



L-6 Encryption

Key messages

- Important data can be intercepted and misused unless encrypted.
- Encryption is like a code that only the sender and receiver know how to solve (via a password or PIN).
- The padlock symbol is one way of indicating the information being sent is encrypted; also check for “https”
- Public Wi Fi can be a dangerous place to send unencrypted data.

Illustrating the topic

Video clip: http://www.youtube.com/watch?v=jJrICB_Hvul

(Unplugged: The show. Part 9: Public key encryption – this shows children passing a locked box back and forth and is extremely helpful in understanding encrypted transactions).

Discussion questions

- How does encryption work?
- When would you need encryption?
- What symbols on a website where you are sending confidential information are displayed to indicate it is encrypted?
- How could public Wi Fi be a dangerous place to send confidential information? (See information under ‘resources’).

Activities

- Recreate the encryption video using members of the class.
- In groups, recreate the encryption with ‘data’ in the box instead of chocolate. What data would need to be protected in different situations? (eg paying someone when purchasing something Online).
- Solve problems where you need to crack a code.
<http://www.mylearning.org/learning/investigate/Cracking%20Codes.pdf>
- Create your own ‘cracking the code’ problems for a partner to solve as well as learn about the history of codes: http://www.cerias.purdue.edu/education/k-12/teaching_resources/lessons_presentations/cryptology.html

- Read the 'Beware of public Wi Fi' advice under 'Resources'. Re-enact using public Wi Fi at the local library where a malicious individual using specific software to intercept your data is lurking. Act out the consequences of this information being shared
- Explore the interactive safety tips for Wi-Fi hotspots.
<http://www.gcflearnfree.org/internetsafetyforkids/6.2>
- Using 'encryption made easy' information under the resources section, create a comic strip to illustrate the process, using each line as the heading for each frame.

Resources

Code cracking problems and solutions, research suggestions and links:

<http://www.mylearning.org/learning/investigate/Cracking%20Codes.pdf>

Calling all cryptologists – solving codes, historical importance and creating your own:

http://www.cerias.purdue.edu/education/k-12/teaching_resources/lessons_presentations/cryptology.html

Be wary of public Wi-Fi

(Don't use public Wi-Fi for doing sensitive things like online banking or social networking).

Most Wi-Fi hotspots do not encrypt information and once a piece of data leaves your device headed for a web destination, it is "in the clear" as it transfers through the air on the wireless network. "That means any 'packet sniffer' [a program which can intercept data] or malicious individual who is sitting in a public destination with a piece of software that searches for data being transferred on a Wi-Fi network can intercept your unencrypted data. If you choose to bank online on public Wi-Fi, that's very sensitive data you are transferring. We advise either using encryption [software], or only using public Wi-Fi for data which you're happy to be public – and that shouldn't include social network passwords."

(<http://www.theguardian.com/technology/2013/may/12/20-ways-keep-internet-identity-safe>)

Interactive safety tips for using Wi-Fi hotspots:

<http://www.gcflearnfree.org/internetsafetyforkids/6.2>

General information including encryption

<http://www.staysmartonline.gov.au/home>

[http://msdn.microsoft.com/en-us/library/92f9ye3s\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/92f9ye3s(v=vs.110).aspx).

Encryption made easy:

Sender encrypts and sends a message to receiver

Receiver encrypts the encrypted message and sends it back

Sender decrypts his encryption leaving the receivers encryption and sends it back

Receiver decrypts his encryption

The receiver can now read the message.