Relative clauses: choose the correct answer.

1) "Who's that over there?"
   "Oh, it's our new teacher, …… just started work today."
   A) That
   B) Who he
   C) Which he
   D) Who
2) "Which CD did you get Marcus in the end?"
   "I got him the one …… said he really wanted to hear."
   A) That
   B) Who he
   C) Which
   D) Which he
3) "Who did you send a Valentine's card to?"
   "I'm not telling you, but it was someone …… name begins with 'B'."
   A) Which
   B) Who her
   C) Whose
   D) Whose her
4) "Have you seen Jason Green's latest film?"
   "Is that the one in …… joins the FBI?"
   A) Which he
   B) That he
   C) Whom he
   D) Which
5) "Why do you like Tania so much?"
   "Well, she's one of the few people to …… I can really talk."
   A) Which
   B) Whom
   C) That
   D) Who
6) "Why don't we go to Lionel's for dinner tonight?"
   "Is that the new restaurant …… has just opened on the other side of town?"
   A) Which
   B) That it
   C) Where
   D) Which it
7) "Could you lend me some money?"
   "I'd like you to give me one good reason …… I should."
   A) That
   B) Why
   C) Which
   D) Who
8) "What do you want to do this summer?"
   "I think we should go somewhere …… has plenty of sun and sand."
   A) Who
   B) Where
   C) When
   D) That

Practicing Rewrites: Look at the sentence below and try to rewrite it using the prompts below.

You must never take your helmet off while you are riding a motorcycle.

(3 words) Helmets must be worn _____ while riding a motorcycle.

(4 words) It is _____ your helmet while riding a motorcycle.

Wearing _____ while riding a motorcycle.

_____, one _____.

Source: Williams, Erica J. *Presentations in English*. Honkong: MacMillan, 2008.
"Grizzly Steppe – Russian Malicious Cyber Activity." JAR. Department of Homeland Security. 29 Dec. 2016.
Malcolm Mann and Steven Taylore-Knowles. *Destination B2: Grammar & Vocabulary*. Oxford: Macmillan, 2008.)

Week 4 Presentations

2. Signposting

Signposting helps you structure and shape the main content of your presentation. Signposts create 'verbal paragraphs' or 'verbal signals' and raise the attention curve at the beginning and end of each point of your presentation. The technique allows you to guide the audience through the structure of your presentation linking one point to the next. The audience can't see your notes and can't look forward to see what is coming. You know where you're going on your journey and you need to guide your audience by telling them exactly where you are on the roadmap of your presentation. This is simple but highly effective technique that adds clarity to your presentations.

1. Moving on now to ...
2. I would like to begin by ...
3. Let's now turn to ...
4. Let's start with my presentation ...
5. So, first of all ...
6. Now, turning to ...
7. Now, what about ... ?
8. Let me move on to ...
9. So, that's the general picture for ...
10. I'd like to conclude this point by saying ...
11. This leads me to a point ...
12. So, we've looked at ...
13. That completes my overview of ...
14. Let's just recap ...
15. So, that's pretty much ...
16. and this is ...
17. Next we come to ...
18. So, that was ...
19. My next point is ...
20. That's all I want to say about ...
21. So, that covers this point. ...
22. And finally ...

Match the phrases with functions 1-5:

For instance As you can see So moving on to look at Next I'd like to look at
In my presentation today I'm going to look at OK, that was For example
I'll then move on to look at firstly …, and secondly … So if we look at the slide

1. Introducing the structure of the presentation
2. Introducing new point
3. Referring to a visual
4. Moving on to a new point
5. Giving an example

You will read on the activities of two entities, Advanced Persistent Threat (APT) 29 and ATP28, belonging to the Russian civilian and military intelligence Services (RIS) and their intrusion into a U.S. political party. Discuss the following before reading the text:

1) **What do you think these two actor groups have usually targeted?**
2) **How long do you think these actors operated?**
3) **Which techniques do you think ATP29 and ATP28 used while infiltrating their targets??**

Source: Williams, Erica J. *Presentations in English*. Honkong: MacMillan, 2008.
"Grizzly Steppe – Russian Malicious Cyber Activity." JAR. Department of Homeland Security. 29 Dec. 2016.
Malcolm Mann and Steven Taylore-Knowles. *Destination B2: Grammar & Vocabulary*. Oxford: Macmillan, 2008.)

The two groups have historically targeted government organizations, think tanks, universities, and corporations around the world. APT29 has been observed performing **spearphishing** campaigns **leveraging** web links to a malicious **dropper**; once executed, the code delivers **Remote Access Tools** (RATs) and evades detection using a range of techniques. APT28 is known for leveraging domains that closely **mimic** those of targeted organizations and tricking potential victims into entering legitimate **credentials**. APT28 actors relied heavily on shortened URLs in their spearphishing email campaigns. Once APT28 and APT29 have access to victims, both groups **exfiltrate** and analyze information to gain intelligence value. This data is then used to gather credentials and other valuable information from their targets. At the same time, the actors also spread their influence by multiple means throughout the web.

In summer 2015, an APT29 spearphishing campaign directed emails containing a malicious link to over 1,000 recipients, including multiple U.S. Government victims. APT29 used **legitimate** domains, to include domains associated with U.S. organizations and educational institutions, to host malware and send spearphishing emails. During that campaign, APT29 successfully **compromised** a U.S. political party, and at least one targeted individual activated links to malware. APT29 delivered malware to the political party's systems, established persistence, escalated privileges, **enumerated** active directory accounts, and exfiltrated email from several accounts through encrypted connections back through operational infrastructure.

In spring 2016, APT28 compromised the same political party, again via targeted spearphishing. This time, the spearphishing email tricked recipients into changing their passwords through a fake webmail domain hosted on APT28 operational infrastructure. Using the harvested credentials, APT28 was able to gain access and steal content, likely leading to the exfiltration of information from multiple **senior** party members. The U.S. Government assesses that information was leaked to the press and publicly disclosed.

Actors likely associated with RIS are continuing to engage in spearphishing campaigns, including one launched as recently as November 2016, just days after the U.S. election.

Match the definitions below to the words in bold in the text.

a) *a document proving a person's identity or qualifications.*
b) *A usually malicious piece of software that allows one to control a system from distance*
c) *to bring sb/sth/yourself into danger or under suspicion, especially by acting in a way that is not very sensible*
d) *withdraw (troops or spies) secretly, especially from a dangerous situation.*
e) *mention one by one, or establish the number of*
f) *to look or behave like sth else*
g) *Use something to maximum advantage*
h) *high in rank or status*
i) *A program that installs some sort of malware (virus, backdoor, etc.) to a target system.*
j) *able to be defended with logic or justification; valid.*
k) *An email that appears to be from an individual or business that you know; usually sent to a specific target*

Work in groups and discuss the following:

a) What did you find interesting or surprising in the text?
b) What is your evaluation of the problem?
c) What is likely to happen if the problem is not dealt with? Can you suggest ways of avoiding this in the future?

Source: Williams, Erica J. *Presentations in English*. Honkong: MacMillan, 2008.
"Grizzly Steppe – Russian Malicious Cyber Activity." JAR. Department of Homeland Security. 29 Dec. 2016.
Malcolm Mann and Steven Taylore-Knowles. *Destination B2: Grammar & Vocabulary*. Oxford: Macmillan, 2008.)