

# CYBER DEFENSE

*Stay Safe in a Digital World*



**Dr. Jaskaran Singh**

# What Is Cyber Defense?



Cyber defense is the practice of protecting computers, phones, networks, and data from digital attacks.

*Think of it like having a strong lock on your house — but for your online life.*

**4.9B**

people online today

**2,200**

cyber attacks per day

**95%**

attacks target humans



# Common Cyber Threats



## Phishing

Fake emails or messages tricking you into giving up your password or personal info.



## Malware

Harmful software secretly installed on your device to steal data or spy on you.



## Public Wi-Fi Attacks

Hackers on the same network can intercept your data on unsecured Wi-Fi spots.



## Cyberbullying & Stalking

Using technology to harass, threaten, or monitor someone without their consent.



## Account Takeover

Someone guesses or steals your password and gains access to your accounts.



## App Scams

Fake apps that look real but steal your information or charge hidden fees.



# Spotting a Phishing Attack

inbox — Your Email

From: security@paypa1.com

Subject: 🚨 URGENT: Verify your account NOW!

Dear Customer,

We have detected suspicious activity. Your account will be suspended in 24 hours unless you verify your identity immediately.

[CLICK HERE TO VERIFY](#)

© PayPa1 Corp. All Rights Reserved. 2024

## ⚠️ Suspicious sender

'paypa1.com' — the letter 'l' is actually '1'!

## ⚠️ Creates panic

Urgency + fear = pressure to act without thinking.

## ⚠️ Fake link button

Hovering shows a completely different URL.

## ⚠️ Vague greeting

'Dear Customer' — real companies use your name.

# Password Power

How long to crack your password?

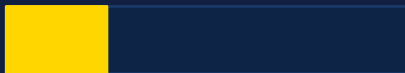
password

 Instant



P@ssw0rd

 Minutes




Tr0ub4dor&3

 Months



L!on\$Jump\*River2024

 Billions of years



## Strong Password Tips

- ✓ Use 12+ characters
- ✓ Mix UPPER & lower case
- ✓ Add numbers & symbols
- ✓ Avoid your name or birthday
- ✓ Use a passphrase
- ✓ Never reuse passwords
- ✓ Use a password manager



# Safe Social Media Habits

## ✓ DO

- ✓ Set accounts to private
- ✓ Only accept friends you know IRL
- ✓ Think before you post — it's permanent!
- ✓ Use strong, unique passwords
- ✓ Enable two-factor authentication
- ✓ Report suspicious messages

## ✗ DON'T

- ✗ Share your full name & address online
- ✗ Post photos of your school or daily routine
- ✗ Click links from strangers
- ✗ Share your passwords with friends
- ✗ Meet online strangers in person
- ✗ Respond to mean or threatening messages

# Device & Network Safety



## Lock Your Device

- › Use a PIN, fingerprint, or face lock
- › Set auto-lock after 1 minute
- › Never leave devices unattended



## Public Wi-Fi Risks

- › Avoid banking on public Wi-Fi
- › Use a VPN when on public networks
- › Look for HTTPS in website URLs



## Keep Software Updated

- › Updates patch security holes
- › Turn on auto-update for your phone
- › Update apps regularly too



## Download Safely

- › Only use official app stores
- › Check reviews before downloading
- › Avoid cracked or pirated software



## Backup Your Data

- › Back up weekly to cloud or USB
- › Protect against ransomware loss
- › Check backups actually work



## Privacy Settings

- › Review app permissions
- › Disable location for most apps
- › Turn off Bluetooth when not using



# What to Do If You're Attacked

1

## Stay Calm

Don't panic. Take a breath and think clearly before acting.

2

## Disconnect

Turn off Wi-Fi and disconnect from the internet to stop further damage.

3

## Tell an Adult

Tell a parent, teacher, or trusted adult immediately — you're not in trouble!

4

## Change Passwords

From a safe device, change passwords for all affected accounts right away.

5

## Report It

Report cyberbullying or attacks to your school or local cybercrime authority.

6

## Document Everything

Take screenshots of threats or suspicious messages as evidence.



