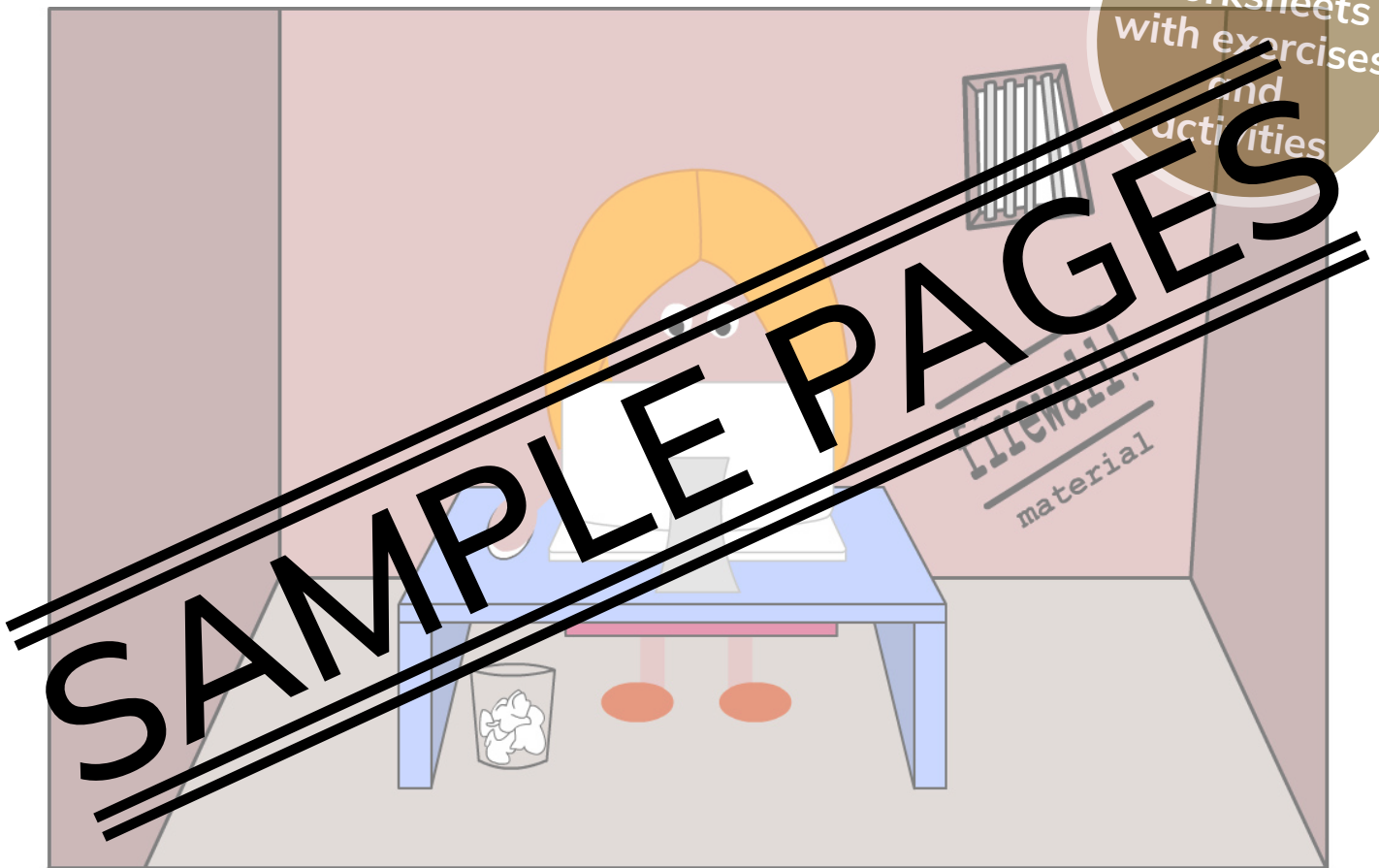


PERSONAL SAFETY IN CYBERSPACE

Includes
worksheets
with exercises
and
activities



Contents

7	Introduction
10	History of Computing and Malware
12	How the Internet and the World Wide Web Began
15	Technical Dangers in Cyberspace
15	Viruses
15	Worms
15	Trojan Horses
16	Page-Jacking
16	Adware
16	Spyware
16	Spam
17	Email Scams
17	Email Hoaxes
17	Phishing
17	SPIM
18	Problems with Email
18	More About Spam
19	More About Email Scams
20	More About Email Hoaxes

