No part of the candidate's evidence in this exemplar material may be presented in an external assessment for the purpose of gaining an NZQA qualification or award.

Mana Tohu Mātauranga o Aotearoa
New Zealand Qualifications Authority

Level 2 Digital Technologies 2024

91898 Demonstrate understanding of a computer science concept

EXEMPLAR

Excellence

TOTAL 07

INSTRUCTIONS

There are three questions in this assessment, on the topics of:

- computer security (page 3)
- error control (page 9)
- artificial intelligence (page 15).

Choose only ONE question to answer. Note that parts (c), (d), and (e) of each question include options for you to choose from.

Read all parts of your chosen question before you begin. Do not repeat your response in different parts of the question.

Candidates must complete their assessments individually under teacher supervision, in accordance with the NCEA Assessment and Examination Rules and Procedures. The material submitted for assessment must be the candidate's own work.

Candidates are not permitted to access any resources (either in hard copy or online) other than those supplied in the assessment itself.

Schools, teachers, and candidates are not permitted to share or discuss the assessment or their assessment responses with any other schools, teachers, or candidates until after the final date for submission (30 October 2024).

The use of chatbots, generative AI, paraphrasing tools, or other tools that can automatically generate content is not permitted and material generated by these tools should not be submitted as part of the candidate's work.

(Assessment Specifications, NZQA 2024)

EITHER: **QUESTION ONE: Computer security**

(a) (i) What issues do online retailers have with computer security?

Online retail stores hold sensitive information regarding their customers. like customer bank details, names and addresses. Due to this, One issue that online retailers have to manage would be hackers trying to retrieve this information. If there was a vulnerability in the program that allowed the hackers to guess the passwords then that would then put the users at risk.

Another issue that online retailers would have to face when dealing with computer security would be a dos or ddos attack. Either one of these attacks would slow down the website and making it harder for the users to be able to use it thereforth losing on revenue and credibility.

(ii) Explain two separate ways in which online retailers can protect themselves and their customers during transactions.

When purchasing on an online retail store, they typically require you to sign into an account. The account would store customers valuable details. To prevent any hackers trying to get into their account with passwords, the store could implement hashing andsalting. Hashing is turing the password into a fixed number of string that cannot be reversed. This means the website does not store their password making it harder for hackers to retrieve this information. If the password is slightly changed, the hash could come out completely different.

A disadvantage is that if 2 people were to use the same password then the hash would remain the same for these 2 individuals. To add an extra layer of security the next step salting, is adding extra values to the end of the password before the hashing process, so when it is then hashed, the same 2 passwords would get back 2 different hashes.

Another way that a retail store could protect themselves and their customers is by adding 2FA or 2 factor authentication. 2FA requires the user to input their password, and confirm who they are through another method. This could be in something they know, something they have or something they are. This then checks whether the person trying to get into an account or make a purchase is authorised to make that purchase. This could be implemented when the customer is trying to log into their account or just before they make a purchase. This protects the online retailer too, if they have access to more things on the website as a staff including company bank statements, employee details, customer details.

A student has created a program to generate passwords. It works by randomly selecting two words that start with a capital and have four letters in them from a list of 100 words; it then adds the current hour with a '!' at the end. Below is an example of the program running.

```
How many passwords do you want? 4
TideBeam11!
HideCold11!
BeamBeam11!
LaceNine11!
```

(b) (i) Explain how secure these passwords are that have been generated by the student's program.
Suggest ways in which they can be improved.

It's somewhat secure with the randomness of unrelated words together. However this is to some extent because with the use of a brute force attack, the password could easily be guessed. This could be from a rainbow table, a list of very common words or a dictionary attack. Due to the way these passwords are generated, there is a patterm within each password. If a hacker were to find the pattern then all passwords are then at risk. There will always be an exclamation point at the end, numbers of 1-12, and a combination of 2 words from the same list, and these words can be repeated. This then makes the passwords faulty in terms of security. This can be improved in different ways.

One of the ways that this can be approved would be to randomise the order that the words, numbers and add more special characters. This then maxmises the amount of passwords that can be generated making it harder to brute force. To extra maxmise this, instead of just the hour, the minutes could be added to the time thereforth increasing the amount of possibilities used.

(ii) Explain the advantages and disadvantages of this program, once your suggested changes are made.

When you randomise the order, it throws off the original formula of the old generated password. This means it would be harder for hackers to brute force their way into getting access as there are now more combinations that they would have to attempt. When also adding the minutes with the hour, which increases the amount of combinations. However this is also disadvantageous as minutes only go up to 60, and hours going up to 12, so by using hr-min order, it can be bruteforced. By adding more special characters this makes the password even more unique securing the password.

The disadvantage is that if the hacker would have access to the list of words used, this could still be brute forced. As there are a set word combinations that could be used throughout the different passwords. But with the use of randomising the order of how the password is formatted this would then make it significantly more difficult to be guessed.

(c) Choose ONE of the following to answer:

- Identify the common issues people face with computer security. How can they protect themselves from these threats?

