Parent's Guide to Online Safety

Educate your kids

It's important that you educate your kids on security online so they are aware of what to look out for and how to stay safe online. You must prepare them for the fact that there are threats online. Encourage them to be vigilant and be involved in their online activities as much as you can.

Kids Online Safety Checklist

- Use a shared email address for younger children so you can see what emails they are getting.
- Children must be 13+ to register on social media.
- Make sure correct birthdate is used in setting up their social media accounts so the correct filters will be applied.
- Parents should have an account on the same platforms so you can guide them. Don't comment on their posts, just keep an eye on their activity.
- Use the parental controls that come with your devices.
- Have the password to your kid's online accounts and mobile devices.
- For tighter controls you can purchase additional software e.g Net Nanny, Kapersky Safe Kids, Qustodio
- Learn the lingo and stay up to date with new technology. Check out www.safekids.com and www.netnanny.com for parent's resources
- Apply the tips for general online safety to your accounts as well as your kids will learn from you.

SafeKids.com Kids' Rules for Online Safety

1. I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.
2. I will tell my parents right away if I come across any information that makes me feel uncomfortable.
3. I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.
4. I will never send a person my picture or anything else without first checking with my parents.
5. I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the service provider.
6. I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.
7. I will not give out my Internet password to anyone (even my best friends) other than my parents.
8. I will check with my parents before downloading or installing software or doing anything that could possibly hurt our computer or jeopardize my family's privacy
9. I will be a good online citizen and not do anything that hurts other people or is against the law.
10. I will help my parents understand how to have fun and learn things online and teach them things about the Internet, computers and other technology.

General Tips for Online Safety

1. Use strong passwords

Strong passwords consist of letters, numbers and symbols. And are between 8 -12 characters. Don’t use your birthday or other easy to guess words as your password. Hacking bots can try millions of word combinations to guess your password so you need to be truly random.

You can use a password manager like Lastpass or 1Password to keep track of your passwords. You only have to remember the one master password for your password manager and it will keep the rest of your passwords secure for you.

Don’t use the same passwords on different sites. If one site is compromised it won’t affect your other online accounts if you have different passwords.

2. Use 2 factor authentication

Implement 2 factor authentication where available. This means that when you log into a site with your username and password, the site then sends you a code by sms to the phone number you provided. You’ll have to enter the code to complete your log in.

If someone gets a hold your password, chances are they also don’t have your phone so this adds an extra layer of protection.

A lot of financial institutions use this method by default. You can turn this on for email services, social media sites and other online services that you use.

3. Use firewalls and antivirus

Your computer comes with an operating system which includes a firewall. This provides a level of protection against cyber attacks. For business computers, consider installing an additional firewall for added protection.

You should also install updates to your operating system when provided by your service providers. They discover new threats all the time and write updates to keep your computer safe from those threats. You are only protected if you install those updates.

Install an antivirus on your computer and keep them up to date. Even the free versions provide you strong protection if you are also vigilant about protecting your computer from risks.

4. Be careful with flash drives

Flash drives are an easy way to spread malware. You don't know how diligent other people are with keeping their computers safe from computer viruses. It's better to be safe than sorry.

When asked to provide a file on a flash drive, use a new one that you have brought yourself and don't take it back after it's been used on another person's device.

The best solution is to send documents by email or share online using file sharing services like WeTransfer, Dropbox, Google drive, etc.

5. Protect your Wifi

Protect your wifi router by changing the default settings.

Change the default admin user name and password. Also change the wifi network password from the default that comes with your router.

Use strong passwords that consist of numbers, letters and symbols. And remember to change your passwords often.

All routers come with instructions on how to access the admin interface. You should change this before you start to use the router to access the internet.

6. Be vigilant

Don't open attachments or click on links in suspicious emails. If the email if from somebody you don't know, delete it immediately. If you know the sender, call them and check they actually sent you that file before you click on the attachment.

Links in email can also send you to phishing sites that will trick you into providing your personal information. Don't click on links asking you to provide personal information in an email.

Your bank will never ask you to click on a link in an email to verify your account. Even if it looks like it might be a genuine request, type in the url yourself instead of clicking on the link.

Pay attention to the url in the address bar when you visit a website. If the url looks even the slightest bit different from what you're used to, get out of there fast and phone your service provider to confirm if they have made any changes.

Don't shop on a site where the url doesn't show https. The https protocol shows that the site has implemented protocols to keep your data secure.

7. Beware free wifi

Free wifi networks are not secure. Assume that everything you do on there can be accessed by anyone who wants to steal your data.

Don't log in to your company server or access your financial records using these types of networks.