Emirates American School

المدرسة الإماراتية الأمريكية

CYBER SECURITY

Emirates American School

Senior Section

What is Cyber Security ?

Cyber security in simple terms can be defined as the security of electronic information.

What is a Cyber Threat ?

Cyber threats are any damage or harm that can be caused on the data and the electronic information.

What is a Cyber Bullying ?

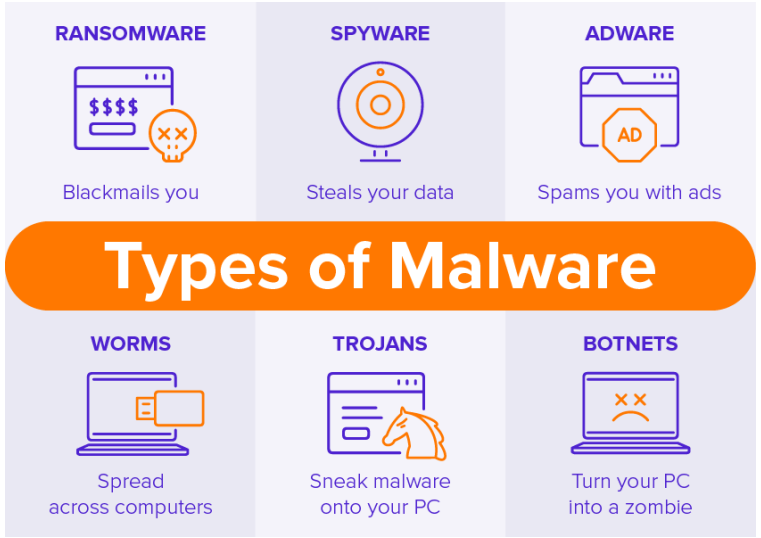
Cyberbullying is the act of bullying using digital means and platforms.

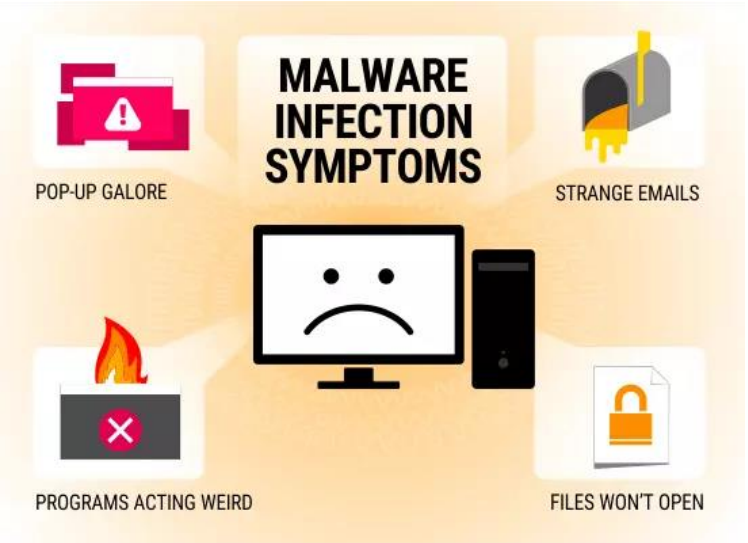
Online Safety

- **Online safety is in short is being safe in the online world while having the freedom to utilize the internet. As online users you have to be aware of the following.**

