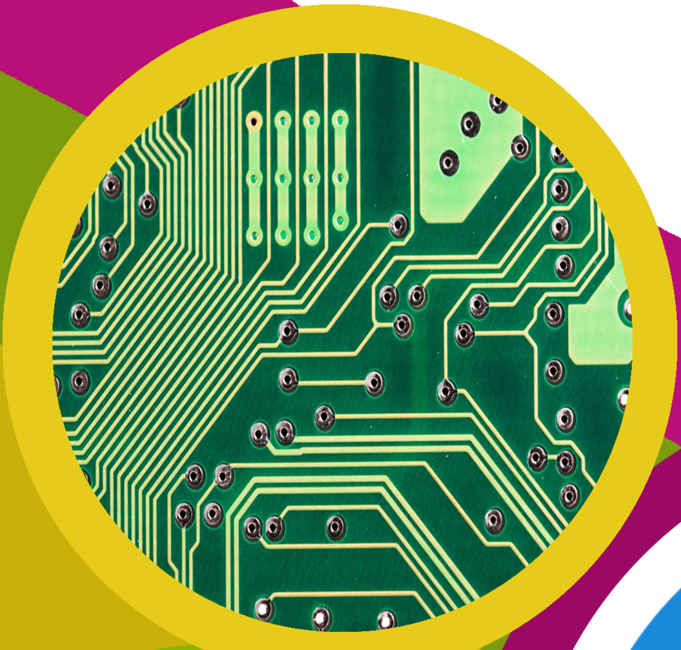
technocamps

Cyber Security In Secondary



Llywodraeth Cymru
Welsh Government

Prifysgol Abertawe
Swansea University

Cardiff University
Prifysgol Caerdydd

Prifysgol Bangor University

Cardiff Metropolitan University
Prifysgol Metropolitan Caerdydd

University of South Wales
Prifysgol De Cymru

Cyngor Cyllido Addysg Uwch Cymru
Higher Education Funding Council for Wales
hefcw

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

Prifysgol Aberystwyth University

Prifysgol Glyndŵr Wrecsam
Wrexham Glyndŵr University

institute of CODING in wales
technocamps

Introduction

Overview

Cyber Security is essential for keeping data safe. Password security in particular affects everyone and is especially important for learners to understand due to how many data breaches are caused by passwords.

In this workshop we will look into how to make strong passwords and encryption as well as looking into ways that hackers crack this security and decryption.

Online Resources

Digital Resources:

https://tc1.me/educonf23resources

Learning Objectives?

- Understand why strong passwords are important and be confident in creating strong passwords.
- Understand what encryption and decryption means particularly in the context of Morse Code and Caesar Cipher.
- Understand the methods websites use to try and store our passwords safely, and that this is will never be perfect.

Curriculum Links

Links to Science and Technology AoLE

Computation:

(PS4) I can plan and implement test strategies to identify errors in programs.

(PS4) I can explain the techniques used to store and transfer data and understand their vulnerabilities.

(PS3) I can explain the importance of securing the technology I use and protecting the integrity of my data.

(PS3) I can explain how my data is used by services, which can help me make more informed decisions when using technology.

(PS3) I can explain how data is stored and processed.

(PS3) I can effectively store and manipulate data to produce and give a visual form to useful information.

Links to Other AoLEs

Health & Wellbeing:

(PS4) I can consider relevant factors and implications when making decisions individually and collectively.

(PS3) I can identify and assess risks, and I can take steps to reduce them.

The Four Purposes and Cross-Curricular Skills

This resource provides **Critical Thinking and Problem-Solving** opportunities. Students are required to follow instructions and use the information provided to decode "corrupted" files and to create an algorithm using block-based programming. They are able to analyse errors, identify solutions, and deduce the next steps.

While discussing cyber security and online safety learners will have the opportunity to develop their **Personal Effectiveness** by evaluating how safe they are online, and use **Planning and Organising** to develop strategies to protect themselves and others

The **Interacting and Collaborating** and **Data and Computational Thinking** sections of the **DCF** apply to this resource. Students will learn to break down the problems presented to them, and code efficiently using selection and events to create an algorithm. Learners will work together to build a server simulation with their micro:bits.

Why Is Learning This Important?

