2

NZQA
NEW ZEALAND QUALIFICATIONS AUTHORITY
MANA TOHU MĀTAURANGA O AOTEAROA

QUALIFY FOR THE FUTURE WORLD
KIA NOHO TAKATŪ KI TŌ ĀMUA AO!

COMMON ASSESSMENT TASK

Level 2 Digital Technologies and Hangarau Matihiko 2021

91898 Demonstrate understanding of a computer science concept

Credits: Three

Achievement	Achievement with Merit	Achievement with Excellence
Demonstrate understanding of a computer science concept.	Demonstrate in-depth understanding of a computer science concept.	Demonstrate comprehensive understanding of a computer science concept.

Type your School Code and 9-digit National Student Number (NSN) into the space below. (If your NSN has 10 digits, omit the leading zero.) It should look like "123-123456789-91898".

There are three questions in this document. **Choose ONE question to answer.**

You should aim to write **800–1500 words** in total.

Your answers should be presented in 12pt Times New Roman font, within the expanding text boxes, and may include only information you produce during this assessment session. Internet access is not permitted.

Save your finished work as a PDF file as instructed by your teacher.

By saving your work at the end of the examination, you are declaring that this work is your own. NZQA may sample your work to ensure this is the case.

Excellence

TOTAL 07

ASSESSOR'S USE ONLY

Instructions

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

- Computer security (page 3)
- Encryption (page 8)
- Error control (page 13).

Choose only one question to answer. Note that parts (b), (c), and (d) of the question include options for you to choose from.

Read all parts of your chosen question before you begin.

Either: **Question One: Computer security**

(a) (i) Name a **specific** New Zealand-based company or organisation that uses computer security.
Note: If you want to discuss your school, state "My school".

My School

(ii) Give at least two examples of ways computer security is used by this organisation.

At , N4L (network for learning) provides the school with a **firewall** that helps restrict access to sensitive information (including incoming requests from outside and outgoing requests from inside) AND helps monitor the network for suspicious activity. It also restricts outgoing traffic in the form of website filtering to dangerous sites. The **firewall** is a cybersecurity tool that is used to filter traffic on a network. Its primary goal is to block malicious traffic requests (from the outside) and viruses while ALSO giving legitimate users (eg. students and teachers) undisrupted access to the data. In other words, it's like the digital 'security guard'.

Another example is **Anti-virus software** which is an important tool for protecting data and computer systems from getting corrupted. It works by **scanning** files on the computer/server for any malware or known malicious patterns. It can also scan new files from other sources like the internet, email, or those copied from a removable device. Once detected, the malicious software will be quarantined or deleted to prevent malware from causing damage to the computer.

(iii) What do these uses of computer security enable this organisation to do that would otherwise be difficult or impossible?

If the school doesn't have a **firewall** in place, it would be like openly inviting criminals to hack into our network. It also means that everyone can gain access to the school network and it would be impossible to monitor potential threats and untrustworthy traffic.

Without a **firewall**, we are giving attackers free access to all the information that the school has, including teaching materials, important files, student records etc. With that, there can be potential consequences like: the attacker having the option to steal the data, leak it to the public, encrypt it and hold it for ransom, or simply delete it. Therefore, it would be difficult to work comfortably and recover the data if it's not backed up.

If **website filtering** is not enabled, certain websites won't be blocked at school. All students and staff will be able to visit any sites including dangerous ones. This will put the entire school network security at risk.

Due to the nature of a virus being able to replicate itself, without **Antivirus software,** a single virus could rapidly spread over the entire school network and any devices connected to it, including the students'. The school runs a high risk of losing valuable data/files and overall, it would be impossible to keep it safe for students and staff to work normally.

(b) Choose **two** of the following to answer:

- In what ways do firewalls protect an individual user's computer?
- What methods do hackers use to get malware onto an individual user's computer?
- Users are advised to regularly update their operating systems and applications. How does this improve protection against malware for an individual user's computer?

Choice (1) – (copy and paste below)

What methods do hackers use to get malware onto an individual user's computer?

Response

Malware could be embedded in **email attachments**. Hackers can send emails with attachments to people in the school and someone opening the attachment on their computer will immediately run the malware and it will also start to infect other computers.

The attacker can get malware onto a computer that a student/staff uses via **phishing emails** sent to them. These emails are disguised to look genuine (eg. from a teacher) and they convince the user to click on a link that eventually makes them download the malware.