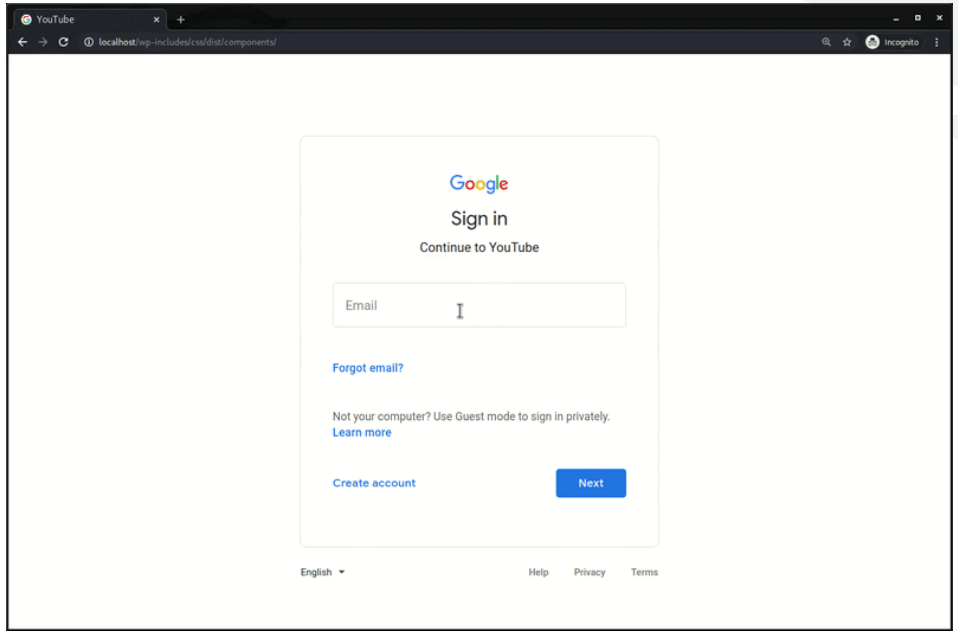
- **Hacking** - When someone gains access to others devices

- **Malware** – These are malicious software that is designed to steal your information or cause harm to your device. One example of a malware is the computer virus.



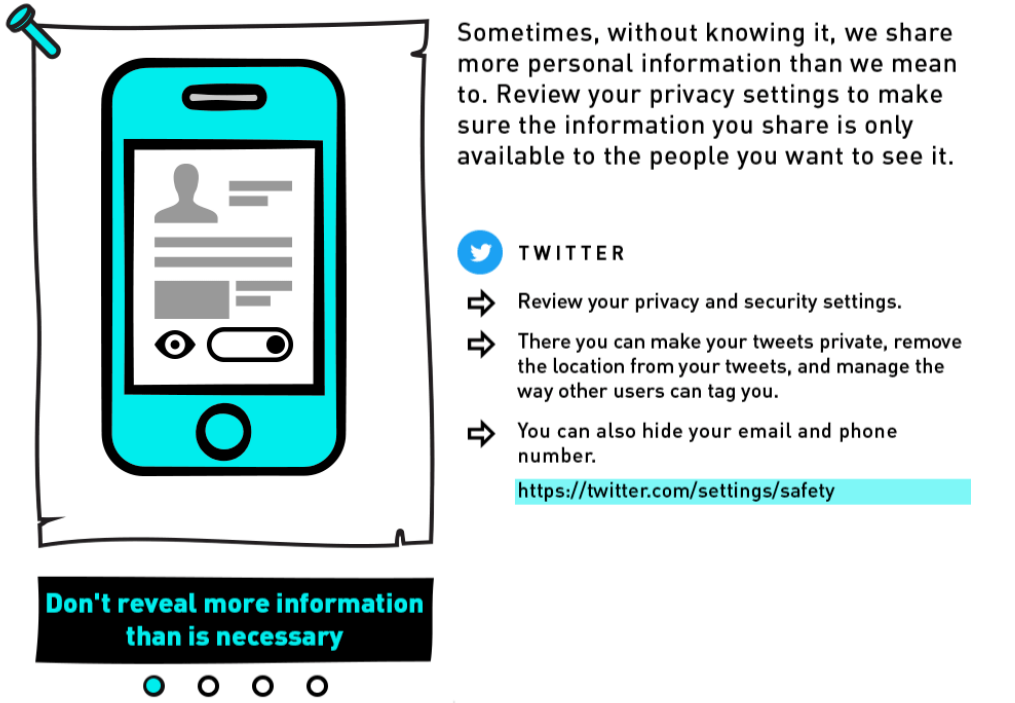


- **Cyberbullying** – As we all have been learning during the positive education sessions at school. Cyberbullying is a form of bullying that takes place over the internet. The bully uses online platforms as tools for bullying.



- **Phishing** – This is a kind of a cyber threat where the user is tricked and the sensitive information is stolen. For example you may receive emails with a link which looks just like your social media platform but its a phishing link.

- **Privacy** – The privacy of your personal information is very important in the digital world. Information on social media, gaming sites, etc. have to always dealt with care.



- **Online Identity Theft** - A person can take the identify of you after collecting/stealing your information. The attacker can then pose as you on social media platforms and contact people from your circle to obtain sensitive information from them.

Always protect your identity online and make sure you protect your privacy, your day to day internet searches, your social media accounts, etc can all contribute towards information collected about you.