This resource provides learners with the opportunity to learn about the importance of online safety and the prevelance of cyber crime. They will create simple algorithms with a demonstrable application, using a block-based programming language. It introduces concepts such as selection, loops, and event-based programming which are critical to most common programming languages. The resource also teaches the importance of strong and secure passwords and allows for collaborative and interactive activities to showcase this. This resource can be expanded to introduce students to text-based programming such as Python.

Suggested Approaches Key

In this suggested approach we use the following colours to differentiate the types of activities:

- **Yellow - Explain.** Teachers should explain the slide/example to the class.
- **Green - Discuss.** Teachers should start an open discussion with the class to get them to feedback some answers/ideas.
- **Purple - Activity.** Students are expected to complete an activity whether it be in their workbooks or on the computer, followed by a discussion of their solutions.
- **Green - Introduction/Conclusion.** The introduction/conclusion is also colour coded green. Teachers should hand out materials in the introduction and conclude the session and collect materials at the end.

Introduction

Begin with introductions, and a brief explanation of the Technocamps programme, before handing out any resources required by learners and any additional aids for learners with additional learning needs.

Explain: Topics Covered Today

Today we will be learning how to be secure online by creating strong passwords. By the end of the session we will understand the way in which passwords are easily crackable and the importance of being secure.

Why Are Passwords Important?

Ask the class why they think passwords are important:

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

A strong and secure password reduces the risk of cybercriminals accessing our data - because more complex and longer passwords are more difficult to guess or crack through brute force methods.

Also, having a poor password has the potential of exposing both the hash and the hash algorithm (should the password be cracked) used to store it securely, which in turn puts other people's data in jeopardy.

Note: Hashes will be explained later in this workshop.

Cyber Attacks Are Constant

Go to **tc1.me/threatmap** to see live cyber attacks taking place right now. It outlines the most targeted countries, industries and malware types (software used with malicious intent to compromise a computers security).

Allow the learners to explore the website looking at the different features of the website, such as the breakdown by country or increasing the rate of attacks (top left of the website).

Note: These are only the threats that have been caught. Meaning successful attacks will not appear on this website. Is this concerning?

It Won't Happen To Me...

Explain to the learners the fallacy that many people assume they are not in danger of a cyber attack, as they aren't someone who would be targeted.

Demonstrate (with the CyberThreat website) that the majority of these attacks take place against large servers and systems, not individuals. Meaning that all accounts and passwords exposed in the attack are vunerable, and anyone unprotected may be caught in the blast.

Have I Been Pwned?

Go to **tc1.me/pwned** to check if your email address has been identified in any past data breaches.

Try multiple email accounts, ideally personal and work/school accounts (as Hwb accounts are unlikely to have been affected).

If you're unlucky and have a class of 0 breaches, then you can try a random email - or marl@gmail.com, who has been caught in 39 data breaches over a variety of platforms including a leak of their Polish Credentials (confirming their citezenship for all!), making this an interesting case to look at.

Also be aware that there are also leaks from pornagraphic websites that will be listed. Only the website name will appear, but this is worth mentioning.

Note: The number of "pwned" accounts is over **12.5 billion!**

What Data Can Be Leaked?

Have a brief discussion with learners about what personal data can be leaked during a hack?

This is an extensive and almost endless list, though many examples are included on the sildes.
Essentially any data stored online, public or private, can be hacked and leaked.
Additionally any computer with an internet connection can be hacked.

Then What's The Point?

Have a brief discussion on why we should still care about password security.

Most (all trustworthy) websites will encrypt your password to store it, this means that your password is only vunerable if it is very simple, the hash is already known, or it includes enough personal details to be guessable.

This is demonstrated on the slides where both users who used the password "password" have the same encrypted password (hash). This immediately tells a hacker that this encryptedted password is likely a common enough password for multiple people to use.

The hacker could then look up any known (previously cracked) passwords and their encryptions, or try and work it out themselves by guessing the password (made easier by snooping online using the username/email to find relevant information on the user).

CyberChef

Go **tc1.me/cyberchef**. This website can perform encryption, encoding, compression and data analysis. This workshop will focus on demonstrating **encryption** and some **data analysis.**

For this task we will be demonstrating how hashing works as a method of password encryption. Once choosing our encryption method we can enter any input text, press Bake, and watch the encrypted output appear. This output is how the password would be stored in a company's database so that not even the company can read your password.

