Information Privacy and Security (9-13) - Cyber Skills Aotearoa

Te Mōhiohio Tūmataiti me te Whakahaumaru (9-13) – 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

Ngā Ihirangi | Table of Contents

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.

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

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

Nau mai, haere mai | Welcome

This guide supports kaiako to create an effective learning programme based on the Cyber Skills Aotearoa Yr 9-13 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.

Let's start with a definition: cyber security is a fancy name for a collection of tools and methods that people or companies use to protect themselves, their networks, systems or programs from attack. Attackers are usually trying to get access to electronically stored sensitive information, or to steal money.

So understanding these tools and methods is a pretty good way to learn how to keep yourself safe online. But not just that - cyber security is a great source of future jobs. There is a significant shortage of people with the skills to help protect companies and other people.

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, and problems to test understanding and skills. The video resources are designed to teach ākonga cyber security concepts, as well as 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 4-6 hours, but may take longer depending on time spent on off-line activities and classroom discussions.

How the challenge relates to The New Zealand Curriculum

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

> "With its focus on design thinking, technology education supports students to be innovative, reflective and critical in designing new models, products, software, systems and tools to benefit people while taking account of their impact on cultural, ethical, environmental and economic conditions.
>
> 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 Technology learning area addresses cyber security in these key areas:

Digital Technologies (NZC)

- **Computational Thinking for Digital Technologies and Designing and Developing Digital Outcomes** focus on developing students' capability to create unique digital outcomes for specific needs and 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.

- **Computational Thinking for Digital Technologies** (CTDT) – ākonga will develop an understanding of computer science principles that underlie all digital technologies. They'll learn core programming concepts so that they can become creators of digital technology, not just users.

- **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 information security 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.**

NZC Technology/Digital Technologies
Computational Thinking for Digital Technologies Progress Outcome 7 (CTDT PO7)

In authentic contexts and taking account of end-users, **students analyse concepts in digital technologies** (for example, information systems, encryption, **computer security**, error control, complexity and tractability, autonomous control) **by explaining the relevant mechanisms that underpin them, how they are used in real world applications, and the key problems or issues related to them**.

Assessment specifications Level 2 Digital Technologies and Hangarau Matihiko 2023 DCAT

For **computer security**, questions may cover: ***spam emails, two-factor authentication, reCAPTCHA, common issues, steps individuals should take to protect their data, data privacy, ways to protect individual computers*** and computers managed by an organisation, policies or practices of a multi-national technology corporation. Assessment Specifications » NZQA

DDDO progress outcome 3 covers learning up to approximately Year 10. CTDT progress outcome 7 covers learning up to approximately Year 12. 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:

- guide students to determine the impacts different technologies have had on society and/or the environment over time. (Level 3)
- guide students to understand that "expanding human possibilities" can result in positive and negative impacts on societies and natural environments and may be experienced differently by particular groups of people. (Level 4)
- guide students to analyse a range of examples of technologies to examine how people’s perceptions and/or level of acceptance has influenced the practices and decisions underpinning their development and implementation (Level 5)

It should be noted that the Technology learning areas were revised in 2017 to strengthen the digital technologies content. 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 NZC supports ākonga to develop future focused capabilities. The overarching principles of the curriculum 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

Hōtaka ako | Learning programme

Learning intentions

After completing the challenge, ākonga will be able to:

- Determine what information is best kept private
- Be conscious of what they are sharing over time
- Understand risks to personal safety from careless sharing
- Explain the difference between good and bad passwords
- Understand the risks of reusing passwords across multiple sites
- Determine if their personal information has been put at risk via a data breach
- Take appropriate action if their personal information has been involved in a data breach
- Utilise multifactor authentication (MFA) to provide extra-security when protecting their online information.
- Recognize phishing and scam messages and take appropriate action in their responses to these messages.

Module outline

The challenge consists of four modules:

1. **Purposeful sharing -** *Learning Focus: Be secure, Be share-aware, Know the risks*

   As they work through this module, ākonga should start to understand just how much personal information is being given away online through their profiles and posts. They also see how friends and whānau can inadvertently share private information about them. A key message is that lots of small pieces of information can provide a bigger picture for hackers and scammers.

   This module introduces the concept of sleuthing - gathering information from what they as well as friends and whānau post online. All problems that involve sleuthing are done openly and without malice.

2. **Passwords -** *Learning Focus: Be secure, Be share-aware, Know the risks*

   In this module, ākonga learn about the importance of keeping passwords safe, how hackers can guess passwords from information they have shared, and how to create strong passwords. They learn about poor password practices like using very common, easily crackable passwords and sharing passwords with others.

   In the problems, 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.

