## Online safety

**Being safe online is very similar to when an adult drives a car-you may have common sense and pay attention to potential dangers but you can't always predict what others are going to do.**

## Scams

**Some email scams can be identified by:**
1. Sentences that don't make sense
2. Unusual URL addresses
3. Terminology, spelling and grammar that is incorrect

Most scammers do not know how much money someone has. Often scammers will send the emails to as many people as possible, hoping to trick at least one person.
- A small amount of money quickly adds up, if many people are tricked.
- It is important to maintain a good security program or antivirus software program on your devices
- Read about the latest scams and report scams to Scamwatch.
- Cybercrimes such as attacks on computer systems, identity theft and email spam and phishing can be reported to the ACORN.

## Scam statistics

- From January 2015-December 2015, over 105,000 scams were reported with $84.9 million lost.
- Don't be embarrassed if you are scammed– it is important to report any incidents.
- The top type of scam is dating and romance. Others then include:
  1. Investments scheme
  2. Inheritance scams
- Many scams are get rich quick schemes and always remember if it is too good to be true, then it probably is!
- Scams in 2015 were mainly delivered by phone and then by email.

## Privacy

Think before you reveal personal information about yourself or your friends. Ways that you may give away Personal information may include:

- Tagging photos
- Posting photos with details identifying the location of your house and school
- Posting holiday photos that show you are not home
- Mentioning where you or someone is located
- Completing 'How well do you know your friends' quizzes
- Forwarding chain mail emails
- Saying yes to address sharing on apps
- Asking for information publicly – such as phone numbers

### Know how to report problems

- Many apps have reporting features. Ask for help if you can't find where to report.
- See the eSafety webpage below for details to report on popular apps and sites.

## Security trends

- Banks may use Emoji passwords in the future– the reason is that 44 emojis allow more combinations than a standard PIN.
- Two factor or two step authentication allows a user to log in to a service or device using a second piece of information in addition to a password. Often a short code sent to the user's mobile phone.

### Security terms

**Scams:** are dishonest schemes that seek to take advantage of people to gain a benefits such as money, or access to personal details.

**Malware:** tricks you into installing software that allows scammers to access your files and track what you are doing.

**Ransomware:** is a type of malware that blocks or limits access to your computer or files, and demands a ransom be paid to the scammer for them to be unlocked.