Information Privacy and Security (6-8) - Cyber Skills Aotearoa

Te Mōhiohio Tūmataiti me te Whakahaumaru (6–8) – Pūkenga ā-Ipurangi Aotearoa

Kaiako guide

grok academy

Cyber Skills Aotearoa

CORE EDUCATION Tātai Aho Rau

Cyber Skills Aotearoa

A guide to supporting ākonga engagement

Supported by:

ASB aws bnz certnz Te Tāhuhu o te Mātauranga Ministry of Education

N4L netsafe netsafe.org.nz Te Kāwanatanga o Aotearoa New Zealand Government NCSC

He aha te Grok Academy? What is Grok Academy?

Grok Academy provides resources, online courses and competitions, teacher workshops, curriculum guidance and general online cyber security advice for all future focused teachers.

Our Mission

At Grok Academy, our mission is to educate all learners in transformative computing skills, knowledge and dispositions, empowering them to meet the challenges and seize the opportunities of the future.

To us, computing encompasses basic digital literacy through to advanced computer science and related disciplines, and the application of these skills across all disciplines.

Our Goal

We believe that a solid computer science understanding is vital whether you want to fight climate change, make the next blockbuster movie or unlock the secrets of the universe.

We've taught thousands of students to program in classrooms, lecture halls and online, and are now bringing top-notch STEM education into classrooms and homes around the world.

Partner Acknowledgements

Cyber skills Aotearoa has been developed by Grok Academy in partnership with CORE Education Tātai Aho Rau, Te Tāhuhu o te Mātauranga | Ministry of Education, AWS, ASB, BNZ, CERT NZ, Netsafe, The National Cyber Security Centre (NCSC), and te Kāwanatanga o Aotearoa | the New Zealand Government.


ASB

aws

bnz

certnz

Te Tāhuhu o
te Mātauranga
Ministry of Education

CORE
EDUCATION
Tātai Aho Rau
www.core-ed.org

N4L

netsafe
netsafe.org.nz

Te Kāwanatanga
o Aotearoa
New Zealand Government

NCSC

Nau mai, haere mai | Welcome

This guide supports kaiako to create an effective learning programme based on the Yr 6-8 Information Security and Privacy Challenge.

We hope this guide will build your confidence as you support your ākonga to get the most out of the challenge. We hope that in turn their motivation and engagement grows alongside their understanding of cybersecurity.

If you have any feedback or questions about Cyber Skills Aotearoa, please email us at help@grokacademy.org.

The challenge aims to provide ākonga with an authentic and accessible insight into cybersecurity.

The first step in understanding cyber security is knowing how to keep you and your information safe from people, and the software that they create, seeking to do you harm.

In this challenge, ākonga begin by analysing the sharing habits of typical teen characters as they interact on social media and in online calls.

The learning materials in every module include notes, guided experimentation, programming activities and problems to test understanding and skills. The video resources are designed both to teach ākonga about specific programming/cipher concepts, but also to give ākonga a view into what working in cybersecurity is really like, and what people working in this field do on a day to day basis.

No computer programming languages are used in this challenge.

The challenge is designed to be completed over 2-3 hours of online work. However, it may take longer depending on the integration of offline classroom activities that are suggested in this guide.

How the challenge relates to The National Curriculum

The challenge has close ties to the Hangarau wāhanga ako and Technology learning area. The intent of the Hangarau wāhanga ako and Technology learning area is about the relationship between people, technology and the environment; to understand about 'intervention by design'.

> "The aim is for students to develop broad technological knowledge, practices and dispositions that will equip them to participate in society as informed citizens and provide a platform for technology-related careers." Technology in the New Zealand Curriculum (2017)

The Hangarau wāhanga ako | Technology learning area addresses cyber security in these key tupuranga | areas:

Hangarau Matihiko (TMoA)

Whakaaro Rorohiko (Computational thinking) (WR) – E waru ōna whakatupuranga e wetewetehia ana ngā whakaaro rorohiko kia whai māramatanga ki ngā rapanga o te papatono rorohiko matatini me ōna momo hātepe, e whaitake ai te waihanga papatono ki te ao tūturu.
(There are eight progressions which unpack computational thinking in order to gain an understanding of the problems of complex computer programming and its various algorithms, which make programming relevant to the real world.)

