IELTS – PASSAGE 3

You should spend about 20 minutes on Questions 1-15.

How should I protect my Windows PC from malware and viruses?

Malware threats

Most of the major AV products started out when many viruses were written by amateurs who were showing off. That's no longer the case. Today's malware is written by professionals who are in business to make money. They are less interested in viruses that replicate themselves – their delivery mechanisms are emails and websites. They don't want to show off: they want their malware to stay hidden.

They are interested in collecting financial information and passwords etc, but there's also a trend towards ransomware.

Coding and screening

Most of the major AV products started out when Windows and its major browsers were insecure. That's no longer the case. In 2002, Microsoft cofounder Bill Gates launched the Trustworthy Computing Initiative to make security the company's highest priority. TCI training and methodologies changed the way Microsoft designed and developed software, and the result has been a dramatic reduction in Windows PC infection rates.

Windows 10 now includes a vast array of security and "threat mitigation" technologies, to the point where the main threats to Windows users come from third-party programs such as Oracle Java and some Adobe software.

There has also been a huge improvement in the security of web browsers, particularly Google's Chrome and Microsoft's Edge.

The result is that Windows 10 users are not sitting ducks, like Windows XP users, as long as they keep their software up to date. This includes updating browsers and other third-party software.

The AV problem

Anti-virus companies started out protecting vulnerable operating system and browser code, but we may have reached the point where vulnerable anti-virus software is doing more harm than good. Normally, programmers won't talk about these problems, because they need the AV supplier's cooperation when AV cripples or crashes their software. And they can't tell users to turn off their AV, because they'll be blamed if something bad happens. That leaves one alternative.

Windows Defender may not do the most good, in protecting you from malware, but it does the least harm.

Security strategy

Stop thinking that malware protection means running an anti-virus program and adopt a layered approach.

First, run Windows 10 with Windows Defender.

Second, run Windows as a standard user, not as an administrator. Running as a standard user may eliminate 90% of threats.

Third, make sure Windows and all your PC's software is updated. Most malware exploits security holes that have already been patched, sometimes several years earlier.

Fourth, make sure you have good backups of all your personal data.

Fifth, run periodic scans to make sure your chosen anti-virus program hasn't missed anything.

Sixth, remember that Windows 10 provides good refresh, reset and recovery options. If those don't do what you want, be prepared to wipe your hard drive and reinstall Windows 10 from scratch, either from a DVD or a thumb drive. Microsoft provides instructions. Your authentication and preferences are stored online against your Microsoft account, and the Windows Store will reinstall any apps you've downloaded, so it's relatively easy to get back to where you were.

AV Choice

If you are not on Windows 10, if you are accident-prone, or if you have other reasons for wanting better protection, there's still a place for anti-virus programs. From the current free programs, I recommend Avira or Bitdefender, though both Avast and AVG (which is now owned by Avast) are still acceptable choices. Kaspersky is probably the best paid-for option, but Trend Micro is worth a look.

Try a couple of AV programs to see if you like any special features, the user interface, the impact on performance, whether it seems to interfere with any other software, the scanning speed and so on. There are at least a dozen decent alternatives, so you don't have to use one you don't like.

Adapted from: *https://www.theguardian.com/technology/askjack/2017/apr/13*

Questions 1-5
Complete the sentences below with words taken from the passage.
Use NO MORE THAN THREE WORDS for each answer.

Malware threats are no longer written **1.** ....

Most AV were produced when major browsers were **2.** ....

Now vulnerable anti-virus is doing **3.** .... than good.

Malware protection requires the adoption of a **4.** ....

There are at least a dozen **5.** .... for AV programs.

Questions 6-10
Do the following statements agree with information given in the passage?
Write:
TRUE if the statement is true according to the passage
FALSE if the statement is false according to the passage
DOES NOT SAY if there is no information about this in the passage

6. Malware is written to show off. ....

7. There has been a dramatic reduction of computer infections thanks to AV. ....

8. Nowadays some AV software can cause damage. ....

9. Just running an AV program is not enough to protect a PC. ....

10. Avira is an open source AV program. ....

Questions 11-15
Complete the flow chart with words taken from the passage.

Security strategy
↓
Run Windows 10 with **11.** ....
↓
Run Windows as a **12.** ....user
↓
Make sure that Windows and all the software is updated
↓
Make sure you have good **13.** .... of data
↓
Run periodic **14.** ....
↓
Remember that Windows provides good refresh, reset and recovery **15.** ....