White hat hacker social engineering training exercise

Social engineering, in the context of information security, refers to the psychological manipulation of people into performing actions or divulging confidential information.

In order to help defend themselves against scammers, businesses use **white hat hackers** to try out scams on employees and see if they are well trained enough to spot them. Being aware of the lengths that criminals will go to to get personal information should make you more cautious in your personal life about giving out information on the telephone or taking unsolicited calls.

Try out the different scenarios below and partner up with someone to demonstrate the use of social engineering techniques. You get a point for each item of personal data you get, or each answer to potential security questions you gather (see information sheet for details).

The teacher will partner up with one student to demonstrate the technique, then each student has five minutes to plan their scam before trying it out on their partner.

Number	Description of scam	Type of scam	Points earned
1.	Scammer (impersonating an historian) rings an elderly person at home saying that they have been researching family trees of people living in the area and they need some personal information to confirm their identity before introducing them to some long-lost relatives.	Pretexting	
2.	Scammer (impersonating an IT professional) calls an employee in a company telling them that they have just downloaded a virus that can be fixed if they provide information for the 'IT professional' so they can remotely access the account.	Quid pro quo	
3.	Scammer (impersonating a salesperson) calls a stay-at-home dad and offers him shopping vouchers if he can answer a survey (which includes a lot of personal data).	Baiting	
4.	Invent your own scenario.		

Try to use the persuasion techniques that you learned in English lessons (**FOREST**) to help here:

F	Facts: provide the victim with some true facts to entice or scare them.
O	Opinion: give your personal opinion about the benefit to them of providing information.
R	Repetition: keep repeating the message.
E	Emotive language: make the victim feel sad, happy, worried, or intrigued.
S	Statistics: use some statistics to persuade them (make them up if required).
T	Three (rule of): summarise your case in three points.

Information sheet for white hat hacker social engineering exercise

1. Pretexting
Attackers focus on creating a good pretext, or a fabricated scenario, that they can use to try and steal their victims' personal information. This type of attack commonly involves a scammer pretending that they need certain bits of information from their target in order to confirm their identity.

2. Baiting
Baiting is similar to phishing. The scammer provides the promise of an item or goods to entice victims.

3. Quid pro quo
Quid pro quo attacks promise a benefit in exchange for information, usually a service.

Personal data or security question answers that could provide useful answers to a scammer:

Personal data	**Typical security questions**
1. First name 2. Last name 3. Address 4. Phone number 5. Date of birth 6. Name of school or workplace 7. Job position 8. Email address 9. National Insurance number 10. Passport number 11. Vehicle registration plate number 12. Driver's licence number 13. Credit/debit card numbers 14. Birthplace 15. Login name 16. Password	1. What is the first and last name of your first boyfriend or girlfriend? 2. Which phone number do you remember most from your childhood? 3. What secondary school did you attend? 4. What is the name of your first school? 5. What is your favourite movie? 6. What is your favourite website? 7. What is your favourite online platform? 8. What is your mother's maiden name? 9. What street did you grow up on? 10. What was the make of your first car? 11. What is your father's middle name? 12. What was the name of your Year 1 teacher? 13. What is your favourite social media website? 14. What was the name of your first pet? 15. What was the name of the town in which you were born?

Personal data	Example
1. First name 2. Last name 3. Address 4. Phone number 5. Date of birth 6. Name of school or workplace 7. Job position 8. Email address 9. National Insurance number 10. Passport number 11. Vehicle registration plate number 12. Driver’s licence number 13. Credit/debit card numbers 14. Birthplace 15. Login name 16. Password	1. Elli, Evan, Adriana, Lupe, Mina, Heidi 2. Garden, Kayser, Patel, Singh, McGinn, Petkov 3. 44 Welcome Street CW23 8RJ, 56 Plenty Road LL34 8HJ 4. 07855 654 123, 07864 321 465, 07823 987 465 5. 22.2.68, 10.10.69, 23.1.01 6. St Margot’s Trust Academy, Liverpool Chronicle, Rasdas 7. Till operative, project manager, retired, teacher, pupil 8. Name123@gmail.com, Name123@gmail.co.uk 9. HJ 547389B, KJ 673423A, HJ 237698A 10. 234789234, 578923475, 238472839 11. Y378PUX, X0JLKJ, OX65AWD, KN140XD 12. JONES8493398AD, PATEL8433348JH 13. 1234 5678 1234 5678, 8765 4321 8765 4321 14. Malvern, Leominster 15. Holidaysoon123, Threetwenty123, Pekingese123

Typical security questions	**Example**
1. What was the first and last name of your first boyfriend or girlfriend? 2. Which phone number do you remember most from your childhood? 3. What secondary school did you attend? 4. What is the name of your first school? 5. What is your favourite movie? 6. What is your favourite website? 7. What is your favourite online platform? 8. What is your mother's maiden name? 9. What street did you grow up on? 10. What was the make of your first car? 11. What is your father's middle name? 12. What was the name of your Year 1 teacher? 13. What is your favourite social media website? 14. What was the name of your first pet? 15. What was the name of the town in which you were born?	