

D.A.V. PUBLIC SCHOOL, SECTOR-14, GURUGRAM
CYBER BRIGADE SESSION: 2021-2022

S.NO.	NAME	CLASS
1	Simran Gandhi	XII K
2	Nitika Verma	XII A
3	Muskan	XII A
4	Priyanshi Roy	XI E
5	Adarsh Kumar	X A
6	Manya Jain	X E
7	Sachit Bansal	X E
8	Haarit Arora	X F
9	Bhriigu Arora	X F
10	Ansh Kamboj	IX B
11	Daksh Juneja	IX F
12	Hiral Sharma	IX F
13	Ishita Sharma	IX F
14	Muskaan Yadav	IX F
15	Naksh Aggarwal	IX F
16	Rudraksh Sharma	IX F

WIFI SECURITY

Most often open Wi-Fi networks cause lot of threats to our mobile phones if connected in these networks



Keep the Bluetooth connection in an invisible mode, unless you need some user to access your mobile phone or laptops.

Don't perform financial, medical or business tasks while logged in to open Wi-Fi. If you have to, then get a VPN or use a secured network.

Don't use any passwords and sensitive data while logged in to open Wi-Fi.

Shutdown the Access Point when not in use

Change the default username and Password of the Access Point



1.PASSWORD SECURITY

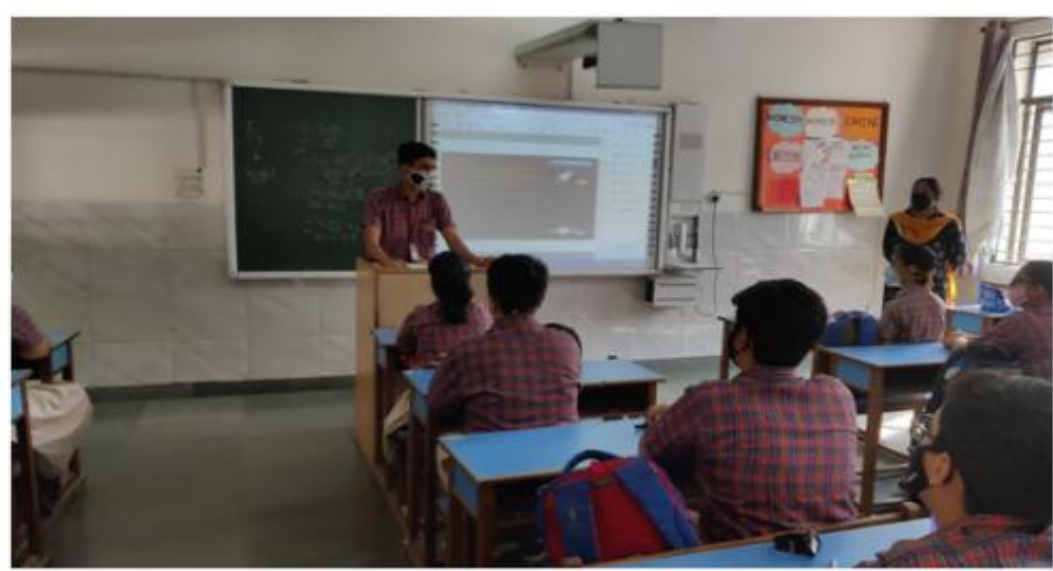
- use of strong passwords for your Wi-Fi network, system, email accounts, remote desktop systems, VPN connection etc. paraphrase your password...ex use a slogan as password
- Enable two factor authentication to ensure security on most of your online accounts, like your:
 - Email accounts
 - Social media networks



UNSECURED WI-FI NETWORKS

Personal Wi-Fi networks installed at home can be controlled to make it secure. However, if it is chosen to use public Wi-Fi networks it may lead to sniffing/monitoring your internet activities

The collage includes several key elements: a person with a question mark, a Wi-Fi router, a 'HOTEL' sign, a smartphone with a red 'WARNING' button, a 'Private' label, an email inbox with 'COMPOSE' and 'Inbox (6)' buttons, stacks of money, and a person covering their face. The background features a circuit-like pattern.



A screenshot of a virtual meeting interface. It features a grid of six video call windows. The top row shows three participants: a boy with headphones, a girl with glasses, and a boy with glasses. The bottom row shows three participants: a boy, a girl, and a girl. At the bottom of the screen is a horizontal bar with circular icons representing other participants.



UNSECURED WI-FI NETWORKS

Personal Wi-Fi networks installed at home can be controlled to make it secure. However, if it is chosen to use public Wi-Fi networks it may lead to sniffing/monitoring your internet activities

The collage includes several images: a person with a question mark, a Wi-Fi router, a 'HOTEL' sign, a 'Private' label, an email 'Inbox (6)', a 'BLACKMAIL' button, stacks of money, and a person looking stressed.

A Zoom meeting grid at the bottom of the slide showing several participants in a row.