• Data Security

- Data security is basically the process of keeping certain information private
- It involves the use of various methods to make sure that data is kept confidential and safe
- Data security ensures the integrity and the privacy of data, as well as preventing the loss or corruption of data.

Online Safety - Measures

As students of the "ICT Generation" consider the following measures that could be taken in order to have more protection on the internet.

- **Password Protection** - Create and use secure passwords.

#1	**Choose a phrase with at least 8 words.** *This is my favorite sandwich in the world*
#2	**Take the first letter of each word.** *timfsitw*
#3	**Switch one (or two) to an uppercase.** *TimFsitw*
#4	**Switch one to a number.** *T1mFsitw*
#5	**Switch one to a special character.** *T1mF$itw*
#6	**Add something unique from each site.** **(i.e. add a b for banking, an f for facebook, etc.)** *T1mF$itwB*

360 TOTAL SECURITY

Make it impersonal

Do not include easy-to-guess personal info such as name and birthday, e.g. Peter0413

Make it diverse

Mix uppercase letters, lowercase letters, numbers and symbols
E.g. Str0ngPa$$w@rd3

Make it long

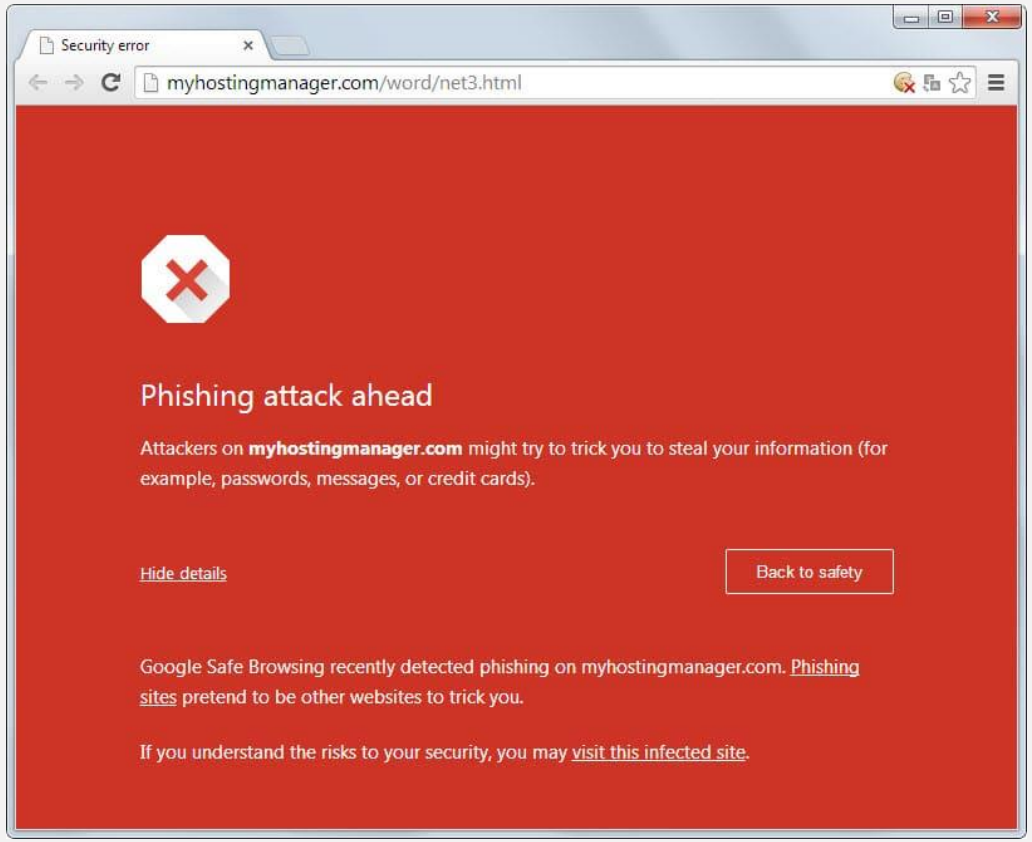
The minimum recommended password length is at least 8 characters

