#SatarkNagrik

CHILDREN & CYBER SECURITY- An e-Book

NATIONAL CYBER SECURITY AWARENESS MONTH (NCSAM), 2024

Secure Our World

Theme: Cyber Surakshit Tripura

TABLE OF CONTENTS

INTRODUCTION

The Internet offers a world of opportunities.

People of all ages are:

- posting video from mobile devices
- building online profiles
- texting each other from their mobile devices
- creating alter egos in the form of online avatars
- connecting with friends online they don't see regularly in person
- sending photos to friends
- broadcasting what they're doing to hundreds of people

These ways of socializing and communicating can be fulfilling and, yet, they come with certain risks:

Inappropriate conduct.

The online world can feel anonymous. Kids sometimes forget that they are still accountable for their actions.

Inappropriate contact.

Some people online have bad intentions, including bullies, predators, hackers, and scammers.

Inappropriate content.

You may be concerned that your kids could find pornography, violence, or hate speech online.

You can reduce these risks by talking to your kids about how they communicate—online and off—and encouraging them to engage in conduct they can be proud of.

This guide covers what you need to know, where to go for more information, and issues to raise with kids about living their lives online.

The best way to protect your kids online? Talk to them.
Research suggests that when children want important information, most rely on their parents.

Not sure where to begin?

Consider the following:

Start early.

After all, even toddlers see their parents use all **kinds of devices. As soon as your child is using** a computer, a cell phone, or any mobile device, it's time to talk to them about online behavior, safety, and security. As a parent, you have the opportunity to talk to your kid about what's important before anyone else does.

Create an honest, open environment.

Kids look to their parents to help guide them. Be supportive and positive. Listening and taking their feelings into account helps keep conversation afloat. You may not have all the answers, and being honest about that can go a long way.

Initiate conversations.

Even if your kids are comfortable approaching you, don't wait for them to start the conversation. Use everyday opportunities to talk to your kids about being online. For instance, a TV program featuring a teen online or using a **cell phone** can tee up a discussion about what to do—or not—in similar circumstances. News stories about Internet scams or **cyberbullying**, for example, also can help start a conversation with kids about their experiences and your expectations.

Communicate your values.

Be upfront about your values and how they apply in an online context. Communicating your values clearly can help your kids make smarter and more thoughtful decisions when they face tricky situations.

Be patient.

Resist the urge to rush through conversations with your kids. Most kids need to hear information repeated, in small doses, for it to sink in. If you keep talking with your kids, your patience and persistence will pay off in the long run. Work hard to keep the lines of communication open, even if you learn your kid has done something online you find inappropriate.

ADVICE FOR PARENTS OF KIDS AT DIFFERENT AGES

- Young Kids
- Tweens
- Teens

Young Kids

When very young children start using a computer, they should be supervised closely by a parent or caregiver. Parents may wish to choose the websites their kids visit early on—and not let them leave those sites on their own. If little kids aren't supervised online, they may stumble onto sites that could scare or confuse them.

When you're comfortable that your young children are ready to explore on their own, it's still important to stay in close touch while they go from site to site. You may want to restrict access to sites that you have visited and know to be appropriate—at least in terms of their educational or entertainment value.

Tweens

During the tween years—ages 8 to 12—children start exploring more on their own, but that doesn't mean you don't want—or need—to be close at hand. It's important to be with them—or at least nearby—when they're online. For this age group, consider keeping the computer in an area where the child has access to you or another adult. That way, they can be "independent," but not alone.

For younger tweens, **parental controls**—including filtering or monitoring tools—can be effective. However, many middle school kids have the technical know-how to find a way to get around them. If children aren't already using the Internet for their schoolwork, this is when they're likely to start. It's also when they can discover resources for hobbies and other interests. Many tweens are adept at finding information online. That's often helpful to the rest of the family, but they still need adult guidance to help them understand which sources are trustworthy.

As you consider what your tweens see and do on the Internet, think about how much time they spend online. Consider setting limits on how often they can be online and how long those sessions should be.

