10 CYBERSECURITY TIPS FOR TEENAGERS

1 DON'T FEED THE TROLLS

Trolls can be individuals with the sole intention of creating arguments and controversial conversations online.

However, they might also aim to manipulate you into revealing information accidentally or to bully you. It's better not to engage at all if you feel triggered.

2 REPORT THE BULLY

Being victims of online harassment can lead to severe anxiety and depression. Don't respond to hurtful or offensive messages; instead, flag and block the person.

Keep a record of abusive messages or posts as evidence if needed. Especially if you notice particularly aggressive behavior, violent hate speech, or personal attacks, talk to your family and teachers or consider involving the authorities if necessary.

3 LOVEBOMBING AND CATFISHING ARE VERY DANGEROUS

Someone may pretend to be someone else, using direct messages or chats to show love and support and express interest in having a close relationship.

They never reveal their true identity, and many details about them may seem confusing. However, they might ask you to meet, send intimate videos and photos, or reveal sensitive information. There is a high risk of these individuals being predators, sex offenders, or scammers.

4 IF AN ONLINE FRIEND IS A REAL FRIEND SHOULDN'T BE A SECRET

Understand that online friends may not always be who they claim to be. Do not automatically trust someone online just because it seems like you have a lot in common.
If you have a close online friend who asks you to keep them a secret from your family and friends, it's a sign that they may not be who they say they are.

5 DON'T ALWAYS BELIEVE WHAT YOU SEE

Scammers use AI to generate fake images and audios, pretending to be someone else, even people you know.

This means they can pretend to have "compromising" material about you that is created with AI to blackmail you or pretend they are someone famous, asking you to do something for them.

6 PHISHING HAPPENS EVERYWHERE

Don't click on any links you see on social media, in your email, or in direct messages, especially if the link leads you to a page where you are asked to enter data, such as login information for your social media or payment details, promising something very inviting, like a giveaway, a free event entry, or juicy news about your favorite celebrities.

7 DON'T PLUG YOUR DEVICES ANYWHERE

As useful as they are, public charging stations can be used by hackers to install viruses and trojans on your device, stealing your personal information and taking control of your phone or tablet without you noticing until it's too late. It's safer to use your power bank or carry your charger and connect to an electrical outlet.

8 DO NOT POST OR SEND ANYTHING YOU WILL REGRET

Sending intimate photos/videos or posting them is never a good idea, even if you know the recipient.
The recipient can intentionally or accidentally share your content (if their devices are hacked, for example), and your photos can be shared and sold by strangers, or used to create fake profiles and adult content.

9 BE CAREFUL WITH APP PERMISSIONS

When you install a new app, it will request access to various features of your device, such as contacts, location, microphone, camera, photos, battery information, and more. Check what permissions each app requests and consider whether it makes sense. For example, why would a weather app need access to your camera and calls?

10 PARENTS BE ALERT

If your children's behavior changes when using devices—becoming moody, secretive, or anxious—it's time to address the issue. This could indicate social media addiction, electronic screen syndrome, or targeting by cyberbullies or scammers. Open communication without judgment is crucial. If under 18 and the situation worsens, consider using parental control apps on their devices