

technocamps



Llywodraeth Cymru
Welsh Government



Prifysgol
Abertawe
Swansea
University



Cardiff
Metropolitan
University

Prifysgol
Metropolitan
Caerdydd



Cyngor Cyllido Addysg
Uwch Cymru
Higher Education Funding
Council for Wales

hefcw



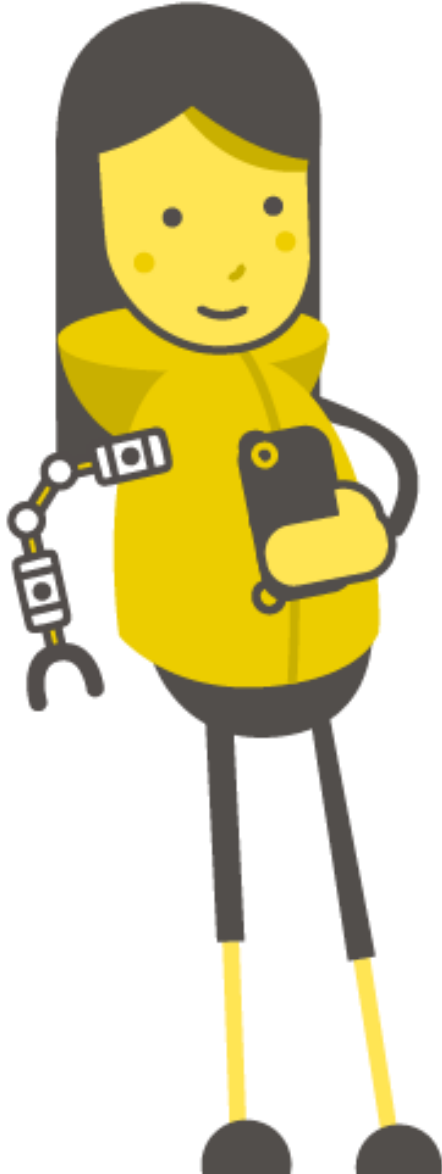
PRIFYSGOL
ABERYSTWYTH
UNIVERSITY



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Cyber Security In Secondary





Passwords

Why Are Passwords Important?

- They secure our data
- They protect our identities
- They prevent unauthorised access to our accounts



Why Is Password Security Important?

“Compromised passwords caused 80% of all data breaches in 2019” – Keeper^[1]

- A strong and secure password reduces the risk of cybercriminals accessing our data.

Cyber Attacks



Cyber Attacks Are Constant

Threat Map is a live service that shows attempted cyber attacks around the world in real time.

Follow this link to see for yourselves:

tc1.me/threatmap

“It Won’t Happen To Me...”

Many people incorrectly assume that they aren’t in any danger of a cyber attack because they aren’t important / don’t have much money etc.

“It Won’t Happen To Me...”

Many people incorrectly assume that they aren’t in any danger of a cyber attack because they aren’t important / don’t have much money etc.

This is entirely false.

“It Won’t Happen To Me...”

Many people incorrectly assume that they aren’t in any danger of a cyber attack because they aren’t important / don’t have much money etc.

This is entirely false.

The majority of cyber attacks on individuals are not aimed at anyone in particular, but carried out on millions of people at once.

If you leave yourself unprotected you will be caught in the blast.

Have I Been Pwned?

The website [have i been pwned](https://haveibeenpwned.com) searches through all known data breaches, from hackers to spambots, and lets you know if your email address is present in any of them.

Try it out for yourself! How many times has your data leaked?

haveibeenpwned.com

Is there any difference between your personal and Hwb accounts?

What Data Can Be Leaked?

What Data Can Be Leaked?

- Email addresses
- IP addresses
- Physical addresses
- Phone numbers
- Names
- Date of birth
- Gender
- Employer
- Job title
- Marital Status
- Device information
- Apps Installed
- Website activity
- Social media profiles
- Private messages
- Geographic location
- Security questions/answers
- Account balances
- Usernames
- Passwords

What Data Can Be Leaked?

Anything you put online, publicly or privately, can be stolen.

Even files you store on a computer with an internet connection can be hacked.

This can easily be enough information to impersonate you and gain access to all your accounts.

If Passwords Can Be Leaked Then What's The Point?

Early websites (and even very bad modern ones) used to store user passwords with their usernames in plaintext.

Username	Password
johnSmith	password
caseyH25	notpassword
americanWizard	september15
giraffesAreCool	password
ShrekTheHalls	pi31415etc

What are the issues with this? What are the benefits?

If Passwords Can Be Leaked Then What's The Point?

Modern websites should not be storing your password without encrypting it, that is very bad practice and very uncommon these days.

How do the issues and benefits differ with this system?

Username	Encrypted Password
johnSmith	gfefdti37232rjhsfgj
caseyH25	ytf28e7fro8dlhucy
americanWizard	6t23or8gyfbco872
giraffesAreCool	gfefdti37232rjhsfgj
ShrekTheHalls	767248o73yrph1d

CyberChef

We can see how a website will encrypt a password using CyberChef.

Open the CyberChef website, using this link:

tc1.me/CyberChef

The first thing to do is turn off 'Autobake' on the bottom of the screen!

CyberChef

On the CyberChef website, go to Hashing and drag in MD5.

Type any password into input and watch the hash appear in output!

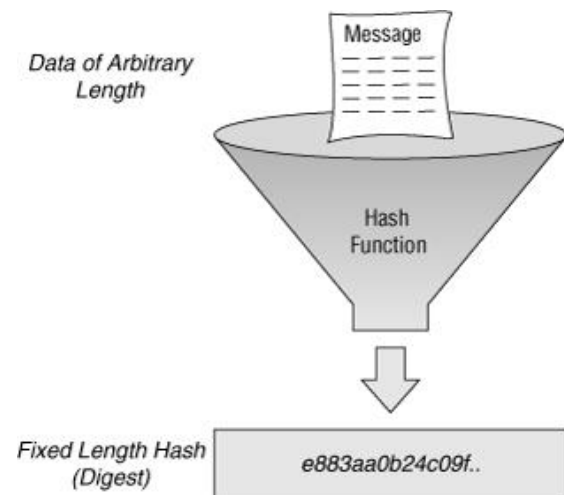
This is how a website stores your passwords. When you enter your password to log in it is the hashes that are compared.

Hashing

The reason we use a hash is that they are one way functions, they are practically impossible to reverse which means that your password is securely encrypted.

However, there are many different hashing algorithms with varying complexity - MD5 is an outdated hash and is no longer considered to be secure!

Can you guess one of the reasons why it has become insecure?



Hashing

Any password you use will always give you the same hash for that password!

All you need to do to find a particular hash is run it through an MD5 encryption tool, as you've just done.

Therefore entire tables of common passwords for MD5 exist.

