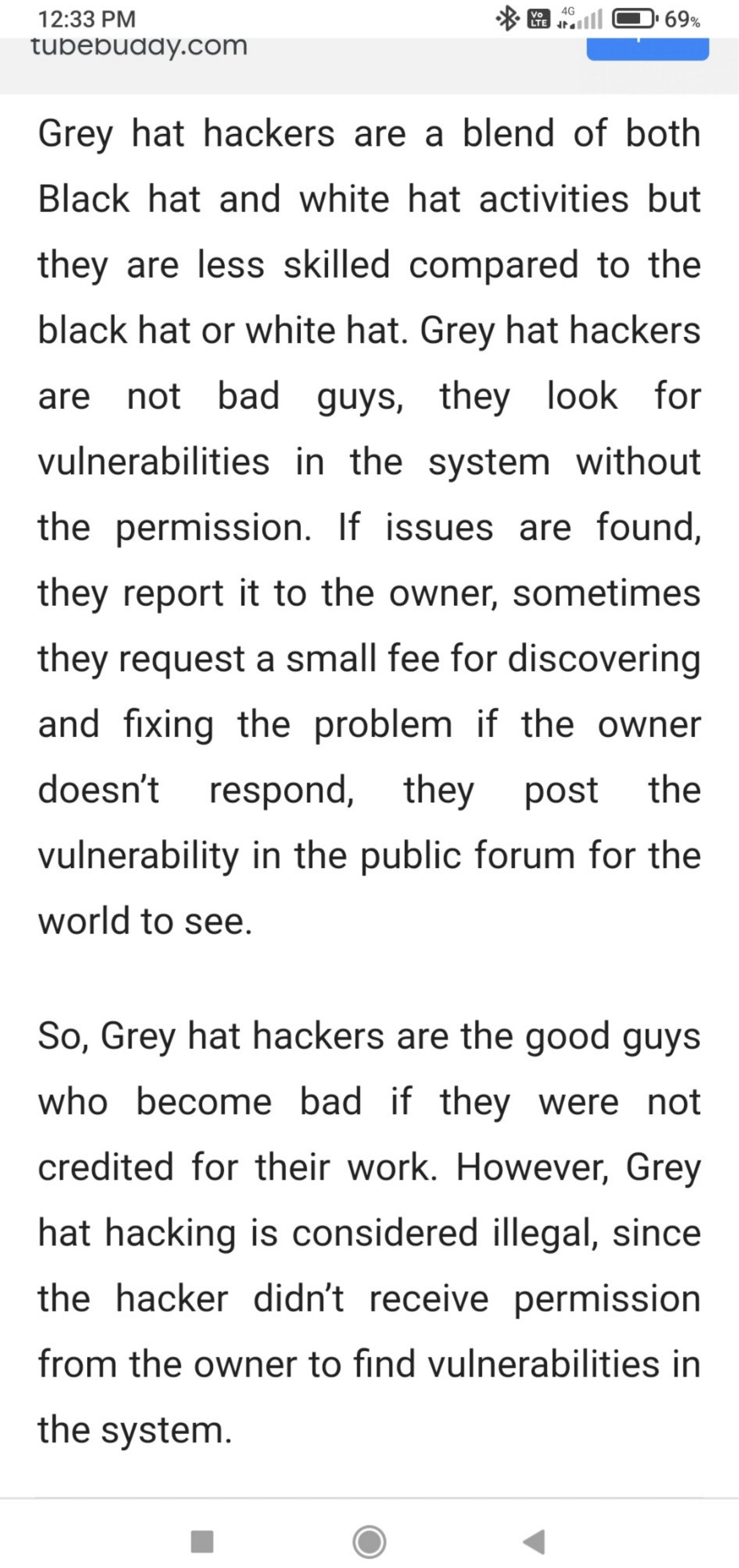
In short, Black hat hackers are the bad guys who will never think twice to steal your credit card details to hack into your bank account.



