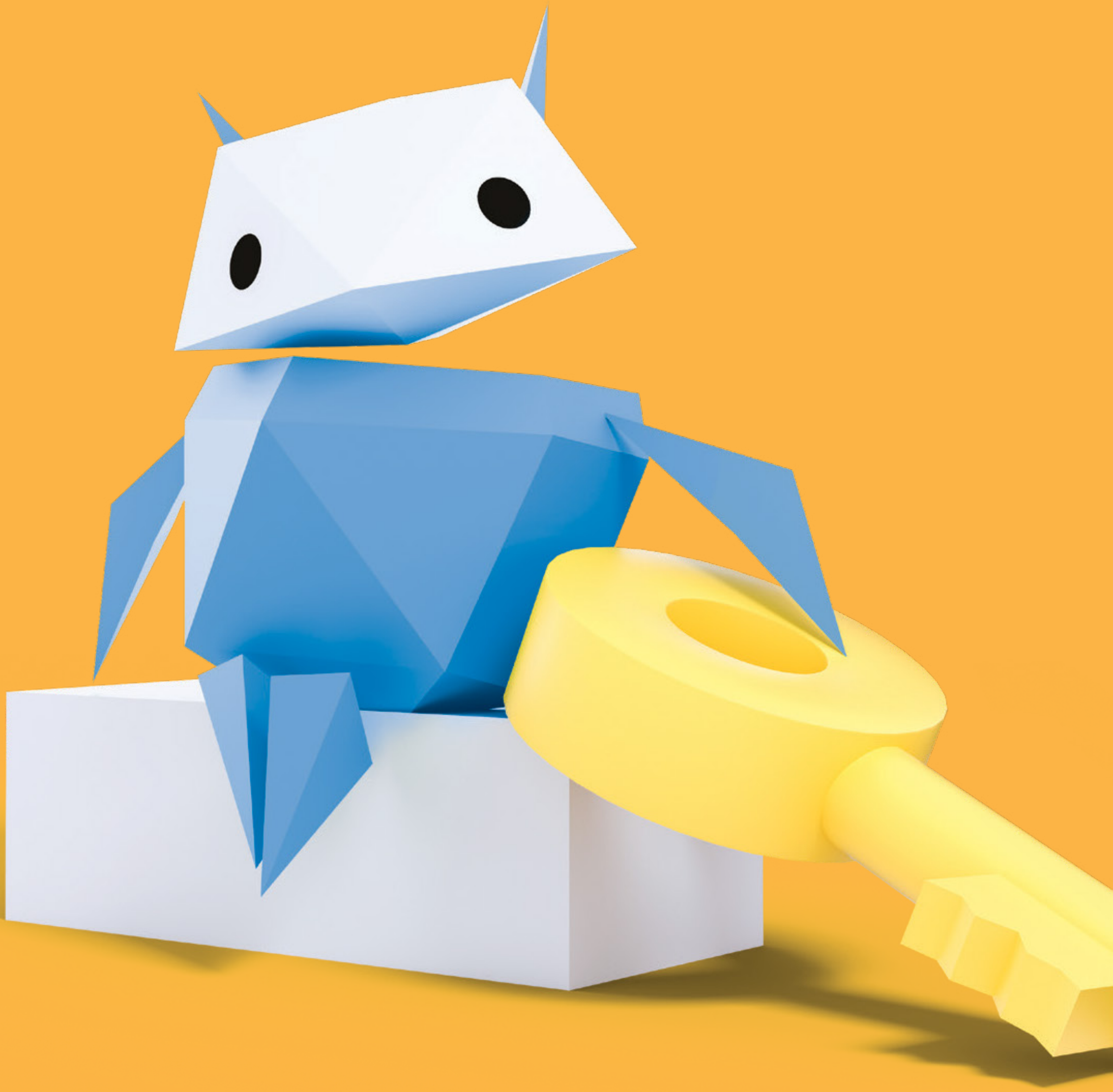
Be Internet Secure: Pillar 3

Protect Your Stuff



Be Internet Legends.

Activity pack

Welcome to your Be Internet Legends Secure pack

In this pack, you will find a range of activities that will teach pupils to Protect Their Stuff when they're online.

The activities look at ways of protecting information online and asking for help if you are concerned about yours or others' safety.

They also teach children the importance of having private and secure passwords for their accounts and devices.

The activities help pupils understand why protecting their personal information online is so important and to be aware that the information they put online is not necessarily safe nor private.

Getting Started

On the next page, you will find an in-depth guide to teaching these activities – including objectives, outcomes, assessment opportunities and plenary.

You will also find a vocabulary sheet, containing definitions of the words and phrases used in the activities.

You can use this pack alongside the curriculum lesson plans, which you can download separately.