Teens

Young tweens are likely to reflect the values of their parents. By the time they age into their teen years, they're forming their own values and beginning to take on the values of their peers. At the same time, older teens are maturing physically, emotionally, and intellectually, and many are eager to experience more independence from their parents.

Teens have more Internet access through cell phones, **mobile devices**, or friends' computers, as well as more time to themselves. So it isn't realistic to try to always be in the same room as your teens when they're online. They need to know that you and other family members can walk in and out of the room any time and can ask them about what they're doing online.

It's important to emphasize the concept of credibility to teens. Even the most tech-savvy kids need to understand that not everything they see on the Internet is true, that people on the Internet may not be who they appear to be, that information or images they share can be seen far and wide, and that once something is posted online, it's close to impossible to "take it back."

Because they don't see facial expressions, body language, and other visual cues online, teens may feel free to do or say things online that they wouldn't offline. Remind them that behind the screen names, profiles, and avatars are real people with real feelings.

When you talk to your teen, set reasonable expectations. Anticipate how you will react if you find out that he or she has done something online you don't approve of. If your teen confides in you about something scary or inappropriate they've encountered online, try to work together to prevent it from happening again. Since your teen is closing in on being an adult, she needs to learn how to behave and how to exercise judgment about using the Internet safely, securely, and in accordance with your family ethic.

Social networking sites, chat rooms, virtual worlds, and blogs are how teens and tweens socialize online. Kids share pictures, videos, thoughts, and plans with friends, others who share their interests, and sometimes, the world at large.

Socializing online can help kids connect with friends, and even their family members, but it's important to help your child learn how to navigate these spaces safely. Among the pitfalls that come with online socializing are sharing too much information or posting pictures, video, or words that can damage a reputation or hurt someone's feelings. Applying real-world judgment and using common sense can help minimize those downsides.

What can you do?

Remind your kids that online actions can reverberate.

The words they write and the images they post have consequences offline.

Explain to your kids why it's a good idea to post only information that they are comfortable with others seeing.

Some of your child's profile may be seen by a broader audience than you or they are comfortable with, even if privacy settings are on. Encourage your child to think about the language they use online, the pictures and videos they post, and the consequences of altering photos posted by someone else. Employers, college admissions officers, coaches, teachers, and the police may view your child's posts.

Remind your kids that once they post information online, they can't take it back.

Even if they delete the information from a site, they have little control over older versions that may exist on other people's computers and circulate online.

Use privacy settings to restrict who can access and post on your child's profile.

Some social networking sites, chat rooms, and blogs have strong privacy settings. Talk to your kids about these settings and your expectations for who should be allowed to view their profile.

Review your child's friends list.

You may want to limit your children's online "friends" to people they actually know.

Talk to your teens about avoiding sex talk online.

Research shows that teens who don't talk about sex with strangers online are less likely to come in contact with predators. In fact, researchers have found that predators usually don't pose as children or teens, and most teens who are contacted by adults they don't know find it creepy. Teens should not hesitate to ignore or block them.

Know what your kids are doing.

Get to know the social networking sites your kids use so you know how best to understand their activities. If you're concerned that your child is engaging in risky online behavior, you may want to search the social networking sites they use to see what information they're posting. Are they pretending to be someone else? Try searching by their name, nickname, school, hobbies, grade, or community.

Encourage your kids to trust their gut if they have suspicions.

Encourage them to tell you if they feel threatened by someone or uncomfortable because of something online. You can then help them report concerns to the police and to the social networking site. Most of these sites have links for users to report abusive, suspicious, or inappropriate behavior.

Tell your kids not to impersonate someone else.

Let your kids know that it's wrong to create sites, pages, or posts that seem to come from someone else, like a teacher, a classmate, or someone they made up.

Create a safe screen name.

Encourage your kids to think about the impression that screen names can make. A good screen name won't reveal much about how old they are, where they live, or their gender. For privacy purposes, your kids' IM names should not be the same as their email addresses.

Help your kids understand what information should stay private.

Tell them why it's important to keep some things—about themselves, family members, and friends—to themselves. Information like their Social Security number, street address, phone number, and family financial information—say, bank account or credit card numbers—is private and should stay that way.