TYPE	HASH	PASS	STATUS	TIME	SUBMITTED
md5	7e89bcc6151b24992a255cd665d4aa16		waiting	0:0:46	2006-11-11 10:45:31
md5	0696eeaff05bf2105b0bcf6d93ac73a0		waiting	0:0:47	2006-11-11 10:45:30
md5	db549b9d18aabe8ad07aa3d9338d441c		waiting	0:1:38	2006-11-11 10:44:39
md5	70c9ecbd2512460fa861de25fb3d7c6e		waiting	0:24:8	2006-11-11 10:22:09
md5	c32cf089d464d3ed1a3af347ae208188		processing3	0:25:6	2006-11-11 10:21:11
md5	c6fe5851aff10a64e8a52e82b323304f		processing3	0:46:29	2006-11-11 09:59:48
md5	a79c879d28c5c8a4707d52bbaa57607f	12050	cracked	0:45:41	2006-11-11 09:51:43
md5	a79e1c64d27737e3f959a6a56b41c650		processing3	0:57:18	2006-11-11 09:48:59
md5	2ef5b8b0eee93568a1126bb923664057		processing3	0:57:36	2006-11-11 09:48:41
md5	e53cc072934b25e45dc273c6c342556d		processing3	0:58:7	2006-11-11 09:48:10
md5	d38ad0e58c9525343f492161b87400a1	htnldb	cracked	0:58:23	2006-11-11 09:44:01
md5	d926dbaeb7fac97612ec219f7f172610		processing3	1:4:30	2006-11-11 09:41:47

Hashing

I have hashed a very common password,
who can work it out first?

5f4dcc3b5aa765d61d8327deb882cf99

Avoidable Password Leaks

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.



Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.



Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.



Shoulder Surfing

Observing someone typing their password.



Unavoidable Password Leaks

Interception

Passwords can be intercepted as they are transmitted over a network.



Brute Force

Automated guessing of billions of passwords until the correct one is found.



Key Logging

An installed keylogger intercepts passwords as they are typed.



Searching

IT infrastructure can be searched for electronically stored password information.





Password Security

Secure Passwords

**A survey of UK
passwords
reveals popular
password
choices**



National Cyber
Security Centre
a part of GCHQ

Cyber
Aware



15% use their pet's names

14% use their family
members names

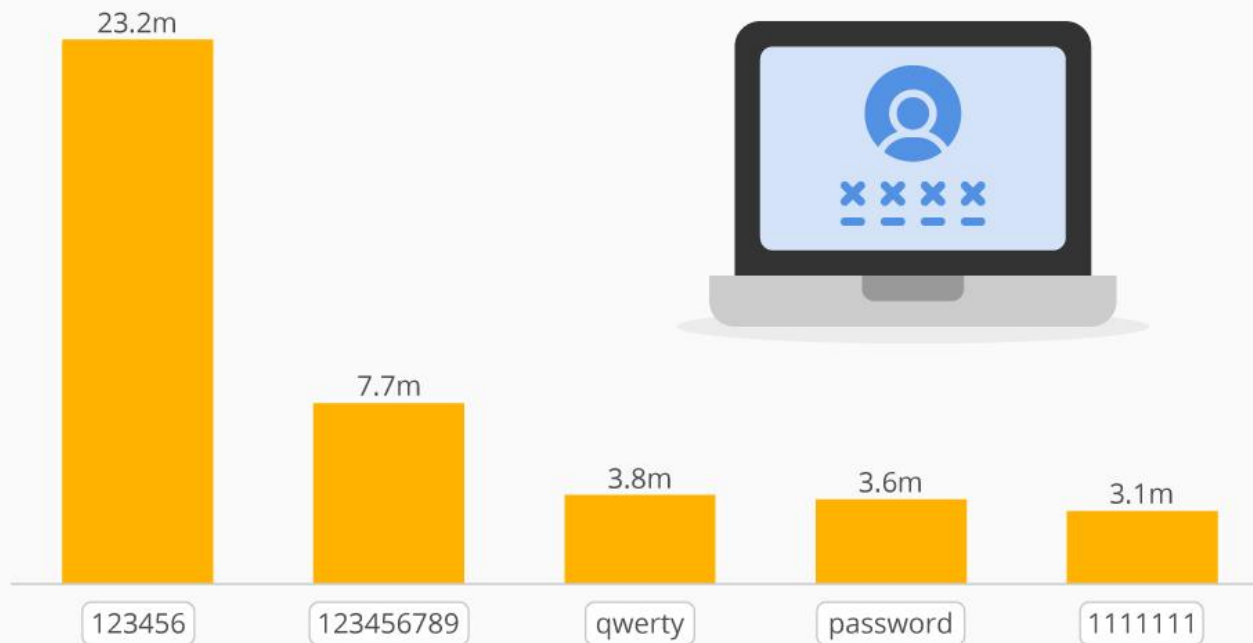
13% use a significant date

6% use their favourite
sports team

Secure Passwords

Millions in the UK are using vulnerable passwords

Most commonly re-occurring passwords in cyber breaches in 2019



Secure Passwords

So how do we ensure our passwords are secure?

Secure Passwords

So how do we ensure our passwords are secure?

- A mix of upper and lower case letters
- Include numbers
- Include symbols
- Avoid any personal details (i.e. name, pets, birthdays etc.)
- Avoid common words
- Avoid just replacing letters with numbers (i.e. p4ssw0rd)

Secure Passwords

All of these things are true, but the most important thing is length!

A very long password all in lower case is more secure than a short password with all the bells and whistles!

Go to:

tc1.me/nord

Secure Passwords

Check the following 2 passwords:

T3chn0c4mps!

and

saltedsalmonsausageswimmingsecurely

Secure Passwords

Test out your own passwords, or other passwords you can think of!

- There is a show/hide password button for your security
- Your password will not be sent to the website by typing it in.

How To Stay Secure

So we now know that length is the most important thing!

That is not to say that numbers and symbols don't help, include them where you can.

But the most important thing is a very long password that you can remember!

How To Stay Secure

But so many websites have outdated password checkers that make you use CAPS, lowercase, numb3r5 and \$ymbøls!

What can we do to avoid remembering these overly complicated passwords?

How To Stay Secure

But so many websites have outdated password checkers that make you use CAPS, lowercase, numb3r5 and \$ymbøls!

What can we do to avoid remembering these overly complicated passwords?

USE A PASSWORD MANAGER!

Password Managers

A lot of people are apprehensive about using password managers, as you're storing all of your security measures in one place!

If someone hacks your password manager then you're completely compromised!

Password Managers

A lot of people are apprehensive about using password managers, as you're storing all of your security measures in one place!

If someone hacks your password manager then you're completely compromised!

However they are very secure, and you know how to make a secure password...

Remembering one 30 character password is better than remembering thirty 10 character passwords.

Password Managers

Lots of password managers exist:





Digital Forensics

Digital Forensics

Digital forensics is the study of combing through digital files for evidence.

This is largely used by the police to solve crimes.

