2023

Cyber Safety & Security

Orb education

Dan Collingbourne

☐	1. Wordlist
☐	2. Cautious Connections
☐	3. Cyberbullying
☐	4. Passwords & Security
☐	5. Your Personal Information
☐	6. Big Data
☐	7. Digital Footprints
☐	8. Data Privacy
☐	9. Data Security
☐	10. Securing Your Data
☐	11. Collaboration
☐	12. Encryption
☐	13. Encryption Spreadsheets
☐	14. Copyright
☐	15. Accessibility & Inclusion

The internet offers you the world. Whether communicating with friends, listening to your musical idols, sharing your holiday photos, following the news, ordering a pizza, doing your banking or playing computer games, the internet is now likely to be involved.

Aim: *To learn about the benefits of, and problems with, connecting over the internet.*

But all that amazing connectivity brings with it some dangers. By using the internet, you are opening yourself up to the actions of bullies and criminals, whilst exposing yourself to a mountain of fake news and misinformation. As a society, we are learning to hold off the first whilst perhaps finding it difficult to recognise the second.

Task 1 – The Internet: Good and Bad

Organise the points below into a table like the one shown. The ideas are in matching pairs; for every positive you should be able to find a word of caution.

The Good	The Bad

Cautious Connections (page 2)

Task 2 – A Safety Overview

The information below shows some of the problems you may experience when using the internet. Along with the name of each problem, there is brief description and some advice on how to deal with it.

Match the problems to their descriptions, and then to the applicable advice.

	Problem	Description	Advice
a.	Cyberbullying	Posting information that reveals our identity online.	Be suspicious of anyone you meet online that you don't know in the real world.
b.	Sharing PII	Posting images and comments that make you look bad.	Take screenshots of the bullying and report it to a trusted adult, teacher or the police.
c.	Predators	Send, post or share content that is harmful to another person.	Don't publicly share Personally Identifiable Information such as addresses and holiday plans.
d.	Bad presentation	People that lure children into dangerous personal encounters.	Look after your personal image online. It can be very difficult to delete your history completely.
e.	Inappropriate content	Deleted from sample	Deleted from sample
f.	Hacking	Deleted from sample	Deleted from sample
g.	Phishing	Deleted from sample	Deleted from sample
h.	Scams	Deleted from sample	Deleted from sample
i.	Malware	Deleted from sample	Deleted from sample

Your digital footprint is the trail of data left behind when using the internet. This might include a list of the websites you have visited, your social media posts, a record of the videos you have watched, your emails and any other information shared online. Some of this information can be on the web forever and could be used in a way that harms you. It is therefore hugely important to manage your digital footprint.

Aim: *To learn about our digital footprint and how to reduce it.*

Task 1 – Active or Passive?

An *active digital footprint* is created when you deliberately share information about yourself. You might, for example, post on TikTok, complete an online survey or set up a bank account.

A *passive digital footprint* is created when information is collected without your knowledge. This includes the data websites collect about your location and the time spent on each page. It also includes the analysis of your likes, shares and comments which is then used to target you with specific adverts and other content.

Say whether you think each of the following examples result in an active (A) or passive (P) footprint.

a. ***A*** Posting a comment on TikTok.

b. _____ Opening a bank account.

c. _____ A sports website recording your location when you visit.

d. _____ Sharing your holiday photos online.

e. _____ Signing up for a basketball newsletter.

f. _____ Using a shopping app to purchase a hat.

g. _____ Your browser keeping a history of all the websites you visit.

h. _____ Facebook working out how many people you live with.

i. _____ Creating a Netflix account.

j. _____ Forwarding a private and personal email to other people.

k. _____ Websites noting the search that brought you to them.

l. _____ Completing questions in an online survey.

m. _____ Google saving all your location data when using maps.

n. _____ Taking a quiz on social media.






Personal information is valuable to criminals. They can use it to access your accounts, steal your money and spy on you. They may also sell your data to other criminals.

Data Security is the practice of protecting digital information from unauthorised access, accidental loss and damage.

