# Self-study, Lesson 6, March 25

## EN Version: 9E – Cyber crime (p. 88-89)

**Lesson objective:** I can understand texts about modern crime

**Tasks:**

* Read about some interesting computer crimes which are common in our times. Do exercises 1, 2, 3 without a dictionary. Try to guess the meaning of unknown words from the context.
* Then use a dictionary to learn the meaning of words such as: *cash machine, astonished, bank account, delighted, spread around, get rid of,* etc.
* Do exercises 4 and 5
* Copy questions 1,2,3,4 from exercise 6 into your notebook and answer them with full sentences**\***
* **Read today´s article (on the last page) about the rise of cybercrime during the coronavirus pandemic. Think about the questions:**
	+ Why are hackers attacking more during this crisis? What are their motives?
	+ What is „ransomware“?
	+ What negative consequences do the cyber attacks have?

**What have I learnt?**

I have learnt vocabulary related to computer crime. I practised reading comprehension.

**\*Poznámka:** Všetky úlohy, čo vám dávam vypracovávať do zošita (aj do knihy, ale hlavne do zošita), si po návrate do školy skontrolujem, ohodnotím, vaša známka za tento polrok bude závisieť aj od nich. Píšem si hodnotenie aj za to, čo posielate na mail (Kamila, Ilya zatiaľ)

## Answer key – Správne odpovede

Ex. 1

They are all related to computers/internet/cyber space

Ex.2

A1,B4,C2,D3

Ex.3

A,B,D,D,A,C,B,C

Ex. 4, 5 – should be no problem

**Further tasks and exercise / ďalšie precvičovanie a úlohy**

**Workbook – p. 84 – the whole page. How would you translate the heading „Crime doesn´t pay“ ?**

# Cybercrime rising during coronavirus pandemic



* The head of global research and analysis at Kaspersky, Costin Raiu, warned that a cyberattack against a hospital can result in a loss of human lives (Photo: [Wikimedia](https://www.google.com/url?q=https%3A%2F%2Fupload.wikimedia.org%2Fwikipedia%2Fcommons%2Fa%2Fa5%2FUS_Navy_030423-N-6967M-090_A_central_computer_system_monitors_the_heart_rates_of_each_patient_in_the_Intensive_Care_Unit_%2528ICU%2529_to_ensure_a_quick.jpg&sa=D&sntz=1&usg=AFQjCNGKXB01_RvjNPla7f71HzVHLvw7XQ" \t "_blank))

By [**ELENA SÁNCHEZ NICOLÁS**](https://www.google.com/url?q=https%3A%2F%2Feuobserver.com%2Fsearch%3Fquery%3D%2522Elena%2BS%25C3%25A1nchez%2BNicol%25C3%25A1s%2522&sa=D&sntz=1&usg=AFQjCNF1Sd2P0HCzkO2OhyRW9fonesN9eQ)

BRUSSELS, TODAY, 07:07

The president of the European Commission, Ursula von der Leyen, warned on Tuesday (24 March) that cybercrime in the EU has increased due to the coronavirus outbreak.

Cybercriminals are taking advantage of the increasing amount of time that people spend online due to new measures taken by member states to stop the spread of the virus - while they also benefit from the health crisis itself.

"They follow us online and exploit our concerns about the coronavirus. Our fear becomes their business opportunity," von der Leyen said in a video message.

As a result, the police cooperation agency Europol is fighting [trafficking in counterfeit coronavirus 'medicines'](https://www.google.com/url?q=https%3A%2F%2Fwww.europol.europa.eu%2Fnewsroom%2Fnews%2Frise-of-fake-%27corona-cures%27-revealed-in-global-counterfeit-medicine-operation&sa=D&sntz=1&usg=AFQjCNEUcE2Y_9tB6bWljNJWBTcGpNj50A" \t "_blank).

Meanwhile, the internal market commissioner Thierry Breton is consulting with telecom operators how to protect EU networks against cyberattacks.