APPS

Do you—or your kids—download "apps" to a phone or social networking page? Downloading may give the apps' developers access to personal info that's not even related to the purpose of the app. The developers may share the information they collect with marketers or other companies. Suggest that your kids check the privacy policy and their privacy settings to see what information the app can access. And consider this: Is finding out what flavor ice cream you are really worth sharing the details of your life—or your children's?

CYBERBULLYING

Cyberbullying is bullying or harassment that happens online. It can happen in an email, a text message, an online game, or comments on a social networking site. It might involve rumors or images posted on someone's profile or passed around for others to see, or creating a group or page to make a person feel left out.

Talk to your kids about cyberbullying. Tell your kids that they can't hide behind the words they type and the images they post. Hurtful messages not only make the target feel bad, but they also make the sender look bad—and sometimes can bring scorn from peers and punishment from authorities.

Ask your kids to let you know if an online message or image makes them feel threatened or hurt. If you fear for your child's safety, contact the police.

- **Read the comments.** Cyberbullying often involves mean-spirited comments. Check out your kid's page from time to time to see what you find.

- **Protect their profile.** If your child finds a profile that was created or altered without his or her permission, contact the company that runs the site to have it taken down.

- **Block or delete the cyberbully.** If the bullying involves IM or another online service that requires a "friends" or "buddy" list, delete the bully from the lists or block their user name or email address.

- **Help stop cyberbullying.** If your child sees cyberbullying happening to someone else, encourage him or her to try to stop it by not engaging or forwarding anything and by telling the bully to stop. Researchers say that bullying usually stops pretty quickly when peers intervene on behalf of the victim. One way to help stop bullying online is to report it to the site or network where you see it.

- **Recognize the signs of a cyberbully.** Could your kid be the bully? Look for signs of bullying behavior, such as creating mean images of another kid.

- **Keep in mind that you are a model for your children.** Kids learn from adults' gossip and other unkind behavior.

Email, chat, IM, video calling, and texting are fast and convenient ways to communicate.

But the fundamentals—what we say, when we say it, and why we say it—are the same online and off. Common courtesy and common sense are important parts of all communication, regardless of where and how it takes place.

What can you do?

Talk to your kids about online manners.

- **Politeness counts.** You teach your kids to be polite offline; talk to them about being courteous online as well. Texting may seem fast and impersonal, yet courtesies like “pls” and “ty” (for *please* and *thank you*) are common text terms.
- **Tone it down.** Using ALL CAPS, long rows of exclamation points, or large bolded fonts are the online equivalent of yelling. Most people don’t appreciate a rant.
- **“Cc:” and “Reply All:” with care.** Suggest that your kids resist the temptation to send a message to everyone on their contact list.
- **Avoid chain letters.** Most chain letters or emails are nuisances at best and scams at worst. Many contain malware, like viruses or spyware. Ask your kids not to open or forward them.

Set high privacy preferences on your kids' IM and video calling accounts.

Most IM programs allow parents to control whether people on their kids' contact list can see their IM status, including whether they're online. Some IM and email accounts allow parents to determine who can send their kids messages and block anyone not on the list.

Ask your kids who they're in touch with online.

Just as you want to know who your kids' friends are offline, it's a good idea to know who they're talking to online.

Talk to your kids about using strong email passwords and protecting them.

The longer the password, the harder it is to crack. Personal information, your login name, common words, or adjacent keys on the keyboard are not safe passwords. Kids can protect their passwords by not sharing them with anyone, including their friends.

Remind your kids to protect their personal information.

Social Security Number, account numbers, and passwords are examples of information to keep private.

PHISHING

Phishing is when scam artists send text, email, or pop-up messages to get people to share their personal and financial information. Then they use the information to commit identity theft.

