Staying Safe Online

2020

Resources adapted from Media Literacy Counsel Singapore

How to stay safe online: The S.M.A.R.T. rule

S.M.A.R.T. — SAFE

Be careful about the amount of personal information you reveal to strangers as well as on your own online profile, such as:

1. Name
2. Email
3. Phone number
4. Home address
5. Details of friends and family members
6. Schedules
7. School

And any other information that may possibly be harmful.

Such information given out may not seem to be able to do much harm, but the accumulation of them can be dangerous.

S.M.A.R.T. — MEETING

: Meeting someone you have only (just) met online can be dangerous. However, if you really want to do so, we advise you to bring along a trusted adult, and never a friend. If unable to do so, do inform your parent/guardian of the time and place of the meeting and who you are meeting with.

S.M.A.R.T. — AWARE

Never accept and open emails, direct messages or files from people you do not know or trust as they can be very dangerous and may contain viruses or nasty messages.

S.M.A.R.T. — RELIABILITY

Not everything that is portrayed online is what it actually is. Always be on guard and remain careful when conversing with people you do not know.

A lot of information on the Internet can be untrue - always be extra careful if you see things that are too good to be true.

S.M.A.R.T. — TELL

It is important that the moment your conversation with someone online makes you uncomfortable or worried, you should not hesitate to inform a parent or a trusted adult to prevent the situation from getting worse.

Internet Dangers

DANGER: Phishing

Definition:

Phishing is a method cyber criminals use to illegally obtain your personal and financial information (such as your login details, and your parents' bank account numbers and credit card numbers).

Dangers:

After cyber criminals steal your sensitive information, they may use it against you. For example, they may use your parents' credit card details to purchase goods online.

Red Flags:

- The website is not secure. Its URL does not begin with "https" and there is no closed lock icon near the address bar.
- The website requests for confidential information. Most organisations will never ask for your personal information to be sent over the Internet, such as your NRIC, address, birthday and phone number. If you receive a message asking for your personal information, clarify with your parents before providing the information.
- The link is not what it appears to be. The cyber criminal may use a popular website with a misspelling, for instance www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n'.

DANGER: Scams

Definition:

Scams are dishonest activities that take money or other goods from an unsuspecting person. Online scams are more concerned with stealing money, property and information.

Dangers:

People with ill intentions can use information you provide when they are attempting to scam you. They may sell your information to others or use your parent's credit card.

Red Flags:

- You do not know the sender of the email and the email has links or attachments (most commonly .exe files)
- Email subject and contents do not match
- Email contains request for you to forward the message to more people, sometimes offering money for you to do so
- Emails or advertisements contain urgent offers (e.g. "Buy NOW") or offers that are too good to be true (e.g. "You just won an iPhone from a lucky draw!")

Scams can seem genuine at first because scammers can pose as people you know, such as family members or friends. However, you must remain vigilant and ensure that you do not click on any link or attachment that will enable scammers to have access to your information. If you are unsure, ask your parents to help you check the source of the email and ask the sender if they actually sent the email to you.

DANGER: Identity Theft

Definition:

Identity theft is when someone “steals” your name and personal information in order to commit crimes such as taking over your accounts or buying things online.

Dangers:

You could be mistaken for committing crimes and be held accountable for paying for things that you did not buy.

Red Flags:

- 🚩 Seeing your name or your photo in accounts that do not belong to you is an indication that someone else is using your name and pretending to be you.
- 🚩 Receiving summons/letters/warnings/charges for things that you did not do/ buy. This shows that someone else is making use of your account to do/buy things.

DANGER: Virus

Definition:

Viruses are softwares that copy and paste its own codes into the computer programs, causing the programs to become corrupted or become unusable.

Dangers:

It can steal information about your activity on your computer, which can potentially be used against you.

Red Flags:

- 🚩 If many people received the same email from you after you have clicked on a link, your computer would very likely have been infected.
- 🚩 In many cases, viruses cause a decrease in performance of the device you are using. For example, your computer may load much slower than normal due to viruses in it.
- 🚩 If your files/applications suddenly begin to crash very often or can no longer be opened, it is also likely that it was corrupted by the virus (the virus inserts its own code between the files or applications, preventing them from functioning normally).

Be Safe & Be S.M.A.R.T

Resources adapted from Media Literacy Counsel Singapore