21	More About Phishing
23	Malware
23	More About Spyware
24	Cookies
25	More About Adware
26	How to Protect Yourself from Malware
27	Browser Hijacking
28	How to Avoid Your Browser Being Hijacked
30	Instant Messaging
30	What is Instant Messaging?
32	The Threat from Malware on IM
33	Social Media
34	Social Media History
34	Facebook
34	X (Formerly Twitter)
34	LinkedIn
35	Why People Use Social Media
35	The Sinister Side to Social Media
36	People Are Not Always What They Seem
37	Photographs on the Internet
38	Identity Theft
38	Chat Rooms and Forums
39	Online Safety
40	Cyberbullying

42	What to Do About Cyberbullying
43	Online Grooming
43	What is Grooming?
43	Grooming Children and Young People
44	Grooming Adults
44	Sexual Grooming
45	How Grooming Develops
46	Signs of Grooming
48	Sexting
48	How to Tackle Grooming
50	The Future of Information Technology
52	WORKSHEET 1
53	WORKSHEET 2
53	<i>Dangers on the Internet</i>
54	WORKSHEET 3
55	WORKSHEET 4
56	WORKSHEET 5
57	WORKSHEET 6
59	WORKSHEET 7
60	WORKSHEET 8
61	WORKSHEET 9
62	WORKSHEET 10
63	WORKSHEET 11
63	<i>Fill in the Gaps</i>

64	WORKSHEET 12
64	<i>The Threat from Malware on IM</i>
65	WORKSHEET 13
66	WORKSHEET 14
67	WORKSHEET 15
68	WORKSHEET 16
69	WORKSHEET 17
70	WORKSHEET 18
71	WORKSHEET 19
72	WORKSHEET 20
73	Useful Online Information

Introduction

Young people today are immersed in technology. Anyone under the age of 30 will find it difficult to imagine a world without mobile phones, laptops, text messaging, chat rooms, smart phones, online forums, podcasts etc.

The growth in social networking websites and apps such as Facebook, Twitter, YouTube and Instagram is also staggering and they continue to expand at a phenomenal rate. They enable users to ‘meet’ people throughout the world—never before has communication on a worldwide scale been so easy and accessible.

Give out **WORKSHEET 1**. How many people have a smart phone, laptop, tablet or home computer? Ask the class for a show of hands and ask the group to fill in the first table on the worksheet.

How many people have done or participated in the following?

- Downloaded a podcast
- Downloaded music
- Downloaded videos/films
- Used a chat room
- Posted to a forum
- Posted on X
- Joined a networking website such as Facebook or Snapchat
- Uploaded a video to YouTube
- Used Skype or Zoom to communicate with someone
- Joined a virtual reality world or role playing game such as Second Life or Minecraft

Ask for a show of hands and tell the group to fill in the second table on the worksheet.

History of Computing and Malware

In the past, computers were large, expensive machines called mainframes which cost millions of pounds and were used by large organisations.

- Ask the group to conduct research into the first computers.
- Can they find any information or pictures of old, mainframe computers?
- How do these computers compare with the PCs we use now?

With the invention of the micro-chip, computers became smaller and less expensive and small businesses could afford them. Eventually many people were able to afford a computer in their own home. When IBM launched its personal computer in 1981, the personal computer industry exploded. New computing languages were developed and computers became widespread in homes and businesses throughout the world.

Computers and the internet have opened up a whole new world of communication and the possibilities are endless. For example, when we think of the term ‘cyberspace’, we usually imagine a huge, virtual ‘world’ of connected computers enabling communities to spring up on a local, national and international level. We no longer have to be sitting at a desk to use the web—we can access the internet with various wireless equipment such as smart phones, laptops and tablet computers.