However it can also be used by security companies to check systems for weaknesses, or criminals to find their way into secure systems.

Digital Forensics

We are going to attempt performing some digital forensics on a memory stick we found.

There have been reports from schools that their secure data is being leaked somehow. Police have noticed the one common factor in all schools affected is that Technocamps had recently visited them!

While the police are performing their own investigation, we have found a memory stick in the office with what appears to be corrupted files on it. It's probably nothing but we're going to need to analyse it just incase.

Digital Forensics

Download the contents of the memory stick here:

tc1.me/MemoryStick

Then drag and drop the files into CyberChef:

tc1.me/CyberChef

Digital Forensics

Is there anything that stands out after importing the files into CyberChef?

Digital Forensics

Okay so one of the files is actually a picture!

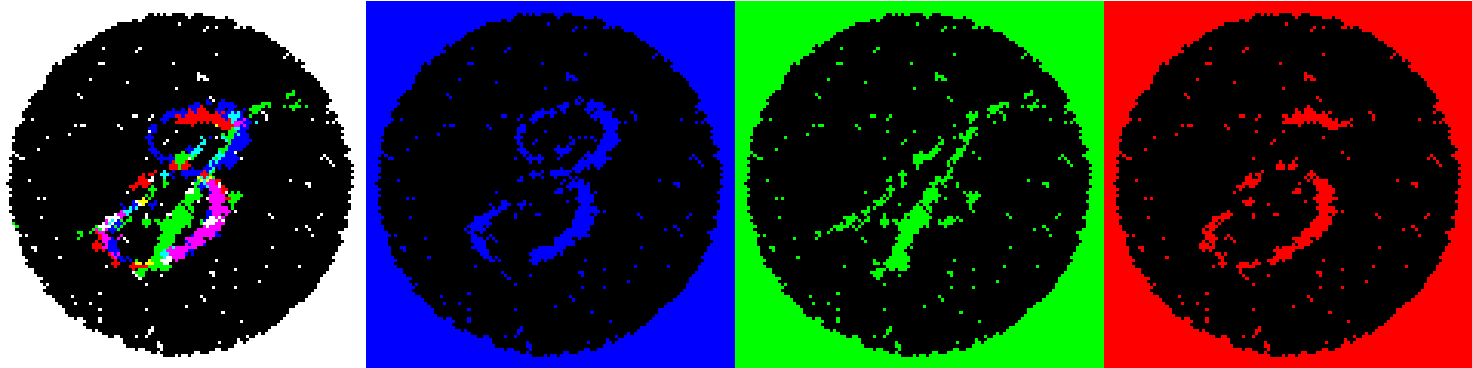
Well it's probably just an old corrupted file, which is why our computer doesn't recognise it.

However, there is a field of encryption know as Steganography!

Steganography

Steganography is the method of concealing text or images within another text or image!

This can be performed in a number of ways.



Steganography

Before



After



Steganography

TEXT STEGANOGRAPHY

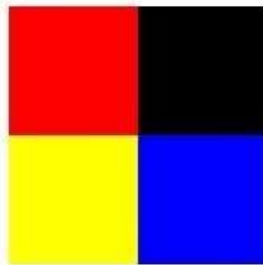
**Since Everyone Can Read, Encoding Text
In Neutral Sentences Is Doubtfully Effective**



SECRET INSIDE

Steganography

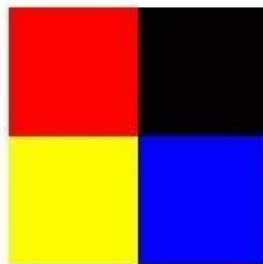
Original Image



11111111	00000000
00000000	00000000
00000000	00000000
11111111	00000000
11111111	00000000
00000000	11111111

Least Significant Bit Steganography

Stego Image



11111101	00000011
00000010	00000001
00000000	00000010
11111100	00000011
11111101	00000001
00000001	11111100



c	a	t
01 10 00 11	01 10 00 01	01 11 01 00

Digital Forensics

Have a look in the Forensics tab on CyberChef.

How might we test whether this image is actually hiding something?

Digital Forensics

How might we test whether this image is actually hiding something?

We can randomise the colours of the image so that any hidden text is made visible.

Digital Forensics

Our first clue!

It would seem that someone is trying to hide something in these corrupted files!

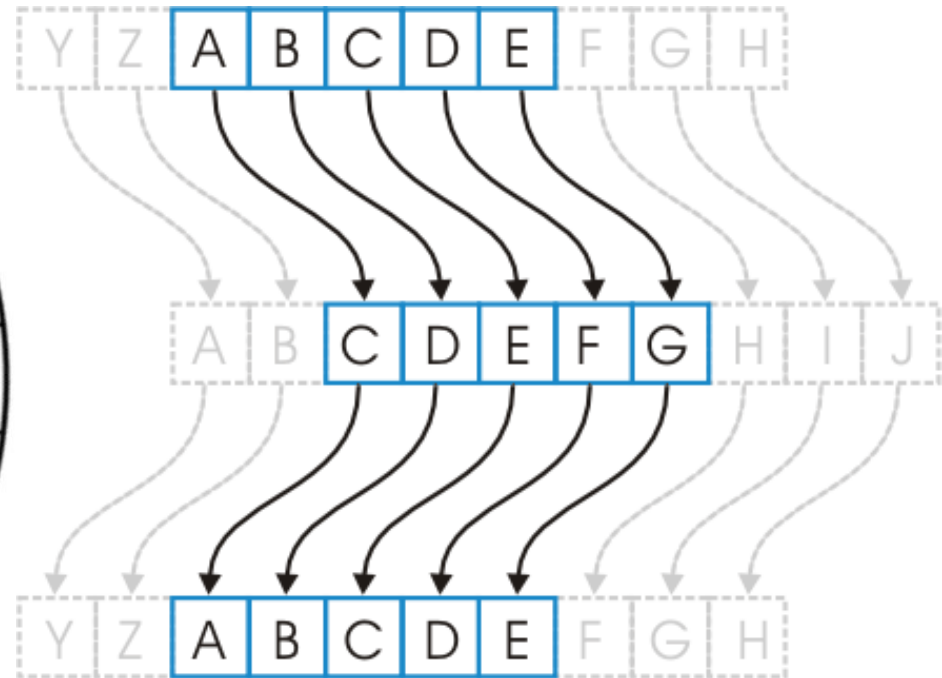
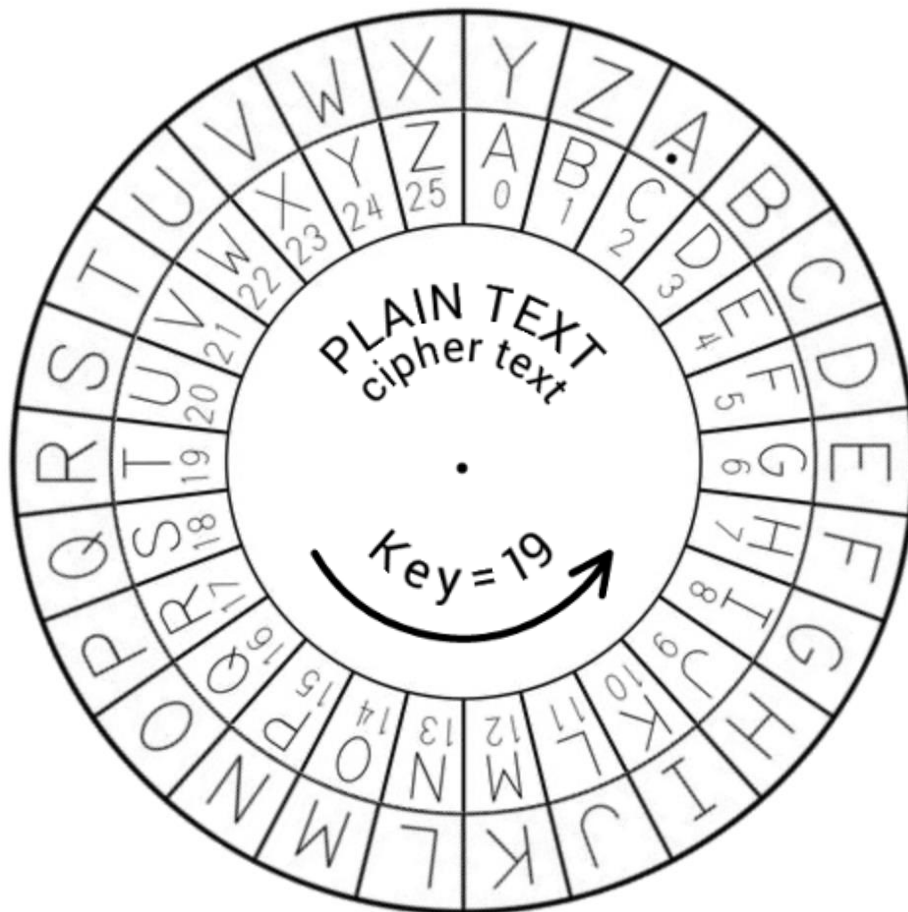
Luckily, we now know what encryption method they've used!

