**Part 1: Vocabulary and introduction**

|  |  |  |
| --- | --- | --- |
| **Difficult word/phrase** | **Translation** | **Easier replacement** |
| evaluation |  | process of figuring out the worth, amount, or quality of something |
| interpretation |  | (understanding/ explanation) |
| traits |  | qualities |
| manipulate |  | control/move around/mislead |
| several |  | (more than two, but not a lot of) |
| persuade |  | convince |
| trait |  | feature |
| rhetoric |  | (attention-getting talk) |
| previously |  | (before that/before now) |
| interpreted |  | understood/explained |
| perspectives |  | opinions/points of view |
| humanity |  | people/(the kindness of people) |
| incite |  | start (trouble), to move to action |
| liberating |  | freeing |
| overthrow |  | (permanently end, by force) |
| dictatorships |  | (periods of harsh rule by one powerful person) |
| malicious |  | evil and cruel |
| as well |  | also |
| benevolent |  | kind |
| sentences |  | series of words that make sense and that have a subject |
| intention |  | plan/purpose |

**Part 2: Vocabulary quiz**

Answer the “Think”-questions here: https://ed.ted.com/on/UrWLfveg

**Part 3: Video (5 min)**Watch the video *Don't Be Manipulated (Evaluating Information Sources):* [**https://youtu.be/E1NKW5QPlSY**](https://youtu.be/E1NKW5QPlSY)

### Part 4: Could you be a victim of online fraud? Work in pairs (or in a group of three). Read the dialogue. (You can listen to the dialogue here: <https://www.bbc.co.uk/learningenglish/features/6-minute-english/ep-201112> )

**Neil** Are you good at remembering your computer passwords, Georgina?

**Georgina** Um, not really, Neil – I mostly use something easy to remember, like my mother’s maiden name or the street where I was born.

**Neil** Or the name of your first pet! Yes, me too - but we should be more careful about online security, Georgina, because of a worrying trend, and the topic of this programme – online fraud.

**Georgina** Online fraud involves using the internet to trick someone into giving away their money or data. It takes many forms, from deceptive emails which trick us into paying money to the wrong bank account, to the theft of credit card details.

**Neil** It’s regarded by some as a highly profitable and relatively low-risk crime, so in this programme we’ll be finding out why it’s so easy for criminals, or fraudsters, to steal our money.

**Georgina** And of course, we’ll be learning some related vocabulary along the way.

**Neil** But first, it’s time for our quiz question. In July 2020, nine British men were arrested for defrauding the Coronavirus Job Retention Scheme – a government fund for workers who’ve lost their job to Covid-19. They set up fake companies and applied, fraudulently, for money. But how much money has been claimed in total through the coronavirus job scheme in the UK? Is it:

a) 17 billion pounds,
b) 27 billion pounds, or
c) 37 billion pounds?

**Georgina** Hmm, it must be a lot, so I’ll say a) 17 billion pounds.

**Neil** OK, Georgina, we’ll find out later. Now, Rachel Tobac, CEO of Social Proof Security, is an expert in cyber crime. She describes herself as an ’ethical fraudster’. Businesses wanting to combat fraud employ her to hack into their computer systems to find their weak spots.

**Georgina** Here, Rachel explains to BBC World Service programme, The Inquiry, how getting people’s information is the key to online fraud:

**Rachel Tobac** The reason why we’re able to do that, from an attacker **mindset**, is because we use what’s called OSINT – open source **intelligence**. We look up everything about you. We can figure out who your assistant is, who your accountant is on LinkedIn. We know what emails you use from screen shots that you’ve put on your Instagram…

**Neil** Rachel looks at fraud from a criminal’s **mindset** - someone’s way of thinking and the general attitudes and opinions they have about something.

**Georgina** From a fraudster’s perspective, the most valuable thing is **intelligence** - secret information about a government or country, or in this case a person, such as the information people unwittingly post on social media.

**Neil** Fraudsters use this **intelligence** to build up a picture of someone’s online activity.

**Georgina** And as BBC World Service The Inquiry presenter, Charmaine Cozier, explains, there are many ways of doing this:

**Charmaine Cozier** Fraudsters have thousands of **cover stories** but the end goal is always the same – to trick people out of cash or possessions. Rachel says they have options for how to do that. Login details stolen during a **data breach** from one company, often using software or viruses called **malware**, are used to **infiltrate** customer accounts at another.

**Neil** To access people’s data, fraudsters use **cover stories** – false stories told in order to hide the truth. For example, they may pretend to be calling from your bank or credit card company.

**Georgina** If people believe these **cover stories** and share personal data, this can result in a **data breach** - an occasion when private information can be seen by people who should not be able to see it.

**Neil**
**Malware** - computer software and viruses that are designed to damage the way a computer works – can also be used to gain login details and passwords…

**Georgina** …data which is then used to **infiltrate** other online accounts - secretly enter a place, group or organisation in order to spy on it or influence it.

**Neil** Modern fraudsters are so devious at collecting online information that many victims only realise what’s happened after their bank accounts have been emptied.

**Georgina** Which I guess was the **mindset** behind those British fraudsters you mentioned earlier, Neil.

**Neil** Ah yes, the nine men who tried to defraud the Coronavirus Jobs Retention Scheme. Remember for my quiz question I asked you how much the scheme has paid out in total so far in the UK.

**Georgina** I said, a) 17 billion pounds.

**Neil** Well, in fact it’s even more – the correct answer is b) 27 billion pounds. Luckily, the 495 thousand pounds which these fraudsters tried to steal was recovered.

 **Part 5: Discuss** Work in pairs (or in a group of three)

How can we better protect ourselves in our online environments?