

A GUIDE FOR STUDENTS

CYBER SECURITY 101

Staying safe, smart, and in control online.

Presented by Dr. Dhiman Saha, CSE, IIT Bhilai

TODAY'S SESSION

What We'll Cover

01 Passwords & Authentication

02 Phishing & Scams

03 Social Media Safety

04 Personal Info & Privacy

05 Cyberbullying

06 Safe Browsing Habits

07 Device & Malware Basics

08 Careers In Cybersecurity

01

Passwords & Authentication

Building A Strong Password

12+

Length

A long passphrase beats a short, complicated jumble every time.

Aa1!

Variety

Mix letters, numbers, and symbols so it can't be easily guessed.

1:1

Uniqueness

One password per account — a leak on one site shouldn't unlock the rest.

Two-Factor Authentication

Something You Know

Your password.



Something You Have

A code sent to your phone or an authenticator app.

Even if someone steals your password, they still can't get in.

Quick Check

Rate That Password

password123

Tigers#22!

**purple-tacos-moon-
run**

Which one would you trust with your accounts — and why?

02

Phishing & Scams

Spotting A Phishing Message

- 01** Urgent language — "act now or lose access"
 - 02** A sender address that doesn't match who they claim to be
 - 03** Links that lead somewhere unfamiliar
 - 04** Requests for passwords, codes, or payment
-

PHISHING & SCAMS

Common Scam Tactics

TACTIC

WHAT IT LOOKS LIKE

"You Won!"

A prize or gift card you never entered to win

Fake Tech Support

A pop-up claiming your device is infected

Impersonation

A message pretending to be a friend or a game's support team

Too-Good Deals

Free skins, gems, or gift cards for "verifying" your account

Quick Check

Real Or Phishing?

Message A

"Your account will be deleted in 1 hour. Click here to confirm your password."

Message B

"Hey, it's mom — running 10 minutes late to pick you up."

Which one is trying to trick you — and what gave it away?

03

Social Media Safety

Privacy Settings Matter

Who Can See You

Set profiles to private so strangers can't view your posts.

Tag Review

Approve tags and mentions before they appear on your page.

Location Off

Turn off location tagging — it shows more than you think.

SOCIAL MEDIA SAFETY

Think Before You Post

The Screenshot Test Anything can be saved and shared, even if it "disappears."

The Audience Test Would you be okay with a teacher or parent seeing it?

The Future Test Could this show up again in five years, in a bad way?

04

Personal Info & Privacy

What Not To Share Online

Never Share

Full name and home address

Passwords or account codes

School name and daily schedule

Family financial details

Share Carefully

First name, to people you actually know

General hobbies and interests

Photos, with location tags off

Vacation plans, after you're back

05

Cyberbullying

CYBERBULLYING

Recognizing Cyberbullying

Mean Messages

Insults, threats, or harassment sent directly or in group chats.

Exclusion

Being deliberately left out of group chats or online spaces.

Impersonation

Someone creating a fake account pretending to be you.

Spreading Rumors

Sharing private messages or photos to embarrass someone.

CYBERBULLYING

What To Do If It Happens

01 Don't respond or retaliate

02 Save the evidence — screenshot it

03 Tell a trusted adult right away

04 Block and report the account

06

Safe Browsing Habits

SAFE BROWSING HABITS

Browsing Safely

Check For The Lock

A padlock icon and "https" mean the connection is secure.

Skip Unknown Downloads

Don't install files or apps from sites you don't recognize.

Watch Public Wi-Fi

Avoid logging into accounts on open networks you don't trust.

Stick To Trusted Sites

Use school-approved or well-known sites for research and work.

07

Device & Malware Basics

DEVICE & MALWARE BASICS

Malware: What It Is

TYPE	WHAT IT DOES
Virus	Spreads between files and devices, causing damage
Spyware	Quietly watches what you type and do
Ransomware	Locks your files until you pay to get them back

Best defense: keep software updated, and don't open unknown files or links.

08

Careers In Cybersecurity

Where This Skill Can Take You

Security Analyst

Watches for threats and keeps systems protected.

Ethical Hacker

Tests systems for weaknesses before real attackers find them.

Incident Responder

Steps in fast when something goes wrong to limit the damage.

Strong passwords. A skeptical eye. Careful sharing. That's most of the job.