Silly criminals, you should never hide your passwords/hints in the same place as the thing you've protected.

Morse Code

A	..	J	..---	S	...	1-
B	-...	K	-.-	T	-	2	..---
C	-....	L	U	..-	3	...--
D	-..	M	--	V	...-	4-
E	.	N	--.	W	..--	5
F	O	---	X	-...-	6	-.....
G	--.	P	Y	-...-	7	--....
H	Q	---.-	Z	-....	8	--....
I	..	R	0	- - - - -	9	- - - - .

Caesar Cipher



Digital Forensics

Navigate to the tab for the file “temp”.

Digital Forensics

Navigate to the tab for the file “temp”.

We know that there are two steps to this encryption:

1. We will need to use Morse Code to go from the dots and dashes to text.

Digital Forensics

Navigate to the tab for the file “temp”.

We know that there are two steps to this encryption:

1. We will need to use Morse Code to go from the dots and dashes to text.
2. We will need to use a Caesar Cipher (ROT13) to shift the letters until they reveal words.

Digital Forensics

We could keep trying different keys for our Caesar Cipher, or instead we could Brute Force it.

This means letting the computer try all possible combinations one after the other. This is a common way to crack simple passwords.

As the Caesar Cipher is fairly simple, this is easy to do.

Replace the 'ROT13' block with the 'ROT13 Brute Force'.

Digital Forensics

Now we have both our encryption method (RC4)
and our encryption passphrase (T3CHN0C4MPS!)

Try using these to break the encryption on the final file!



micro:bit Passwords

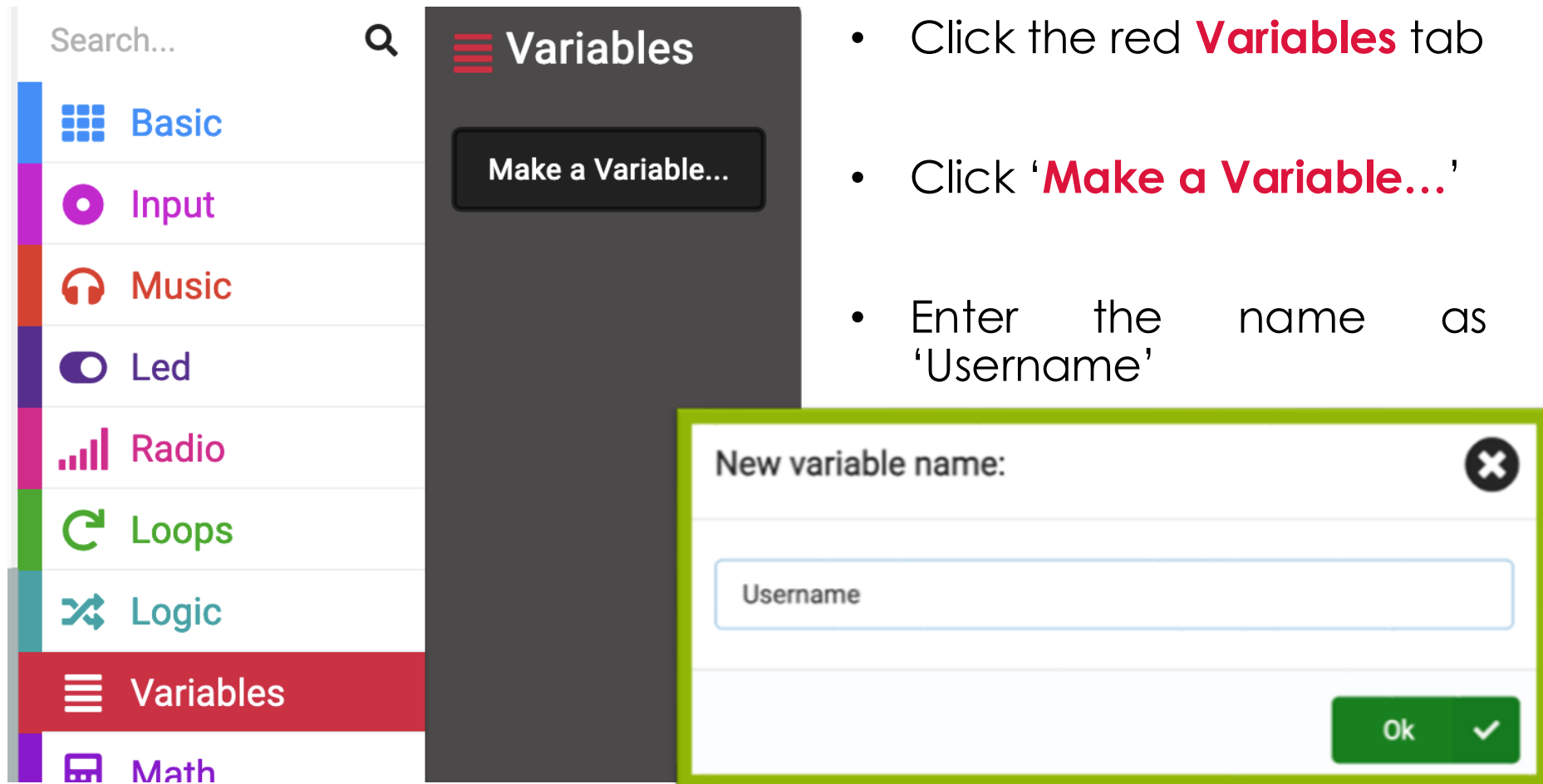
micro:bit Passwords

We're now going to try making a password checker with a micro:bit!

