DIGITAL SAFETY

**Digital safety is an aspect of virtual security about user and the online safety and privacy.
This involves being aware of the dangers associated with what you do online, as well as preventing being exposed to undesired information, materials, or risks on the Internet that could harm your devices. (Sadiku et al., 2021)**

MODULE NAME:DIGITAL SKILLS

MODULE CODE:LCLM4002

NAME STUDENT:
CHIARA ALAIMO

ID:2414747

GROUP:6

PROTECT YOUR PASSWORD AND PERSONAL DATA

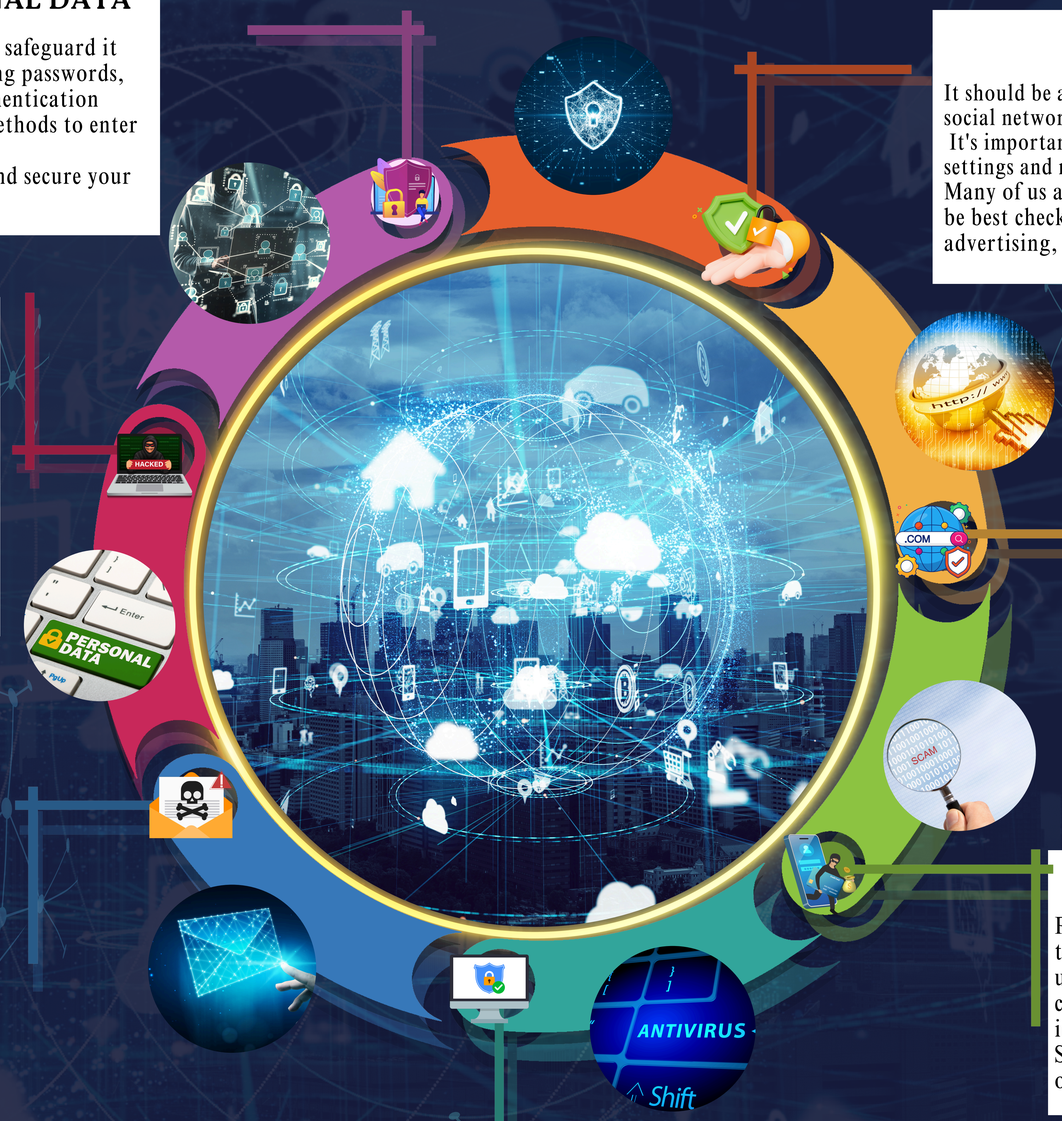
Personal information is incredibly valuable, and it's essential to safeguard it against potential online threats. To protect yourself from sharing passwords, locations, or any other sensitive details online. Multifactor authentication (MFA)can also help user to provide two or more verification methods to enter a website, rather than just request a login and password.
MFA request additional information to confirm your identity and secure your data.

