FAQs for Internet Safety

Part 1: Manage your privacy and security

1. *How do I secure my passwords online?*

Passwords are the first line of defense against cybercriminals. It is crucial to pick strong passwords that are different for each of your important accounts, and it's a good practice to update your passwords regularly. We recommend the following tips to create strong passwords and keep them secure.

Use a unique password for each of your important accounts like email and online banking
Choosing the same password for each of your online accounts is like using the same key to lock your home, car and office – if a criminal gains access to one, all of them are compromised. For this reason, do not use the same password for an online newsletter as you do for your email or bank account. It may be less convenient, but picking multiple passwords keeps you safer.

Use a long password made up of numbers, letters and symbols
The longer your password is, the harder it is to guess. So make your password long to help keep your information safe. Adding numbers, symbols and mixed-case letters makes it harder for would-be snoops or others to guess or crack your password. Please don't use '123456' or 'password,' and avoid using publicly available information like your phone number in your passwords. It's not very original, and it isn't very safe!

Try using a phrase that only you know
One idea is to think of a phrase that only you know, and make it be related to a particular website to help you remember it. For your email you could start with "My friends Akshay and Sheetal send me a funny email once a day" and then use numbers and letters to recreate it. "MfA&Ssmafe1ad" is a password with lots of variations. Then repeat this process for other sites.

Set up your password recovery options and keep them up-to-date
If you forget your password or get locked out, you need a way to get back into your account. Many services will send an email to you at a recovery email address if you need to reset your password, so make sure your recovery email address is up-to-date and an account you can still access.

Sometimes you can also add a phone number to your profile to receive a code to reset your password via text message. Having a mobile phone number on your account is one of the easiest and most reliable ways to help keep your account safe.

Your mobile phone is a more secure identification method than your recovery email address or a security question because, unlike the other two, you have physical possession of your mobile phone.

However, if you can’t or don’t want to add a phone number to your account, many websites may ask you to choose a question to verify your identity in case you forget your password. If the service you’re using allows you to create your own question, try to come up with a question that has an answer only you would know and isn’t something that you’ve posted about publicly or shared on social media.

Try to find a way to make your answer unique but memorable – you can do this by using the tip above – so that even if someone guesses the answer, they won’t know how to enter it properly. This answer is very important for you to remember – if you forget it you may never be able to get back into your account.

2. *How can I keep my email account safe?*

Make sure your email is not getting forwarded or shared unless you want it to be

Check forwarding and delegation email settings that grant others access to your account to make sure your email is being directed properly.

If you forget your password, you need a way to get back into your account

You may receive a recovery email address if you need to reset your password, so make sure that recovery email address is up-to-date and is an account you can access. You can also add a phone number to email account to receive a code to reset your password via text message.

Having a mobile phone number on your account is one of the easiest and most reliable ways to help keep your account safe. Your mobile phone is a more secure identification method than your recovery email address or a security question because, unlike the other two, you have physical possession of your mobile phone.

Check for unusual access or activity in your account

Regularly review your account for unfamiliar or suspicious activity. Click on the “details” link at the very bottom of the page to find the most recent IP addresses your mail was accessed from, and their associated locations. If you see suspicious account activity, immediately change your password and logout of your account.

When you’re signing into your email, you should check to make sure the web address begins with https:// (and not just “http://”). This signals that your connection to the website is encrypted and more resistant to snooping or tampering.

3. *How do I keep my device safe?*

If you’re getting redirected or seeing pop-up ads, unwanted toolbars, or strange search results, your computer may have malware. Malware is software designed to damage and take control of your computer.

Signs you might have malware

If you have malware on your computer, you may see these symptoms:

- Pop-up ads

- Unwanted toolbars
- Inappropriate search results or ads
- Being redirected from a site you’re trying to visit
- Getting results from the wrong search engine

Remove malware from your computer or browser

Check your computer for programs you don’t recognize, and uninstall them.

Use the browser reset feature to undo the changes you see and get your settings back to normal. Use antivirus software to detect and remove malware from your computer.

Keep your browser and operating system up to date.

Most operating systems will let you know you when it’s time to upgrade – don’t ignore these messages. Old versions of software can sometimes have security problems that criminals can use to easily get to your data.

Keep an eye on what you click and download.

Without meaning to, you may click a link that installs malware on your computer. To keep your computer safe, only click links and downloads from sites that you trust. Don’t open any unknown file types, or download programs from pop-ups that appear in your browser.

Also pay attention to the fine print details and any auto-checked checkboxes when downloading. Make sure that you understand what programs are being installed.

When in doubt, throw it out

Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it’s best to delete it.

Think before you act

Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.

Don’t get caught by phishers

Phishing is when you get an email or a social media message that looks like it’s coming from a legitimate place such as a bank or social networking site. If you click on a link in the message, you're taken to a website that looks legitimate but could be run by criminals trying to trick you to sign in with your username and password so they can capture that information. Your best bet is not to click on the link but rather type the web address into your browser window and go to the site that way.

Be careful where you click

Fake or malicious websites (or legitimate ones that have been hacked by criminals) can jeopardize your device and the data on it. Sometimes called “drive-by downloads,” these sites can install malicious software onto your device if you visit them or perhaps click on the sites’ links. Often they look legitimate, offer something too good to be true or contain some type of inappropriate or illegal content.

