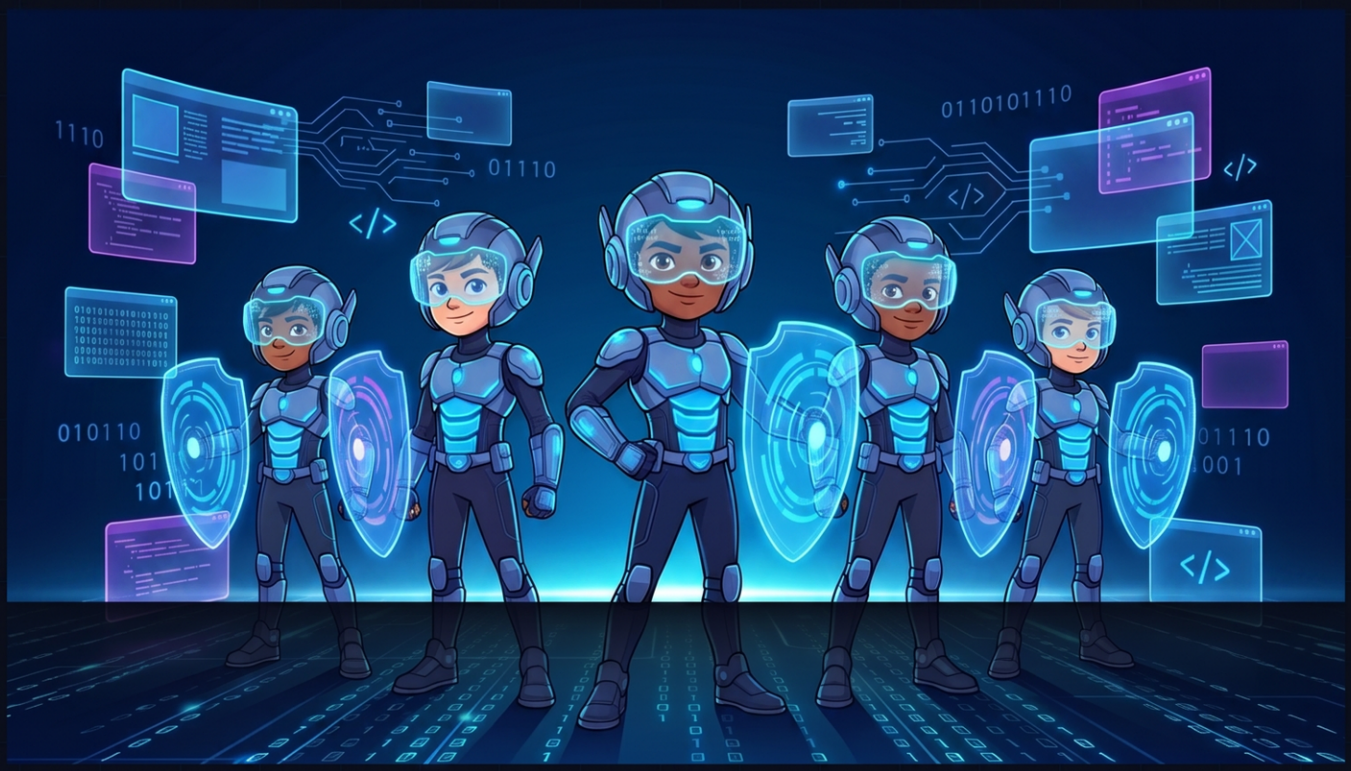


// STEALTHBLUE CYBER PRESENTS

CYBERSECURITY TIPS FOR STUDENTS

STAY SAFE ONLINE // A GUIDE FOR STUDENTS

You're growing up in an amazing digital world full of learning, creativity, and connection. But just like the real world, the internet has risks you need to know about.