3. **Password reuse and MFA -** *Learning Focus: Be secure, Be critical, Know the risks*

   In this module, ākonga learn about what can happen when they reuse passwords. When people come up with a strong password that they can easily remember, they have a tendency to reuse that password in multiple locations and this puts their data and privacy at risk.

   They learn about data breaches and how if someone gains access to their password through a data leak, they can access all their accounts that use that email/password combination!

   In addition to using strong unique passwords, ākonga learn about other ways to protect their online accounts, such as using multi-factor authentication.

4. **Scams and phishing -** *Learning Focus: Know what's hidden, Be critical, Know the risks*

   Scams are really common. Many of us receive scams in our feeds, our inbox, our messages and through phone calls every week! It's almost impossible to avoid receiving scams, so it's really important to learn how to recognise one, and how to respond to it, in order to help protect personal information (and money!)

   Ākonga learn all about the most common scams that people receive, and find out how best to respond.

   They will also hear from industry experts - people who spend their work days stopping these scams, and helping people who have fallen for them

Kōwae 1: Te tuari whaitake | Module 1: Purposeful sharing

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

Computer-based Activity : Yr 9-13 Information Security and Privacy Challenge

Complete Module 1: Purposeful sharing

As ākonga 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.

Video: These children face the reality of growing up online I UNICEF These children face the reality of growing up online I UNICEF

Discussion

Discuss in small groups:

Why are ākonga in the UNICEF video so uncomfortable about strangers knowing so much about them when ākonga themselves posted this information? Would they feel comfortable sharing their personal details and social media conversations with a stranger?

What are the differences between online vs real friendships as well as sharing information with online friends, contacts and followers vs real-world friends. Do ākonga know all their online friends and followers personally?

🎞**Video: Growing Up Digital - Privacy Segment**
Growing Up Digital - privacy segment - FUSE - Department of Education & Training

🎞**Video: Teen Voices: Oversharing and Your Digital Footprint**
Teen Voices: Oversharing and Your Digital Footprint

✏ Ākonga watch either one or both of these videos 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 "Oversharing", in the resources we talk about "Purposeful sharing".

What do you think are the differences between these two terms? Do you like the use of oversharing? Or Purposeful sharing or some other term and why?

Lead and support ākonga to talk about what is meant by oversharing or purposeful sharing. The terms are very similar, the reason we chose purposeful sharing is because it doesn't imply that sharing is **bad,** just that you need to be thoughtful about the picture you're building about yourself.

Example questions: Have you heard a message that children shouldn't share much at all on social media? Is that practical? Where do you think the line is between what's OK to share and what isn't? Is not sharing at all on social media practical? Why?

Through previous cyber safety education programs or from home, ākonga may have been given messages ranging from "don't go on social media" to "be careful on social media". Depending on the prior learning of ākonga in the class, the discussion can either start from checking what they know about purposeful sharing or examples they might be able to provide of purposeful sharing.

Maybe talk about different content being appropriate for different audiences. Discuss the fact that even when you share with only a few people that data is only as safe as the platform it's posted on and the site has access to everything for marketing purposes.

✏ **Unplugged Activity: Cyber Security Card Games "Know your risks"**

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.

Reflection **Group Activity**

Teens overwhelmingly spend much of their social lives online.

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

Additional privacy and security information

Now that ākonga have completed this module, they may want to consider their privacy settings. Here is some guidance about privacy settings on different social media sites:
Keep it Real Online: Privacy and security

Kōwae 2: Ngā kupuhipa | Module 2: Passwords

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

Computer-based Activity : Yr 9-13 Information Security and Privacy Challenge

Complete Module 2: Passwords

As ākonga work through the this 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.

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: How to Play Mastermind With a Pencil and a Piece of Paper: 8 Steps

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…

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

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!

Video: Dictionary and Substition attacks - NordVPN

Dictionary Attacks Explained | NordVPN

Text article link: What is a dictionary attack? | NordPass

In addition to trying different combinations of letters or numbers, password-cracking programs use a variety of techniques to try to discover a password. For example, they will check passwords against the lists of known common passwords or against words from regular dictionaries.

Another password-cracking technique is known as a substitution attack. They take common words and names and replace letters with numbers and symbols, such as 3 for E, or @ for a. So a password of *s3cr3t @g3nt* is no more secure than the password of *secret agent*. They also look for sequences of numbers or letters such “123456” or “asdf”.

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.*

Wrap up:

Reflection **Group Activity**
Passwords are used everywhere

In small groups ākonga start to develop the rules of good passwords - at least 3.

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.
🔐 🔓 🔑 🤫🛑

Kōwai 3 - Te whakamahi anō i te kupuhipa me te MFA | Module 3 - Password reuse and MFA

Preparation and timing

Before starting this activity ākonga should have completed the Module 2 Passwords online activity. This is an extension of those ideas.