Tangata me te Rorohiko (Human Development and computing) (TmtR) – E rima ōna whakatupuranga e whakatau ana i ngā tikanga me ngā mātāpono ki te whakahaere tūmahi e tū ai hei kiriraurau matihiko.
(There are five progressions which define the principles and practices of digital technologies and citizenship.)

In particular, the challenge is related to:

> **TMoA Hangarau Matihiko/Hangarau**
> **Te Tupuranga Tangata me te Rorohiko (TmtR)**
> **Whakatupuranga 2**
>
> Ka whakatau tikanga ki te waihanga; te raweke; te pupuri; te tiki; te tuari me te whakamātau rānei i te kōrero o tētahi pūnaha tūturu.

(Determine methods to create; manipulate; store; obtain; share or test the content of a real system.)

Digital Technologies (NZC)

Computational Thinking for Digital Technologies and Designing and Developing Digital Outcomes focus on developing students' capability to create digital technologies for specific purposes. These two areas also significantly contribute to students developing the knowledge and skills they need as digital citizens and as users of digital technologies across the curriculum. They also provide opportunities to further develop their key competencies:

- thinking
- using language, symbols, and texts
- managing self
- relating to others
- participating and contributing.

Designing and Developing Digital Outcomes (DDDO) –ākonga will develop an understanding that digital applications and systems are created for humans by humans, with a focus on designing and producing quality, fit-for-purpose, digital outcomes. They develop their understanding of the technologies people need in order to locate, analyse, evaluate and present digital information efficiently, effectively and ethically.

In particular, the challenge is related to:

NZC Technology/Digital Technologies
Designing and Developing Digital Technologies Progress Outcome 3 (DDDO PO3)

In authentic contexts, students follow a defined process to design, develop, store, test and **evaluate digital content** to address given contexts or issues, **taking into account immediate social, ethical and end-user considerations**. They identify the key features of selected software and choose the most appropriate software and file types to develop and combine digital content.

Ākonga understand the role of operating systems in managing digital devices, security, and application software and are able to apply file management conventions using a range of storage devices. **They understand that with storing data comes responsibility for ensuring security and privacy.**

This progress outcome covers learning up to approximately Year 10. The elements in bold are covered in this challenge.

Nature of Technology (NZC)

There are also many connections to the Nature of Technology strand and learning outcomes where the relationship between humans and technology is explored at each Year level.

> *The nature of technology strand guides teachers to develop learning activities that support students to question why the world around them is the way it is. They develop perspectives and become aware of the relationship between people as users and designers/creators of technology and how that technology in turn impacts on more people, the environment, and on culture.*
>
> *They learn to critique the impact of technology on societies and the environment and to explore how developments and outcomes are valued by different peoples in different times. Students have opportunities to increase their understanding of the complex moral and ethical aspects that surround technology and technological developments. They ask big questions such as "if it can be done, should it be done?"* *TKI - Nature of technology*
>
> **Characteristics of Technology (CoT) -** Technology is defined as "purposeful intervention by design", and technological practice as the activity through which technological outcomes are created and have impact in the world. Technological outcomes are designed to enhance the capabilities of people and expand human possibilities. They change the made world in ways that have positive and/or negative impacts on the social and natural world. TKI - Characteristics of technology
>
> **CoT Teacher Guidance**:
>
> - Provide times to explore a range of technologies and guide them to identify examples of positive and negative impacts on people, society and/or the environment. (Level 2)
> - guide students to determine the impacts different technologies have had on society and/or the environment over time. (Level 3)

It should be noted that the Hangarau aho and Technology learning areas were revised in 2017 to strengthen the digital technologies content. Te Marautanga o Aotearoa and the New Zealand Curriculum is currently being refreshed and a new progressions based curriculum will be provided for implementation throughout Aotearoa from Term 1 2025.

The challenge supports future focused capabilities and 21st century skills

The TMoA and NZC support ākonga to develop future focused capabilities. The mātāpono whānui | overarching principles of both curricula serve as the first foundations on which educators, communities, and ākonga can begin to co-design their future focused and sustainable vision for learning.

