Students' copies

Example 1 :

With the increase in the number of cyberattacks and their complexity, they now concern everybody. Moreover, according to the French Ecological Transition Agency, 79% of carbon diaoxyde emissions come from hardware crafting. Thus, improving software security while addressing pollution will shape the digital market.
Cybersecurity technologies have already quickly adapted. Groups like SFR, Orange or Verizon have conceived advanced security services for firms, while Apple developed an optional security for people who may be subject to state-sponsored cyberattacks. The spreading of this kind of advanced technologies might be an answer to security risks. However, since 90% of successful hacks aim at uninformed users, education to cybersecurity is also part of the answer. Finally, the increase in former repaired devices sales prevents new security-optimized devices from spreading. The future answer might be to allow second-hand devices to support new security technologies. (140 words)

Example 2:

For two years, and globally, the cybercrime rate has increased exponentially, reaching a point where upgrading our technologies has become mandatory. The same goes for the digital carbon footprint from the high-tech industry that is everyday more concerning. Those challenges will reset the telecommunications market.
Companies are developing solutions, softwares and resources are being upgraded or created to protect companies against hacking and to monitor their systems. Another way could be to make available to the public extremely efficient private systems like Cryptosmart. But protection also means teaching people how to react properly to digital threats. However, those technologies are environmentally concerning which pushes for the development of the second-hand market, thus going against the democratization of those news tools. As a consequence, the future will most likely reside in the optimization of the latter for low-end technologies. (138 words)

Example 3:

As technologies have ever growing roles in our society, they create new risks and dilemmas, such as cyberattacks, needing proper solutions. However, the production of new devices to counter cyberattacks has a real impact on C02 emissions. This dilemma calls for new solutions, addressing both problems.
The increase of organized cyberattacks creates the need for new digital security measures. Indeed, IT companies use new technologies such as AI working with ecosystems of devices to counter phishing against companies. New sophisticated softwares, normally reserved to people at risk such as Presidents could also be used for the average individual. But all those solutions require the consumption of new devices, thus creating e-waste and CO2 emissions. A better solution lies in the education of citizens and companies against cyber threats paired with second-hand devices working with new security technologies. (137 words)

Example 4:

Now more than ever, cybersecurity and greener technologies are a top priority. Cybercriminals are now better organized and operate in teams. As both companies and individuals are victims of cyberattacks, new tech companies like SFR, Orange and Verizon developed tools to either protect terminals, track down cybercriminals or identify the breaches. As for individuals, Apple now proposes an increased security option and Orange's impenetrable tech is installed on the French President's phone. However, as for today, the best security is still to inform people about how to use their devices properly.
The issue is that those tools are energy-consuming and that digital pollution doesn't cease to increase. Still, we see that second-hand products are favored. So the solution might be to equip them with the latest cybersecurity technologies. (128 words)

Example 5:

In our digital society, updating our cyberdefense is crucial. Indeed, the threat of a cyberattack concers everyone, from individuals to companies. This threat is increasing with hackers becoming more organized, resourceful and the number of cyberattacks has increased a lot in the last few years. To counter those attacks, telecommunications companies have developed new tools, services and ecosystems that protect users from attacks, using Machine Learning, AI and experts in the field. Yet, 90% of successful attacks are down to user errors, which is why we should also teach people safe practices.

Digital pollution should also be taken into account with CO2 emissions that could double by 2025, owing primarily to tech manufacturing. The development of second-hand markets reduces the amount of new devices but should be adapted to be compatible with the latest digital security solutions. (137 words)

Example 6:

Since the pandemic, there has been an exponential growth of cyberattacks, due to the increasing quality of attacks that come from organized groups sharing knowledge and resources. In response, there has been an increase in cyber defense. New technologies, developed with AI and machine learning, could one day be normalized for the general population. Apple, Verizon, Cryptosmart and others are developing technologies that aim to protect communications, terminals, to identify weaknesses in a system, to isolate devices and more. But in 90% of cases, users are at fault. The best protection is awareness.

On the other hand, the increase of digital devices has caused the increase of CO2 emissions. This problem can be nullified by the use of second-hand devices, but needs security technologies to adapt to older devices as to not decrease security. (134 words)

Example 7:

Since the beginning of the Covid crisis, cyberattacks have become more numerous, sophisticated and organized. On the other hand, the impact of digital technologies on the environment could double between 2023 and 2025, with most of the CO2 emissions coming from the manufacturing of computers. To protect companies and individuals, telecommunication companies are using artificial intelligence, data bases and other cutting-edge technologies to analyze threats, track them down on computers and give security reports. With such improvements, technologies only available to exposed personalities, for example a President, could be used for anyone in the future. However, users are still accountable for 90% of hackers' successful attacks and we need to raise their awareness on safe practice. We also need to keep using second-hand devices to limit pollution while at the same time adapt them to state-of-the-art security features. (138 words)

Example 8:

Online hacking is becoming increasingly frequent and organized. To protect users, telecommunication companies try to come up with new ways of thinking: protection systems based on AI, isolation techniques to reduce weak points, quick identification of threats, or data bases that record attacks to better understand how to defend against them. These ideas need to evolve as quick as the hacking world does. On the other hand, successful attacks are often due to users allowing the access to their machines. These uninformed users need proper teaching on the new online threats.

Moreover, digital pollution is increasing and already representing 2.5% of the CO2 emissions in France. Most of this pollution is created during the fabrication of devices and that is why some think the solution to both pollution and hacks lies in the development of reusable devices that can support cutting-edge protection systems. (143 words)