This will imitate logging into a website, where one micro:bit acts as the device trying to log in, and the other behaves as the website server checking the password.

First, we will program our server (both of your micro:bits can be programmed with both parts if you wish)

micro:bit Server



The image shows the micro:bit Server interface. On the left is a sidebar with a search bar and a list of categories: Basic, Input, Music, Led, Radio, Loops, Logic, Variables (highlighted in red), and Math. The main area displays the 'Variables' tab, which includes a 'Make a Variable...' button. A dialog box titled 'New variable name:' is open, showing a text input field containing 'Username' and an 'Ok' button with a checkmark. A green border highlights the dialog box.

Search...

- Basic
- Input
- Music
- Led
- Radio
- Loops
- Logic
- Variables**
- Math

Variables

Make a Variable...

- Click the red **Variables** tab
- Click '**Make a Variable...**'
- Enter the name as 'Username'

New variable name:

Username

Ok ✓

micro:bit Server

Find these blocks and drag them into the **on start** block:



The radio group functions like the IP address of the website, ensuring we are connecting to the right place.

micro:bit Server

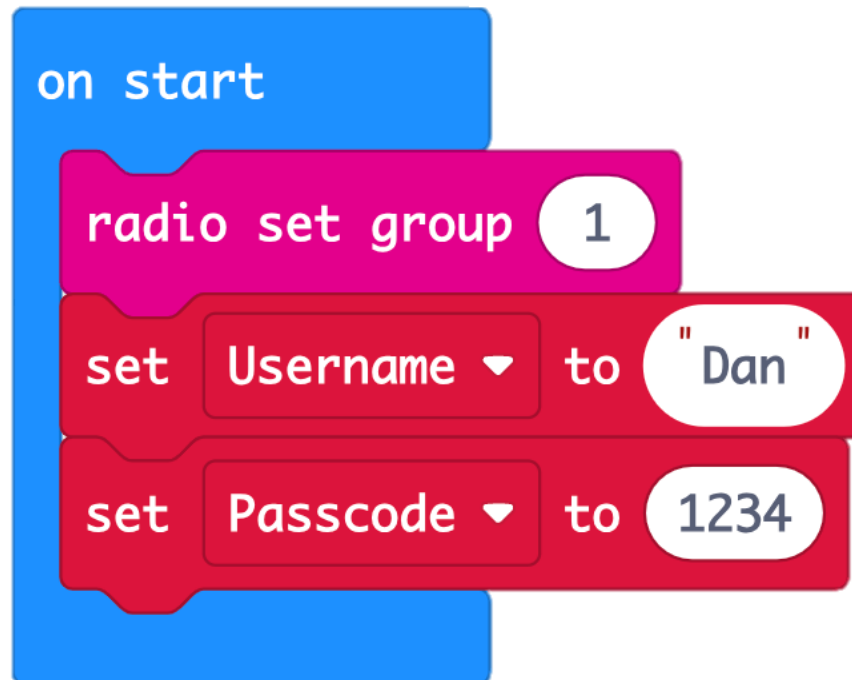
Set your variables to these values:



The username will require an extra block from the **Text** menu under **Advanced**, in order to be set as a string.

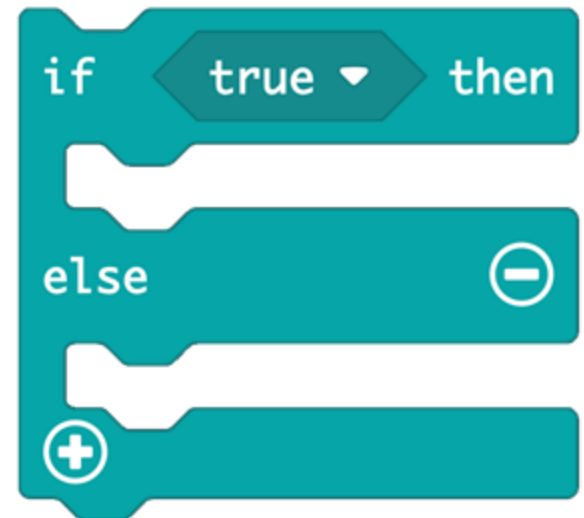
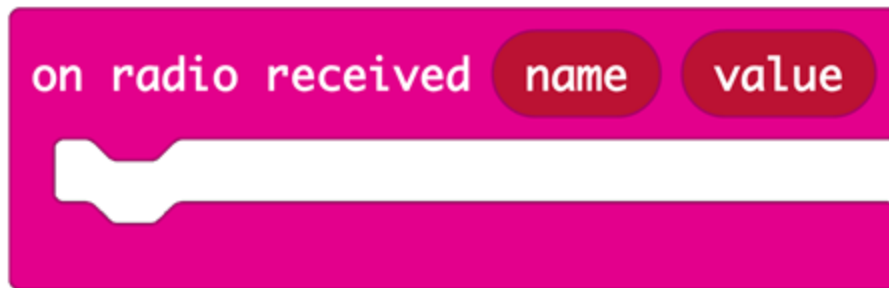