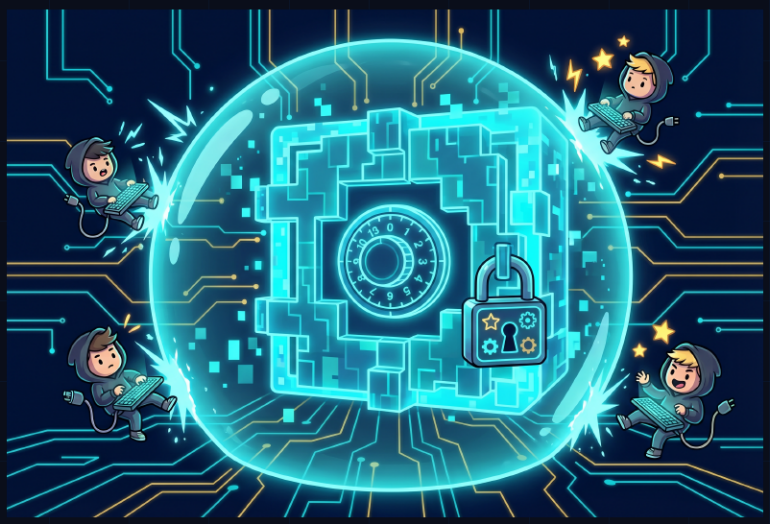
This guide will teach you how to protect yourself, your accounts, and your personal information -- so you can enjoy the internet safely and confidently.

WHAT'S INSIDE

// CHAPTER 01

STRONG PASSWORDS

Your First Line of Defense Against Hackers



Your password is like the lock on your front door. If it's weak, anyone can walk right in.
A strong password keeps hackers out of your accounts, games, and personal information.
Here's how to build passwords that are nearly impossible to crack:

DO THIS

- Make passwords at least 8 characters long
- Mix UPPERCASE and lowercase letters
- Include numbers and symbols (!@#$%)
- Use a DIFFERENT password for each account
- Try a passphrase: 'MyDog8Pizza!AtNoon'
- Use a password manager app to remember them
- Change passwords every 3 months
- Enable Two-Factor Authentication (2FA) when available

NEVER DO THIS

- Use your name, birthday, or pet's name
- Use simple passwords like '123456' or 'password'
- Share your password with friends
- Use the same password everywhere
- Write passwords on sticky notes
- Let websites 'remember' you on shared computers
- Ignore password change reminders
- Skip 2FA because it takes extra time

DID YOU KNOW?

A password with 8 random characters takes a computer about 8 hours to crack.
But a 12-character password with symbols? Over 34,000 YEARS. Length matters!

// CHAPTER 02

SOCIAL MEDIA SAFETY

Think Before You Post -- The Internet Never Forgets

Social media is fun for staying connected with friends, but it can also expose your personal information to strangers. Here's how to enjoy social media safely:

NEVER SHARE THESE THINGS ONLINE

- Your home address or phone number
- Your school name or location
- Your daily schedule or routine
- Photos with location tags or identifiable landmarks
- Your full birthday (month + day + year)
- Family vacation plans (wait until you're back!)

SMART SOCIAL MEDIA HABITS

- Keep your account set to PRIVATE -- not public
- Only accept friend requests from people you know in real life
- Think before you post -- would you be okay with your teacher seeing it?
- Block and report anyone who is being mean or creepy
- Don't post photos of other people without their permission
- Review your privacy settings regularly -- apps change them!
- Remember: screenshots exist -- DMs are not truly private

// CHAPTER 03

EMAIL & PHISHING SCAMS

Don't Take the Bait – Spot Fake Emails Like a Pro

Phishing is when someone sends a fake email or message pretending to be a real company to trick you into giving up your password or personal info. It's one of the most common cyberattacks -- and students are a major target.

HOW TO SPOT A PHISHING EMAIL

- The sender's email address looks weird (like support@amaz0n-deals.xyz)
- It says 'Act NOW!' or 'Your account will be DELETED!' -- urgency = red fiag
- It asks you to click a link or download an attachment
- There are speiling mistakes or weird formatting
- It asks for your password -- real companies NEVER do this
- The 'from' name says one thing but the email address says another

WHAT TO DO

- DON'T click links in suspicious emails -- hever over them first to see the real URL
- Check the sender's full email address carefully
- If unsure, go directly to the website by typing the address yourself
- Tell a parent or teacher if you get a suspicious email
- Use a strong, unique password for your email -- it's the master key to everything
- Enable Two-Factor Authentication (2FA) on your email account

