From

Director Secondary Education, Haryana,

Panchkula

To

1. All District Education Officers
2. All District Elementary Education Officers
   in the State of Haryana

Memo No. 1/16-2016 e-Gov./IT cell

Dated, Panchkula the

Sub: Regarding building Cyber Security Hygiene among students studying in schools (Govt./Pvt.) in the State of Haryana.

Refer to the subject cited above.

Secretary to Government, Haryana, electronics and Information Technology Department has vide letter No. Admn/315/1-SIT-7249 dated 06.08.2018 has intimated that with the increasing usage of internet and mobile technology need has been felt to build cyber security hygiene among students studying in schools in Haryana in various age groups.

For this Content has been prepared by E&IT Department to include information security awareness/ ready reckoner tips on cyber security related aspects impacting school going children. It is expected that this would help sensitize students about information security and develop strong foundation on knowledge among students on basic hygiene factor on information security in day to day life and prevent them from unknown cyber threats. The contents are designed considering various age groups of students ad under:-

a) Age Group of 5th to 8th Class – Annexure 'A'
b) Age group of 9th to 12th Class – Annexure 'B'

Copy of letter under reference and Annexure 'A' and 'B' are attached herewith with the directions to paste the contents on the notice boards and organize a small workshop covering all students under the mentioned age groups/ classes as per modules prepared and sensitize them on the content in order to build the basic cyber security hygiene.

Sd/-
Deputy Director (IT)
For Director Secondary Education,
Haryana, Panchkula

Endst. No. Even Dated: 09.08.2018

A copy is forwarded to the following for information and necessary action:-

1. PS/ACSSE.
2. PS/DSE
3. PA/DEE
4. AM to SPD
5. All officers at the State Headquarters of Elementary and Secondary Education Directorate and HSSPP.
6. Programmer (Varun) to uploading on the website.

Deputy Director (IT)
For Director Secondary Education,
Haryana, Panchkula

Endst. No. Even Dated: 09.08.2018

A copy is forwarded to the following for information :-

1. Secretary to Government, Haryana, Electronics and Information Technology Department with reference to his letter No. Admn/315/1-SIT-7249 dated 06.08.2018.
2. Sh. Munish Chander – Head SeMT/CIST (munish.chandan@semt.gov.in) (ciso.haryana@nicipc.gov.in).

Sd/-
Deputy Director (IT)
For Director Secondary Education,
Haryana, Panchkula

Annexure 'A'

[redacted]

Information Security Management Office (ISMO),

HARTRON Bhawan Sector-2, Panchkula – 134151

Technology has become an essential part of education, the learning process and socializing. Students are actively using advanced technology to learn, enhance knowledge and socialize. If used for exchanging knowledge and learning, can be of a great added value. However, if the same tools are used for sharing inappropriate content, it could be unsafe for the students.

Prior knowledge of cyber security tips would help students and kids to have a seamless experience of using technology enables services and social media and avoid being victims unknowingly to cyber crimes

Handy tips for students/children's to stay safe online:

Do's

1. Protect your identity: The internet is not the right place to share any private information that reveals their real identity.
2. Protect your computer using licensed/genuine software and byregularly updating computer can protect you against hackers and other online threats that can compromise your computer system and other private information
3. Create unique passwords: For online safety, we have to use different passwords for every online account. They help to prevent others from accessing their personal information. Make sure that we use strong passwords which include elements like symbols, numbers, uppercase and lowercase letters
4. Always lock your computer/mobile with strong password
5. Keep your Internet browser, Operating System (Windows) and antivirus up-to-date

[redacted]

[redacted]

6. Keep Bluetooth connection in an invisible mode
7. Always log off from your email account after use

Don'ts

1. Don't post personal information on social networks. Sharing personal pictures with online friends is nice however; once pictures are posted or shared online, they stay online forever
2. Don't give out personal information, such as name, home address, or telephone number, to anyone through email, Twitter, Facebook, WhatsApp or in online chat rooms.
3. Don't visit inappropriate websites, and notify your parent or teacher about any hurtful messages, inappropriate image, video or page.
4. Don't save your username and password on the browser
5. Don't respond to any suspicious email, instant message or web page asking for personal information.
6. Don't open or download any attachments from an unknown source as they may contain viruses.
7. Don't plug-in unknown USB drive into your computer
8. Disconnect your PC when not in use
9. Don't use PIN numbers that match your personal information like date of birth, vehicle number, door number etc
10. Don't share your parent's credit card number details through e-mail with anyone

[redacted]

Annexure 'B'

Information Security Management Office (ISMO),

HARTRON Bhawan Sector-2, Panchkula - 134151

Most of us are 'connected' via Social Media on Facebook, WhatsApp, and Google etc. using our mobile phones, tablets, laptops or personal computers. Internet is a valuable resource for learning, entertainment, making friends, sending e-mails etc. But if you use the internet without safety awareness, you could be at risk of illegal activity or something more serious. Internet safety is every ones responsibility. It is important to learn how to stay safe online.