Here's how you—and your kids—can avoid a phishing scam:

- **Don't reply** to text, email, or pop-up messages that ask for personal or financial information, and don't click any links in the message. Resist the urge to cut and paste a link from the message into your web browser, too. If you want to check a financial account, for example, type in the web address from your billing statement.
- **Don't give personal information** on the phone in response to a text message. Some scammers send text messages that appear to be from a legitimate business and ask you to call a phone number to update your account or access a "refund." If you give them your information, they use it to run up charges in your name.
- **Be cautious** about opening any attachment or downloading any files from emails you receive, regardless of who sent them. Unexpected files may contain viruses or spyware that the sender doesn't even know are there.
- **Use security software**, and update it regularly.
- **Read your mail**; review credit card and bank account statements as soon as you get them to check for unauthorized charges.
- **Report about phishing email at www.cybercrime.gov.in -** and to the company, bank, or organization impersonated in the phishing email.
- **Get your kids involved** in these activities, too, so they can develop good Internet security habits. Look for "teachable moments"—if you get a phishing message, show it to your kids to help them understand that messages on the Internet aren't always what they seem.

MOBILE PHONES: SOCIALIZING AND COMMUNICATING ON THE GO

Teach your kids to think about safety when using a cell phone.

What age is appropriate for a kid to have a mobile phone? That's something for you and your family to decide. Consider your kid's age, personality, maturity, and your family's circumstances. Is he or she responsible enough to follow rules you or the school sets for phone use?

Many online apps also are on mobile phones—including social networking, blog posting, content uploading, media sharing, and video editing. Teach your kids to think about safety when using a cell phone.

What Can You Do?

Use photo- and video-sharing by phone with care.

Most mobile phones now have cameras and video capability, making it easy for teens to capture and share every moment on the go. These tools can foster creativity, yet they also present issues related to personal reputation and safety. Encourage your teens to think about their privacy, and that of others, before they share photos and videos via cell phone. It's easy to post photos and videos online without the knowledge—let alone the OK—of the photographer or the person in the shot. It could be embarrassing and even unsafe. It's easier to be smart up front about what media they share than to do damage control later on.

Don't stand for mobile bullying.

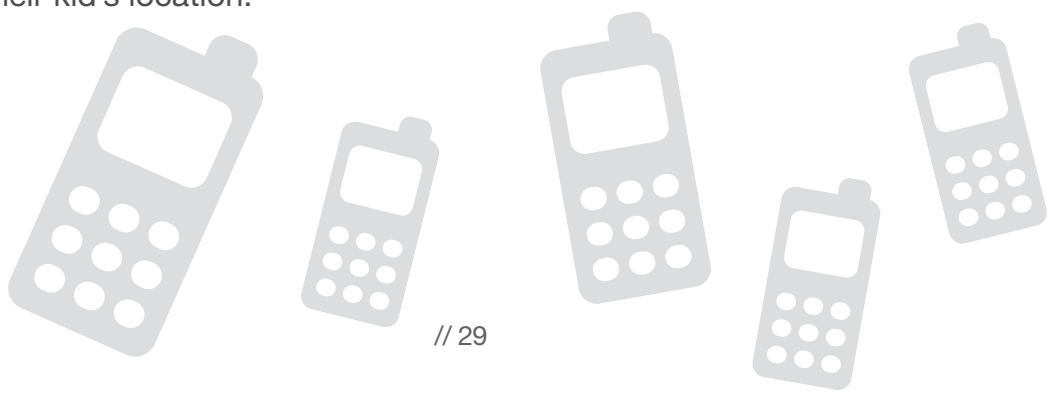
Mobile phones can be used to bully or harass others. Talk to your kids about treating others the same way they want to be treated. The manners and ethics you've taught them apply on phones.

Use good judgment with mobile social networking.

Many social networking sites have a feature that allows users to check their profiles and post comments from their phones, allowing access from anywhere. That means the filters you've installed on your home computer won't limit what kids can do on a phone. If your teens are going mobile with their profiles or blogs, talk to them about using good sense when they're social networking from their phones.

Get familiar with social mapping.

Many mobile phones now have GPS technology installed: Kids with these phones can pinpoint where their friends are—and be pinpointed by their friends. Advise your kids to use these features only with friends they know in person and trust, and why not to broadcast their location to the world, 24-7. In addition, some carriers offer GPS services that let parents map their kid's location.