// CHAPTER 04

GAMING & ONLINE FRIENDS

Play Smart -- Not Everyone Online Is Who They Say

Online gaming is awesome, but it also connects you with strangers from around the world. Some of those people might not be who they claim to be. Here's how to stay safe while still having fun:

GAMING SAFETY RULES

- Use a username that doesn't reveal your real name, age, or location
- NEVER share personal info with online players -- even if they seem nice
- Keep gaming accounts secure with strong passwords and 2FA
- Block and report players who are mean, creepy, or inappropriate
- Never download files, mods, or 'free backs' from strangers -- they're often malware
- If someone asks to move the conversation to a private app -- that's a red flag
- NEVER agree to meet an online friend in person -- this is VERY dangerous

IMPORTANT WARNING

- Adults who want to be friends with students online often have bad intentions
- If someone asks you to keep your friendship SECRET from your parents -- tell an adult immediately
- It doesn't matter how long you've been talking -- an online stranger is still a stranger

// CHAPTER 05

DEVICE & WIFI SECURITY

Lock Down Your Phone, Tablet & Computer

Your devices hold your photos, messages, accounts, and personal data. If someone gets access to your phone or tablet, they can access everything. Here's how to keep them safe:

PROTECT YOUR DEVICES

- Use a strong PIN, password, or pattern to unlock
- Enable fingerprint or face recognition
- Install software updates when prompted
- Only download apps from official stores
- Check app permissions before installing
- Never leave your device unattended
- Turn off Bluetooth when not using it
- Log out of accounts on shared devices

WIFI SAFETY

- Don't connect to random public WiFi networks
- Public WiFi at malls/cafes can be monitored
- Never enter passwords on public WiFi
- Ask a parent about using a VPN
- Make sure your home WiFi has a password
- Don't share your home WiFi password widely
- Watch for fake WiFi networks (like 'Free_WiFi')
- Use cellular data for sensitive activities

WATCH OUT FOR APP PERMISSIONS

Does a flashlight app really need access to your contacts and camera? Probably not!
Always question why an app needs certain permissions. If it doesn't make sense, don't install it.

// CHAPTER 06

SCAMS, AI & DEEPFAKES

Not Everything You See Online Is Real

Scammers are getting smarter, and now they have AI to help them. Deepfake technology can create fake videos of real people, and AI can write convincing fake messages. Here's what you need to know to protect yourself.

COMMON SCAMS TARGETING STUDENTS

- 'You won a free iPhone!' -- No, you didn't. It's always a scam.
- 'Free gift cards!' -- These are ALWAYS fake. No one gives away free money.
- 'Click here to get free V-Bucks/Robux' -- These steal your account credentials
- Fake celebrity giveaways on social media -- celebrities don't DM random students
- Chain messages: 'Forward this to 10 people or...' -- Just delete them

AI & DEEPFAKES -- THE NEW THREAT

- AI can now create fake videos that look completely real (deepfakes)
- AI can clone someone's voice from just a few seconds of audio
- Scammers use AI to write more convincing phishing emails
- Look for signs: weird eye movements, biurry edges, unnatural mouth movements
- Just because you see a video of someone saying something doesn't mean it's real
- Verify news from multiple trusted sources before believing or sharing it
- If something seems too shocking or too good to be true -- investigate before reacting

// CHAPTER 07

CYBERBULLYING

You Are Not Alone -- And It Is Never Your Fault

Cyberbullying is when someone uses technology to be mean, threaten, or embarrass another person. It can happen through texts, social media, gaming, or any online platform. If it's happening to you or someone you know, here's what to do:

IF YOU'RE BEING CYBERBULLIED

- DON'T respond or retaliate -- don't send mean messages back
- SAVE the evidence -- take screenshots of every mean message
- BLOCK the person on every platform and app they contact you on
- REPORT them using the app's or website's reporting feature
- TELL a trusted adult -- a parent, teacher, or school counselor
- Remember: It is NOT your fault. You did nothing wrong.
- If you feel unsafe, call 911 or the Cyberbullying Hotline: 1-800-248-2723

HOW TO BE AN ALLY

- If you see someone being bullied online, don't just watch -- speak up or report it
- Send a kind message to the person being bullied -- it makes a bigger difference than you think
- Don't share, like, or comment on posts that are meant to hurt someone
- Tell a trusted adult if you see cyberbullying happening -- even if it's not happening to you

// CHAPTER 08

SCREEN TIME & DIGITAL WELLNESS

Balance Your Online and Offline Life

Technology is an amazing tool, but spending too much time on screens can affect your health, sleep, mood, and relationships. Finding balance is key to staying healthy and happy.

