IT Security

1 Listening

Listen to the following recording about Cybersecurity and answer the questions.

1 What is the analogy used to describe the development of the internet?
2 What was the original purpose of the Internet and who had access to it?
3 How did the internet evolve over time?
4 Why is it difficult to make the internet completely secure?
5 What are some characteristics of a perfectly secure Internet ?
6 What are some measures that would be required to log onto a website in a perfectly secure internet?
7 Despite the mentioned safeguards what is the possibility of a hacker finding a way into a perfectly secure internet?
8 What are some actions that can be taken to protect oneself in the current flawed internet?

2 Reading 1: Cybercrime and Hacking

Read the following text and choose the correct option.

The internet has become the integral part of today's generation of people; from communicating through instant messages and emails to banking, travelling, studying and shopping, internet has touched every aspect of life. With the growing use of the internet by people, protecting important information has become a necessity. A computer that is not having appropriate security controls can be infected with malicious logic and thus any type of information can be accessed in moments. Number of infected Web Pages and malicious websites can be seen every day that infects the computer and allow hackers to gain illegal access to other computer systems.
Hacking of important data, network outages, computer viruses and other cyber related threats affect our lives that range from minor inconvenience to serious incidents. Cyber threats can be caused due to negligence and vulnerabilities, or unintentional accidents. The main objectives of such type of system attackers or hackers are to steal confidential information, to make illegal monetary transactions, to destroy or to change data and the like. System attackers can be terrorists, crackers or recreational hackers. They have a variety of tools that can harm or infect the computer; usually they use malicious logic or virus to gain unauthorized access to a computer. Opening email attachments that carry the virus, clicking malicious links or websites or unintentionally downloading a dangerous program are common ways through which a computer can be infected and data can be stolen.
As the number of data networks, digital applications, as well as internet and mobile users are growing, so do the chances of cyber exploitation and cybercrimes. Even a small mistake in securing data or bad social networking can prove to be extremely dangerous.

If accounts are not properly secured, it makes easier for hackers or unauthorized users to spread viruses or social engineered attacks that are designed to steal data and even money. Such types of issues highlight the need for cyber security as an essential approach in protecting and preventing data from being used inappropriately.

In simple language, Cyber Security or Information technology security means protecting data, networks, programs and other information from unauthorized or unintended access, destruction or change. It encompasses all the mechanisms and processes that protect digital equipment, information and records from illegal or unintended access, manipulation or destruction.

In today's dynamic environment, cyber security has become vital for individuals and families, as well as organizations (such as military, government, business houses, educational and financial institutions, corporations and others) that collect and store a wide range of confidential data on computers and transmit that to other computers across different networks. For families, protection of children and family members from cybercrime has become substantially important. For an individual, protecting information that could impact social life as well as personal finance is essential.

The internet has provided a wide array of learning opportunities, but there are risks too. Photos, videos and other personal information shared by an individual on social networking sites such as Facebook, Twitter can be inappropriately used by others may lead to serious and even life-threatening incidents. Social networking sites have become the most popular medium for sharing information and connecting with other people. But these sites have created varied opportunities for cybercrimes, compromised personal identities and information leakage. Therefore, it is important for individuals to understand how to protect against cyber threats, and must also comprehend the difference between virtual and real world. One should learn how to protect computers and personal information from being hacked and should engage in appropriate online behaviour in order to eliminate changes of cyber threats and thereby creating a safer online environment.

Q1. According to the author what does cyber security mean?

(**a**) Cyber Security means the dispersion of important data and devise a structural engineering that allow easy flow of information.
(**b**) Cyber Security means protecting data, networks, programs and other information from unauthorized or unintended access, destruction or change.
(**c**) Cyber Security means the Hacking of important data, network outages, computer viruses and other cyber related threats affect our lives that range from minor inconvenience to serious incidents.
(**d**) None of the above

Q2. According to the author, what is the main reason behind cyber threats?
(a) the unknown person with malice
(b) due to intelligence, veneration and intentional threats.
(c) due to negligence and vulnerabilities, or unintentional accidents.
(d) None of the above

