

# Cyber Crime

How to Stay Safe Online



Created by the Hallam Fields Junior  
School i-vengers

 i-vengers

Learn to be a hero.

# How to stay safe and avoid Cyber Crime

We all want to continue being informed and inspired by the wonderful capabilities of the internet. But we also need to be able to protect ourselves against the growing amount of cyber crime. Knowing what is fact, understanding what dangers exist and taking appropriate steps can go a long way towards

protecting yourself and your family.

The i-vengers have compiled some top online safety tips which can help to keep you all safe...

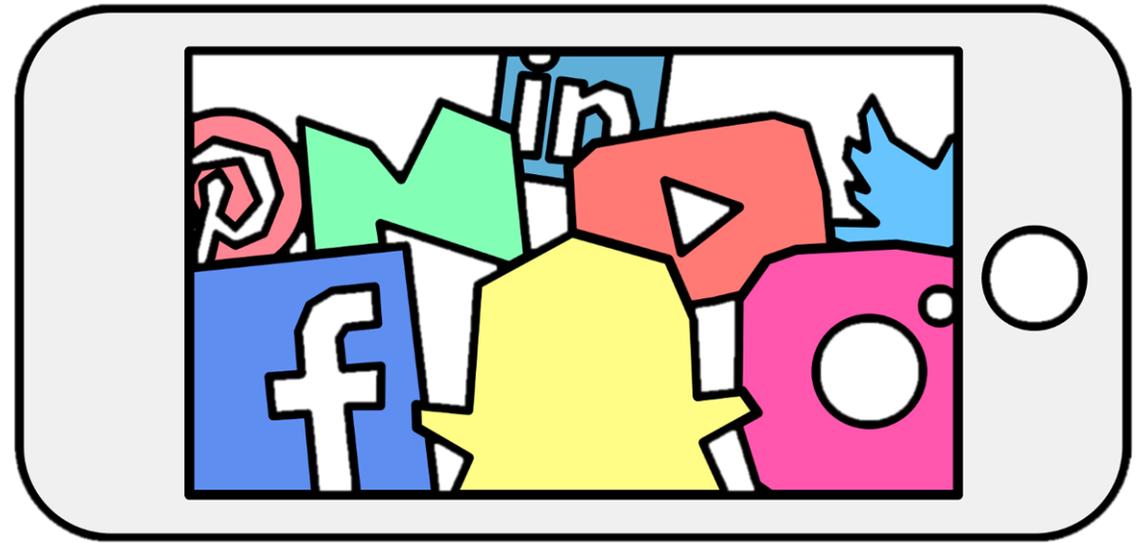
# 1. Stop Phishing Bait



Phishing messages are untargeted mass messages asking for sensitive information (e.g. usernames, passwords, bank details) or encouraging people to visit a fake website. It's safest to learn the warning signs of phishing and increase your awareness.

Too good to be true? Spelling or punctuation errors? Odd sense of urgency? These are all red flags. Don't click on links or follow demands: if you're unsure, tell a trusted adult who may be able to help.

## 2. Don't over share



Are you sharing too much on social media? Do you post things about your private life, upload images of your home, or discuss your friendships online? Criminals could gather this information and may try to use it for identity theft or other offences such as fraud. To combat this, ensure your privacy settings mean you are only sharing information with family and close friends.

# 3. Strong Passwords



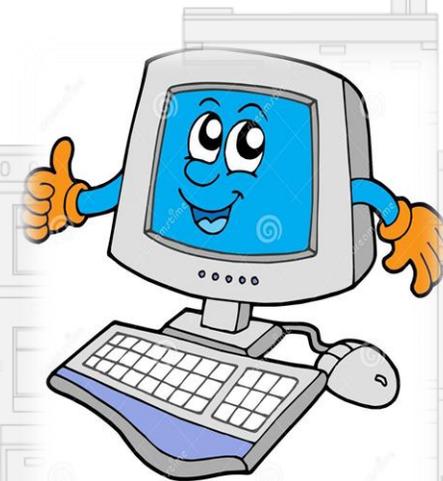
Weak passwords make it faster and easier for someone to gain access to your online accounts or get control of your device – giving them a route to your personal information.



Make sure to never use the same password on different accounts. Try to use three random words for a stronger password e.g. trianglefishcastle

# 4. Stay Updated

People often put off installing updates to apps or software because they don't feel it's necessary or that it can be time consuming. But updates help protect users from new viruses which could infect your device. You can usually set updates for them to run automatically – Ensure updates are installed as soon as possible after you're notified they're available.



## 5. Be wary of public Wi-Fi



It can be common for people to use free public wi-fi when they are out and about, but very often the network is not secure. It is possible that someone could access your personal information without you even realizing. Try to avoid using public wi-fi if you can and use your mobile data if possible.

# Remember to follow the SMART rules to stay safe online;

**S – Safe** – (Don't give strangers personal information)

**M – Meet** (Never arrange to meet with strangers)

**A – Accept** (Never accept online messages from strangers, these could contain a virus)

**R – Reliable** (Not everything that you read on the internet is true)

**T – Tell** (If anything upsets you on the internet always tell a trusted adult)

**The online world needs heroes...  
Heroes like you!**



**We are an**

**i-vengers**

**school**