Part 2: Protection from online scams and threats

4. What are the steps I can take to prevent identity theft online?

Knowing the common tricks that criminals employ will help you protect yourself from online fraud and identity theft. Here are a few simple tips:

- Don’t reply if you see a suspicious email, an instant message or a web-page asking for your personal or financial information.
- Never enter your password if you’ve arrived at a site by following a link in an email or a chat that you don’t trust.
- Don’t send your password via email, and don’t share it with others.
- If you see a message from someone you know but it doesn’t seem like it’s from them, their account might have been compromised by a cybercriminal who is trying to get money or information from you. Be careful how you respond, or don’t respond at all. Common tactics include asking you to urgently send them money, claiming to be stranded in another country or saying that their phone has been stolen so they cannot be called. The message might also tell you to click on a link to see a picture, an article or a video, which actually leads you to a site that might steal your information.

5. How can I stay safe from online scams?

The web can be a great place, but not everyone online has good intentions. Here are three simple ways to avoid scammers and stay safe on the web.

Beware of strangers bearing gifts.
If someone tells you you’re a winner and asks you to fill out a form with your personal information, don’t be tempted to start filling it out. Even if you don’t hit the Submit button, you might still be sending your information to scammers if you start putting your data into their forms.

Do your research.
When shopping online, research the seller and be wary of suspiciously low prices, just as you would if you were buying something at a local store. Scrutinize online deals that seem too good to be true. No one wants to get tricked into buying fake goods.

When in doubt, play it safe.
Do you just have a bad feeling about an ad or an offer? Trust your gut! Click on ads or buy products only from sites that are safe, reviewed and trusted.

Part 3: Family Safety Basics

6. *As parents, how can we ensure our children are safe online?*

For busy parents, here are some quick suggestions for how to help keep your family safe online:

Protect passwords

Help your family learn how to set secure passwords online. Remind your family not to give out their passwords, except maybe to trusted adults, such as a parent. Make sure they make a habit of signing out of their online accounts when they are on public computers at school, in a café or at the library.

Use privacy settings and sharing controls.

Many sites are available for sharing thoughts, photos, videos, status updates and more. Many of these services offer privacy settings and controls that help you decide who can see your content before you post it. Talk with your family about what they should and shouldn't share publicly. Help them respect the privacy of others by keeping personal details about family and friends private, and by not identifying people by name in publicly shared content.

Check age restrictions

Many online services have age limits restricting who can use their services. For example, you may have to meet age requirements to have a specific online account, and some products are restricted to users 18 and older. Always check a website's terms of use before allowing your child to sign up for an account, and be clear with your children if you have family rules about which sites and services they can use.

Teach your family to communicate responsibly

Here's a good rule of thumb: If you wouldn't say it to someone's face, don't text it, email it, instant message it or post it as a comment on someone's page. Talk about how what you say online might make other people feel, and come up with family guidelines about what kind of communication is appropriate.

Talk to other adults and experts

Open the conversation to your friends, extended family, teachers, coaches and counselors. Other parents and professionals who work with children can be a great resource to help you decide what feels right for your family, especially if you're dealing with an area of technology that you are unfamiliar with.

Protect your computer and identity

Use antivirus software and update it regularly. Talk with your family about the types of personal information—such as a Social Security number, a phone number or a home address—that should not be posted online. Teach your family not to accept files or to open email attachments from unknown people.

Keep it going

Staying safe isn't a one-time thing—technology evolves, and so will the needs of your family. Make sure you keep up an ongoing dialogue. Re-establish your family's ground rules, check in on everyone's progress and set aside time to talk at regular intervals. The following tips from our partners address common issues that parents are concerned about.

7. ***How do I educate my children about cyber bullying?***

Cyber bullying is usually not a one-time communication, unless it involves a death threat or a credible threat of serious bodily harm. Kids usually know it when they see it, while parents may be more worried about the lewd language used by the kids than the hurtful effect of rude and embarrassing posts.

It’s important to help children understand what bullying is so they know what to do if they are being bullied. Bullying goes beyond meanness or drama -- it’s intended to harm and is a repeated threatening or aggressive behavior. It is imperative to talk to kids about the difference. Following are a few pointers that one should keep in mind while talking to their children.

Make sure kids know what to do and how to respond if they are being bullied.
Children should be encouraged to not react or retaliate and instead talk to a parent, teacher, or other trusted adult and have them help resolve the problem.

Importance of being an upstander and not a bystander
While the majority of kids don’t engage in bullying, some will be witness to it. Talk to kids about the importance of being an upstander -- not a bystander -- when it comes to bullying at school or online. Emphasize the importance of dignity, empathy, and respecting differences, and encourage them to speak up in difficult situations.

Teach them to not share passwords.
A common form of cyberbullying is when kids log in to another child's email or social networking account and send fake messages or post embarrassing comments. Kids can protect themselves from this by learning early on that passwords are private and should only be shared with their parents.

Teach responsible, respectful online behavior.
Draft a code of behavior that you expect your kid to follow (and check in occasionally to make sure.) The code should include standing up for anyone that they witness being bullied, because peers standing up for peers is one of the most effective ways to thwart a bully.