**Unit 1: Digital Security**

**Value:**This unit is valued at 20pts.

**Meaning:** Do you take the electronic steps to 100% guarantee your safety?

[**Introduction**](https://bbtnb.cdxauto.ca/mod/page/view.php?id=4)**:**

Protecting what is yours is not a new concept. You have locks on your locker, you have smoke detectors in your homes and some even have high priced security systems monitoring their homes all day long. If you don't have a firewall protecting your 24/7 internet access and you don't password protect your devices and wifi you may as well be handing the keys to your information to complete strangers. In this unit we will look deeper at why and how we protect our property in the digital era.

**Fact:** " Young people on the internet often view strangers as potential friends that they just haven't met yet" (Gross 2009) This leads to an over-abundance of trust and often is the first step to opening the door to digital property theft and damage.

The Issues:

1. Community threats such as terrorist claims online

2. School threats such as hackers and viruses

3. Personal Security such as online stalking, identity theft, cyberbullying, and phishing

4. Hardware and network threats such as malware and viruses

---Complete **all of the following** Assignments or those indicated by your teacher ---

**Assignment 1: Battleship**

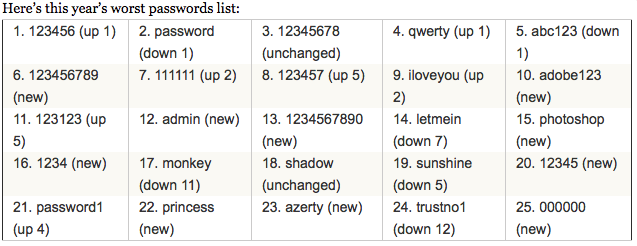
The classic board game Battleship would last only seconds if two computers were playing it. Computers can guess numbers and letters at remarkable speeds, and it is not humans who are trying to hack into your online accounts but rather sophisticated computer programs working while the criminals are sleeping.

Have a look at the below examples of the worst passwords you could use to protect your online life.

 A close up of a sign

Description automatically generated

Or this list:



[Complete This Digital Security Assignment 1](https://bbtnb.cdxauto.ca/pluginfile.php/125/mod_page/content/12/securityassign1.pdf" \o "Security Asignment 1) Click on this link or find in Microsoft Teams FILES Section.

-------------------------------------------------------------

A close up of a sign

Description automatically generated

**Assignment 2: Hercules Code**

So we have seen the examples of the weakest and worst passwords a person can use to protect their online life..... Let's take a look at the strongest passwords you can use.

A modern **STRONG** password is **not** a single word, it is **not** a word with numbers, it is a **FULL SENTENCE** complete with the following:

Capital and lowercase lettering

Symbols

Numbers

**Here is an example:**

If someone were to like the Toronto Maple Leafs, they should not use that in any password, but they can stay with the topic in general.

Sentence **" Toronto Maple Leafs lose forever kids"**

Now that would be a pain to peck into a smartphone over and over so let's shorten it and strengthen it at the same time.

**TMLLose4evakids**   - it is long enough but still just letters and numbers

Let's make the S a $ sign and the letter "e" let's flip into a number 3 (backwards E)

**TMLLo$343vaKid$**    -  Now this is a very very strong password that Microsoft would call "BEST". All you have to do is remember what the sentence says and spot where you may have tweaked it. Computers can still crack this but it would take FAR TOO LONG and so they would just move on to a new target.

**Kapersky's Password Checker:**

[**PASSWORD CHECKER HERE**](https://password.kaspersky.com/)

**Complete the following:**

1. **Paste in the above password** example above to prove it is BEST

2. Make sure nobody is looking and **test a few of your passwords** to see just how WEAK or STRONG they are. *It will tell you how long a normal computer takes to guess your password running a simple guessing program.*

3. Make up a password that is AWESOME using the tips above and write it down for your teacher to check. Make sure this is one you would **not really use yourself**. (3pts)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_-

4. When you go home (or use some time now) **invent a new BEST password** or more than one that you can protect you major accounts with like Facebook, Emails, Pay Services, Apple/Google Accounts, Instagram, TikTok etc...)

----------------------------------------------------------------

**Assignment 3: Beat the Odds**

Let's do some **MATH!!!!!!!**

Let's see how math can prove a password's value.

The average iPhone is protected by a four digit lock code with number going from 0-9

The odds of guessing each number are **1/10** and you simply multiply the **1/10** by itself **4** times to get

**1/10 x 1/10 x 1/10 x 1/10 = 1/10,000**

**Meaning** Best case senario (for you) it would take a hacker who doesn't know you 10,000 guesses to get into your phone.( It would take a computer just a few moments.)

If you made the password 8 values long it would be 1/10 x 1/10 etc.... EIGHT TIMES and increase the odds by a lot but not that much.

There are **26 letters in the alphabet**, and **52 letters** if you count lowercase and capitals, and there are roughly **10 symbols** that could be used. Of course, there are **10 number digits**.

**SOLVE:** If you had a four-digit password which could be **Letters (Cap or LC) Numbers**, or **Symbols**...... what is the probability of guessing the four digits? (3)

Hint: Total up the entire choices and multiply that by itself four times.

Now, a typical NBED password must be **7 digits** and contain Letters (Cap and LC) Numbers, and Symbols. What is the probability of guessing that password? (3)

**Let your teacher know your answers in the preferred format.**

**Conclusion:** Password protection is just a start in the world of Digital Security, but it is a part of all of our lives and therefore worth understanding fully. Make a pledge moving forward to always secure your accounts with **STRONG passwords and keep you SYSTEMS UPDATED WITH PATCHES AND UPDATES** as frequently as possible.

------------------------------------------- EXTRAS

Additional Security measures to take immediately:

1. Be careful not to give APPS access to your Google and Facebook accounts and if you do allow it know exactly what you are sharing with these APPS.

2. Be careful with emails that arrive in your box that appear to be from Microsoft, Google, Banks, Co-workers, etc....  You can verify by clicking on the senders’ email address to see if the company is legit.

EX -->  **ADMIN@microsoftdatacollections.net**  is **not legit** where as, admin@Microsoft.com is most likely legit.

3. Avoid all phone scams that say they have spotted an issue with you machine. They are always 100% just trying to gain access to your machine.

4. Help seniors and other adults who did not get this training secure themselves better. It may be the best gift you can give someone who isn't digitally savvy.