  OR

- What are email blacklists and whitelists? Explain how they work, and the challenges when they are used.

Choice (copy and paste below):

Identify the common issues people face with computer security. How can they protect themselves from these threats?

Response:

One common issue that people face with computer security is phising. Examples of phishing is emails and websites that appears to look legimitate when in reality these can be extremely dangerous. Phising can produce different outcomes which can be harmful to the user whether it be by downloading malware through links or inputting personal information in fake websites.

People can protect themselves from phishing threats by checking the legitimacy of the email and website ensuring that they are keeping their computer and information safe. They could do this by checking any spelling errors, any date errors, names and if there is a link that the email tries to get you to click, to hover your mouse over it to see if it takes you to the right address. Phising is a form of social engineering as it could invoke different emotions of the user to increase the likelihood of them clicking the links or putting in details.

Another issue that people would have to face is threats from malware due to the amounts of harm that they can cause to a computer such as gathering person information for profit. As there is in increasing amount of ways to prevent malwares from distrupting a computer, the malwares are constantly developing ways to infect a computer.

This can be protected against by regularly updating antivirus's and computer defenders. When you first purchase your computer, it likely came with an antivirus however with time there will be new malwares and new approaches into preventing these from getting into your computer, thereforth it is necessary for someone to update these antivirius's to better protect their device.

(d) Choose ONE of the following to answer:

- Explain the ethical issues organisations face with data privacy. How should organisations behave regarding data privacy?

  OR

- Explain how organisations can future-proof themselves from computer security threats.

Choice (copy and paste below):

Explain how organisations can future-proof themselves from computer security threats.

Response:

Organisations can futureproof themselves from security threats by taking some of the following measures.

They could have a backup of their company information and servers. This could be in the form of physical or digitally on the cloud. By having a backup that is stored away from the main servers, if a natural factor of computer threats were to occur such as fires and floods, then the backup is safely stored away from the main server and does not get affected by these.

To further improve the futurabilty of the application, they could also have a strong enough network to defend against attacks such as ddos. As DDOS attacks would "overwhelm" the servers by taking up its ram and memory, by having multiple servers and backups it would help prevent attacks from this security threat and others.

Another way that having backups and having stronger networks, is that this strengthens the weaks points and the location of any making harder to locate from these attacks. Applying firewalls to the organisation applications increase the computer security as a firewall would monitor the incoming and outgoing flow of the network managing it easier. For the implication of futurablity constantly updating this is crucial to prevent damages from security threats. Updating the firewall and monitoring programs would also include any network monitoring programs that would monitor the application for disturbances. Monitoring services include monitoring malware and DDOS attacks.

(e) Choose ONE of the following to answer:

- Explain what 'biometric authentication' is. What are the advantages and challenges of using this method instead of passwords?

  OR

- Explain what 'social engineering' is and how organisations can help to ensure that neither they nor their users fall for scams, or are prevented from falling for scams.

In your response, ensure that you demonstrate clear links to computer science concepts.

Choice (copy and paste below):

- Explain what 'biometric authentication' is. What are the advantages and challenges of using this method instead of passwords?

Response:

Biometric authentication is one of the authentication processes, This would fall under the category of what you are. Biometric authentication is when the application would confirm your identity and who you are with the use of physical attributes of the user. Derived from your face, your fingerprint, eyes, voice.

Advantages with using biometric authentication is that this would always be with you. Unlike passwords that can be forgotten, this is something that you wouldn't have to think about as this is something that you are. Biometric authentication is also unique to each user, as no persons face would be like anothers in contrast to passwords where people can make their passwords something that is not unique. This makes it harder to replicate. A password can also be shared, allowing multiple users to gain access into the same account whilst using biometric authentication only the user would be able to.

With the use of hashing and salting, applications don't store the users passwords, however with biometric authentication there are privacy concerns on what the application would then have. When you set up biometric security, you give the application your biological information, which can make users sketical as this is private information and may not feel comfortable allowing it to have their faces or voices.

Another disadvantage that arises when using biometric authentication is how the information cannot be altered or changed if the biological information gets compromised. You can change a password but not how your face appears, fingerprints and voice. This becomes a problem as any use of biometric authentication that the user utilizes then all gets put at risk.

Excellence

Subject: Digital Technologies

Standard: 91898

Total score: 07

Q	Grade score	Marker commentary
Error control	E7	The candidate explained the value of information that online retailers hold, and gave two strong ways in which retailers can protect themselves and customers. The benefits and limitations of the passwords generated by the program were explained and potential improvements were given. These changes were improvements to the program, not suggestions to abandon the program. A good explanation of the advantages and disadvantages of the improved program was delivered. The candidate gave good, detailed examples of threats individuals have, followed by sensible ways to reduce the risk. The candidate gave solid suggestions on how an organisation can 'futureproof' itself. The answers did not repeat from earlier responses and were all appropriate for an organisation. A convincing explanation of biometric authentication was given, along with a comparison to passwords. Suitable advantages and challenges were given. This candidate gained an Excellence by providing detailed, non-repetitive answers throughout their response.