Decide on the right options and features for your kid's phone.

Both your mobile carrier and the phone itself should give you some choices for privacy settings and child safety controls. Most carriers allow parents to turn off features like web access, texting, or downloading. Some cell phones are made especially for children. They're designed to be easy to use and have features like limited Internet access, minute management, number privacy, and emergency buttons.

Be smart about smartphones.

Many phones include web access. If your children are going to use a phone and you're concerned about what they might find on the Internet, turn off web access or turn on filtering.

Develop cell phone rules.

Talk to your kids about when and where it's appropriate to use their cell phones. You also may want to establish rules for responsible use. Do you allow calls or texting at the dinner table? Do you have rules about cell phone use at night? Should they give you their cell phones while they're doing homework or when they're supposed to be sleeping?

Set an example.

More mobile apps mean additional distractions. It's illegal to drive while texting, surfing, or talking on the phone in many states, but it's dangerous in every state. Set an example for your kids, and talk to them about the dangers of driving while distracted.

SEXTING

Sending or forwarding sexually explicit photos, videos, or messages from a mobile phone is known as "sexting." Tell your kids not to do it. In addition to risking their reputation and their friendships, they could be breaking the law if they create, forward, or even save this kind of message. Teens may be less likely to make a bad choice if they know the consequences.

TEXTING

Any kid with a cell phone probably uses it to send and receive text messages and images. It's similar to using email or IM, and most of the same etiquette and safety rules apply. If your kids are texting, encourage them to:

- respect others. Texting shorthand can lead to misunderstandings. Think about how a text message might be read and understood before sending it.
- ignore text messages from people they don't know.
- learn how to block numbers from their cell phone.
- avoid posting their cell phone number online.
- never provide financial information in response to a text message.

What Can You Do?

The security of your computer can affect the safety of your online experience—and your kid's. Malware is software that monitors or controls your computer use, installs viruses, sends unwanted pop-up ads, redirects your computer to websites you're not looking for, or records your keystrokes. Malware on your computer could allow someone to steal your family's personal information.

Use security software, and update it regularly.

Anti-virus and anti-spyware software scan incoming communications for troublesome files; a firewall blocks communications from unauthorized sources. Look for software that can reverse the damage and that updates automatically.

Keep your operating system and web browser up-to-date, and learn about their security features.

Hackers take advantage of operating system software and browsers that don't have the latest security updates. Increase the security of your computer by changing the built-in security and privacy settings in your operating system or browser. Check the "Tools" or "Options" menus to learn how to upgrade from the default settings.

Watch out for “free” stuff.

Free games, ring tones, or other downloads can hide malware. Tell your kids not to download anything unless they trust the source and they’ve scanned it with security software.

P2P FILE SHARING

Some kids share music, games, or software online. Peer-to-peer (P2P) file-sharing allows people to share these kinds of files through an informal network of computers running the same software. If your kids download copyrighted material, you could get mired in legal issues. Sometimes spyware, malware, or pornography can be hidden in a shared file. Some tips to help your kids share files safely:

- **Install file-sharing software properly.** Activate the proper default settings so that nothing private is shared. By default, almost all P2P file-sharing apps will share downloads in your “save” or “download” folder. That’s why it’s important to set it not to. If you don’t set the defaults properly, other P2P users may access files you never meant to share, including personal documents on your hard drive, like your tax returns or other financial documents.

- **Before your kids open or play any downloaded file, advise them to use security software to scan it.** Make sure the security software is up-to-date and running when the computer is connected to the Internet.

If you're concerned about what your kids—especially elementary school kids—see when they surf the Internet, there are tools to consider. Keep in mind that while parental controls work well for young children, teens who've been online for years probably won't have much trouble working around them or finding other computers to use.

What Can You Do?

Parental control options include:

Filtering and blocking.

These tools limit access to certain sites, words, or images. Some products decide what's filtered; others leave that to parents. Some filters apply to websites; others to email, chat, and IM.

Blocking outgoing content.

This software prevents kids from sharing personal information online, in chat rooms, or via email.