If you have any questions, email **legends@parentzone.org.uk**.

Be Internet Secure: Pillar 3

Protect Your Stuff

Be realistic about privacy and security

Detailed lesson plans

Ages 7-9: Lesson 2, Lesson 4
Ages 9-11: Lesson 9

Pillar summary

Anyone who uses a device that's connected to the internet – a game console, a phone, a digital assistant, a computer, etc. – needs to know the basics of online privacy and security. Protecting those devices and the personal information on them – all that stuff about you, your family and your friends – means thinking about what's incoming and outgoing and being smart about passwords.

Objectives
Pupils will learn

- ✓ **Why** privacy and security matter and how they relate to each other.
- ✓ **Practise** how to create strong passwords and keep them to yourself (and the adults who watch out for you).
- ✓ **Review** the tools and settings that protect against scams, hackers and other threats.

Outcomes
Pupils can

- ✓ **Explain** why it's important to keep personal information private online.
- ✓ **Describe** ways to keep personal information private online by using safety tools and privacy settings.
- ✓ **Describe** how to find and ask for help if someone feels unsafe online.

Activity guide

Activity 1	**But that wasn't me!**	Ages **7-11**
Activity 2	**How to build a strong password**	Ages **7-11**
Activity 3	**Shh... Keep it to yourself**	Ages **7-11**
Activity 4	**Taking care of yourself and others**	Ages **7-11**
Activity 5	**Interland: Tower of Treasure**	Ages **7-11**

Assessment opportunities

- Assessing pupils' pre-existing knowledge in the introductory activity.
- Think, pair and share with peers
- Class discussion and teacher circulation during activities.
- Pupils responding to scenarios.

Plenary

Pupils share advice based on what they've learnt.

Be Internet Secure
Vocabulary

Activities 1–5

Privacy: Protecting people's data and personal information (also called sensitive information).

Security: Protecting people's devices and the software on them.

Settings: Options in a software program or a hardware device that changes it to the user's preference. E.g., if you struggle to read small writing, you can change the font settings to a larger size.

Activity 1

Digital footprint: Your digital footprint is all the information about you that appears online. This can mean anything from photos, audio, videos and texts to 'likes' and comments you post on friends' profiles. Just as your footsteps leave prints on the ground while you walk, what you post online leaves a trail too.

Reputation: The ideas, opinions, impressions, or beliefs that other people have about you – something that you can't be totally sure about but that you usually want to be positive or good.

Activity 2

Hacker: A person who uses computers to gain unauthorised access to other people's or organisations' devices and data.

Password or passcode: A secret combination used to access something. It can take different forms; for example, you may have a numbers-only code that you use for your phone lock and much more complex passwords for your email and other accounts. In general, it's important to make your passwords as long and complex as you can while still being able to remember them.

Activity 3

Settings: This is the area in any digital product, app, website, etc., where you can manage, or 'set' what you share and how your account is handled – including your privacy settings.

Two-step verification (also called two-factor verification and two-step authentication): A security process where logging in to a service requires two separate steps or two 'factors,' such as a password and a one-time code. For example, you may have to enter your password and then enter a code that was texted to your phone or a code from an app.

Be Internet Secure: Activity 1

But that wasn't me!

Pupils explore outcomes of sharing their passwords and the impact those actions can have.

Activity

You'll need:

- Worksheet: 'But that wasn't me!' (one copy per pair)

Pupils complete this in pairs.

1. Pick an account

Pupils choose what type of account they're sharing a password for and fill it in at the top of the worksheet: social media account, gaming account, phone, tablet/computer or streaming service.

2. Pick an action

Partners fill in the first box with an action they choose from the choices below – or think this up themselves. This is an action taken by someone who has been given the password to their account. They can draw or write what they come up with **or** choose from these possible actions:

- 'Likes' all of your crush's recent posts.
- Buys £500 worth of clothes.
- Sends a message like, 'Don't you think Pratheesh is so annoying?'
- Plays your favourite game but loses points.
- Downloads new apps.
- Shares an embarrassing picture on your social media page.
- Reads all your texts and shares them with someone else.
- Watches episodes of an inappropriate TV programme.

3. Create an outcome

In the second box, pupils create a possible outcome to the action they chose or created.

4. Discussion

As a class, ask a few pupils to share the action and outcomes they chose or created. Below are some questions:

- Why did you pick (or create) that action?
- How did you decide on the outcome?
- If you knew this was the outcome, how would you change your action?

5. Digital Footprint

Write a sentence of how this action and outcome impacts a person's feelings, life or digital footprint – any or all of those things. Guide pupils to think about how this affects their reputation or how others view them. Discuss different responses.