However, all is not well in cyberspace. This is because there are people using the internet who want to cause chaos by spreading malicious software. To make matters worse, most of the world’s computers, ranging from desktops to mobile phone software, run the same operating system or software which is developed by the same organisation. This has made it easier for clever criminals to create malware (malicious software).

Technical Dangers in Cyberspace

Before we examine some of the dangers that lurk in cyberspace in more detail, here is a brief overview of some of the problems you may encounter when using IT systems and devices.

Viruses

A computer virus is a program which spreads by attaching itself to software or documents. It can easily be transferred from an infected computer to other computers by email, USB drive, via a network or the internet. Once activated, the virus can damage programs, delete files, or even reformat the hard drive.

Worms

A worm makes copies of itself and spreads across networks and into other PCs. Unlike viruses, a worm does not need to attach itself to other software. When a computer is booted up (switched on), the worm will also be activated. Worms usually infect a PC via a network through an open port. A port is a specific place where a PC is connected to a piece of apparatus. It can be a physical piece such as a socket to attach scanners or printers, or it can be a virtual point where data is transferred, such as the internet.

Trojan Horses

A Trojan horse or Trojan is a piece of harmful computer code which is hidden in a computer program or other file. It can trick computer users into thinking it is something useful or interesting which needs to be installed. A hacker may put a Trojan into a piece of software, or the Trojan may be hidden by an image or computer game. Trojan horses are attached to the host software and do not infect other pieces of software in the way that viruses do.

Browser Hijacking

It is getting more common for people to go to a favourite website only to find that they are locked into a pornography site or another website that they didn't want to visit. This is often followed by a stream of pop-up pages without menu-bars or other controls which makes it hard for the user to close the site. If you try to close a page, another one opens up in its place. Most people do not know how to stop this from happening and it can be very embarrassing and upsetting. It is more serious if young people are using the internet as the images that appear can be inappropriate and even harmful.

This is called browser hijacking and it is a big problem. It used to be more common if the user was using Microsoft Internet Explorer simply because this was the most widely used browser in the past, although browser hijacking can affect any browser. Many browsers need patches to stop malicious websites changing the settings within a program without the user's knowledge or permission. Sometimes internet shortcuts are added to your favourites folder without your knowledge. The purpose of hijacking is to force you to visit a website which you would not normally visit. This is done to increase traffic figures for advertising purposes or to sell goods or services.



Social Media

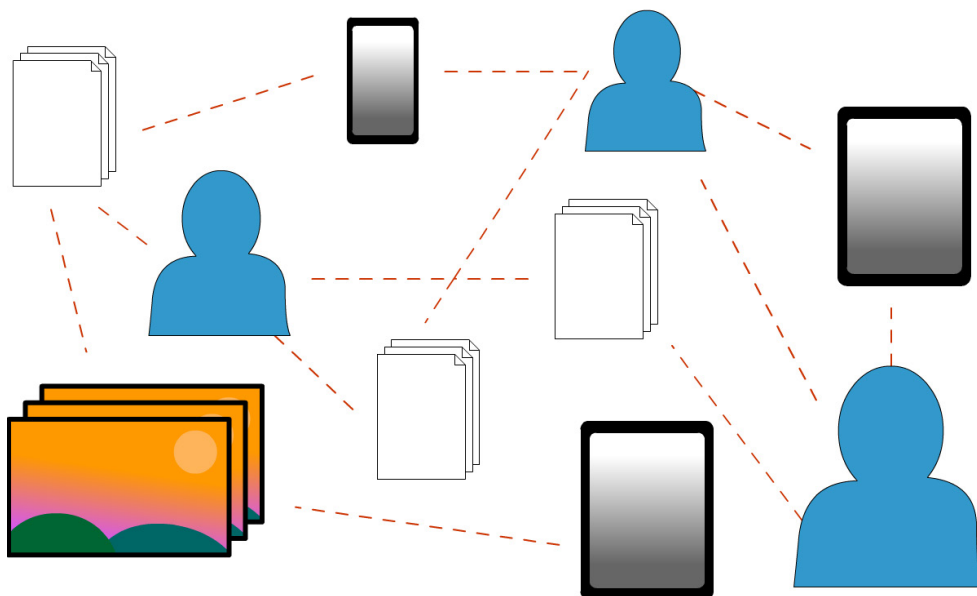
Chat apps and online social networking are now key parts of millions of young people's lives. They use social media sites such as Facebook, Snapchat, Twitter, Instagram, Reddit, Tumblr, YouTube and Qzone every day to keep in touch with their family, friends and peers.

