TOPIC: Fundamentals of cyber security: Social Engineering Techniques

LEARNING OBJECTIVES:

- Social Engineering
- Blagging and Shoulder Surfing
- Pharming and Phishing

	Teacher Activity	Pupil Activity
Starter activity (5-10 mins) [individual/ paired or group]	*Define the term social engineering. Describe what social engineering is and how it can be protected against*	Discuss (individual/paired or group)

Main activity one (15 mins)	***Blagging:*** *Define the term 'Blagging'* ***What is it?*** *Blagging is trying to invent a scenario to convince someone that you are a person you are not. A very unlikely example of this would be a bank robber dressing up a cleaner (or anyone else who works in the bank) to gain access to restricted parts of the Bank. It could also be to convince someone that you are someone who they can share information with.* ***What is blagging used for?*** *Blagging is used to get information that people shouldn't have access to or it could be used to get into restricted locations.* ***Shoulder Surfing:*** ***What is it?*** *Shoulder Surfing is when a crook is looking over your shoulder while you are carrying out a transaction at a cash dispenser or looking at sensitive/personal information* ***What is it used for?*** *To steal PIN Numbers or Passwords* *Retrieve sensitive/personal information* ***What types of programmes use it?*** *n/a* ***Prevention:*** *To prevent shoulder surfing, it is recommended that you shield paperwork or your keypad from view by using your body or cupping your hand.*	As the students come through the door ask them for their password for their computer logins as the IT team need to carry out some important maintenance work. See how many students divulge their information and once everyone is seated explain what you have done and let them see how easy it was to do. **Role Play** In groups of 2/3 create a scenario in which someone is trying to blag information from someone or their way into a building. The best or most convincing scenario will win a prize. Good examples could be pretending you are an Ofsted inspector to get into the school etc. **Practical activity:** Split the class in two and take one half outside of the room and tell them to try and shoulder surf the others in the class and look at what they are typing without them realising what is happening. This tests whether the shoulder surfers can retrieve information correctly as well as seeing the vigilance of the other students.

Plenary one (5-10 mins)	*Assess learning against the learning objectives* *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.*	**For example:** • 5 minute timed writing exercise on what has been learned so far • Fill in class notes • Have a discussion • Answer open questions • Answer directed questions • What is blagging? • How would you prevent blagging? • What is shoulder surfing? • How would you prevent shoulder surfing?

Main activity two (15 mins)	***Pharming***: *Define the term 'Pharming'* *Pharming is a cyber-attack intended to redirect a websites traffic to another fake site in order to steal user data. Like phishing but without the luring.* ***Why? Purpose:*** *To get innocent people to go on to fraudulent websites without consent or knowledge so the 'pharmers' can get personal information and passwords off the user.* ***How?*** *Malicious code installed on to a victims computer. Pharming redirects Internet users from legitimate websites to malicious ones using a strategy called DNS (domain name system) cache poisoning. The 'pharmer' hijacks the user's computer and takes them to a copycat website. The site it takes them to is most commonly a page that looks identical to that of their bank, eBay, or Amazon. From this point, they ask you to submit your passwords and financial information, all of which go straight into their databanks.* ***Protecting against it:*** • *Check the web address of the website – fake websites will have slightly altered addresses than that of the real addresses.* • *Make sure the website is secure – look for HTTP or HTTPS at the start of the web address.* ***Keywords:*** • ***DNS Server:*** *Computers responsible for resolving internet names into their real IP addresses.* • ***DNS cache poisoning:*** *type of attack that exploits vulnerabilities in the DNS to divert Internet traffic away from legitimate servers and towards fake ones* ***Phishing:*** ***What is phishing?*** *Phishing refers to the process of deceiving recipients of an email into sharing sensitive information with an unknown third party (cyber-criminal).* ***What is it used for?*** *Typically a victim receives an email that appears to have been sent by a known contact or reputable organisation, such as banks, social media, departments in your organisation, etc. An attachment or link in the message may then install malware on the user's device or direct them to a malicious website set up to trick them into divulging personal and financial information such as passwords, account IDs or credit card details.* ***How to identify Phishing Emails:*** 1. ***Take a look at the sender's email address*** *– If it looks suspicious, don't open the email.* 2. ***Look before you click*** *- Hover your mouse over any hyperlinks found in the email and if the address looks weird, don't click on it.*	Discuss (individual/paired or group) • What is 'pharming' • How does 'pharming' work? • How can users protect themselves from 'pharming'? **Activities:** • Get the students to see if they can spot the difference between real and fake versions of websites. • A larger activity would be to get the students to split into groups and see if they can recreate a fake version of a legitimate website, like amazon. This could be done in word or a similar application instead of getting them to make an actual website from scratch. Phishing email activity – give everyone same phishing email. See who can find most problems with email Note how you can identify Phishing emails?