Limiting time.

This software allows you to limit your kid's time online and set the time of day they can access the Internet.

Browsers for kids.

These browsers filter words or images deemed inappropriate for kids.

Kid-oriented search engines.

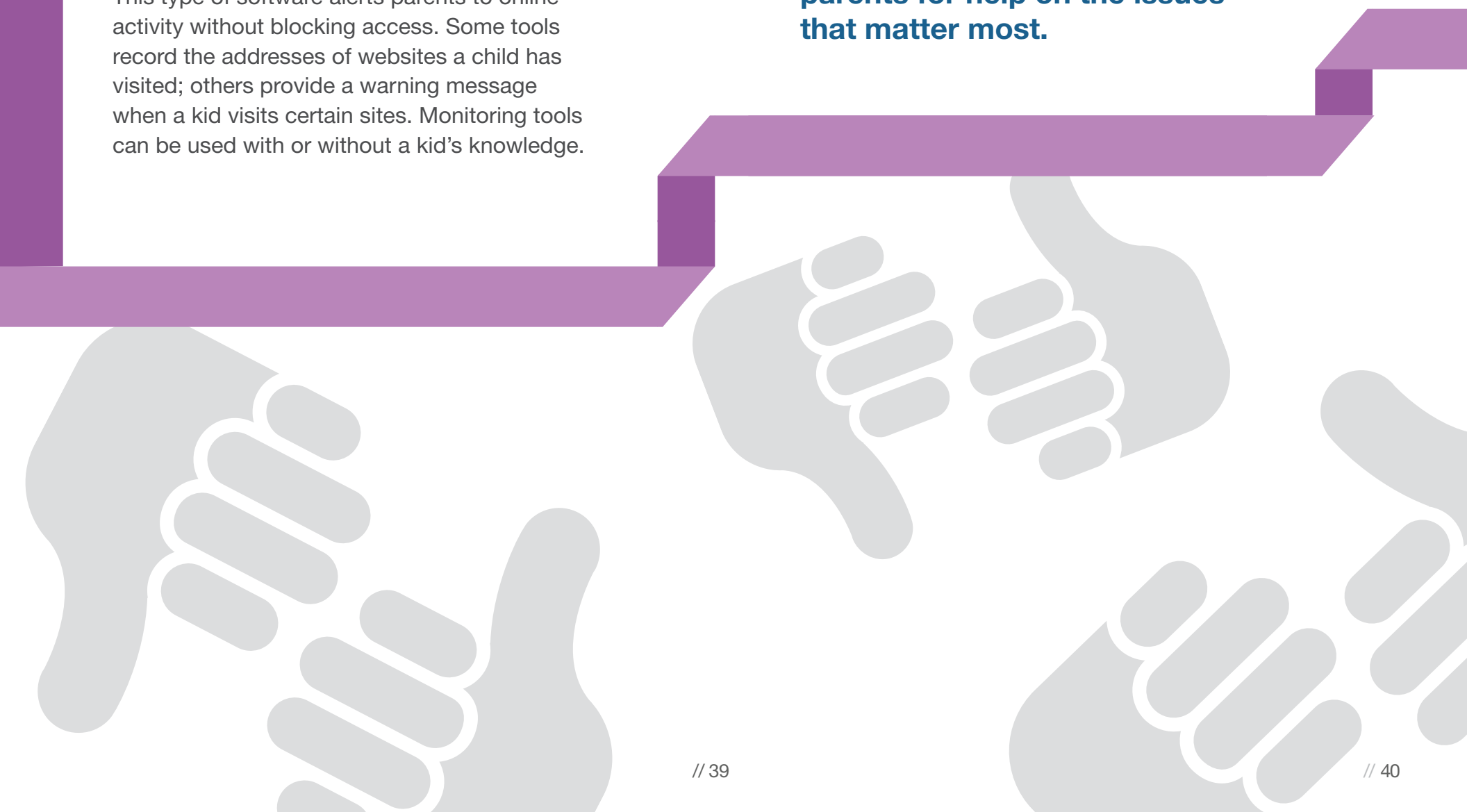
These perform limited searches or screen search results for sites and material appropriate for kids.

