Quick Guide

Online Safety

Online Safety

The aim of this quick guide is to introduce you to online safety.

By the end of this quick guide, you should be able to:

- State ways in which you can stay safe online
- Identify ways in which you can protect your personal and sensitive data

Online Safety Subjects

Online safety covers a wide range of subjects, including:

- Online behaviour – how to behave safely and with respect for others
- Protecting your online reputation
- How to use social networking safely
- Understanding the reliability and validity of online information
- Data security – keeping your personal information safe
- Being aware of viruses and hacking
- Knowing what to do if anything bad happens

t2 Commitment

Information and communications technology (ICT) is part of our lives.

We use it every day for study, work, entertainment, shopping and getting in touch with our family and friends.

Most of us know how to safeguard ourselves and others at work and at home but in a world which relies increasingly on technology, it pays to know how to keep yourself safe online as well.

t2 takes its responsibility to learners seriously and that includes online safety. t2 is committed to protecting and educating staff and learners in their use of technology as well as making sure that we intervene and support you where appropriate.

Social Networking Sites

Social networking sites like Instagram, Twitter, Facebook, Pinterest, WhatsApp and Tik Tok are becoming more popular all the time; they are used by people of all ages and backgrounds and you have no way of knowing whether the person behind the profile is really who they say they are.

Ask yourself if you would be happy to put a giant photograph of your family on the side of your house. When you upload something to Facebook, Instagram, Twitter or any other social network site, unless you have attended to your privacy settings, this is essentially what you are doing.

When you use a hashtag for example, you are opening up your post to a much wider audience than perhaps you intended. Consider how private “private” really is.

Social media allows us to interact with people from all walks of life.

Most of the time, social media is a fun way to meet people from different cultures and share ideas about everything from political debate to inspiration for arts and crafts.

Sometimes this can take a more sinister turn and people have found themselves to be the victim of online bullying through social media platforms. This is called cyber-bullying.

Cyberbullying can take many forms; from someone posting a spiteful comment about another person to an entire web page being created with the purpose of humiliating someone.

Think Before You Post

If you or someone you know is being bullied online, use the 'report abuse' button to let the administrators of the social media platform know there is a problem and tell someone you trust who can support you.

Do not respond to the bullying; it is likely to make things worse.

Remember that whatever you post online has consequences.

Once you put something on the internet, it is no longer yours; anything you post can be copied and altered and pasted somewhere else.

Before you post anything, think about whether it might embarrass you later….

Steps to keep yourself and others safe

It is also important to remember that not everyone's intentions are good.

There have been many cases of people on social media pretending to be someone they are not in order to take advantage of other people.

This deceptive behaviour, often called "catfishing" or "online impersonation" can have a number of motives:

- Targeting victims for abuse such as online grooming for sexual abuse
- Targeting victims for fraud for financial gain
- To compromise a person in some way
- Trolling
- Radicalisation

Steps to keep yourself and others safe

Online Grooming

There are several steps you can take to keep yourself safe:

- Always keep your profiles private
- Never tell anyone on social media your real name, address or any other information which would allow them to identify you, such as where you work.
- Never give anyone your passwords
- Never meet up with anyone you have met online
- Respect other people's views. It is fine to disagree with what someone else writes but consider how you respond. Any personal or aggressive comments could be seen as harassment or bullying.

As we have already discussed, it's easy to pretend to be someone else on the internet. Children and vulnerable adults can sometimes end up having conversations with people whose real identities they may not know.

Steps to keep yourself and others safe

Online Grooming – Case Studies

Please watch the following videos on two case studies which talk through and reconstruct real life cases of online grooming and the devastating consequences.

- Kayleigh's Love Story is a dramatisation of real events that show the dangers of grooming created by the Leicestershire Police to tackle child sexual abuse and exploitation.
- A short video about 'Murder Games' the docudrama from BBC3 of Breck Bednar, a 14-year-old schoolboy who was lured to his death after being groomed online while gaming.

Online Grooming – Where can I get help and information?

There are lots of resources providing advice and guidance for a range of different age groups at www.internetmatters.org

What should I do if I believe that someone is being groomed or that I may be being groomed?

Online grooming is a criminal offence and should be reported to the police. If you are unsure about what to do, talk to an adult who you trust – this could be a family member, friend, teacher or work colleague.

If you have a safeguarding concern please contact t2's Safeguarding Team at
http://www.t2group.co.uk/safeguarding-and-radicalisation.html#contact_anchor

Internet Fraud

During the Coronavirus pandemic there has been a significant increase in online fraud and scams, some of which can appear entirely genuine.

"Phishing" or **"Spoofing"** are common types of internet fraud. Both terms deal with forged or faked electronic documents.

Spoofing generally refers to the dissemination of e-mail which is forged to appear as though it was sent by someone other than the actual source.

Phishing, also referred to as vishing, smishing, or pharming is often used in conjunction with a spoofed e-mail. It is the act of sending an e-mail falsely claiming to be an established legitimate business in an attempt to deceive the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information after directing the user to visit a specified website.

Internet Fraud - 5 Ways to detect a phishing email

The following tips on how to identify a phishing email have been identified by the National Cybersecurity Alliance.

1. The email asks you to confirm personal information

Keep an eye out for emails requesting you to confirm personal information that you would never usually provide, such as banking details or login credentials. Do not reply or click any links and if you think there's a possibility that the email is genuine, you should search online and contact the organization directly – do not use any communication method provided in the email.

Internet Fraud - 5 Ways to detect a phishing email

2. The web and email addresses do not look genuine

Anyone can buy a domain name from a registrar. And although every domain name must be unique, there are plenty of ways to create addresses that are indistinguishable from the one that's being spoofed.

e.g. a hacker could buy the domain 'acurnencoaching.com' which at a quick glance can be difficult to differentiate from the genuine 'acumencoaching.com'

Malicious links can also be concealed with the body of email text, often alongside genuine ones. Before clicking on links, hover over and inspect each one first.

Internet Fraud - 5 Ways to detect a phishing email

3. It's poorly written

It is amazing how often you can spot a phishing email simply by the poor language used in the body of the message. Read the email and check for spelling and grammatical mistakes, as well as strange turns of phrase.

Emails from legitimate companies will have been constructed by professional writers and exhaustively checked for spelling, grammar and legality errors. If you have received an unexpected email from a company, and it is riddled with mistakes, this can be a strong indicator it is actually a phish.

Internet Fraud - 5 Ways to detect a phishing email

4. There's a suspicious attachment

Alarm bells should be ringing if you receive an email from a company out of the blue that contains an attachment, especially if it relates to something unexpected.

The attachment could contain a malicious URL or trojan, leading to the installation of a virus or malware on your PC or network. Even if you think an attachment is genuine, it's good practice to always scan it first using antivirus software.

Internet Fraud - 5 Ways to detect a phishing email

5. The message is designed to make you panic

It is common for phishing emails to instill panic in the recipient. The email may claim that your account may have been compromised and the only way to verify it is to enter your login details.

Alternatively, the email might state that your account will be closed if you do not act immediately. Ensure that you take the time to really think about whether an email is asking something reasonable of you. If you're unsure, contact the company through other methods.

Further Information

If you see content which makes you feel uncomfortable or pressured into doing something you don't want to do, report it and leave the website straight away.

For further information about staying safe online, you can have a look at these websites:

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.getsafeonline.org