	3. ***Check for spelling mistakes*** - *Legitimate messages usually do not have major spelling mistakes or poor grammar.* 4. ***Who is the email addressed to*** - *Is the email addressed to a vague customer or is it addressed to you personally. Legitimate businesses generally give personal greetings.* 5. ***Don't give up personal information*** – *Legitimate companies will never ask for personal information via email.* 6. ***Be wary of demanding language*** - *Invoking a sense of urgency or fear is a common phishing tactic.* 7. ***Look at the email signature*** – *If there is a lack of contact details in an email signature, it could be a phishing email* 8. ***Don't click on attachments*** - *Including malicious attachments that contain viruses and malware is a common phishing tactic. Don't open any email attachments you weren't expecting.* 9. ***Don't believe everything you see*** – *If it's too good to be true, it probably is!*	

Plenary two (5-10 mins)	*Assess learning against the learning objectives* *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.*	**For example:** • 5 minute timed writing exercise on what has been learned so far • Fill in class notes • Have a discussion • Answer open questions • Answer directed questions Define the term 'Pharming' How would you protect against 'pharming'? Define the term 'Phishing' How you can identify Phishing emails?
Homework (optional)	*Teacher choice based on homework policy of school.*	**For example:** • Make a phishing email and make it look as legitimate as possible • Find the meaning of these terms: 'Spearphishing' and 'Whaling'

Key Terms: Fundamentals of cyber security: Social Engineering Techniques

Blagging	Blagging is trying to invent a scenario to convince someone that you are a person you are not. A very unlikely example of this would be a bank robber dressing up a cleaner (or anyone else who works in the bank) to gain access to restricted parts of the Bank. It could also be to convince someone that you are someone who they can share information with. **What is Blagging used for?** Blagging is used to get information that people shouldn't have access to or it could be used to get into restricted locations.

Shoulder Surfing	Shoulder Surfing is when a crook is looking over your shoulder while you are carrying out a transaction at a cash dispenser or looking at sensitive/personal information **What is it used for?** To steal PIN Numbers or Passwords Retrieve sensitive/personal information **What types of programs use it?** n/a **Prevention:** To prevent shoulder surfing, it is recommended that you shield paperwork or your keypad from view by using your body or cupping your hand.
Pharming	Pharming is a cyber-attack intended to redirect a websites traffic to another fake site in order to steal user data. Like phishing but without the luring. **Why? Purpose:** To get innocent people to go on to fraudulent websites without consent or knowledge so the ‘pharmers’ can get personal information and passwords off the user. **How?** Malicious code installed on to a victims computer. Pharming redirects Internet users from legitimate Web sites to malicious ones using a strategy called DNS (domain name system) cache poisoning. The ‘pharmer’ hijacks the user’s computer and takes them to a copycat website. The site it takes them to is most commonly a page that looks identical to that of their bank, eBay, or Amazon. From this point, they ask you to submit your passwords and financial information, all of which go straight into their databanks. **Protecting against it:** • Check the web address of the website – fake websites will have slightly altered addresses than that of the real addresses. • Make sure the website is secure – look for HTTP or HTTPS at the start of the web address.
DNS Server	Computers responsible for resolving internet names into their real IP addresses.
DNS cache poisoning	Type of attack that exploits vulnerabilities in the DNS to divert Internet traffic away from legitimate servers and towards fake ones

Phishing

What is phishing?

Phishing refers to the process of deceiving recipients of an email into sharing sensitive information with an unknown third party (cyber-criminal).

What is it used for?

Typically a victim receives an email that appears to have been sent by a known contact or reputable organisation, such as banks, social media, departments in your organisation, etc. An attachment or link in the message may then install malware on the user's device or direct them to a malicious website set up to trick them into divulging personal and financial information such as passwords, account IDs or credit card details.

How to identify Phishing Emails:

1. **Take a look at the sender's email address** – if it looks suspicious, don't open the email.
2. **Look before you click** - Hover your mouse over any hyperlinks found in the email and if the address looks weird, don't click on it.
3. **Check for spelling mistakes** - Legitimate messages usually do not have major spelling mistakes or poor grammar.
4. **Who is the email addressed to -** Is the email addressed to a vague customer or is it addressed to you personally. Legitimate businesses generally give personal greetings.
5. **Don't give up personal information** – Legitimate companies will never ask for personal information via email.
6. **Be wary of demanding language** - Invoking a sense of urgency or fear is a common phishing tactic.
7. **Look at the email signature –** If there is a lack of contact details in an email signature, it could be a phishing email
8. **Don't click on attachments -** Including malicious attachments that contain viruses and malware is a common phishing tactic. Don't open any email attachments you weren't expecting.
9. **Don't believe everything you see –** If it's too good to be true, it probably is!