# Your Cyber Hero Checklist



I use strong, unique passwords for each account



I can spot signs of a phishing email



I have two-factor authentication enabled



I avoid clicking suspicious links



I keep my software and apps updated



I know who to tell if something goes wrong



I lock my phone/device automatically



I back up my important files regularly



I don't share personal info on social media



# Two-Factor Authentication (2FA)

## What is 2FA?

Two-Factor Authentication adds a second layer of security beyond just your password. Even if a hacker steals your password, they still can't get in without the second factor.

- 1 Enter your username & password
- 2 A code is sent to your phone or app
- 3 Enter the code to confirm it's really you

## Types of 2FA

### SMS Code

A text message with a one-time code

### Authenticator App

Apps like Google Authenticator generate codes

### Email Code

A code sent to your registered email


### Biometrics

Fingerprint or face scan as second factor

# Understanding Privacy Settings


*Who can see your data? It depends on your settings.*

## Facebook / Instagram

 Public by default — strangers can see your posts, photos, and location.


✓ Fix: Set to 'Friends Only' or 'Private Account'

## Gaming Platforms

 Other players can message you, see your real name or location.

✓ Fix: Disable 'Find me by name', enable friend-only chat

## Location Services

 Apps can track everywhere you go — even when not in use.

✓ Fix: Set location to 'Only while using' or turn off

## Search Engines

 Your searches are stored and used to build a profile of you.

✓ Fix: Use private/incognito mode for sensitive searches



# Cyberbullying — What You Can Do

Cyberbullying is when someone uses technology — texts, social media, games, or apps — to harass, threaten, embarrass, or exclude another person.

## Signs of Cyberbullying

- ✗ Hurtful or threatening messages
- ✗ Spreading rumors online
- ✗ Sharing embarrassing photos/videos
- ✗ Excluding someone from online groups
- ✗ Impersonating someone to cause harm
- ✗ Doxing — sharing private info publicly

## What To Do

- ✓ Don't respond or retaliate
- ✓ Block the bully on all platforms
- ✓ Screenshot and save the evidence
- ✓ Tell a trusted adult or teacher
- ✓ Report to the platform or app
- ✓ You are NOT alone — reach out for help

# AI, Deepfakes & Misinformation

AI can create incredibly realistic fake images, videos, audio, and text. Here's how to stay sharp:

## Deepfake Videos

AI-generated videos that swap someone's face or voice. Can make it look like someone said something they never did.

### How to Spot It:

- › Look for unnatural blinking or lip sync
- › Blurry edges around face/hair
- › Odd lighting or skin tone
- › Verify with the original source

## AI-Generated Text

Fake news, fake reviews, spam emails written by AI — designed to manipulate and mislead readers.

### How to Spot It:

- › Check the original source or website
- › Cross-reference with trusted news sites
- › Look for emotional language / extreme claims
- › Use fact-checking sites

## Fake AI Images

Realistic photos of people or events that never happened. Often used to spread false narratives on social media.

### How to Spot It:

- › Look for odd hands or fingers (extra/missing)
- › Blurred or repeated backgrounds
- › Reverse image search to find origin
- › Check if image metadata matches



# Online Gaming Safety

**3.2B**

gamers worldwide

**40%**

experienced harassment

**\$1B+**

lost to gaming scams

## Gaming Risks

- ✗ Strangers asking to meet in real life
- ✗ Sharing location or school name in chat
- ✗ In-game scams — 'free skins for your password'
- ✗ Harmful or abusive chat from other players
- ✗ Purchases on parents' linked accounts

## Safe Habits

- ✓ Use a gamertag — not your real name
- ✓ Only friend people you know in real life
- ✓ Report toxic players using in-game tools
- ✓ Never share your account credentials
- ✓ Set spending limits with parental controls



# Ransomware — Digital Kidnapping

Ransomware is malware that locks your files and demands payment to unlock them. Schools and businesses are top targets.

## How a Ransomware Attack Works:



## How to Protect Yourself:

- ✓ Back up files regularly to an external drive or cloud
- ✓ Never open attachments from unknown senders
- ✓ Keep your operating system and antivirus updated
- ✓ Don't download software from unofficial sites

# Your Digital Footprint


Everything you do online leaves a trail. Your digital footprint can affect college admissions, future jobs, and your safety.