micro:bit Server

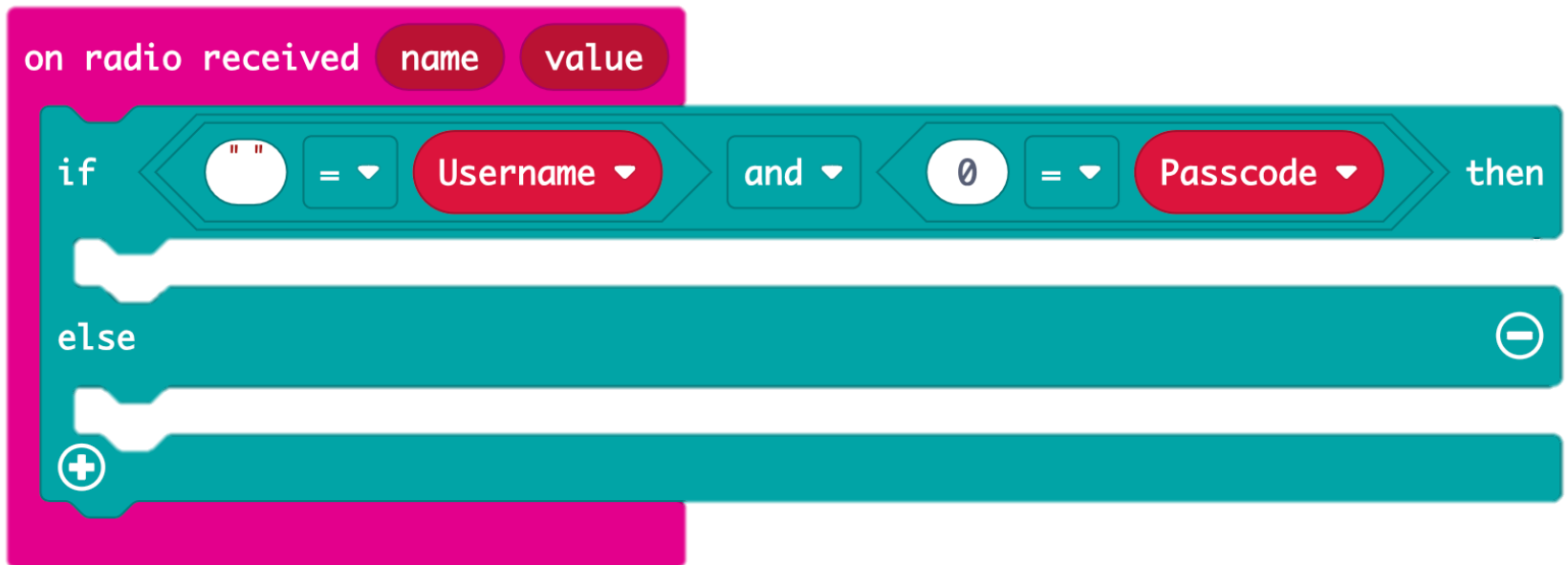


micro:bit Server

Find these blocks and drag them into the coding area, try and assemble them correctly:

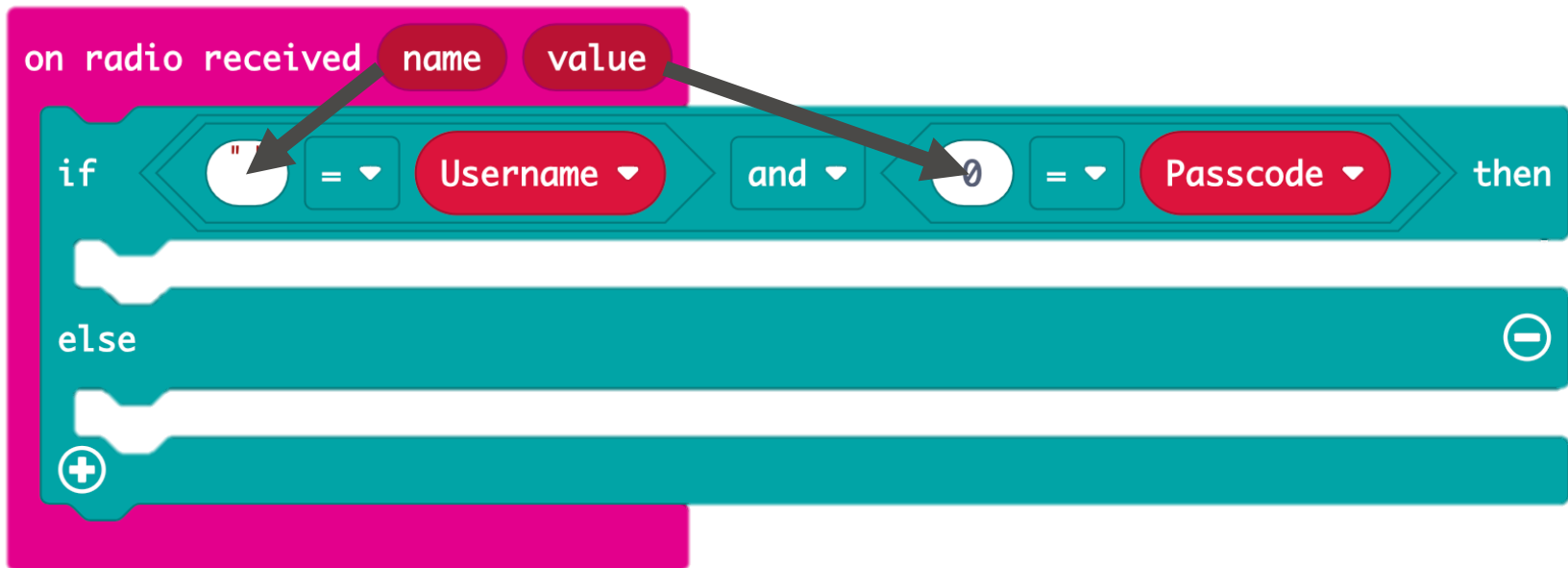


micro:bit Server

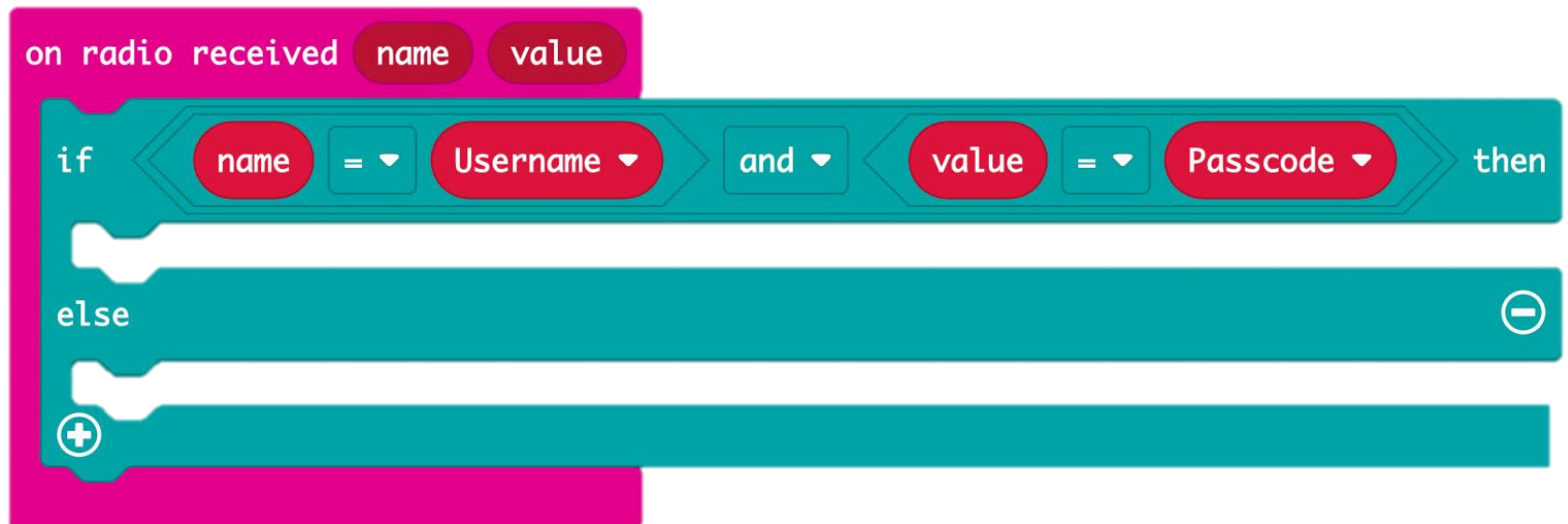


micro:bit Server

Once assembled we can drag out the script variables '**name**' and '**value**' into our if statement.