Make it different

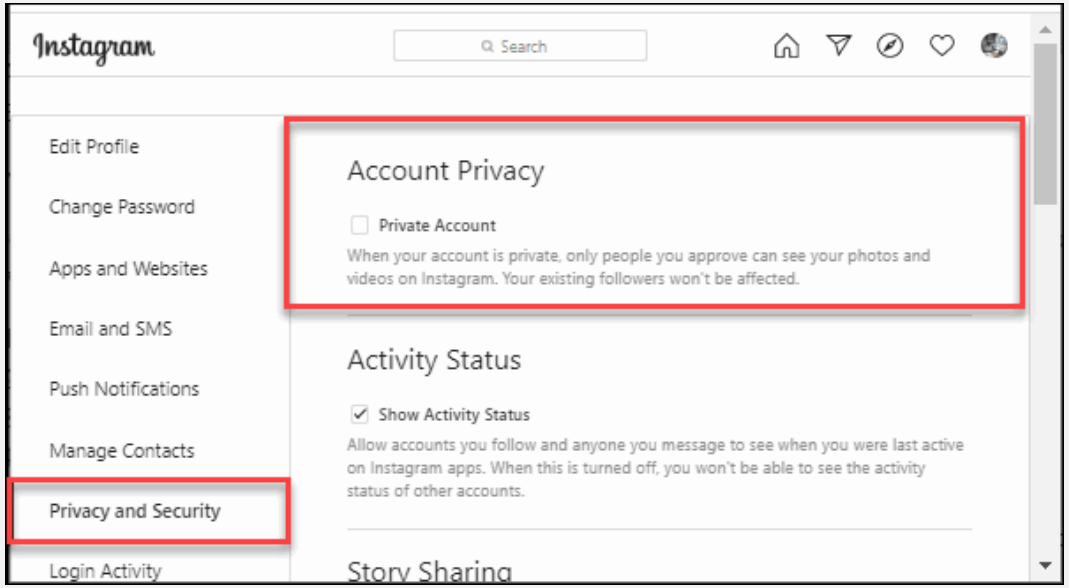
Use unique passwords specific to each sites
E.g. 123_Site.Name_456

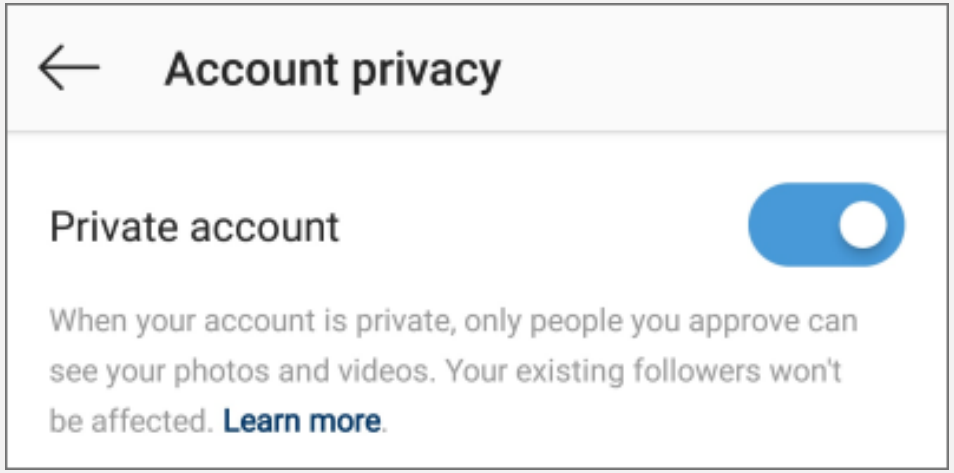
How to Create a Strong Password

- **Domain Check** - Check domains of links provided in emails and never login to a page that you access from an email message. An examples of domain names are www.facebook.com or "www.youtube.com".



- **Account Privacy** - Remove unnecessary identifying information from your online profiles (e.g., your address and phone number from your Facebook account) and other documents and make your profiles as private as possible;





Google

My Account

Welcome, Eric Griffith

Control, protect, and secure your account, all in one place

My Account gives you quick access to settings and tools that let you safeguard your data, protect your privacy, and decide how your information can make Google services work better for you.

Sign-in & security

Control your password and Google Account access.

- Signing in to Google
- Device activity & security events
- Apps with account access

Security Checkup

Protect your account in just a few minutes by reviewing your security settings and activity

GET STARTED

Find your phone

Whether you forgot where you left it or it was stolen, a few steps may help secure your phone or tablet

GET STARTED

Personal info & privacy

Manage your visibility settings and the data we use to personalize your experience.