Learning Overview

- What are the issues surrounding password reuses?
- What is a data breach and what are the consequences, especially when passwords are reused?
- What are issues with security questions?
- How can MFA provide extra security than passwords alone?

Suggested Implementation

Computer-based Activity : Yr 9-13 Information Security and Privacy Challenge

Complete Module 3: Password reuse and MFA

As ākonga work through this 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.

Video: Cyber Security (by Crash Course Computer Science) https://www.youtube.com/watch?v=bPVaOlJ6ln0 (12:30)

Information
Note that this video is designed to get across a lot of information in a very short amount of time. The ākonga are not expected to understand all that information on the first viewing. It's more important that they engage with it and have a discussion afterwards.

This video moves pretty fast. Write down 2-3 things you learned from the video, maybe that's a definition or maybe it's something you haven't heard of before or something that made you think..

Discussion: What did we learn from the video?

Get ākonga to share their 2-3 things they learned with another student and decide which of the 4-6 things they both agree are the most important. Then get the pair to work with another group, and

try to convince the other group why the thing they thought was important should be chosen by all four...
Continue this process until there is one agreed point as the most important. Why did we all agree this was the most important one? Share a couple of the others.

💬 Discussion: Well-known data breaches and their consequences

This is an opportunity to have a class discussion about well-known data breaches and their consequences. A resource that provides information about large data breaches is 98 Biggest Data Breaches, Hacks, and Exposures [98 Biggest Data Breaches, Hacks, and Exposures [2022 Update] - Termly](#) . Students may have accounts on some of these sites, for example, Neopets.

💬 Discussion: The importance of having different passwords for different sites and apps

Reusing passwords, especially on important accounts where money or private information is stored, can put you at risk for cybercrime. Discuss with students the importance of having different passwords for different sites and apps. Do all websites and apps have the same level of security? What are some websites or apps they use that would be low-security vs high-security? Do they use the same password for social media apps like TikTok and Instagram? If they use online banking or shopping, do they use the same password as for their social media apps?

This is also a good opportunity to have a class discussion on password reuse and for students to think about what might happen if their email and password were leaked in a data breach. Do they use the same password for everything?

🖥 Computer-based Activity : Have i been pwned?

As an activity, students can use the website [Have i been pwned?](#) to check whether any of their emails have been involved in a data breach. Encourage students to change their passwords if they have discovered any that have been breached

💬 Discussion: The importance of having strong device passwords

Often we overlook the importance of a strong, unique device password. Many ākonga use simple device passwords because they don't recognise that once a person has access to their device, they can access all passwords saved in a browser. They also often share device passwords with their friends.

It is a good opportunity to have ākonga update their device passwords and consider the pros and cons of saving their passwords in the browser. Ākonga could also research various password managers for their personal use.

Email is the key: Background information

If someone can get into your email account, they can get access to other places. Think about going on to a social media site that you haven't been to in a while. If you don't use the same password for everything - which is a really good idea - then there's a possibility that you might have forgotten the password.

How do you resolve this problem? Well, that's easy. You just click on the forgot password link and you type in your email address. A couple of seconds later you will have an email with a link to enter a new password and you're on your way.

Have you ever stopped to think what would happen if someone else could have access to your email?

Even if you have strong, unique passwords for all your different accounts, they can likely be reset using your email in the same way you found so convenient.

As well as that, bad people can use the information in your email to discover all the various accounts that you have, and try to gain access to them.

If a person who now has access wants to do you harm, they could lock you out of your own social media accounts. They could pretend to be you online and say things you may not say yourself.

Some email providers will let you know if you sign on from a different location or different device. This is great because it gives you a chance to quickly block any unauthorised access. Depending on how quickly you respond, some damage might already have been done.

When choosing passwords and balancing risk, remember your email account is like a master key to your online presence. So make it especially secure.

Discussion: Email is the key

Have ākonga brainstorm all the accounts that they access using their email address. Then in small groups have them create a list of potential threats that can arise if somebody has access to their email accounts. Groups can share their ideas with the class.

🎞Video: Introduction to Multi-Factor Authentication: Network Direction
[Introduction to Multi Factor Authentication (MFA)]

🎞Video: Trend Micro Cyber Academy - Episode 2 – Two Factor Authentication

[Trend Micro Cyber Academy - Episode 2 – Two Factor Authentication]

These videos explain MFA and 2FA for students. Choose one to use with your students, depending on suitability and age group.

💬Discussion: When should you use MFA?

Ask students to brainstorm a list of the different types of multi-factor authentication they currently use. What types of apps or websites do they think are important to have MFA enabled? Are there accounts where they haven't turned on MFA and think they should? Where appropriate, allow students time to add MFA to the accounts they feel need extra security.

💬 Bonus Discussion:
Lead the discussion to talk about Biometric data such as fingerprints, iris scans and facial recognition. What kinds of issues are raised by these forms of security?

