Entry3/Level 1 Literacy Digital Skills Health and Safety Term 2

PART 2 – Setting up a password and keeping it safe

I can	Date when achieved
1. Create a safe password.	
2 Keep my password secure.	

Task 1

Look up the meaning of following words and write their synonyms:

(A synonym is a word that means the same thing. E.g. cold – cool)

malicious	
legitimate	
memorable	
certain	
fraud	
impersonate	
random	
disclose	
to hack	

Read the text

Your passwords are the most common way to prove your identity when using websites, email accounts and your computer itself. The use of strong passwords is therefore essential in order to protect your security and identity. The best security in the world is useless if a malicious person has a legitimate user name and password.

Passwords are commonly used in conjunction with your username. However, on secure sites they may also be used alongside other methods of identification such as a separate PIN and/or memorable information. In some cases you will also be asked to enter only certain characters of your password, for additional security.

Task 2 Look at the questions below and discuss with your partner.

1. What are the risks of having a weak password?

2. How to create a strong password? What makes a password weak?

Give some examples.

3. How do you look after your passwords so they remain secure?

Read the article below. Were your ideas right?

(adapted from https://www.getsafeonline.org/shopping-banking/passwords/)

The Risk Of Using Weak Passwords And Not Having A Separate Password For Your Email Account

People impersonating you to commit fraud and other crimes, including:

- Accessing your bank account
- Purchasing items online with your money
- Impersonating you on social networking and dating sites
- Sending emails in your name
- Accessing the private information held on your computer

Choosing the Best Passwords. Do:

- Always use a password.
- Use a strong, separate password for your email account.
- To create a strong password, simply choose three random words. Numbers, symbols and combinations of upper and lower case can be used if you feel you need to create a stronger password, or the account you are creating a password for requires more than just letters.
- There are alternatives, with no hard and fast rules, but you could consider the following suggestions:
- Choose a password with at least eight characters (more if you can, as longer passwords are harder for criminals to guess or break), a combination of upper and lower case letters, numbers and keyboard symbols such as @ # $ % ^ & * ( ) _ +. (for example SP1D3Rm@n – a variation of spiderman, with letters, numbers, upper and lower case). However, be aware that some of these punctuation marks may be difficult to enter on foreign keyboards. Also remember that changing letters to numbers (for example E to 3 and i to 1) are techniques well-known to criminals.
- A line of a song that other people would not associate with you.
- Someone else's mother's maiden name (not your own mother's maiden name).
- Pick a phrase known to you, for example 'Tramps like us, baby we were born to run"' and take the first character from each word to get 'tlu,bwwbtr'

Don't use the following as passwords:

- Your username, actual name or business name.
- Family members' or pets' names.
- Your or family birthdays.
- Favourite football or Formula 1 team or other words easy to work out with a little background knowledge.
- The word 'password'.
- Numerical sequences.
- A single commonplace dictionary word, which could be cracked by common hacking programs.
- When choosing numerical passcodes or PINs, do not use ascending or descending numbers (for example 4321 or 12345), duplicated numbers (such as 1111) or easily recognisable keypad patterns (such as 14789 or 2580).

Looking After Your Passwords

- Never disclose your passwords to anyone else. If you think that someone else knows your password, change it immediately.
- Don't enter your password when others can see what you are typing.
- The routine changing of passwords is not recommended, unless the accounts to which they apply have been hacked, in which case they should be changed immediately. This also applies if another account or website for which you use the same login details have been hacked.
- Use a different password for every website. If you have only one password, a criminal simply has to break it to gain access to everything.
- Don't recycle passwords (for example password2, password3).
- If you must write passwords down in order to remember them, encrypt them in a way that is familiar to you but makes them unreadable by others.
- Do not send your password by email. No reputable firm will ask you to do this.

Task 3 - Write a short paragraphs to answer each of the question.

1. What are the risks of having a weak password?

2. How to create a strong password? What makes a password weak? Give examples.

3. How do you look after your passwords so they remain secure?