Continued on the next page ⟶

Let’s talk

What happens when you share your password?
We all make passwords for the different devices we have or websites we use. Discuss if anyone has ever shared their password with anyone else – even a family member. All these passwords go towards making your digital footprint. This represents individuals online – everyone who goes online has one. It’s what all the things you leave online – likes, comments, your screen name, photos, messages, recordings, etc. – add up to and give other people an idea of what you’re really like.

It affects your reputation, how people think of you. People can make guesses, or assumptions, about you based on that footprint you leave. That’s one really important thing to be aware of when you’re online. When passwords are shared, you are giving someone else control of your digital footprint – you’re actually allowing them to help create it and shape how other people think of you. So, if someone with your password does something you don’t like, people will think that was you doing it! That’s why it’s super important not to share your passwords.

For example: Let’s say you share your password to a social media account with a friend. While logged in as you, your friend sends a message to someone in your class like, ‘Can you send me your homework answers?’ The next day in class, the pupil goes to the teacher and says you were trying to cheat on your homework by asking for answers. Then they show your teacher the message your friend sent from your account. Who do you think your teacher will believe? How does this affect your reputation? What else might happen?

Brainstorm with the class possible outcomes. Examples: Teacher calls home. You get into trouble and miss break time at school and lose privileges at home. Your digital footprint shows that you tried to cheat in school. You get into a fight with your friend who sent the message.

Remember, your digital footprint represents you online. Any time you share your password with someone, you are giving them control of your digital footprint, which can impact how people see you on the internet and everywhere else.

Summary

When you share your password, you are giving someone else control of your digital footprint, but you’re still accountable for whatever they do with it. If you want to be in the driver’s seat when it comes to how people see you online, don’t share your passwords with anyone but a parent or other adult you totally trust.

Continued on the next page ⟶

Worksheet: Activity 1

But that wasn’t me!

I shared my password to:

□ social media account □ gaming account □ phone

□ tablet/computer □ streaming service □ ____________________

Action

Outcome

Digital Footprint Impact

Be Internet Secure: Activity 2

How to build a strong password

One thing that can help ensure our personal information is safe online is to use a strong password. What do you think a strong password could be?

Pupils learn how to create a strong password – and make sure that it stays private after they create it.

Activity

You'll need:

- Internet-connected devices for pupils or groups of pupils
- A whiteboard or flipchart
- Handout: 'Guidelines for creating strong passwords'

Let's play the password game:

1. Create passwords

We'll split into teams of two. Each team will have 60 seconds to create a password.
Challenge option: Pupils share clues with the class first to see how much contextual information the class needs to be able to make an accurate guess.

2. Compare passwords

Two teams at a time will write their password on the board.

3. Vote!

For each pair of passwords, we'll all vote and decide whose is stronger.

Let's talk

Better safe than sorry

Digital technology makes it easy for us to communicate with friends, classmates, teachers and relatives. We can connect with them in so many ways: texts, games, posts and messages; with words, pics and videos; using phones, tablets, laptops and digital assistants. What other ways can you think of?

But the same tools that make it easy for us to share information can also make it easy for hackers and scammers to steal that information and use it to damage our devices, steal our identities or hurt our relationships and reputations.

Protecting ourselves, our information and our devices means doing simple, smart things like using screen locks on phones, being careful about putting personal information on devices that are unlocked or used by lots of people (like at school) and, above all, building strong passwords – **and not sharing them!**

- Who can guess what the two most commonly used passwords are? (Answer: '123456' and 'password')

Continued on the next page ⟶

- Let’s brainstorm some other bad passwords and what specifically makes them bad. (Examples: your full name, your phone number, the word ‘chocolate’, your dog’s name, your address.)

Who thinks these passwords are good?

Summary

Here’s an idea for creating an extra-secure password. Think of a fun phrase that you can remember. It could be your favourite song lyric, book title, film, catchphrase, etc.

- Choose the first letter or first two letters of each word in the phrase.
- Change some letters to symbols.
- Make some letters uppercase and lowercase.

Continued on the next page ⟶

Guidelines for creating strong passwords

Here are some tips for creating passwords to keep your information safe.

Strong passwords are based on a descriptive language that is easy for you to remember and hard for someone else to guess – like the first letters in words that make up a favourite title or song, the first letters of words in a sentence about something you did – and include a combination of letters, numbers and symbols. For example, 'I went to Western Primary School when I was in Year 4' could be used to build a password like: Iw2We$t4g3.

Moderate passwords are passwords that are strong and not easy for malicious software to guess, but could be guessed by someone who knows you (for example, 'IwenttoWestern').

Weak passwords commonly use personal information like a pet's name, are easy to crack, and can be guessed by someone who knows you (for example, 'IloveBuddy' or 'Ilikechocolate').