According to the commission, the European network of Computer Security Incident Response Teams (CSIRTs) have also raised the level of alert, urging a strong cyber resilience during this specific period.

Meanwhile, more and more hospitals, research hubs and medical centres are being targeted by organised cyber units which are after information, intelligence, and system accessibility.

"Today's unexpected and extraordinary measures increase the cyber risk in many ways we have never seen before," said Lukasz Olejnik, an independent cybersecurity researcher and consultant who has been [analysing this phenomenon](https://www.google.com/url?q=https%3A%2F%2Fblog.lukaszolejnik.com%2Fcovid-as-a-cyber-risk-theme-why-scams-or-unauthorized-access-attempts-using-coronavirus-theme-is-something-unprecedented-and-risky%2F&sa=D&sntz=1&usg=AFQjCNFirmTLIS55kR_Jo28r5WHAuOTnFQ" \t "_blank).

"The crisis of coronavirus is sadly an enticing for exploitation since people may be easier to scam using the 'coronavirus theme' because now everyone is familiar with it," he added.

The World Health Organization (WHO) recently warned about [suspicious email messages attempting to take advantage of the Covid-19 emergency](https://www.google.com/url?q=https%3A%2F%2Fwww.who.int%2Fabout%2Fcommunications%2Fcyber-security&sa=D&sntz=1&usg=AFQjCNEGDt2vPwk_03xcjM4a47xFI1hN8A" \t "_blank) by stealing money and sensitive information from the public.

However, according to new reports, hacking attempts against WHO's own computer systems and its partners have increased during the coronavirus outbreak.

Although the aim of these attacks is unclear, one might presume a multitude of motives for attacking prominent health organisations during this pandemic.

For example, cybercriminals could be looking for information about cures, tests or vaccines relating to the coronavirus to sell in the black market, encrypt sensitive data and hold it for ransom, or simply disrupt the operability of the institution.

## Patients at risk

Likewise, hospitals and medical centres across Europe are also being the target of cyber attackers as they battle against the coronavirus.

Yet, the vast majority of these attacks are "ransomware" - cybercriminals behind these would encrypt large amounts of critical hospital data and demand a large ransom to restore it.

According to Costin Raiu, head of global research and analysis at Kaspersky, a destructive or ransomware attack against a hospital or any other health organisation can be "very dangerous" as it puts patients at risk.

"In an extreme case, this can result in a loss of human lives, either because the resources required to treat them are no longer available or the processes in the hospital are severely slowed down," said Raiu, adding that it is important for hospitals to be protected and to protect their patient data.

Earlier this month, Brno University Hospital in the Czech Republic - which is a major Covid-19 testing hub - suffered an attack that disrupted the functioning of the institution and caused surgery postponements.

Likewise, a hacker group attacked the computer systems of  [the UK's Hammersmith Medicines Research (HMR)](https://www.google.com/url?q=https%3A%2F%2Fwww.computerweekly.com%2Fnews%2F252480425%2FCyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus&sa=D&sntz=1&usg=AFQjCNFOHQdzV-MiMvTJJUfM7kW8xsJtOg" \t "_blank), which is performing trails on Covid-19 vaccines, publishing personal data of thousands of former patients after the company fail to pay the extortion demand.

According to the French cybersecurity agency, the Paris AP-HP hospital was also the target of a failed cyber-attack last week.

The [Spanish law enforcement announced](https://www.google.com/url?q=https%3A%2F%2Feuobserver.com%2Fcoronavirus%2F147850&sa=D&sntz=1&usg=AFQjCNE9UlZ3DW9IhunbcMjczaBBmsi-hg" \t "_blank) on Monday that malicious software was trying to break the IT system of hospitals and medical centres, urging health workers to avoid opening suspicious emails.

"Disruption can accumulate and negatively contribute to elongated procedures, what may even indirectly lead to a negative impact on human health or in some situations - even life," warned Olejnik.