#White Hat

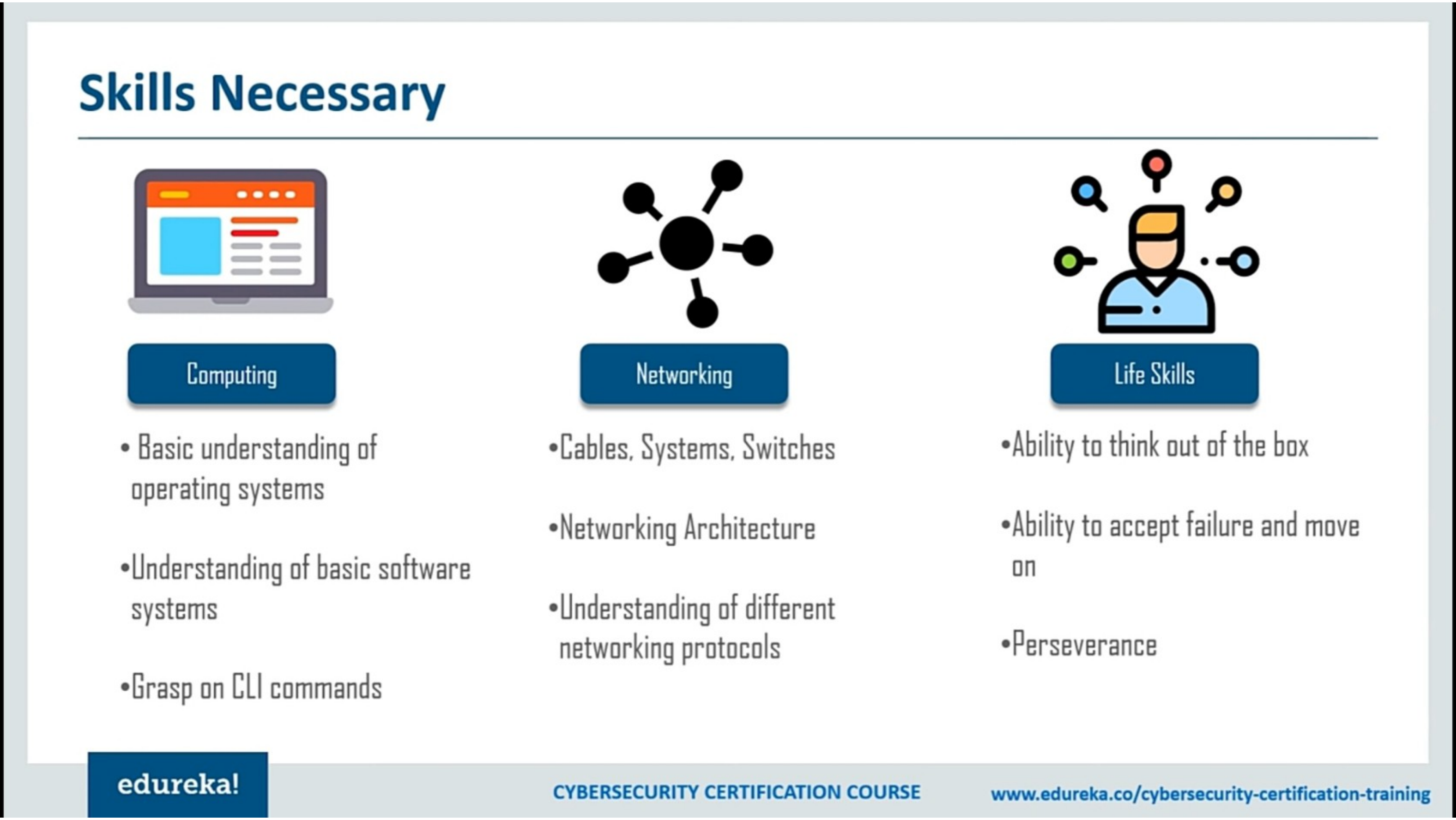
White hat hackers are also known as “Ethical hackers” the working procedure of Black hat and White hat are almost same. But, white hat hackers are the good guys who work for the companies as security specialists that get paid for finding security holes with the help of their hacking capabilities.

There is another major difference between a Black hat and White Hat hackers. White hat hackers do everything with permissions from the owner of the system administrator, which makes it completely legal. White hat hacker after finding any vulnerability would disclose it to the developer, allowing them to patch their product and improve the security before it’s compromised.



Grey hat hackers are a blend of both Black hat and white hat activities but they are less skilled compared to the black hat or white hat. Grey hat hackers are not bad guys, they look for vulnerabilities in the system without the permission. If issues are found, they report it to the owner, sometimes they request a small fee for discovering and fixing the problem if the owner doesn't respond, they post the vulnerability in the public forum for the world to see.

So, Grey hat hackers are the good guys who become bad if they were not credited for their work. However, Grey hat hacking is considered illegal, since the hacker didn't receive permission from the owner to find vulnerabilities in the system.