CHOISE A STRONG PASSWORDS

Password are one of the most importart form of protection again hacker.People usually choose something very obvious when choosing a passcode,like their birthday, a set of numbers,or a part of their phone number. The problem is that this is not the best option. Instead, use genuine random numbers,to make sure your passcode is as long as possible—between 12-15 characters. This number may be a little more difficult to remember, but it will also be more difficult for hackers to figure out, which is ultimately beneficial for the security of your device. Password vaults like NordPass and 1Password can safely remember your passwords.

CHECK EMAIL BEFORE OPENING THEM

Always verify the sender before opening emails, especially if they contain attachments or links. Phishing scams often are emails that trick you into revealing personal information. Malware can infect your device or share your personal information online with a careless click. Therefore, it's crucial to look into them mindfully and stay away from particular types of online content, like spam emails and links from unverified sources, virtual tests, clickbait, "free" offers, and unwelcome ads.
Beware from opening any attachments or clicking on any links in emails you're receiving.
You are not supposed to open an unsafe email. Go immediately to the source if you have any doubts about the authenticity of an email. For example, if you receive a strange email from your "bank," call them and verify whether the communication is legitimate.



PRIVACY SETTINGS

It should be always preferably to enable privacy setting especially privacy on social networking platforms like Facebook, Instagram, LinkedIn, Twitter.
It's important to spend a few minutes and going through all of your privacy settings and make sure that they are adjusted to the level that suits you.
Many of us accept privacy policies without reading the terms, instead it will be best checking them and given the right amount of data used for advertising, marketing, and hacking.(Kasperly,2020)

TRUSTED WEBSITE,URL AND DOMAIN

It's always important to verify the website while brosering on internet. Any website you visit, especially e-commerce site should be reliable. An SSL/security certificate is an essential element to look out for. This means you must search for URLs that begin with "HTTPS" rather than "HTTP", the 'S' it means Secure. Another trust indications it's for example the text that it could be without spelling and grammar errors,and the images not clear . Also is important to verify the domain name to see if anything pops up. This includes misspellings, missing letters, extra letters, and other rigid name or web address changes.

PHISHING AND SCAM

Phishing and scam for example happens when criminals use fake emails, text or messages,to fraud people. The intention usually is to convince user to visit a website that will download a virus or malware in the computer or steal your bank account detail and other personal information. It's important to report them to the National Cyber Security Centre(NCSC)a UK government organisation that investigate on this crime.(National Cyber Security Centre, 2021)

PROTECT THE DEVICES WITH AN ANTIVIRUS

Using an effective antivirus is important. Internet security software like Norton and McAfee protects your devices and data by blocking typical risks like malware and viruses, as well as more sophisticated ones like XSS attacks, spy apps, and "cryptolockers."

REFERENCES

Kaspersky (2020). 'Top 15 Internet Safety Rules & What Not to Do Online', Kaspersky.com, Available at: https://www.kaspersky.com/resource-center/preemptive-safety/top-15-preemptive-safety-rules-and-what-not-to-do-online

Sadiku, M.N.O., Ashaolu, T.J., Ajayi-Majebi, A. and Musa, S.M. (2021). 'Digital Safety'. International Journal Of Scientific Advances, 2(5). Available at:doi:https://doi.org/10.51542/ijscia.v2i5.21.

National Cyber Security Centre (2021). Phishing: Spot and report scam emails, texts, websites and call. Available at: https://www.ncsc.gov.uk/collection/phishing-scams. (Accessed: 17 Nov 2024).