Monitoring tools.

This type of software alerts parents to online activity without blocking access. Some tools record the addresses of websites a child has visited; others provide a warning message when a kid visits certain sites. Monitoring tools can be used with or without a kid's knowledge.

The best way to protect your kids online is to talk to them.

When children want important information, most rely on their parents. Children value the opinions of their peers, but tend to rely on their parents for help on the issues that matter most.



GLOSSARY

Avatar – A graphic alter ego you create to use online; can be a 3D character or a simple icon, human or whimsical.

Badware – Bad software; includes viruses and spyware that steal your personal information, send spam, and commit fraud. (See Malware.)

Backing up – Making copies of computer data in case something happens to your machine or operating system and the information is lost.

Blocking software – A program to filter content from the Internet and restrict access to sites or content based on specific criteria.

Blog – Short for "web log," a site where you regularly post personal observations.

Buddy list – A list of people who you can chat with through an IM program.

Chat room – An online space where you can meet and exchange information through messages displayed on the screens of others who are in the "room."

Cyberbullying – Bullying or harassment that takes place online; includes posting embarrassing pictures or unkind comments on a person's profile or sending them via IM or email.

Firewall – Hardware or software that blocks unauthorized communications to or from your computer; helps keep hackers from using your computer to send out your personal information without your permission.

GPS – "Global Positioning System," a global navigation satellite system that is used in cars or phones to determine location and provide directions.

Hacking – Breaking into a computer or network by evading or disabling security measures.

Instant messaging (IM) – Enables two or more people to chat in real time and notifies you when someone on your buddy list is online.

Intellectual property (IP) – Creative products that have commercial value, including copyrighted property like books, photos, and songs.

Limited user account – An online setting that grants someone access to some of the computer's functions and programs, but allows only an administrator to make changes that affect the computer.

Malware – Short for "malicious software"; includes viruses and spyware that steal personal information, send spam, and commit fraud. (See Badware.)

Password – A secret word or phrase used with a user name to grant access to your computer or protect sensitive information online.

Patch – Software downloaded to fix or update a computer program.

Peer-to-peer (P2P) file-sharing – Allows you to share files online—like music, movies, or games—through an informal network of computers running the same sharing software.

PDA – "Personal Digital Assistant"; can be used as a mobile phone, web browser, or portable media player.

Personal information – Data that can be used to identify you, like your name, address, birth date, or Social Security number.

Phishing – When scam artists send spam, pop-ups, or text messages to trick you into disclosing personal, financial, or other sensitive information.

Privacy settings – Controls available on many social networking and other websites that you can set to limit who can access your profile and what information visitors can see.

Profile – A personal page you create on a social networking or other website to share information about yourself and communicate with others.

Security software – Identifies and protects against threats or vulnerabilities that may compromise your computer or your personal information; includes anti-virus and anti-spyware software and firewalls.

Sexting – Sending or forwarding sexually explicit pictures or messages from a mobile phone.

Smart phone – A mobile phone that offers advanced capabilities and features like a web connection and a portable media player.

SMS – "Short Messaging Service"; technology that allows text messages to be sent from one mobile phone to another.

Social networking site – A website that allows you to build a profile and connect with others.

Spyware – Software installed on your computer, without your consent, to monitor or control your computer use.

Texting – Sending short messages from one mobile phone to another.

Tween – A child between 8 and 12 years old.

User name – An alias used with a password to grant access to accounts and websites.

Video calling – Internet services that allow users to communicate using webcams.

Virtual world – A computer-simulated online "place" where people use avatars—graphic characters—to represent themselves.

Virus – Malware that sneaks onto your computer—often through an email attachment—and then makes copies of itself.

Webcam – A video camera that can stream live video on the web; may be built into the computer or purchased separately.

DIRECTORATE OF INFORMATION TECHNOLOGY

GOVERNMENT OF TRIPURA

IT BHAVAN,ITI ROAD, INDRANAGAR,
AGARTALA, WEST TRIPURA - 799006

/ITTripura