Skills Necessary

Computing

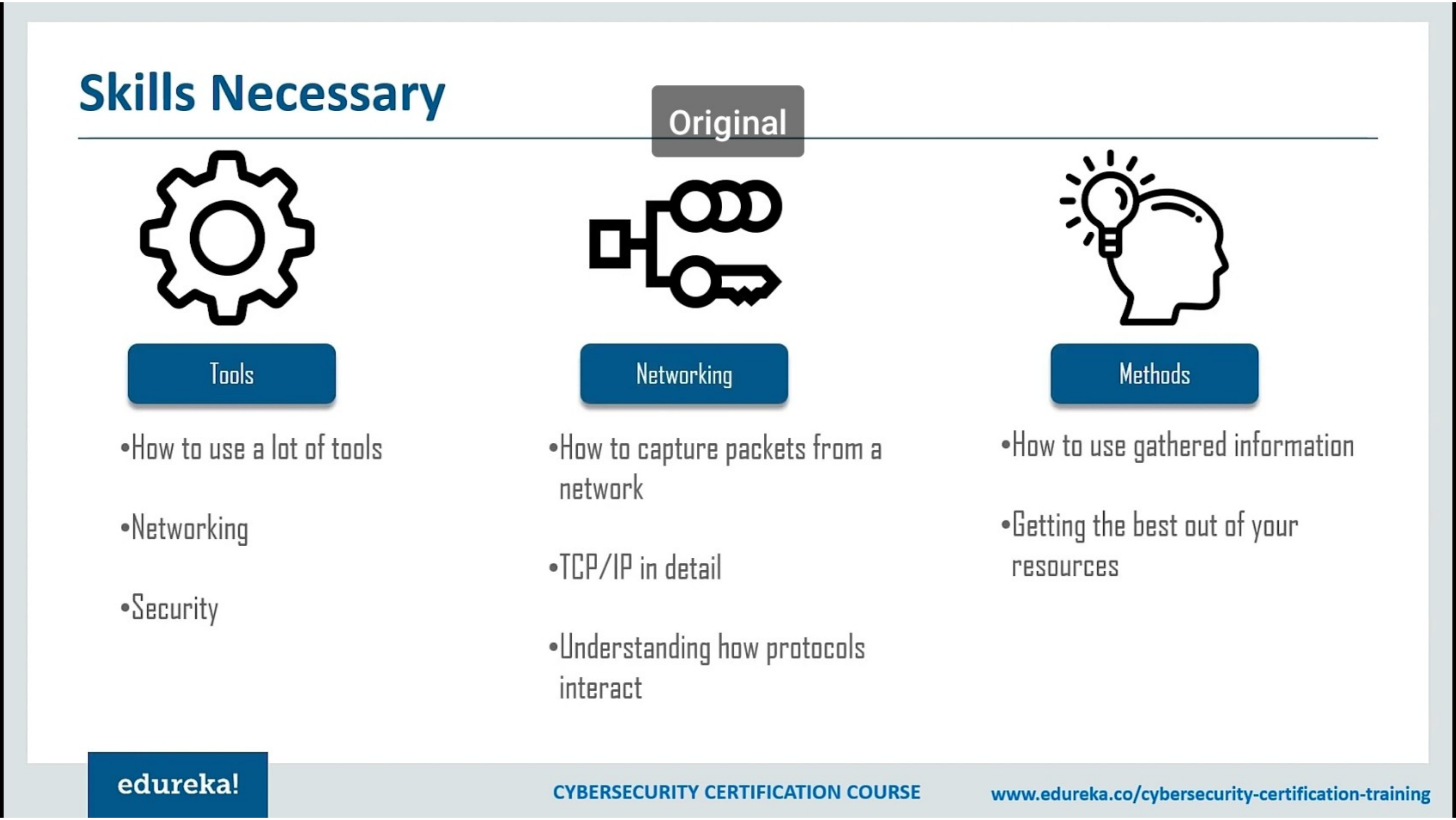
- Basic understanding of operating systems
- Understanding of basic software systems
- Grasp on CLI commands

Networking

- Cables, Systems, Switches
- Networking Architecture
- Understanding of different networking protocols

Life Skills

- Ability to think out of the box
- Ability to accept failure and move on
- Perseverance



Skills Necessary

Tools

- How to use a lot of tools
- Networking
- Security

Networking

- How to capture packets from a network
- TCP/IP in detail
- Understanding how protocols interact

Methods

- How to use gathered information
- Getting the best out of your resources