Malware can also get onto a user's computer when they connect an **external hard drive** or **USB stick** that is (maybe unknowingly) containing the malware. It's quite common for people to copy an entire folder from the hard drive to their computer and the malware gets in.

Choice (2) – (copy and paste below)

Users are advised to regularly update their operating systems and applications. How does this improve protection against malware for an individual user's computer?

Response

Operating systems (eg. Windows 10) often contain security vulnerabilities that could allow attackers to install malware into the system.

Applications (eg. internet browser) may also contain security vulnerabilities. When a student/staff uses an unpatched version of the browser to visit a harmful site, malware could find its way through the vulnerabilities of the unpatched browser.

By keeping these **software** updated, it will remove the vulnerabilities and therefore ensure that they cannot be further exploited. However, it's not 100% guaranteed to protect against malware as there could be other vulnerabilities that have yet to be discovered or reported.

Without the **software updates**, a student might visit a suspicious site, download malware, and risk losing their assignments, having their files locked, or turning their computer into a 'zombie' and be used as part of a DDoS attack.

(c) Choose **one** of the following to answer:

- What are some ways that computer security can be future-proofed?
- What are some ways that human factors influence decisions about computer security?

You should consider this question in the context of the organisation you wrote about in part (a).

Choice (copy and paste below)

What are some ways that computer security can be future-proofed?

Response

The school doesn't currently use **multi-factor authentication** (MFA). This means a student/staff could share the password with someone outside of the school and allow them to gain access to the school network.

Implementing **MFA** will add another layer(s) of security, requiring each user to go through additional steps to verify their identity. Therefore, in the **future**, if one or two layers isn't enough, more can be added to enhance computer security at school.

An onsite backup procedure has already been implemented. To future-proof this, **offsite backup** like Cloud backup could be used because safely storing data online will make it easy to recover if needed and it won't be easily lost as it can be accessed anywhere. However, the downside is that an attacker could hack into the Cloud and access the data so higher levels of **MFA** should be used.

It would be good to provide **cybersecurity training** to every student and staff to future-proof computer security at school. This way, when everyone at school is aware of the potential threats on computers and the internet, they have a better chance of identifying these kinds of attacks and can notify someone so the situation can be dealt with sooner.

(d) Choose **one** of the following to answer:

- An organisation needs to ensure several different types of “updates” are used to keep its network of computers and servers secure. What are some of the challenges these updates pose for an organisation, and how might it deal with them?
- If a computer is infected by malware, what issues might this cause, and what steps could an individual or organisation take to resolve the issues?

You should consider this question in the context of the organisation you wrote about in part (a).

Choice (copy and paste below)

If a computer is infected by malware, what issues might this cause, and what steps could an individual or organisation take to resolve the issues?

Response

Malware is comprised of many different kinds of computer viruses. These viruses can be intentionally programmed to cause damage to the computer which could cause **issues** such as: rendering it unusable or preventing the user from accessing their own data. A hacker can also take control of the infected computer, cause network delays, delete files AND encrypt files while demanding ransom payment.

If a **student/staff’s** computer is infected with a virus, they should **report** the issue to the IT team immediately rather than leaving the problem unattended and risk allowing the virus to continue spreading.

The **school IT team** would first need to contain the malware by **disconnecting** the infected computer from the rest of the network to prevent any further spread of the virus. Sometimes the IT team might be able to completely remove the virus and put the computer back into a safe and usable state. However, in the worst-case scenario, the computer could be in such a bad state that the IT team would have to wipe everything on the computer and hard drive AND perform a full restore from backup in order to return the system to a clean state.

Excellence Exemplar 2021

Subject	Level 2 Digital Technologies	Standard	91898	Total score	07

Q	Grade score	Annotation
1	E7	The candidate has given two good examples of computer security and how they allow the organisation to protect itself. They have given good explanations of three different methods of how hackers get malware are given. The answers include how users can be tricked into installing the malware The candidate has given a good explanation of the need to update to protect against vulnerabilities, and how these vulnerabilities are continually discovered. They have then related this answer to the organisation in part (a), allowing them to explore what their organisation is not currently doing that could be improved upon. The responses are brief but concise, the candidate explaining the implications for the organisation and suggesting a range of methods by which these could be resolved.