Aim: *To learn a little about how our personal data is protected.*

Task 1 – Data Privacy vs Data Security

Research and briefly explain the difference between data privacy and data security.

_____

_____

_____

Task 2 – Data Security Risks

There are lots of ways that private information can be stolen or corrupted. These include:

1. **Accidental Data Exposure**
2. **Phishing Attack**
3. **Malicious Insider**
4. **Malware**
5. **Ransomware**
6. **Physical Theft**
7. **Software Vulnerabilities**

Look up the terms and decide which is being described by each of the statements below:

a. _____ An email or text from someone containing a malicious link to a fake webpage.

b. _____ An employee forgetting to protect a private database with a password.

c. _____ Software that infects computers and opens up access for data theft.

d. _____ Deleted from sample.

e. _____ Deleted from sample.

f. _____ Deleted from sample.

g. _____ Deleted from sample.

Securing Your Data (page 2)

Task 2 – Phishing

You have probably received emails from a company or website that you know. However, these emails are not always genuine. Put the following events in order to show how phishing scams work.

1. You happen to use this shop or bank, so you assume that the email is genuine.
2. The link takes you to a website that looks genuine enough.
3. You receive an email that looks like it's from a shop or a bank. It contains links for you to click on.
4. The website is not genuine. The phishers capture your login details and use or sell them.
5. You enter your username and password to log into the website.
6. You click on one of the links.

Order _____

Intentional Mistakes?

Another type of phishing email tries to engage you in a conversation in the hope that you will send the scammers money. It is usually claimed that it's needed for a sick mother or to help the person access the amazing wealth that they can't quite get their hands on yet. These phishing emails often contain spelling or grammatical mistakes that are included intentionally. The idea is that the scammers don't want to waste their time communicating with clever and alert people; they want to find the gullible ones. Don't put yourself in this category – be very careful how you deal with all suspicious emails.

Task 3 – Protecting your Files

It's not actually very easy to password protect individual files on your computer. Most of the security offered is through user accounts. Your files will be hidden from other users but administrators will likely have permission to view everything. Your files will also be freely available if you share your account with other people, leave your computer logged in or copy files to an unencrypted USB. If emailed, sensitive information may be captured during its journey over the internet.

Do some research and write down a sentence or two about each of the file security solutions below.

a. Secure PDFs
b. Password protected zip files
c. OneDrive personal vault
d. VeraCrypt
e. Encrypted USB drives
f. Password protected Excel spreadsheets and Access databases.

Collaboration means 'working with someone to produce something'. You will likely be asked throughout your education to collaborate with other students. In the workplace, collaboration is generally viewed as the best way to improve results. When collaborating, it's important that everyone involved remains understanding and respectful even when (or especially when) things get difficult.

Aim: *To learn why collaboration is important and how to do it respectfully.*

Task 1 – Collaboration Considerations

Decide whether each of the statements below describes a positive or negative aspect of collaborating (or perhaps a little of both). Discuss your answers as a group.

a. *Difficult problems are better solved by teams.*

b. *Trying to explain your understanding to someone else can show up what you don't know.*

c. *Different people might have very different ways of doing things.*

d. *Collaborating can help build trust and understanding.*

e. *Collaborating is much slower than getting the job done yourself.*

f. *In the past, your collaboration partner might have made mistakes in their work.*

Task 2 – Why Collaborate?

Collaborating can be difficult but it is still increasingly common in the modern workplace. Try and match the problems identified below with the comment that provides a reason to persevere.

	Problem			Comment
1	You might not get on too well with the people you are collaborating with.	•	•	a "Find ways of working together that mean time isn't wasted".
2	Collaborating might slow down your progress.	•	•	b "Assigning responsibilities from the start helps create an even distribution of workload".
3	In the past, your partners might have made mistakes in their work.	•	•	c "Creative friction is a good thing. Listen with respect to each other's ideas".
4	Some people work harder than others.	•	•	d "Perhaps to begin with, but the overall result should be worth waiting for".
5	Too much time is wasted sorting things out.	•	•	e "And they bring these experiences to this project so that they are not made again".