> "Your students will develop their digital fluency through a range of authentic curriculum opportunities. Your local curriculum should emphasise the capabilities, principles, and literacies that students are expected to develop as they become more innovative, creative, and discerning in their use of a range of technologies."
> elearning.tki.org.nz/Teaching/Digital-fluency

Learning programme

Learning intentions

After completing the challenge, ākonga will be able to:

- Determine what information is best kept private
- Explain the difference between good and bad passwords and why
- Be conscious of what they are sharing over time
- Understand risks to personal safety from careless sharing

Module outline

The challenge consists of two modules:

1. Sharing responsibly

   This module introduces the concept of sleuthing - gathering information from what friends post online. It is always done openly and without malice. Ākonga should start to understand just how much information is being given away online.
2. Password security

   This module introduces ākonga to poor password practices like using very common, easily crackable passwords. Password cracking is always done with the express permission of the characters within the challenge. It's important to also address the ethics of hacking with ākonga.

Types of component:

 **Discussion**

 **Worksheet**

 **Computer-based Activity**

 **Group Activity**

 **Unplugged Activity**

 **Video**

 **Read**

 **Animation**

 **Reflection**

 **Game**

 **App**

Kōwae 1: Te Tuari Haepapa | Module 1: Sharing Responsibly

Preparation and timing

No prior knowledge is required for this activity.

Learning overview

- What is privacy?
- What information online can put you at risk?
- What does it mean to be “purposeful” about what you share?

In 2022, around 89 percent of the New Zealand population were active social media users according to Energise Web. Social media is a great way to stay connected with friends and family, but we need to be mindful of what we share and who we share it with.

Suggested Implementation

Online Module 1: Sharing responsibly

Computer-based Activity : Yr 6-8 Information Security and Privacy Challenge

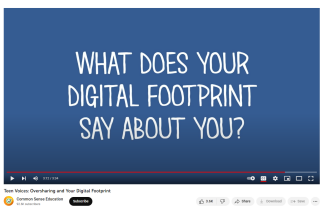
Ākonga can work through the first module of the challenge individually, in pairs or in small groups. As they go ākonga could reflect on the values, morals and ethics of being secure online. What behaviours would they like to see from others and what behaviours would they wish to develop in themselves…?

Kaiako could ask open-ended questions such as “how does this make you feel?” and “is this activity bringing up any new questions for you?”

As they work through the first module, use class time for unplugged activities and discussion on the topics covered in the module. Below are suggested activities to use in the classroom.

Activity 1

Video: Teens views on oversharing online - Teen Voices: Oversharing and Your Digital Footprint - YouTube



Ākonga watch the video and take notes about one thing they agree with, one thing they disagree with, and one thing they thought was interesting or hadn't thought of before.

Discussion:
Share points from the notes taken from the video.
Do ākonga generally agree or disagree with the video? Do they agree or disagree with each other?

In the video ākonga talk about "Digital Footprints" and what it says about you.

In groups, ask ākonga to discuss how they want to be viewed online? What online identity do they want to show the world? How does their digital footprint affect how people view them? What is the difference between "oversharing" and "purposeful sharing"?

Activity 2

Video: Introduction to not knowing who you're sharing with

How Much Should You Share Online? #CyberSafeKids

Easy-read online safety advice from Netsafe

Watch one or both of the videos with your class to provide background information for a discussion on sharing.

Discussion:

Do you really know who you are sharing your information with?
Have a discussion in pairs and then have a whole class discussion about the following questions:

Ask ākonga what the dangers of "oversharing" online are?
Why is privacy and security such a big deal?
What ways can you know exactly who you are sharing your information with?
How can you make sure you have good online security?

Go to this website:
Privacy and security : Keep It Real Online

View the website with ākonga and suggest they use the links suggested to review their privacy settings for any relevant social media accounts.

Activity 3

Unplugged Activity, Discussion : Cyber Security Card Game

This activity can be done with a printed set of cards that can be downloaded and printed from Cyber Skills Aotearoa (note: print double sided)

Cyber security is of increasing interest and concern in a world where we share so much data about ourselves. Students are often unaware of the risks of excessive sharing. Understanding how to protect and secure data is a vital step in being cyber secure. This activity will help students to take a proactive and skills-based approach towards their data.

How to play:
There are three categories of cards, **"Never share"**, **"OK to Share"** and **"Risky to share"**.

1- In groups, ask ākonga to look at the picture side and then sort the cards into two piles — Never share and OK to share — as quickly as possible. Don't mention the Risky to share category at this point.