- Your personal info
- Contacts
- Manage your Google activity
- Ads Settings
- Control your content

Privacy Checkup

Take this quick checkup to review important privacy settings and adjust them to your preference

GET STARTED

My Activity

Discover and control the data that's created when you use Google services

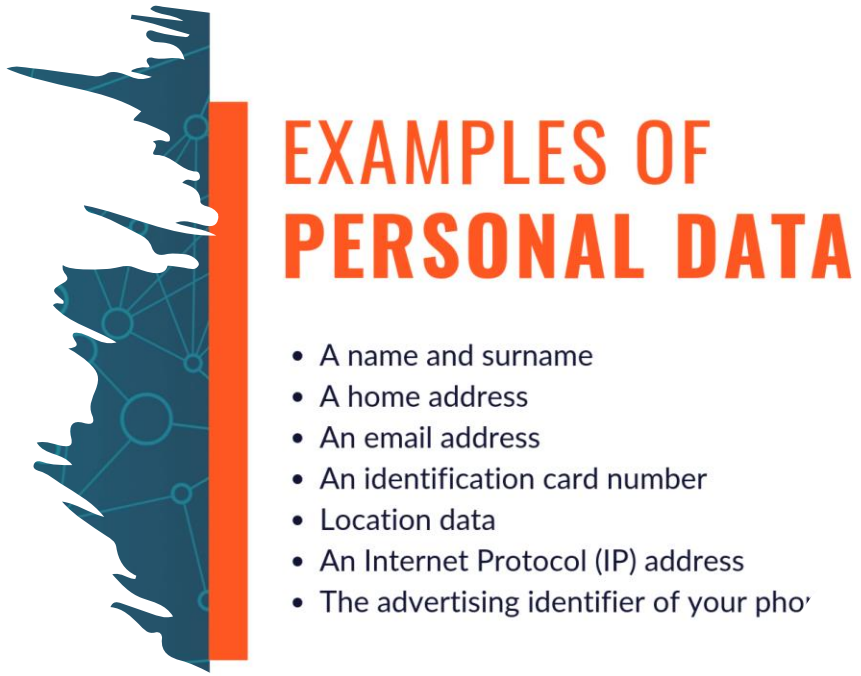
GO TO MY ACTIVITY

Account preferences

Adjust account settings, like payment methods, languages, & storage options.

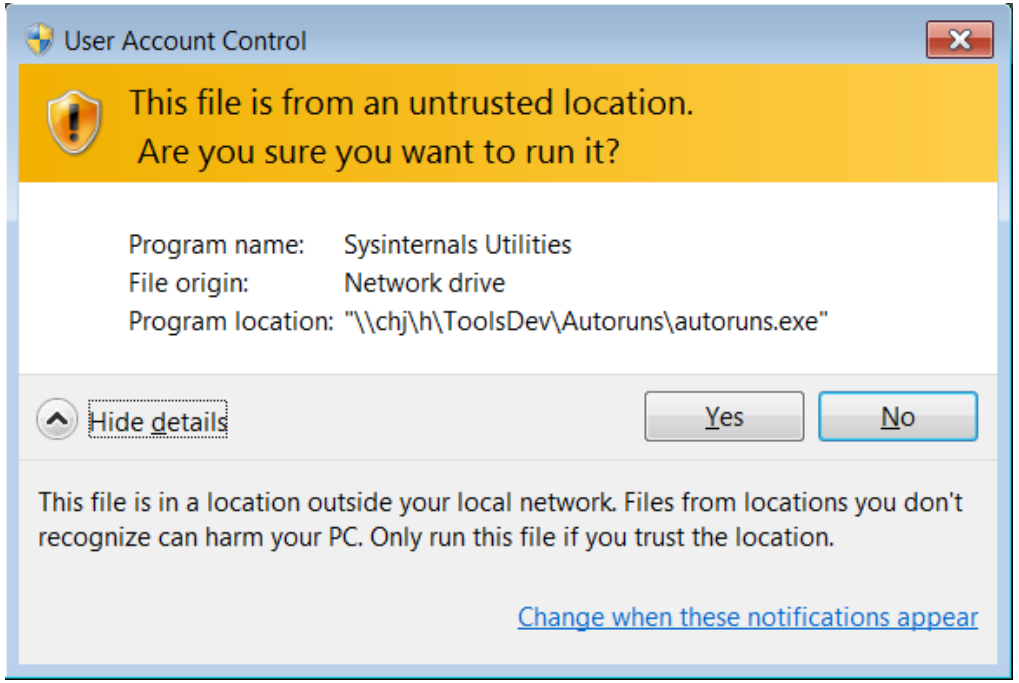
- Payments
- Language & Input Tools
- Accessibility
- Your Google Drive storage
- Delete your account or services