WARNING SIGNS YOU MIGHT NEED A BREAK

- You feel anxious or upset when you can't check your phone
- You're staying up late scrolling instead of sleeping
- You'd rather be online than hang out with friends in person
- Your grades are dropping because of screen time
- You feel worse about yourself after using social media
- You're constantly comparing yourself to others online

HEALTHY DIGITAL HABITS

- Set daily screen time limits and stick to them
- Take a 10-minute break every hour -- stretch, walk, look outside
- No screens 30 minutes before bedtime (blue light disrupts sleep)
- Keep devices out of your bedroom at night
- Use 'Do Not Disturb' mode during homework and family time
- Follow the 20-20-20 rule: every 20 min, look at something 20 feet away for 20 seconds
- Make time for offline hobbies: sports, reading, art, music

SOCIAL MEDIA & YOUR MENTAL HEALTH

- People only post their best moments -- real life isn't like Instagram
- Unfollow accounts that make you feel bad about yourself
- Likes and followers don't define your worth
- If social media is making you sad, it's okay to take a break or delete the app

// CHAPTER 09

WHAT TO DO WHEN THINGS GO WRONG

Emergency Actions, Step by Step

RED FLAGS -- TELL A TRUSTED ADULT IMMEDIATELY

- Someone online asks you to keep your friendship SECRET from parents
- Someone asks for personal information, photos, or your location
- Someone is being mean, threatening, or bullying you online
- You see something that makes you scared or uncomfortable
- Someone tries to move your conversation to a private/hidden app
- You think your account has been hacked or someone is impersonating you
- An adult online wants to meet you in person -- this is VERY dangerous

IF YOUR ACCOUNT IS HACKED -- DO THIS NOW

- 1. Change your password IMMEDIATELY -- use a strong, unique one
- 2. Enable Two-Factor Authentication (2FA) on the account
- 3. Check your account activity for logins you don't recognize
- 4. Tell a trusted adult (parent, teacher, or counselor) right away
- 5. Report the hack to the website or app's support team
- 6. Change passwords on any other accounts that used the same password

// CHAPTER 10

YOUR SAFETY CHECKLIST

Check These Off Every Week to Stay Protected

WEEKLY SAFETY CHECKLIST

- [ ] I'm using strong, unique passwords for all my accounts
- [ ] I haven't shared personal information online this week
- [ ] I've checked my account activity for anything suspicious
- [ ] I've been kind to others online
- [ ] I've taken breaks from screens and done offline activities
- [ ] I've told an adult if something felt wrong or uncomfortable
- [ ] I've updated my apps and devices when prompted
- [ ] I've reviewed my privacy settings on social media

MONTHLY DEEP CHECK

- [ ] Change passwords on your most important accounts
- [ ] Review and remove apps you no longer use
- [ ] Check what personal info is visible on your social profiles
- [ ] Clear your browser history and cookies

// RESOURCES & HELP

NEED HELP? YOU'RE NOT ALONE

Important Resources, Hotlines & Websites

Cyberbullying Hotline

1-800-248-2723

Call for help with online bullying

Crisis Text Line

Text HOME to 741741

Free 24/7 crisis support via text

StopBullying.gov

www.stopbullying.gov

Government resource for bullying prevention

FBI Internet Crime Center

www.ic3.gov

Report internet crimes

MOST IMPORTANTLY: TALK TO YOUR PARENTS, TEACHERS, OR COUNSELOR

The adults in your life want to help you stay safe. You will NEVER get in trouble for telling a trusted adult about something that made you uncomfortable online.

STEALTHBLUE CYBER

Detect | Defend | Secure | www.stealthblue.com

This guide is free to distribute. Share it with friends, classmates, and family!