Q3. What is the downside of Social media, according to the author?
(**a**) by sharing sensitive information, one can be vulnerable to sudden outburst of emotions
(**b**) information shared by an individual for socializing purposes can be distorted and can be used for malignant purpose.
(**c**) the social media owners can steal the information and sell this information for monetary purposes
(**d**) None of the above

Q4. According to this passage, how does the virus get into the computers?
(**a**) by opening a document file in the search history
(**b**) by texting online and receiving files on social media platforms
(**c**) Opening email attachments that carry the virus, clicking malicious links or websites or unintentionally downloading a dangerous program
(**d**) None of the above

Q5. Which words in the text correspond to the following definitions?

a failures or interruptions in use or functioning § 1st line. ....outages.....

b savvy computer users who intrude on networks to impress others § ....recreational hackers

c includes different types of things § ...encompasses....

d to a great or significant extent § second page ....substantially....

e made vulnerable by unauthorized access or exposure § ...compromised.....
second page

3 Internet crimes

Choose the right answer to identify the following internet crimes.

1 Which of the following refers to the forging of the return address on an email so that the email message appears to come from someone other than the actual sender.

a Spamming **b** Spoofing **c** Spooling **d** None of these

2 Which of the following is a fraudulent practice in which someone tries to trick you into giving them your private information via text message.

a Encrypting **b** Vishing **c** Smishing **d** Pretexting

3 In which type of malicious act, a hacker contacts you by phone or email and attemptsto acquire your password.

a Defacing **b** Phishing **c** Bugging **d** None of these

4 Which of the following refers to any fraudulent business or scheme that take money or other goods from an unsuspecting person.

a Hacking **b** Spamming **c** Scamming **d** Pharming

5 Which of the following involves the repeated use of the Internet or other electronic means to harass, intimidate or frighten a person or group.

a Cyberbullying **b** Cyberslaking **c** Cyberstalking **d** Both a and c

4 Phishing

Complete the following passage about phishing with the appropriate words.

The term phishing describes a wide range of tactics cyberattackers use **1**.....you into doing or providing something they want.

These may include entering your **2**.....information to a fake banking website, opening an unsafe **3**.....,...clicking an unsafe link, and transferring money into an overseas bank account. All phishing attacks have something in common, they **4**.....human nature rather than technology. Many phishing emails **5**..... your emotions by telling you something is wrong or that bad things will happen if you don't respond. They often want you to act with urgency, and most of them try to build trust, often, by impersonating a brand or person you know. The From field or email domain may seem **6**..... .

The spear phishing is one type of phishing, in which the attacker focuses on a specific **7**....., perhaps a highly privileged individual within an organization; this

means that they must craft a convincing message that is tailored to the **8/9**..... ..... . The attacker carefully plans the **10**.....gathering data about the victim, their social networks and their online accounts before meticulously tailoring the bait to the individual. Once the victim falls for the bait his **11**..... are captured, the attacker secretly enters the network and installs a persistence mechanism such as a remote access Trojan **12**.....ongoing access to the system.

5 *Language work: Revising compound words*

A Find the missing words to form compounds in the following sentences.

1 Password.....sites are accessible only to users entering the correct password.

2 Cloud.....services or resources made available to users on- demand via the Internet from a cloud.

3 Cyber.....refers to malicious attempts to gain access to a computer network.

4 Human.....search engines rely on human intervention to submit information.

5 Data.....is a large store of data accumulated from a wide range of sources used to guide management decisions.

B Read the following sentences, and then form compounds that refer to them.

1. A website which is designed in a good way.
2. A software designed to work across multiple platforms.
3. An operation which doesn't require hands.
4. A computer which runs on batteries.
5. A hard drive which integrates two different technologies.
6. A special file which redirects to another file or program.
7. A peripheral device which reads and writes flash memory.
8. A file which can be retrieved and displayed, but not changed or deleted.
9. A content created by users of a service.
10. An unauthorized access of a website.
11. Strategies against malware.

6 Cloze test: Phishing

Complete the following passage about phishing with the appropriate words.

The term phishing describes a wide range of tactics cyberattackers use to **1** t.rick..... you into doing or providing something they want.