However, a few interesting things regarding hashing can be observed:

- The same input string will always generate the same output string - this means that once the hash for a password is known, it is always known.
- There is no observable pattern to the encryption, slight changes in input will result in very different outputs - this makes it incredibly hard to reverse engineer the hashing algorithm, so not all passwords are at risk
- The output string is always the same length regardless of input length - there are more inputs than outputs so passwords can share a hash, a simple password could have the same hash as a very complex password.

Important: Turn off **Autobake** (a checkbox at the bottom of the webpage). This helps mitigate the issue of the website crashing so often.

To find MD5 encryption, type **MD5** into the search bar in the left panel (under the **Operations** header) or scroll down to **Hashing**

To apply the encryption to the input, you drag it into the **Recipe** section. Enter an input string under **Input** and then click **Bake**.

Hashing and MD5

Discuss the benefits of hashing (this pairs well with the info above on what CyberChef demonstrates) briefly with learners.

Why is MD5 outdated?

MD5 computes the hash very quickly, which was an advantage when it first came about. However, due to how fast you can compute the hash, with the help of the speed of modern computers you can calculate the hashes of many possible passwords quickly to try and break into someones account.

This also means it's very easy to build tables of passwords and their hashes, making it far easier for you and future hackers to find the corrrect password/ hash combination faster.

This is another reason your password should be difficult to guess.

Hashing

Show a hash of a simple password to the learners and have them use CyberChef to try and match the hash as quick as they can, thereby finding the password.

For example the hash:	**5f4dcc3b5aa765d61d8327deb882cf99**
Is for the password:	**password**

Either use this example or come up with more to encourage learners to try and find the correct password quickest, demonstating the simplicity of breaking into an account with this method.

Avoidable and Unavoidable Password Leaks

Discuss with learners the reasoning behind some password leaks being avoidable or unavoidable - you cannot control someone hacking you, but you can avoid:

- Giving out personal information
- Handwriting passwords somewhere easily discoverable
- Someone seeing your password
- Using personal information in your password

While interception of your passowrd and being keylogged are mostly out of your control, a strong password will still be protected against brute force attacks, or someone searching for stored password hashes in the network.

What Makes a Secure Password?

Discuss the reality of passwords in the UK, with the majority of people still using insecure passwords - either by including personal information (which can easily be scrapped from a search on social networks) or by using incredibly common passwords.

Discuss what makes a strong password:

- what should it include?
- what shouldn't it include?

What Makes a Secure Password?

Explain to learners that while the common quoted elements of a secure password (upper and lower case letters, numbers and symbols) are all important, the most important factor is length.

Computers are very good at performing tasks quickly, and the main factor in stopping a computer from cracking your password is by making it long enough that the computer is unlikely to ever get it right.

Note: This is around 16 characters in length.

Secure Passwords

Have the learners go to **tc1.me/nordpass** to check how secure their passwords are.

Begin by trying the two examples on the slide to demonstate the difference between the seemingly complex password and the longer simple password.

Then have the learners try their own passwords to check how secure they've been!

How to Stay Secure

Now we know that one long easy to remember password is far more secure than a very complex short password. However so many sites have strict requirements on what your password must contain!

Enter the Password Manager!

Many people have reservations about password managers as they're storing all their security measures in one place. However these sites tend to have very good security measures themselves, and we now know how to make a secure password ourselves.

Password managers will create and store complex and secure passwords for each site you have an account with. This means you'll only need one long, easy to remember and secure password, but still have long, complex and unique passwords to each of your accounts that can pass the requirements of each website.

Digital Forensics

Introduce the concept of Digital Forensics and why it is an important skillset for the police and security companies to have. However, as with anything, this knowledge can be abused, and the same tools that make finding criminals possible are the tools they have used to commit the crime.

Then introduce the task required of the class.

Memory Stick

Go to **tc1.me/MemoryStick** and either press the download button in the top right corner of the page to download a zip file, or download each of the files individually.

Before dragging them into the input section of CyberChef (**tc1.me/cyberchef**). Discuss the files they have downloaded, there's no identifiable file type or icon, when opening them they seem like gibberish.

Drag them into CyberChef, one will immediately be identified as an image.

Again make sure "Autobake" is **disabled**.

Steganography

Introduce the concept of steganography to the learners and the different methods through which it can be applied.

Instruct them to look at the Forensics tab on Cyber Chef to see if they are able to retrieve any information from the image.