DOs

- Use a different password for each of your important accounts.
- Use at least eight characters. The longer the better (as long as you can remember it!).
- Use combinations of letters (uppercase and lowercase), numbers, **and** symbols.
- Make your passwords memorable so you don't need to write them down, which would be risky.
- Immediately change your password if you think someone else knows it (besides a parent or guardian).
- Change your passwords every now and then.
- Always use strong screen locks on your devices. Set your devices to automatically lock in case they end up in the wrong hands.
- Consider using a password manager, such as one built into your browser, to remember your passwords. This way you can use a unique password for each of your accounts and not have to remember them all.

DON'Ts

- Don't use personal information (name, address, email, phone number, national insurance number, mother's maiden name, birth dates or even a pet's name, etc.) in your password.
- Don't use a password that's easy to guess, like your nickname, name of your school, favourite football team, etc.
- Don't share your password with anyone other than your parents or guardian.
- Never write passwords down where someone can find them.

Be Internet Secure: Activity 3

Shh... Keep it to yourself!

Use a school device to demonstrate where to look, and what to look for, when you're customising your privacy settings.

Activity

You'll need:

- One school device hooked up to a interactive whiteboard and able to display an example account deemed appropriate for class demonstration (e.g., a temporary email or class account)

Review options

Ensure your laptop/PC is hooked up to a screen/interactive whiteboard. Navigate to the settings page of your chosen site so you can all see what the options are. Discuss:

- Changing your password
- Making your page or online profile – including photos and videos – public or private (visible only to the family and friends you choose)
- Going through your location and other settings. Which ones are best for you?
- Getting alerts if someone tries to log in to your account from an unknown device
- Getting an alert when somebody tags you
- Enabling two-factor or two-step verification
- Setting up recovery information in case you get locked out of your account
- Reporting problems

Which privacy and security settings are right for you is something to discuss with your parents or guardians. But remember, the most important security setting is in your brain. As you grow up, more and more you'll be the one deciding how much of your personal info to share, when and with whom. So, it's important to get used to making these decisions right now.

Let's talk

Privacy and security

Online privacy and online security go hand in hand. Most apps and software offer ways to control what information we're sharing and how.

When you're using an app or website, look for an option like 'My Account' or 'Settings'. That's where you'll find the privacy and security settings that let you decide:

- What information is visible on your page or profile
- Who can view your posts, photos, videos or other content that you share

Learning to use these settings to protect your privacy, and remembering to keep them updated, will help you manage your privacy, security and safety.

In addition to the Settings, a really important thing to think about is who can friend or follow you (that may or may not be in your Settings). The safest choice is to have only your offline friends and family following you or on your friends list. If you allow other people, don't forget that whatever you share can be seen by people you've never met. That can become a bit strange and sometimes parents just don't allow it at all. Talk it over with an adult you trust to figure out what's best for you, what keeps you safer and gives you the most peace of mind.

Your parents or guardians should **always** be making these decisions with you. Plus, it can be fun to go through your privacy settings together (so they can see how smart you are!).

Summary

Choosing a strong, unique password for each of your important accounts is a great first step. Now, you need to remember your passwords and keep them safe. Writing down your passwords isn't necessarily a bad idea. But if you do this, don't leave a page with your passwords in plain sight, such as on your computer or desk. Safeguard your list, and protect yourself, by hiding it somewhere.

Be Internet Secure: Activity 4

Taking care of yourself and others

Activity

You'll need:

- Copies of the scenarios from Activity 4

1. Let's look at the scenarios from Be Internet Sharp Activity 4 in our groups.
2. Discuss the following in your groups:
   - What can someone do if they feel unsafe online?
   - Who can they tell or go to?
   - What might happen when they tell?
   - What might happen after that?

Be Internet Secure: Activity 5

Interland: Tower of Treasure

Mayday! The Tower of Treasure is unlocked, leaving the Internauts' valuables like contact information and private messages at high risk. Outrun the Hacker and build a fortress with strong passwords to secure your secrets once and for all.

Open a web browser on your desktop or mobile device (e.g., tablet), visit **g.co/Interland** and navigate to the land called Tower of Treasure.

Discussion topics

Tower of Treasure will get pupils thinking. After they play, use these questions to start a discussion about the game's themes.

- What are the elements of a super strong password?
- When is it important to create strong passwords in real life? What tips have you learned on how to do so?
- What's a Hacker? Describe this character's behaviours and how they affect the game.
- Did Tower of Treasure change the way you plan to protect your information in the future?
- Name one thing you'll do differently after learning these lessons and playing the game.
- Craft three practice passwords that pass the 'super strong' test.
- What are some examples of sensitive information that should be protected?