Below are some Brilliant Guidelines to follow when you're online:-

1. Don't give personal information such as your address or phone number
2. Don't send pictures of yourself to anyone, especially offensive pictures
3. Don't open emails or attachments from people you don't know
4. Don't forward online chain message through e-mail to everyone you know
5. Don't become online 'friends' with people you don't know
6. If anything you see or read online worries you, inform your parents/teachers about it

It only takes a little bit of effort and some basic information to be safe as you browse the Internet. Follow these guidelines to **protect your personal information and your computer online.**

Do's

1. Install and maintain up to date anti-virus software on your computer or device
2. Always take back up of your important data into removable media and store in safe places
3. Keep your internet browser up-to-date
4. Be alert to unusual computer activity or problems
5. Install and maintain a firewall on your computer
6. Use a modern browser with features such as a pop-up blocker

[redacted]

7. Always open links in web browser only
8. Always use spam filters in e -mail
9. Update your Anti-virus software regularly
10. Use at least 8 characters or more to create a password by using lowercase, uppercase, numbers and special characters

Don't

1. Don't store sensitive material indefinitely on your computer
2. Don't send links via instant messaging and e-mail attachments
3. Don't attach email with file extension such as VBS, SHS, PIF while sending as well as receiving e mails
4. Don't use auto download and auto open features in your PC

Stay safe on social networking sites

Do's

1. Be very careful about sharing content online - especially if it isn't yours to share
2. Use the strongest privacy setting when you set up your profile. This means that only your friends will be able to view your information
3. Use Private Browsing facility of your browser to access the internet without saving any information about sites or webpages visited

Don't

1. Don't make friends you don't already know personally.
2. Don't indulge in illegal downloads on social media websites

[redacted]

[redacted]

Smartphone Security Tips

Do's

1. Install and maintain an Anti-Virus application on your smart device.
2. Carefully consider what information you want stored on the device
3. Be cautious when selecting and installing applications.
4. Always install Mobile apps from trusted source (like Google Play Store, Apple App Store and Microsoft Store App etc.)
5. Note the IMEI (International equipment mobile identity) number of your cell phone
6. Always keep your device; mobile phone, tablet locked up with strong password/PIN
7. Delete all information stored in a device prior to discarding it

Don't

1. Don't join unknown Wi-Fi networks using unsecured Wi-Fi hotspots
2. Don't follow links sent in suspicious email or text messages
3. Don't use interfaces that are not in use, such as Bluetooth, infrared, or Wi-Fi

Security tips on Digital Payments

Do's

1. Always keep your device; mobile phone, tablet locked up with strong password
2. Immediately block your SIM if your mobile phone is lost and inform service providers and police officials
3. Ensure authenticity of applications by validating links from Bank's website
4. While doing internet Banking always prefer using 'virtual keyboard' option

[redacted]

[redacted]

5. Always inform Bank if your Bank a/c registered mobile number has changed. This will ensure that SMS will reach only your new mobile number
6. Be cautious while using Bluetooth in public places as someone may access the confidential data/information
7. Read all term and conditions carefully before opening a mobile wallet a/c or enrolling for loyalty schemes of online shopping
8. Destroy your debit/credit card completely after it has expired
9. Change your PIN details as received via courier from bank after your first login
10. Always tally your sms value details debited and amount shown on your receipts
11. Always update your payment application version
12. Do online shopping only from reputed and verified e-commerce websites

Don't

1. Don't respond any email/text sms/ from unknown sources soliciting login Id/password/OTP
2. Download Payments related applications only from trusted source
3. Don't share ATM PIN with anyone else
4. Don't share your OTP (one time password) with others
5. Don't use banking services or any financial transaction on open 'Wi-Fi' networks
6. Don't share your KYC (ID/Address proof documents) with any agent/Bank representative without verifying his/her credentials
7. Don't share your Bank a/c details with anyone else
8. Don't transfer funds without verifying details of recipients
9. Don't share your CVV (card verification value) number verbally while making payments at restaurants

[redacted]

10. Don't share your M-PIN with anyone

11. Don't us a common password for all wallet accounts

Key points to remember:

- KYC- Know your customer is a set of guideline from RBI (Reserve Bank of India). This comprises of set of documents which is accepted by Banks and Financial Institution as a proof of your identify and address. EX - Voter card, Passport, PAN card, Driving license etc
- M-PIN - Mobile Personal Identification number is issued when we register for mobile banking services with our Bank

[redacted]

Handy tips for women to stay safe online:

Do's:

1. Beware of fake profiles
2. Maintain your privacy online
3. Check your account settings regularly
4. Be careful while downloading applications through Bluetooth or as MMS attachments
5. Keep the Bluetooth connection in an invisible mode, unless you need some user to access your mobile phone or laptops
6. Avoid downloading the content into mobile phone or laptop from an untrusted source
7. Delete the MMS message received from an unknown user without opening it
8. Read the mobile phone's operating instructions carefully mainly regarding the security settings, pin code settings, Bluetooth settings, infrared settings and procedure to download an application
9. Activate the pin code request for mobile phone access. Choose a pin, which is unpredictable and which is easy to remember for you
10. Use the call barring and restriction services provided by operators, to prevent the applications that are not used by you or by your family members
11. Note the IMEI code of your cell phone and keep it in a safe place. This helps the owner to prevent access to the stolen mobile
12. Regularly, backup important data in the mobile phone or laptop by following the instructions In the manual
13. Define your own trusted devices that can be connected to mobile phone or laptop through Bluetooth
14. If you are ready to buy something online check, whether the site is secure like https or padlock on the browser address bar or at the status bar and then proceed with financial transactions

Don'ts

1. Don't let others peep into your accounts
2. Don't participate in chat rooms, they are not for us
3. Don't be happy if someone praises you online

[redacted]

4. Don't get motivated for likes on your pics and upload more
5. Don't click web links in your e-mail and no bank will ask you to update the accounts through online
6. Don't provide personal information including your passwords, credit card information, and account numbers to unknown persons
7. Don't keep username, account name and passwords at one place. Always try to remember passwords
8. Don't access online banking in cybercafes
9. Don't click any images in the web sites if you are unsure
10. Don't provide personal information or information about your organization
11. Don't reveal personal or financial information in email, and do not respond to email solicitations for this information.
12. Don't send sensitive information over the Internet before checking a website's security. Pay attention to the URL of a website
13. Don't make you mobile phone as a source for your personal data, which is dangerous if it falls in to the hands of strangers