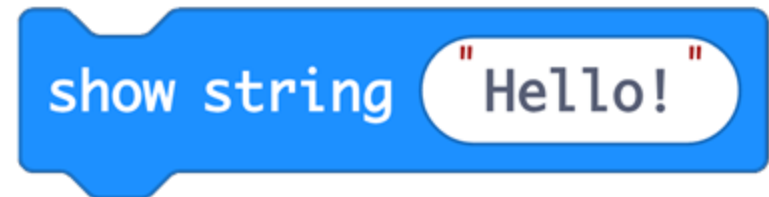


micro:bit Server



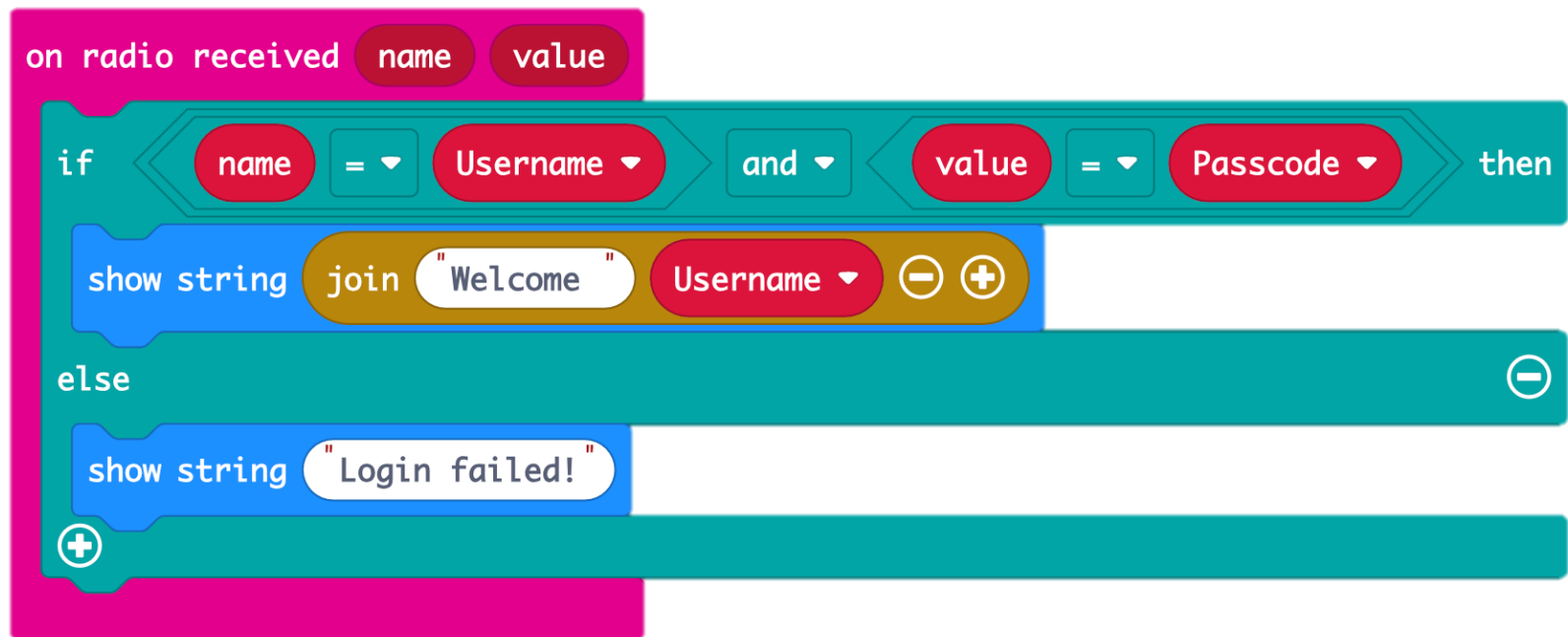
micro:bit Server

Find these blocks and drag them into the coding area, try and assemble them correctly:



Hint: You'll find the **join** block somewhere under **Advanced**

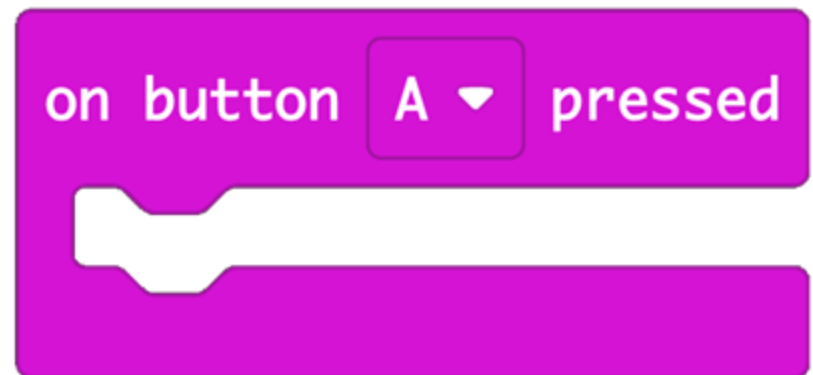
micro:bit Server



This is the completed code for our micro:bit server. Now we need to code the device!