Give out **WORKSHEET 13** and ask the group to fill in the first table and write what they know about each site. Which one do they use/prefer?

Now ask them to fill in the second table giving their reasons for using networking sites. Tell them to explain their reasons in the column below. Does anyone feel pressured by their peers to participate?

Does anyone in the group not use social media? Ask for a show of hands. Ask if they would like to tell the class why they do not use such sites or apps.

Social apps and sites allow users to write their own personal profiles and blogs, join groups and upload photos, music and videos. Friends can communicate in various ways. The networks grow as more people join and start to form groups which share interests and activities.



Online Grooming

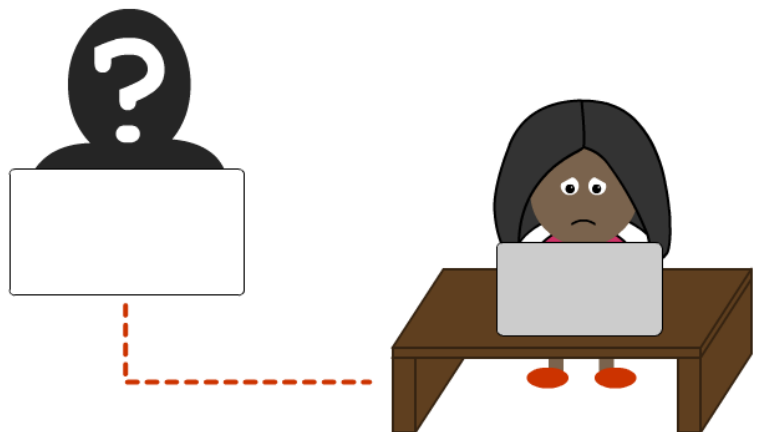
We hear a lot about grooming in the news today, and there have been a number of news reports about cases of grooming that have taken place online and offline. But what exactly is grooming, how is it carried out online, and how can we protect ourselves and our young ones from online predators?

What is Grooming?

Grooming occurs when someone uses lies and deceit to build an emotional relationship with another individual. Online grooming takes place via the internet on a computer, tablet or mobile phone. Very often the groomer will spin a complex web of lies concerning their life and their personal circumstances to elicit pity and/or to encourage the other person to trust them and divulge personal information. They will also use their 'friendship' to coerce the person into doing things they would never normally do.

Grooming Children and Young People

When the target is a child or young person, the groomer may pretend to be a young person too, when they are in fact an adult (although this is not always the case). Their aim is to develop trust and to encourage the young person to open up and share details of their personal and



family lives. They quickly home in on any detail that the young person gives concerning their interests or hobbies. Then, as if by magic, they will discover that they share the very same interests too, and this cements the friendship even more.

WORKSHEET 1

IT and Communication Equipment

Equipment	Mobile Phone	Tablet	Laptop	Home PC	Smart Phone	MP3 Player
TOTAL						

Online Services

Have you used...	Podcasts	Download Music	Download Videos	Chat Rooms	Forums	Social Networking
TOTAL						

Can you think of other surveys to conduct with your friends to try to find out how they use IT?

WORKSHEET 12

The Threat from Malware on IM

Thinking about the things you have learned so far, can you think of at least five things you can do to protect yourself from IM malware?

1.

2.

3.

4.

5.