

**TOPIC: Network security**

**LEARNING OBJECTIVES:**

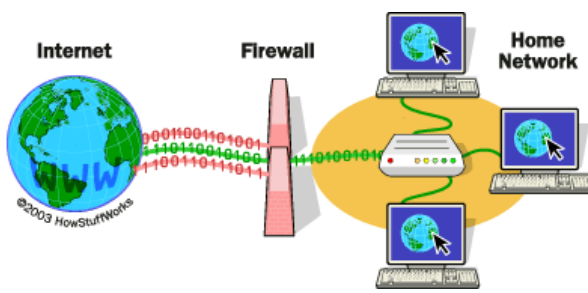
**Methods of network security:**

- **Authentication**
- **Encryption**
- **Firewall**
- **Mac address filtering**

|  | <b>Teacher Activity</b>   | <b>Pupil Activity</b>                |
|--|---|--------------------------------------|
| <b>Starter activity</b><br>(5-10 mins)<br>[individual/<br>paired or group] | <p><i>Understand the need for, and importance of, network security</i></p> <p><b>Passwords:</b></p> <p><i>Network operating systems control user logon and passwords to make the system secure. There should be a password requirement, typically: eight characters, upper and lower case letters, including a number and a symbol such as '\$' or similar</i></p> <p><b>User Access Levels:</b></p> <p><i>File access rights will allow users to read, write, execute or perform a combination of these functions. This is used to maintain the security and privacy of files.</i></p> | Discuss (individual/paired or group) |

|   |  |   |
|---|--|---|
| <p><b>Main activity one</b><br/>(15 mins)</p> | <p><b>Authentication:</b></p> <p><i>Authentication is the process of identifying an individual and is distinct from authorisation, for example a user can enter a username and password at a login screen and prove they 'know' that piece of information but not that they have permission to login.</i></p> <p><i>There are three broad types of authentication, something you...</i></p> <ul style="list-style-type: none"> <li>- ... know (password)</li> <li>- ... have (smartcard)</li> <li>- ... are (fingerprint or other biometrics)</li> </ul> <p><i>Multi-factor, or two-factor, authentication is about using additional types of authentication to increase the difficulty for someone malicious to guess/steal the information/item</i></p> <p><b>Encryption:</b></p> <p><i>Encryption means to scramble data in such a way that only someone with the secret code or key can read it. For <b>encryption</b> algorithms, a <b>key</b> specifies the transformation of plaintext into ciphertext, and vice versa for decryption algorithms.</i></p> <p><b>How does it work?</b></p> <p><i>Encryption works by scrambling the original message with a very large digital number (key). This is done using advanced mathematics. Commercial-level encryption uses 128 bit key that is very, very hard to crack. The computer receiving the message knows the digital key and so is able to work out the original message.</i></p> <p><b>Why is it important?</b></p> <p><i>Encryption is important as it enables you to pass a secret message from one place to another without anyone else being able to read it.</i></p> <p><b>Where is it used?</b></p> <ul style="list-style-type: none"> <li>• <i>Web browsers are able to encrypt your purchase details using an encryption method called 'SSL' (Secure Socket Layer).</i></li> <li>• <i>Built-in encryption functionality of many office productivity applications (for example, Microsoft Office 2010 offers the strong AES-256 algorithm for the encryption of password-protected files).</i></li> <li>• <i>Email encryption and also authentication.</i></li> </ul> | <p><b>Authentication:</b></p> <p>Discuss (individual/paired or group)</p> <p>Design a new type of authentication method, could be as imaginative as they want, for example something that uses smell, or shoe size. Individuals or groups present their authentication methods to the rest of the class and other students discuss how it might be bypassed, pro's and con's etc.</p> <p><b>Encryption:</b></p> <p>Discuss (individual/paired or group)</p> <p>And create a simple encrypted message) and get another group to crack it</p> |
|---|--|---|

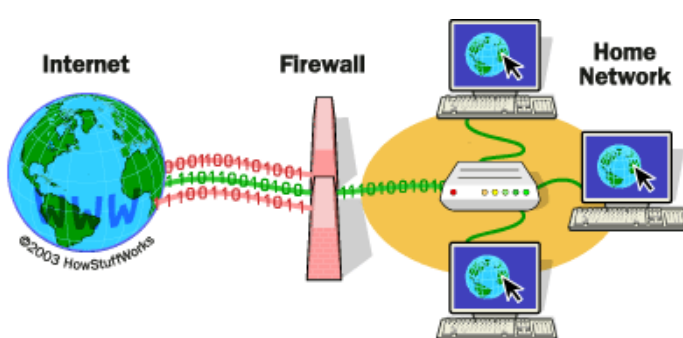
|   |   |  |
|---|---|--|
| <p><b>Plenary one</b><br/>(5-10 mins)</p> | <p><i>Assess learning against the learning objectives</i></p> <p><i>This is an open activity whereby the teacher will decide on the best approach to do this based on the pedagogical approach your school takes on assessment.</i></p> | <p><b>For example:</b></p> <ul style="list-style-type: none"><li>• 5 minute timed writing exercise on what has been learned so far</li><li>• Fill in class notes</li><li>• Have a discussion</li><li>• Answer open questions</li><li>• Answer directed questions</li></ul> <p>On:</p> <ul style="list-style-type: none"><li>• What is authentication?</li><li>• What are the three types of</li><li>• Authentication?</li><li>• What is encryption?</li><li>• Why is encryption important?</li><li>• Where is encryption used?</li></ul> |
|---|---|--|