2 - Ākonga then turn over the cards to see which pile they belong to, and whether their assessment of the risk differs from what's on the cards. They will see the Risky to share category and can discuss how this changes their initial choice. The back of the card explains why that piece of information is categorised this way, and will help prompt discussion.

Information
Most ākonga typically sort the information quite cautiously. The reason we didn't just categorise everything as risky or "not ok to share" is because we want to take into account the realities of social media and how important it is in teenagers' lives; we didn't want to encourage ākonga not to share anything as that would be unrealistic.

End of Module discussion questions:

Reflection **Group Activity**

Teens overwhelmingly spend much of their social lives online.

Come up with 5 Rules of Engagement to give to ākonga who have never been on social media before. How would you advise them to keep themselves safe and their private information private?

Module 1 Videos - Teacher's Notes

The answers to the activities are given in the kaiako notes that are provided for each page of the online challenge. Below are the suggested discussion ideas for each video in the module.

Video, **Discussion**

1. Privacy Settings

Discuss with ākonga about when they sign up to online services like social media apps, that they rarely consider the implications of the details they provide and the privacy settings on their profiles. This can be particularly problematic if the settings are too lenient - they may be giving personal data/information away without realising. Most services have improved their default settings considerably, so remind ākonga that it's still good practice to check what the settings on your profile are before you start using the service.

We use this opening video to raise the risks associated with having profiles set with all of your information public. When ākonga do sign up to services like social media apps, discuss with them how they can consider very carefully whether it is **useful or necessary for them to provide sensitive/personal information.**

What information do you need to enter to set up an account? Does this app need to know your address? Or your birthday?

And of course, once you've registered your account, go into the relevant privacy/security settings and make sure the information you're sharing/publishing is only viewable to the group of people you want to share it with.

Reflect on learning outcomes

- Information you enter into apps might be displayed so others can see it, so think carefully about what you provide; and
- Profiles on social media have settings that change who can see your information.

2. How private is private?

Discuss with ākonga how restricting access to personal information may not necessarily be enough to prevent unintended access to your data. The way you behave and interact with others on the platform plays a major role in what information may be available to others.

When profiles are *private*, the typical behaviour is that people you know on the platform - your *friends* or *followers* - can still see a lot of it. This makes it really important that you only accept friend requests from people you know and trust. It is common for beginning users of these platforms to accept friend requests from as many people as they can - both to increase their friend count (making them look more popular), and to ensure they don't miss out on things going on in their extended social circles.

Reflect on learning outcomes

Ask ākonga how they make important decisions when they ‘friend’ someone on social media. Discuss how ‘friends’ sometimes do things online that they wouldn’t ever do in real-life. Discuss what ākonga think are the reasons for this. Should this influence your choices about ‘friends’ online? Next, discuss with ākonga, how they decide who to connect with online. Do they have a criteria? What are those criteria? Do their parents/caregivers support and guide online use?

- Private profiles are visible to your friends and followers; so
- Only add friends that you know personally, and that you trust - usually people you know in real life and interact with regularly.

3. Information is everywhere

It's not always what you post directly that reveals information about you. You can be careful with the photos you share and updates you post, but the interactions and conversations you have with others when discussing what's been posted can lead to information being revealed. A conversation between a couple of friends might leave a trail for others to see that can be used to work out things like where you are or what you're doing.

This video uses an example of a friend who changes basketball teams. The new team members are discussing their training and game schedule allowing everyone to work out what time they are playing. They use this to go and watch the game to cheer her on, but it should be evident that this information could also be used for wicked or criminal activity.

Whether you're posting your own content, commenting on it, or commenting on the posts of others, it's important you think carefully about what you're sharing and how it could be used to find out more than you want to share.

Reflect on learning outcomes

Discuss with ākonga the ways that they are critical when online. Ask about the strategies they use to ensure their information goes where they intend. Ask if there are any new strategies they'll use after completing these activities.

- Even when you have your privacy settings locked down, conversations and comments can reveal things about you and your friends; so
- Think before you post and comment - never reveal private information in discussions on social media.

4. Information breadcrumbs

Examples before this question all exposed information in a single location, but sometimes it is a combination of information from lots of places - sometimes referred to as *breadcrumbs* (a reference to Hansel and Gretel) - that reveals things about you. The example in the video explains how small bits of information about a special promotional event revealed the location of a celebrity, and talks about how these types of "puzzles" can also be applied to individuals across multiple social media apps and locations.