Steganography

There is information hidden inside the image, to find this on CyberChef use either of the following forensic operations:

- **Randomize Colour Palette**
- **View Bit Plane**

Randomizing gives a random colour to each colour in the image - this means information hidden in plain sight by having a slightly different colour to the surrounding pixels is suddenly made clear.

Viewing the Bit Plane is similar to how Least Significant Bit steganography works - the binary value of each pixel is split up over several different black and white images. This means that what was a very slight difference in the original image become a major difference in the Bit Plane.

The text revealed tells us that the file temp is encrypted with both Morse Code and Caesar Cipher.

Morse Code

Morse code is a system of communication that uses dots and dashes to represent letters.
This allows you to hide you want to say by changing the letters into their equivalent dots and dashes. This is a similar to a substitution cypher, such as Caesar Cypher.

Caesar Cipher

A Caesar Cipher is a method of encryption, which changes each letter of the plaintext by a certain "shift" of the alphabet e.g. the plaintext "ABCDE" with a shift value of 2 would become "CDEFG".

To use the Caesar Cipher wheel, you rotate the outer wheel so that the outer "A" lines up with the number on the inner ring that you wish to shift by.
To encrypt, the message you read from the outside in and to decrypt, you read from the inside out.

Visit **tc1.me/CaeserCipher** to see this in action.

Morse Code & Caeser Cipher

In CyberChef, on the file temp, drag the operation **From Morse Code** into the recipe and Bake. This will change the file contents into what is clearly words but still Caeser Shifted.

Add the **ROT13** (Caeser Cipher) operation into the recipe and Bake. All 25 shifts would need to be tested to find the right one. Instead we can drag in the **ROT13 Brute Force** operation to try all shifts at once!

Note: The correct shift value is **19**.

This gives us our final file encryption (**RC4**) and its passphrase (**T3CHN0C4MPS!**)

RC4

RC4 is an outdated method of encryption, however, it can still be used to understand the principles of encryption.

Drag **RC4** into the recipe section, and type in the passphrase (**T3CHN0C4MPS!**).

Open the file **bin** and Bake. This should then open a list of passwords to fake hwb accounts.

Introduce the micro:bit

If the class has no experience with the micro:bit it's time to introduce it!

The micro:bit is a minature computer built by a partnership between the BBC and Microsoft, created with the intention of inspiring young people to code and demonstrating how hardware and software work together.

The micro:bit is jam packed with different sensors allowing you to create a multitude of programs and ideas. These are all on the accompanying slides.

micro:bit Password Checker

Explain to the learners that we're 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 the server, but both of your micro:bits can be programmed with both parts if you wish.

micro:bit Server

Follow the code provided in the slides to assemble the micro:bit Server.

This is going to operate like a website server, storing your login details so that when you attempt to log in with another micro:bit it checks the username and password you provide against it's records to log you in.

In this scenario the radio group you use is functioning like the IP address of a website, ensuring you are connected to the correct website when you provide your login details.

This can be built on one or both micro:bits. It makes more sense with one, but this is the longer piece of code so if you'd rather avoid one learner doing more than another then that is possible.

micro:bit Device

Follow the code provided in the slides to assemble the micro:bit Device.

This is going to operate like a your personal device, going to the correct IP address of a website and attempting to log in with your username and password. If your details match then the website will log you in and provide a response.

This can be built on one or both micro:bits.

micro:bit Extensions

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. You can do this by making a variable called **LoggedIn** which is usually set to **False** but upon logging in becomes **True**. Use **send** and **received string** blocks instead of the **value** blocks and check whether the user is logged in before displaying the message.

Add a method of encryption so that the 'server' is not storing a plain-text password. You can do this by making the password a number and performing so **mathematical operations** on it (e.g. sine). This is not true encryption but the concept is the same. Store your password as the encrypted value and perform the operation on the **received value**.

Add a list of usernames and passwords that are allowed to log into the micro:bit. You can do this by using a **list (array)** instead of a **variable** to store the usernames and passwords. You will need to check the **location** of one to ensure you are checking the correct password for the correct username.

Extension - How To Rob A Bank

This is a very fun guided activity developed by CyberSkills.

The learners will be guided through using terminal commands to access and search through a banking system for account information. They will then use that information to transfer money out of peoples accounts.