## Active Footprint

- › Posts, comments, and likes on social media
- › Photos and videos you upload
- › Emails and messages you send
- › Reviews and forum posts you write
- › Accounts you register for

## Passive Footprint

- › Websites tracking your browsing habits
- › Location data collected by your phone
- › Search history stored by search engines
- › Cookies remembering your preferences
- › IP address revealing your general location

 Rule of thumb: Never post anything online you wouldn't want your parents, teacher, or future employer to see.



# Safe Browsing Habits

## Can You Tell a Safe Website?



<https://www.mybank.com/login>

HTTPS + padlock = encrypted connection. Legitimate domain.



<http://mybank-secure.ru/login>

No HTTPS. Suspicious foreign domain (.ru). Classic phishing!



<https://amaz0n-deals.net/order>

Zero replaced letter in 'amazon'. Fake domain designed to trick.



<https://google.com/search?q=cats>

HTTPS + well-known domain. Safe to use.



Always check for HTTPS



Hover links before clicking



Avoid pop-up warnings



Bookmark trusted sites



# Protecting Personal Information

## What Is PII?

PII stands for Personally Identifiable Information — any data that can be used to identify you. In the wrong hands, it enables identity theft, scams, and stalking.

## Never Share Online

- ✗ Full name + date of birth
- ✗ Home address or phone number
- ✗ School name and daily schedule
- ✗ Passport, ID, or Aadhaar number
- ✗ Bank account or card details
- ✗ Passwords or OTP codes

## How Identity Theft Works

1

### Collect

Hacker collects your name, DOB, email from data breaches or social media

2

### Build Profile

Combines info from multiple sources to build a full picture of you

3

### Impersonate

Creates accounts, applies for loans, or buys things in your name

4

### Damage

Ruins your credit score, creates legal issues, or sells your data




# Careers in Cybersecurity

There are 3.5 million unfilled cybersecurity jobs worldwide — it's one of the fastest growing and highest paying fields!

## Ethical Hacker

*(Penetration Tester)*


Legally try to break into systems to find vulnerabilities before the bad guys do.

 Avg Salary: ₹6–25 LPA

## Security Analyst


*(SOC Analyst)*

Monitor networks 24/7, detect threats, and respond to security incidents.

 Avg Salary: ₹5–18 LPA

## Cryptographer


Design encryption systems that protect data, messages, and transactions.

 Avg Salary: ₹8–30 LPA

## Digital Forensics


*(Cyber Investigator)*

Investigate cybercrimes, recover evidence, and help bring criminals to justice.

 Avg Salary: ₹5–20 LPA


## Security Engineer

Build firewalls, security tools, and infrastructure to protect organizations.

 Avg Salary: ₹8–35 LPA

## Cyber Educator

Train organizations and students to understand and prevent cyber threats.

 Avg Salary: ₹4–15 LPA



# Quick Quiz — Test Your Knowledge!

**Q1: You get an email saying your Netflix account will be deleted unless you click a link. What do you do?**

- A. Click the link immediately   B. Log into Netflix directly in a new browser tab   C. Share the link with friends

✓ Answer:

[Redacted answer]

**Q2: Which password is the strongest?**

- A. password123   B. P@ssword!   C. T!ger\$Jump\*42

✓ Answer:

[Redacted answer]

**Q3: Someone you met online asks for your school name and home address. What should you do?**

- A. Share it — they seem friendly   B. Refuse and block/report them   C. Only share your school name

✓ Answer:

[Redacted answer]



# Quick Quiz — Test Your Knowledge!

**Q1: You get an email saying your Netflix account will be deleted unless you click a link. What do you do?**

A. Click the link immediately   B. Log into Netflix directly in a new browser tab   C. Share the link with friends

Answer: B — Always go directly to the website, never click links in emails.

**Q2: Which password is the strongest?**

A. password123   B. P@ssword!   C. T!ger\$Jump\*42

Answer: C — Long, random, with uppercase, lowercase, numbers, and symbols.

**Q3: Someone you met online asks for your school name and home address. What should you do?**

A. Share it — they seem friendly   B. Refuse and block/report them   C. Only share your school name

Answer: B — Never share personal info with people you only know online.



# Be Cyber Smart!

*Think before you click. Protect your digital life.*



Strong Passwords



Spot Phishing



Stay Safe Online