|   |   |  |
|---|---|--|
| <p><b>Main activity</b><br/>two<br/>(15 mins)</p> | <p><b>Firewall:</b></p> <p><i>A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules.</i></p> <p><i>Simply compared to a security guard who stands at the entrance of your house and filters the visitors coming to your place. He may allow some visitors to enter while denying others whom he suspects of being intruders.</i></p> <p><b>Who uses it?</b></p> <ul style="list-style-type: none"> <li>• Members of the public</li> <li>• Corporate organisations</li> </ul> <p><b>What systems use it?</b></p> <ul style="list-style-type: none"> <li>• Windows/Mac PC's</li> <li>• Network devices</li> </ul>  <p><b>MAC Address Filtering:</b></p> <p><i>Media Access Control (MAC) address filtering is the process of setting up parameters to allow only certain MAC addresses onto a network or particular router (Access Point). It is a very rudimentary protection method as it can be copied by someone else listening in to the connection (if wireless).</i></p> <p><b>What is it used for?</b></p> <p><i>This is to allow only certain MAC addresses to connect to a network. It is a basic security measure as the user should be the only person that knows what MAC addresses are connected to it. However, if someone is listening to the broadcasts of the router and device, they can determine what the MAC address is through the packets of information and copy it onto their own device.</i></p> <p><b>What types of programs/devices use it?</b></p> <p><i>The main type of device that would use this would be a router or any wireless access point that can be configured with MAC address filtering.</i></p> | <p>Discuss (individual/paired or group)</p> <p>What is a firewall?</p> <p>What kind of rules does a firewall need?</p> <p>What are filters?</p> <p>What does MAC mean?</p> <p>What is MAC address filtering used for?</p> <p>What types of programs or devices use it?</p> |
|---|---|--|

|   |   |   |
|---|---|---|
| <p><b>Plenary two</b><br/>(5-10 mins)</p> | <p><i>Assess learning against the learning objectives</i></p> <p><i>This is an open activity whereby the teacher will decide on the best approach to do this based on the pedagogical approach your school takes on assessment.</i></p> | <p><b>For example:</b></p> <ul style="list-style-type: none"> <li>• 5 minute timed writing exercise on what has been learned so far</li> <li>• Fill in class notes</li> <li>• Have a discussion</li> <li>• Answer open questions</li> <li>• Answer directed questions</li> </ul> <p>On: Firewall; MAC Address Filtering</p> |
| <p><b>Homework (optional)</b></p>         | <p><i>Teacher choice based on homework policy of school.</i></p>  | <p><b>For example:</b></p> <ul style="list-style-type: none"> <li>• Write down a correct version of the new authentication method</li> <li>• Write down the encrypted message and explain how it would be un-encrypted</li> <li>• Draw a diagram of a firewall</li> <li>• What does MAC mean</li> </ul>                     |

### Key Terms: Network security

|                              |  |
|------------------------------|--|
| <p><b>Authentication</b></p> | <p>Authentication is the process of identifying an individual and is distinct from authorisation, for example a user can enter a username and password at a login screen and prove they 'know' that piece of information but not that they have permission to login.</p> <p>There are three broad types of authentication, something you...</p> <ul style="list-style-type: none"> <li>- ... know (password)</li> <li>- ... have (smartcard)</li> <li>- ... are (fingerprint or other biometrics)</li> </ul> <p>Multi-factor, or two-factor, authentication is about using additional types of authentication to increase the difficulty for someone malicious to guess/steal the information/item</p> |
|------------------------------|--|

|                          |  |
|--------------------------|--|
| <p><b>Encryption</b></p> | <p>Encryption means to scramble data in such a way that only someone with the secret code or key can read it. For <b>encryption</b> algorithms, a <b>key</b> specifies the transformation of plaintext into ciphertext, and vice versa for decryption algorithms.</p> <p><b>How does it work?</b></p> <p>Encryption works by scrambling the original message with a very large digital number (key). This is done using advanced mathematics. Commercial-level encryption uses 128 bit key that is very, very hard to crack. The computer receiving the message knows the digital key and so is able to work out the original message.</p> <p><b>Why is it important?</b></p> <p>Encryption is important as it enables you to pass a secret message from one place to another without anyone else being able to read it.</p> <p><b>Where is it used?</b></p> <ul style="list-style-type: none"> <li>• Web browsers are able to encrypt your purchase details using an encryption method called 'SSL' (Secure Socket Layer).</li> <li>• Built-in encryption functionality of many office productivity applications (for example, Microsoft Office 2010 offers the strong AES-256 algorithm for the encryption of password-protected files).</li> <li>• Email encryption and also authentication.</li> </ul> |
| <p><b>Firewall</b></p>   | <p>A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules.</p> <p>Simply compared to a security guard who stands at the entrance of your house and filters the visitors coming to your place. He may allow some visitors to enter while denying others whom he suspects of being intruders.</p> <p><b>Who uses it?</b></p> <ul style="list-style-type: none"> <li>• Members of the public</li> <li>• Corporate organisations</li> </ul> <p><b>What systems use it?</b></p> <ul style="list-style-type: none"> <li>• Windows/Mac PC's</li> <li>• Network devices</li> </ul>   |

---

|                              |  |
|------------------------------|--|
| <b>MAC Address Filtering</b> | <p>Media Access Control (MAC) address filtering is the process of setting up parameters to allow only certain MAC addresses onto a network or particular router (Access Point). It is a very rudimentary protection method as it can be copied by someone else listening in to the connection (if wireless).</p> <p><b>What is it used for?</b></p> <p>This is to allow only certain MAC addresses to connect to a network. It is a basic security measure as the user should be the only person that knows what MAC addresses are connected to it. However, if someone is listening to the broadcasts of the router and device, they can determine what the MAC address is through the packets of information and copy it onto their own device.</p> <p><b>What types of programs/ devices use it?</b></p> <p>The main type of device that would use this would be a router or any wireless access point that can be configured with MAC address filtering.</p> |
|------------------------------|--|