It may not always be obvious, but when you can be recognised across multiple platforms and your identity can be linked between them, then any information shared on any of them can be pieced together to build a profile on you. For this reason, revealing any kind of information that can be associated with you – no matter how mundane it may be in isolation – needs to be carefully considered.

Learning summary

- A profile about you can be constructed from private information collected from multiple sources; so
- Be wary of any information posted on any platform that could include clues about you, your movements and activities.

Kōwae 2: Te whakamaru kupuhipa | Module 2: Password security

Preparation and timing

No prior knowledge is required for this activity.

Learning Overview

- What 'weak' passwords look like
- The risks of having weak passwords
- Features of strong passwords
- The ways that passwords can be shared

Suggested Implementation

Online Module 2 - Password security

Computer-based Activity

Ākonga can work through the second module of the challenge individually, in pairs or in small groups.

As they go ākonga could reflect on the values, morals and ethics of being secure online. What behaviours would they like to see from others and what behaviours would they wish to develop in themselves…?

Kaiako could ask open-ended questions such as “how does this make you feel?” and “is this activity bringing up any new questions for you?”

As they work through the first module, use class time for unplugged activities and discussion on the topics covered in the module. Below are suggested activities to use in the classroom.

Activity 1

Discussion: password strength

Short and commonly used passwords are very easy for computer programs to break. The fewer combinations of characters a computer has to try, the easier it is for a computer program to find the correct combination.

Unplugged Activity **Group Activity: Mastermind**

Go to this website:
https://www.wikihow.com/Play-Mastermind-With-a-Pencil-and-a-Piece-of-Paper

Print out enough Mastermind templates for the class. Templates can be found at
https://cmp.ac/mastermind

Video explanation of the rules:
How to Play - Pen and Paper Mastermind - YouTube

Follow the instructions on the Wikihow page to play the game of mastermind with paper…

Information
This activity is letting ākonga realise how easy simple and short passwords are to crack. It's so easy that humans can do it in about 12 steps so how quickly could a computer "guess" that short password?

Discussion: the first rule of passwords

In the Mastermind game, ākonga "cracked" a 4-character long password simply.
What do you think that tells you about the length of passwords?

Come up with the first rule of passwords!

Activity 2

Computer-based Activity : Kaspersky Password Checker

As an activity, ākonga can try some of the commonly used passwords from the list using Kaspersky Password Checker to determine how long it would take for a computer to crack those passwords. Then give the ākonga some examples of longer and harder-to-crack passwords to try out. Ākonga can try some of their own made-up examples as well. *Note: ākonga should not enter other people's passwords or their own, even though the site is safe.*

End of Module Activity

Discussion

This activity can be done as a class, group or as an extension or home-learning task. **Ideally this activity should be completed after ākonga have completed the online course.**

In groups, ask ākonga to choose an example of a bad password that they currently use. Go around the room and have each group read out their bad password, ākonga outside the group should say reasons why that password is bad.

Repeat the activity, this time asking ākonga to choose an example of a good password. When they read out their password to the class other groups should give reasons why they are good passwords.

How do the examples compare with the suggested rules in this poster?

Passwords - English

Passwords - te reo Māori

Ākonga then change their weak passwords to good passwords wherever they are used.

Information

More good advice about passwords is available at CERTNZ's advice on how to create a good password. Key points:

Make your password long and strong

- A *passphrase* rather then a password, at least 12 characters long:
    - Giraffesinabottle, mousehouserules, iplaypokemonloads (English)
    - Ngapotaemawhero, rerekitemarama, heturuharare i (te reo Māori)
- Includes symbols or numbers:
    - 2020wasatoughyear!, louis16thlosthishead, starwarsepisode3 (English)
    - Ruiatekorakorapiata9000, heomaroa300mita!, kaingiangahamupeka400!! Heahatetauaroote2020?! (te reo Māori)

Catching bad passwords

Common phrases

- There are lots of common phrases that are long and easy to remember but **because they are common they are no longer good candidates for passwords.** Especially if ākonga have shared their enjoyment of what the password is baked on in their social media: Lukeiamyourfather, iloveyou9000, blueyandfriends12

Hard to remember

- Ākonga may get carried away making up passphrases, coming up with overly long or overly complex passwords.
- Filddesticksbananafairybread45gamerkids - is long, but is **very difficult to remember meaning it is no longer a good password**

They should also come up with a symbol that represents a password. Direct ākonga to look at the complete emoji list https://getemoji.com/ ... which one do they choose to best represent password safety and why?