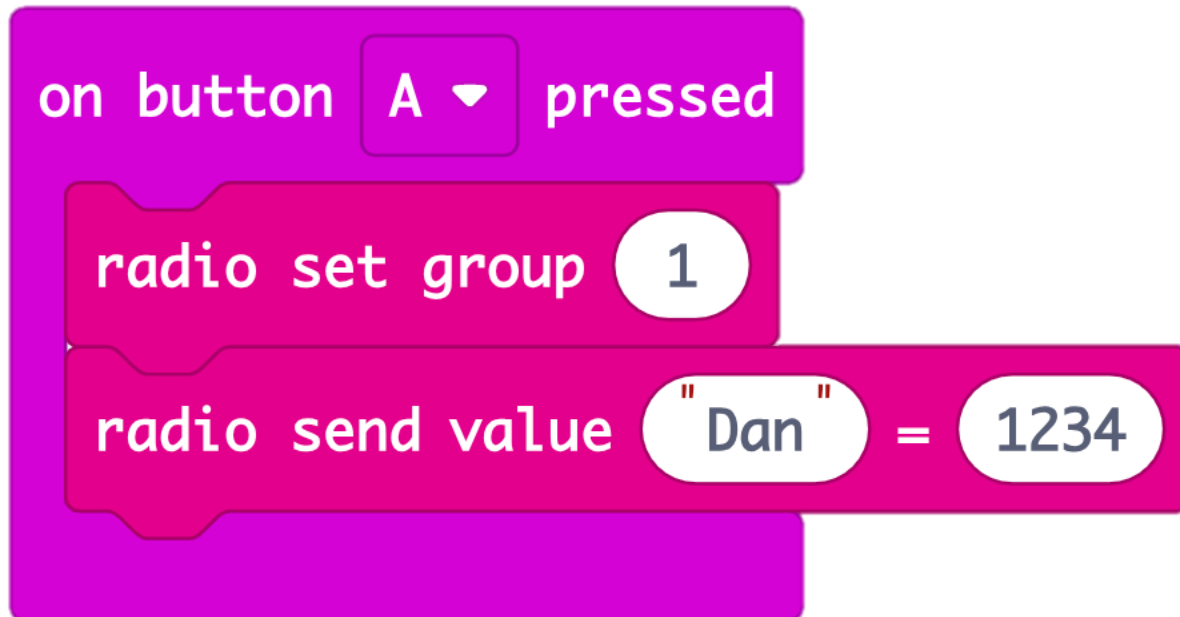
micro:bit Device

Find these blocks and drag them into the coding area, try and assemble them correctly:



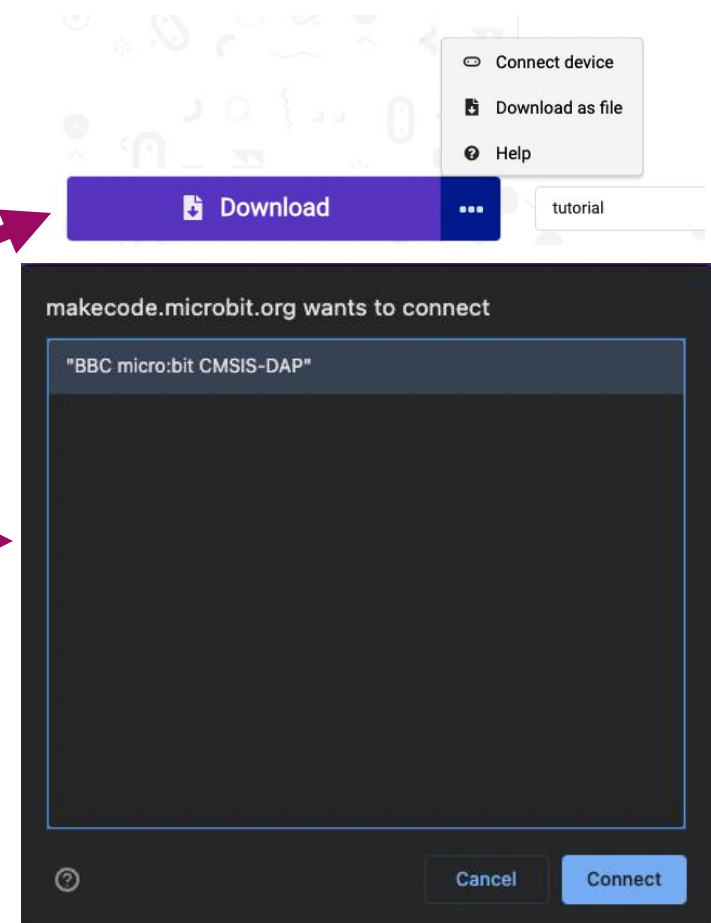
micro:bit Device

Find these blocks and drag them into the coding area, try and assemble them correctly:



Connecting the micro:bit

1. Plug the micro:bit into your computer
2. In the bottom left of your screen, click the 3 dots next to 'Download', then click 'Connect Device'
3. Follow the on-screen instructions until you see this pop-up
4. Click the name of your device (it should be the only option)
5. Click connect



micro:bit Extensions

These are possible extensions you could include for your micro:bit login system:

- Be able to send messages to the micro:bit (as if posting a comment to the website) where the micro:bit first has to check if you are logged in.
- Add a method of encryption so that the 'server' is not storing a plain-text password
- Add a list of usernames and passwords that are allowed to log into the micro:bit



Extension: How To Rob A Bank

How To Rob A Bank

In the final activity we're all going to find out how we can rob a bank!

This is an activity designed by CyberSkills, they have many other similar activities you can try out at home!

Go to this link:

tc1.me/RobABank

Bibliography

Hashing:

<https://blog.rsisecurity.com/wp-content/uploads/2017/05/password-hashing.png>

Password Managers:

<https://s1.npass.app/nordpass/media/1.1860.0/images/web/meta/nordpass-meta-trademark.png>

<https://static.safetynetdetectives.com/wp-content/uploads/2019/11/LastPass-Logo-Color.png>

https://mma.prnewswire.com/media/594937/Dashlane_Logo.jpg?p=facebook

https://upload.wikimedia.org/wikipedia/commons/thumb/c/cc/Bitwarden_logo.svg/1200px-Bitwarden_logo.svg.png

Bibliography

Password Managers:

<https://s3-eu-west-1.amazonaws.com/tpd/logos/50e76bed0000640005205377/0x0.png>

https://upload.wikimedia.org/wikipedia/commons/thumb/f/fa/Apple_logo_black.svg/625px-Apple_logo_black.svg.png

https://www.digitalcitizen.life/wp-content/uploads/2018/12/google_chrome.png

Bibliography

Steganography:

<https://zbigatron.com/wp-content/uploads/2018/10/Steganography.png>

<https://pequalsnp-team.github.io/assets/beforeafterstegorandom.png>

<https://www.cybervie.com/wp-content/uploads/2021/02/text-steganography.png>

<https://img.wonderhowto.com/img/02/61/63645877844452/0/steganography-hide-secret-data-inside-image-audio-file-seconds.w1456.jpg>

Morse Code:

<https://militaryrange.eu/blog/morse-code-history>

Bibliography

Caesar Cipher:

<https://camo.githubusercontent.com/fe4ba137f41af32ee3004e8d9e5a3bec90b5a7f92b8706a90d5aa51a8c66f940/68747470733a2f2f696a6f7368736d6974682e66696c65732e776f726470726573732e636f6d2f323031352f30342f6361657361722e676966>

<https://play-lh.googleusercontent.com/4HWP0WU1N91Uav9dB-iljHvuEu2FHUA6uWRCm6T2fh7peSEiWONlwEHL9YIET3nfxYDP>