**Being secure online**

This document contains the following:

* Stimulus material on passwords
* Comprehension questions on the stimulus
* Vocabulary tasks
* Language focus activities
* Writing task
* Cloze passage
* Creating a password activity
* Links to further resources
* Curriculum links

This lesson is intended to be taught in a Stage 4 English classroom with a focus on reading and writing.



**Passwords, PINS and passphrases**

Passwords, PINS and passphrases are the first line of defence to protect your information from cyber criminals. They should be a secret that only you know.

Weak passwords are easy for cybercriminals to guess. They use automated software that can potentially guess 350 billion passwords per second!

If your password or PIN is captured, guessed or stolen, a cybercriminal can potentially:

* send emails from your accounts
* withdraw money from your bank accounts
* change files on your computer such as invoices
* steal your identity.

The key thing to remember when creating a password is that the longer it is, the stronger it is!

Think of a passphrase that is made up of at least four words, including at least 14 characters, for example 'horsecupstarshoe'. Make it meaningful to you so it is easy to remember.

Using strong passwords lowers your overall risk of a security breach, but they do not replace the need for other effective security controls, such as installing anti-virus software and updates to your operating system as soon as they’re released.

Do not include the following things in your passwords:

* repeated characters
* arbitrarily mixed letters, numbers and symbols
* single dictionary words, your street address or numeric sequences (such as 1234567)
* personal information
* anything you have previously used.

It is better not to change your passwords frequently, for example each month, as it leads to poor passwords being created.

A passphrase is similar to a password. It is used to verify access to a computer system, program or service. Passphrases are most effective when they are:​

* **Used with multi-factor authentication**
* **Unique**– not a famous phrase or lyric, and not re-used
* **Longer**– phrases are generally longer than words
* **Complex**– naturally occurring in a sentence with uppercase, symbols and punctuation
* **Easy to remember** – saves you being locked out.

Passphrases create greater security & more convenience. They are:

* **Harder to crack** against common password attacks
* **Easier to remember** than random characters
* **Compliant with password security requirements** – upper and lower-case lettering, symbols and punctuation

Passphrases will significantly increase security across all of your business’ devices.

Information adapted and curated from <https://www.cyber.gov.au/>

**Activities**

**Comprehension questions:**

1. How many passwords can automated software guess per second?
2. How many words should a passphrase include?
3. What other security requirements should you consider apart from a strong password?
4. Why do you think you should update your Operating System as soon as the updates are released?
5. How frequently should you change your password/passphrase? [*Or Why shouldn’t you change your password each month?]*
6. What is the key thing to remember about creating passwords?

**Vocabulary:**

**Arbitrarily (adv),**

on the basis of random choice or personal whim, rather than any reason or system

**Numeric (adj),**

relating to or expressed as a number or numbers.

**Compliant (adj),**

meeting or in accordance with rules or standards

**Verify (verb)**

make sure or demonstrate that (something) is true, accurate, or justified.

Write a sentence for each word demonstrating correct usage. Remember to use correct tense and subject agreement. For example, a verb such as ‘to run’ – I run, he runs…

**Simple, Compound or Complex**

Identify whether the sentences below are simple, compound or complex. Underline the verbs in each sentence. Be prepared to explain your answer.

*Top Tip*

 *Simple sentences usually only have one verb, compound sentences usually are identified by at least 2 verbs and FANBOYS, complex sentences have a subordinate clause*

1. Using strong passwords lowers your overall risk of a security breach, but they do not replace the need for other effective security controls [compound]
2. A passphrase is similar to a password [simple]
3. They should be a secret that only you know. [complex]

**Answer Key:**

1. Using strong passwords lowers your overall risk of a security breach, **but** they do not replace the need for other effective security controls [compound]

*2 verbs and the coordinating conjunction BUT – FANBOYS.*

1. A passphrase is similar to a password [simple]

*1 verb - is*

1. They should be a secret that only you know. [complex]

*2 verbs – be and know. Subordinate clause ‘that only you know’.*

**Language focus:**

When creating a list of items you should be able to read each point with the stem statement and it forms a sentence. For example, look at this from the article above:

Passphrases are most effective when they are:​

* **Used with multi-factor authentication**
* **Unique**– not a famous phrase or lyric, and not re-used
* **Longer**– phrases are generally longer than words
* **Complex**– naturally occurring in a sentence with uppercase, symbols and punctuation
* **Easy to remember** – saves you being locked out.

Notice how each dot point makes grammatical sense with the sentence stem.

**Writing task:**

Write some guidelines about how to be safe online. In your guidelines you must include a sentence stem with a dot point list. Remember to make sure each dot point makes grammatical sense.

**Create a password**

Create a password/passphrase that uses at least 4 words. Use the categories below and mix and match each.

|  |
| --- |
| **CATEGORIES** |
| Favourite number |
| Pet’s name, or favourite character’s name |
| A symbol (#, $, %, \*, or &) |
| Favourite food |

Use the boxes below to create your passphrase. Cut them out to test different combinations. Use the small boxes for numbers or symbols.

**Curriculum Links:**

EN4-3B - uses and describes language forms, features and structures of texts appropriate to a range of purposes, audiences and contexts



**Cloze Activity:**

Complete the table below first by inserting the missing words into the comments. Then ‘Easy to remember’ section of the table.

|  |  |  |
| --- | --- | --- |
| PASSWORD/ PASSPHRASE | EASY TO REMEMBER | COMMENTS |
|
| password123 |   | One of the most \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ used passwords on the planet. |
| Spaghetti95! |   | Some \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ in the most common areas, and very short \_\_\_\_\_\_\_\_\_\_\_\_. Easy to remember, but easy to crack |
| 5paghetti!95 |   | Not much more complexity than above with character \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, and still short length. \_\_\_\_\_\_\_\_\_\_\_ to remember, but easy to crack. |
| A&d8J+1! |  | \_\_\_\_\_\_\_\_\_\_\_\_ complex, but shorter than the above passwords. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ to remember, easy to crack. |
| I don’t like pineapple on my pizza! |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ character length (35 characters). \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is naturally high given the apostrophe, exclamation mark and use of spaces. Very easy to remember, and very \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_to crack. |

**Cloze:**

Commonly, complexity, substitution, Mildly, Excellent, easy, hard, easy, difficult, excellent, complexity, length

Very easy, Easy, Somewhat Easy, Very difficult, Easy