Information
Some ākonga are likely to pick a padlock and others might possibly pick a shhh face. It's worth having a couple that you've selected to encourage discussion about what features of each image represents a password and which don't.

🔐 🔓 🔑 🤫🛑

Module 2 Videos - Teacher's Notes

The answers to the activities are given in the kaiako/teacher notes that are provided for each page of the online challenge. Below are the suggested discussion ideas for each video in the module.

1. Common passwords

The video introduces the concept of a "hack", and Sam uses this as an opportunity to explain how this often occurs when a password attached to an account is poorly selected.
There are some passwords that get used by people regularly when they don't really care about the account they have set up. These passwords are far more common than most people realise, and should never, ever be used - not even on accounts or services you don't think are important. A list of these passwords is presented in the next problem.

Reflect on learning outcomes

- Really simple/common passwords should never be used because they are easily guessed by hackers. Ask ākonga if they were aware of online "hacks/hackers". Share stories of any incidents of people being "hacked".

2. Easily guessed passwords

We have to manage a lot of accounts for a range of purposes - everything from our social media accounts to our school and TV streaming logins, so having to keep track of lots of different passwords can be really hard. People therefore tend to fall back on setting passwords based on things they can remember and care about; usually hobbies, pets, sports teams, children or similar.

Unfortunately, this information is also easily found by hackers; we often post updates and photos that reveal these kinds of information on a daily basis. When creating passwords, you should avoid basing them on things that are strongly connected to you, since they can be guessed with a little bit of investigation into your online behaviours.

Reflect on learning outcomes

Passwords should never be based on things that can be easily tracked back to you; so

- Never use things like sports teams, pets, favourite foods, hobbies, or other easily guessed topics.

Ask ākonga how they feel their cyber security is developing? Is it helpful to know what goes on in the background online - what other people can do to access/steal their private information/data?

3. Symbols aren’t secure

Due to many organisations requiring complexity in passwords - the need for uppercase, lowercase, numbers and symbols - many people have adjusted their passwords by swapping characters around. This will often meet the requirements for "secure" passwords, but in reality these substitutions are so easily predicted they provide no additional security for your accounts.

The next question uses the information Hine reveals in this video - the use of her cat's name, Popcorn, as a password - as the basis of a symbol substitution. The hints in the problem will walk ākonga through the substitutions required to guess her password, and once aware of this type of strategy, working out how passwords are made "complex" becomes a straightforward exercise for ākonga.

Reflect on learning outcomes

Ask ākonga how they could make it harder to guess a password? Guide them to realise that some people swap letters around for numbers and symbols. This might feel like it's harder to guess, but hackers know that people do this, so they can guess what changes you've made too!

- Swapping characters in passwords for symbols or numbers to meet complexity requirements doesn't make your password more secure; so
- As previously stated, make sure your passwords aren't based on things that can be found out about you.

4. Passphrases quick guide

Passphrases are the solution to many of the issues associated with weak passwords. Even young ākonga can remember them (even though they may seem long), and their length and complexity are automatically built into their construction.

Ākonga should be encouraged to change their existing passwords if they aren't already using passphrases as a strategy.

Reflect on learning outcomes

- Passphrases are strong passwords because they are long, hard to guess and easy to remember; so
- If you aren't already using a passphrase on one of your accounts, make one up and change your password!

5. Reusing passwords is risky

When people come up with a strong password that they can easily remember, they have a tendency to reuse that password in multiple locations. This is particularly bad, since it means if the password is discovered for one account, that same password can be used to break into every other account that user has on other services.

Passwords can be revealed through no fault of the user themselves (and we cover this in more detail in the high school version of this challenge) due to data leaks, so even if you're doing everything else correctly, reusing a password makes all of your accounts susceptible to risk.

Reflect on learning outcomes

Discuss if ākonga have ever reused a password. Ask if they can explain why this isn’t secure.

- Reusing a password means that if one of your accounts is compromised, all of the accounts using the same password can be as well.