

BASIC DIGITAL SAFETY

1

WHAT IS DIGITAL SAFETY

Digital safety is Keeping your personal information safe when using technology is what it entails. It is critical to exercise caution and protect oneself from internet risks.

HOW TO BE SECURED ONLINE

To be secured online you'll have to have strong passwords and avoid sharing personal details . Also don't click on any suspicious email links or message links that you haven't heard of because you can contain a virus. you also have to know the risks online and gain a understanding what youre coming across .

2

3

The Four Cs

BE CAREFUL, WITH WHAT YOU POST ON THE INTERNET INCLUDING DETAILS, PICTURES AND VIDEOS.

2. CONTACTS; ONLY ADD PEOPLE YOU'RE FAMILIAR WITH AND TRUST ONLINE. AVOID ACCEPTING FRIEND REQUESTS OR MESSAGES FROM INDIVIDUALS.

3. CONDUCT; SHOW MANNERS ONLINE BY BEING POLITE, FRIENDLY AND ACCOUNTABLE IN YOUR COMMUNICATIONS.

4. CYBERSECURITY; ENSURE YOUR SAFETY, FROM RISKS BY UTILIZING PASSWORDS UPDATING SOFTWARE REGULARLY AND STAYING ALERT TO DUBIOUS LINKS OR EMAILS.

TYPES DIGITAL SAFETY

digital safety has a lot of different areas such as cybersecurity, online privacy .

4

5

CYPBER SECURITY

Keeping your devices and sensitive information secure, from hackers and cybercriminals is an aspect of cybersecurity. To ensure your safety it is recommended to follow these suggestions; utilize passwords activate two factor authentication and regularly update your software and devices.also always have a password that you will know of and remember.

CYBER SECURITY THREATS

1. Phishing Attacks (Personalized messages with links to damaging software)
2. Scareware (Pop up messages and notifications can lead users to visit websites that may contain viruses.)
- 3.cloud threats (Pop-up messages and notifications that make users visit websites containing viruses)
- 4.DDoS Attacks (attacks that flood websites with traffic to the point where the server can no longer handle them)
- 5.Third Party Apps (Apps that have the potential to threaten sending over your personal information to third parties)

6

7

DOUBLE CHECK TO REMAIN SAFE

Get a new anti-virus and a firewall software. Always update your computer or phone get a usb to make sure all your data is in one item so you can travel while knowing you have the information on you.

STRANGER DANGER

never accept Any friend requests of any random person you don't know. Never communicate with someone you don't know.Always have a burner account just in case. If needed block or report the person threatening you to hack your account.

8