A REVIEW OF HUMAN ERROR IN USING MOBILE DEVICE THAT LEAD TO SECURITY THREAT

INTRODUCTION

Human errors can be defined as the behavior or the actions taken by the user without realizing that it would make their devices vulnerable to the information security threat.

The cyberattack patterns have also changed from attacking the systems or the devices, to attacking mobile devices.

HUMAN ERRORS USING MOBILE DEVICES

As mobile devices become the important tools nowadays, the attackers also focus more on attacking mobile devices. It is because it is easier to attack the mobile devices and they can get lots of information from those devices.

The vulnerabilities are due to the user actions which include not updating their device operating system, not installing the antivirus to protect their mobile device and downloading the malicious app.

THE EFFECTS OF HUMAN ERRORS TO SECURITY THREAT

Connecting with the public wireless connection (WiFi)

Not updating software applications regularly

Clicking on malicious link

Not installing and updating the antivirus

Not installing the Remote Wipe Application

Bring-your-own-device (BYOD)

Download applications without scanning

CONCLUSION

This paper has explained the previous research on human errors in using mobile devices that lead to security threat.