creative SUPPORT

The internet is a great place to look up information, comunicate with friends and family, online shop or simply keep entertained. It makes everyday activities available anytime and anywhere. Unfortunately, there are things you may need to be aware of, such as online scams, privacy issues and cyberbullying. In this booklet, we have put together some top tips to help keep yourself and others safe online.

SAFETY AND PRIVACY

- Install up-to-date anti-virus software on your computer. Most computers come with this software installed and will remind you when it needs updating. Find out more here: https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product
- Create a complex password that includes both capital and lowercase letters, numbers and special characters such as question marks, exclamation marks and asterisks. Make sure you choose something only you will know and try to not use the same password for everything.
- Never give out your password and avoid writing it down.
- When shopping or banking online, make sure the web address starts with 'https' instead of just 'http'. The 'S' indicates the website is secure and your data will be protected.
- Add a screen lock onto your smartphone or tablet. This means that if someone gets hold of your device, they can't access the data on it without entering your password. You can do this in your settings. Some phones now have face recognition or finger print access, which is even easier!
- Make sure you update the app's on your phone or tablet whenever a new version is released, your device will notify you of this in the app store. App updates contain vital security to help protect your devices from cyber criminals.

THINK BEFORE YOU SHARE!

Although social media is a fantastic way to share memories and contact friends, think before you share! Your posts, photos, comments and any other shared material can form a picture of yourself to others. Once you have shared something, it is there for all to see! Even on app's such as Snapchat or Instagram Stories where messages and images are timed. Someone can screenshot your posts without your consent - avoid sharing anything personal or potentially embarrassing!

EMAILS

- If you are unsure who an email is from, don't open it. It may contain a virus.
- Be careful about where you log-in to your emails,. If you are on a public computer such as one in a library, make sure you log out correctly before leaving.
- Block and delete any unwanted emails. You can report the sender to spam@uce.gov if you think it looks suspicious.

VIDEO CALLING

Video calling is a great way to chat to friends and family if you are unable to see them in person. If you are using app's such as Zoom or Houseparty, here are three tips on staying safe:

1. Only share your chat link to friends or family - don't share it on Social Media.

2. Create a password for your chat and only give it to friends or family who you want to join the call.

3. Leave the chat if you feel uncomfortable or if a stranger joins.

Other great ways to communicate with friends or family, is to use the video call function on your phone or tablet such as FaceTime or WhatsApp video chat. This way, you know that the call is secure and there is no chance of a stranger joining!

TIKTOK SAFETY

TikTok is the latest social media trend which mostly shares videos of people lip-synching to popular songs - here's how to make your account private: Go to your profile page and select the three-dot icon in the top-right corner. Select Privacy and Safety. There, click the switch for "Private Account." You can also select who can send you comments and direct messages, who can do a duet with you and who can view your account.

SOCIAL MEDIA SAFETY

- Only add or accept friend requests from people you know, or have met in person.
- Be wary of messages from strangers and don't send photos or personal information to people you don't know.
- Ensure you have a high security privacy setting on all platforms.
- If you feel uneasy about posts or messages from someone report

CHANGING YOUR PRIVACY SETTINGS...

For Twitter

1. Find settings on the left control bar on the home page (or top left on a phone)
2. Select 'Privacy and Safety' and next to 'Protect Your Tweets' tick the box.

For Facebook

1. Find settings at the top right corner on the home page (or bottom right on a phone)
2. Select 'Privacy' and change 'Who can see you future posts' to 'Friends'.

For Instagram

1. Find settings at the top right corner on the home page.
2. Select 'Privacy' and on 'Account Privacy' select 'Private Account'.

IF YOU FEEL UNSURE ABOUT STAYING SAFE ONLINE, ASK FOR HELP!

Friends, family or support workers will be more than happy to help you learn how to stay safe online.

CONTACT US:

0161 236 0829

marketing@creativesupport.co.uk