What happens if a fingerprint or iris scan gets hacked… What do you do then? These are tricky ideas, there isn't really a solution. Multi-factor Authentication is really the only mitigation of issues with biometric data.

✏Unplugged Activity: Security questions guessing game

1. Ask students to write down the answers to some common security questions. They should keep their answers hidden from their classmates. For example:

Favourite sports team
City where they were born
Year 1 teacher
Favourite pet's name

2. Have the students work in small groups. They should take turns trying to guess the answers to each other's security questions.

3. Have the students keep track of how many guesses it takes to break a security question.

4. Ask students to write down whether or not someone would be able to guess their answers just by looking at their social media posts.

Reflection **Group Activity**
Passwords are used everywhere

In the small groups from the previous passwords activity, ākonga finish developing the rules of good passwords. Based on the knowledge from this module, they should be able to add a few new rules.

Put rules in a document and include the emoji from the last module.
Share the rules with the class, do any groups differ on the rules? Do the rules match what is currently used as your school password policy? If not, can you imagine or find out why not?

How do the rules they have developed compare with the suggested rules in this poster?

Passwords - English

Passwords - te reo Māori

Bonus Discussion:
At companies that really care about security you have to change your password immediately if you ever enter it into a different website (e.g. if you use it on another account). Why do they do this? Is it important or overkill?

Other companies have a mandatory policy to force employees to change their passwords regularly (e.g. every 3 months). What might be some of the advantages and disadvantages of this?

Kōwai 4 - Ngā tāware me te hītinihanga | Module 4 - Scams and phishing

Preparation and timing

Before starting this activity ākonga should have completed the Module 3 Password Reuse and MFA online activity. This is an extension of those ideas.

Learning Overview

- What are red flags to look out for in scams?
- The appropriate steps to take if a scam is suspected.
- What are issues with security questions?
- How can MFA provide extra security than passwords alone?

Suggested Implementation

Computer-based Activity : Yr 9-13 Information Security and Privacy Challenge

Complete Module 4: Scams and Phishing

As ākonga work through this 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.

Video: Going phishing: Kiwis losing tens of millions to ‘cyber baddies’

Scams are a huge problem in Aotearoa New Zealand. According to CERTNZ, in 2022 New Zealanders reportedly lost $9 million to internet scams in just three months.

It is no shame to be scammed, it's very common. It's important to know how to spot scams, and how to protect yourself.

This video provides a good introduction to phishing scams and reviews the steps you can take to protect yourself.

Going phishing: Kiwis losing tens of millions to 'cyber baddies'

The most effective way of protecting yourself is having multi-factor authentication (MFA) on all important accounts, and knowing what red flags to look for to identify scams.

The red flags are:

- if it's from an **untrusted source**
- if you're put **under pressure** to answer quickly and act fast;
- if what they're offering is **too good to be true**; and
- if it's an **unsolicited message**.

Additional print resources for the classroom:

Phishing and Scams Poster - English

Phishing and Scams Poster - te reo Māori

✏ Unplugged Activity: identifying red flags

Review the red flags with ākonga and as an activity have them identify red flags in examples that either you as a teacher provide or examples from their own emails/messages/social media feed as appropriate for your class.

Follow up with actions that ākonga should take when they spot a scam, such as not clicking on any links or downloading any attachments, deleting the message, and reporting the message to a trusted adult if necessary.

🎞 Video: Get Cyber Safe | Phishing Shanty

Get Cyber Safe | Phishing Shanty (Ruin a Cyber Criminal's Day)

Do you know what *Phishing* is? It's a special form of scam, where the goal is to steal your identity! Ākonga should understand that scammers can impersonate someone they trust or message them from a compromised account belonging to their friends, family members or trusted organisations. Everyone should look out for red flags of scam messages and, *if you're in doubt that it's really that person or organisation sending the message, check with the person or organisation over the phone.*

💬 Discussion

Discuss with ākonga why it's important to keep answers to secret questions really secret. Scammers can try sneaky ways of getting private information from you, so we recommend being wary of requests for this information that seem dodgy.

It's also important to be cautious when someone requests private information from you, even if it's through something fun like a quiz. This article discusses some more examples of why responding to quizzes like this on social media can be a bad idea.

Group Activity:

In small groups have ākonga discuss if they have taken part in on-line quizzes or social media reposts asking for answers like “favourite” things or “placed lived”, etc. Would any of their answers potentially reveal private information?

Final Reflection on learning outcomes

Throughout the four modules, ākonga have learned cyber security concepts focussing on the following key principles:

- Be secure
- Be share aware
- Know what's hidden
- Be critical
- Know the risks

As a final reflection, have ākonga (either in small groups or as individuals) discuss their key take-away learning in each category and what actions they have taken or will take as a result of completing the modules.