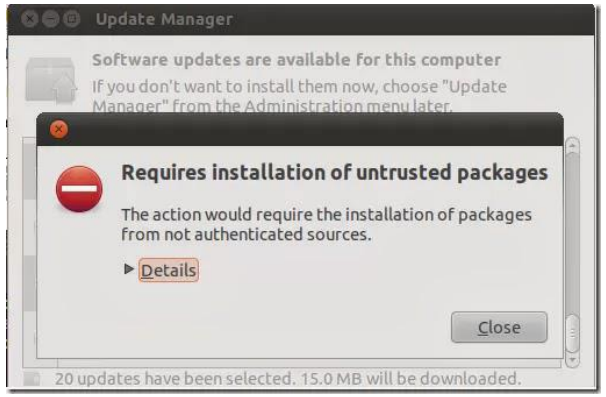
- **Sensitive Information** - Never enter sensitive information (e.g., credit card, bank account, social security number, password) into websites. Always check if the website is legit.

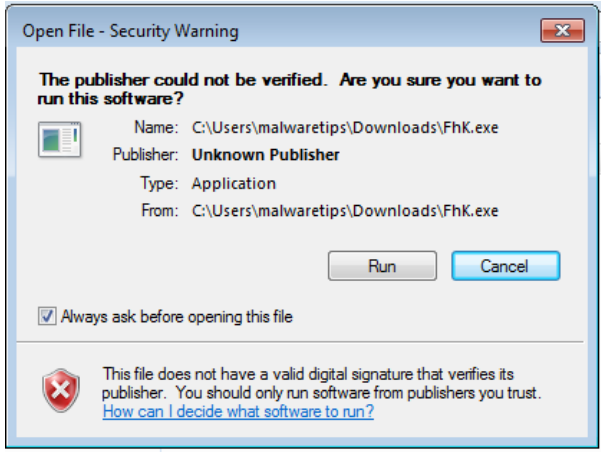


- **Appropriate Software** - Use a reputable anti-virus software, and don't install programs unless you know what they are and what they do. Try to find help from an IT administrator or reliable IT expert.

- Some of the usual confirmation popup messages are shown here. Do not run it unless you are very sure about the application.







ONLINE SAFETY AT SCHOOL

Authorized Access – Always access resources and websites that you are allowed to. The school may have certain ICT Policies in place. Ensure that the resources, websites or tools that goes against these polices.

Information Security – Do not sign in to your personal or secure digital accounts like banks or social media as the devices are used by multiple users which may expose your personal information.

Consulting Adults – If you find anything suspicious or anything that you have no knowledge of, always consult the person in charge. It can be your teachers or supervisors.

Authentication Information – Never save your passwords, pins or OTPs on the common devices that you use as this can be accessed by the other users.

Personal Devices – If in case you are allowed to bring your own devices to the educational institutions, make sure that the devices are secured with a password and the devices are always locked.

Software and Apps – Do not install any software or applications unless you are asked to. Unreliable software can have malware and breach your information as well as the information of others who use the devices.

Digital Citizenship

DIGITAL CITIZENSHIP

A DIGITAL CITIZEN is a person who has the knowledge and skills to effectively use digital technologies to communicate with others, participate in society and create and consume digital content.

- **Digital citizenship refers to the responsible use of technology by anyone who uses computers, the Internet, and digital devices to engage with society on any level. Digital citizenship is about digital wellness.**

Incident Reporting

- If you see/feel/suspect any wrong doing on the internet or in the use of an electronic device, you should report the matter to an adult at home or your teachers or the Supervisor at the earliest.

- You can also inform the School e-Safety Officer by an e-mail through childwelfare@easuae.com
- Your information will be kept confidential depending upon the nature of it.

ALWAYS REMEMBER THAT NOT ALL INFORMATION ON THE INTERNET IS TRUE AND ACCURATE

LET US ALL BE GOOD DIGITAL CITIZENS

THANK YOU