These may include entering your **2** l.ogin.....information to a fake banking website, opening an unsafe email attachment, clicking an unsafe link, and transferring money into an overseas bank account. All phishing attacks have something in common, they **3** explore..... human nature rather than technology. Many phishing emails **4** t.rigger..... your emotions by telling you something is wrong or that bad things will happen if you don't respond. They often want you to act with urgency, and most of them try to build trust, often, by **5** i.mpersonating a brand or person you know. The From field or email domain may seem **6** l.egitimate... .

The spear phishing is one type of phishing, in which the attacker focuses on a specific **7** t.arget....., perhaps a highly privileged individual within an organization; this means that they must craft a convincing message that is customised to the intended victim. The attacker carefully plans the **8** s.tage.....gathering data about the victim, their social networks and their online accounts before meticulously **9** t.ailoring.....the bait to the individual. Once the victim falls for the bait his **10** c.redentials..... are captured, the attacker secretly enters the network and installs a persistence mechanism such as a remote access Trojan to **11** s.ecure.....ongoing access to the system.

7 Reading: Ransomware attack- What is it and How does it work?

A Read the following article and answer the questions below.

Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyberattackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files. Some variants have added additional functionality – such as data theft – to provide further incentive for ransomware victims to pay the ransom.

The modern ransomware craze began with the WannaCry outbreak of 2017. This large-scale and highly-publicized attack demonstrated that ransomware attacks were possible and potentially profitable. Since then, dozens of ransomware variants have been developed and used in a variety of attacks. The COVID-19 pandemic also contributed to the recent surge in ransomware. As organizations rapidly pivoted to remote work, gaps were created in their cyber defenses. Cybercriminals have exploited these vulnerabilities to deliver ransomware, resulting in a surge of ransomware attacks.

In an age dominated by digital risks, a staggering 71% of companies have encountered ransomware attacks, resulting in an average financial loss of $4.35 million per incident. In the year 2023 alone, attempted ransomware attacks have targeted 10% of organizations globally. This marks a notable rise from the 7% of organizations facing similar threats in the previous year, representing the highest rate recorded in recent years. According to Cybersecurity Ventures, ransomware attacks will cost victims over $265 billion in annual damages by 2031.

In order to be successful, ransomware needs to gain access to a target system, encrypt the files there, and demand a ransom from the victim. While the implementation details vary from one ransomware variant to another, all share the same core three stages:

First, Ransomware, like any malware, can gain access to an organization's systems in a number of different ways. However, ransomware operators tend to prefer a few specific infection vectors.
One of these is phishing emails. A malicious email may contain a link to a website hosting a malicious download or an attachment that has downloader functionality built in. If the email recipient falls for the phish, then the ransomware is downloaded and executed on their computer.
Another popular ransomware infection vector takes advantage of services such as the Remote Desktop Protocol (RDP). With RDP, an attacker who has stolen or guessed an employee's login credentials can use them to authenticate to and remotely access a computer within the enterprise network. With this access, the attacker can directly download the malware and execute it on the machine under their control. Others may attempt to infect systems directly.

After ransomware has gained access to a system, it can begin encrypting its files. Since encryption functionality is built into an operating system, this simply involves accessing files, encrypting them with an attacker-controlled key, and replacing the originals with the encrypted versions. Most ransomware variants are cautious in their selection of files to encrypt to ensure system stability. Some variants will also take steps to delete backup and shadow copies of files to make recovery without the decryption key more difficult.

Once file encryption is complete, the ransomware is prepared to make a ransom demand. Different ransomware variants implement this in numerous ways, but it is not uncommon to have a display background changed to a ransom note or text files placed in each encrypted directory containing the ransom note. Typically, these notes demand a set amount of cryptocurrency in exchange for access to the victim's files. If the ransom is paid, the ransomware operator will either provide a copy of the private key used to protect the symmetric encryption key or a copy of the symmetric encryption key itself. This information can be entered into a decryptor program (also provided by the cybercriminal) that can use it to reverse the encryption and restore access to the user's files.

While these three core steps exist in all ransomware variants, different ransomware can include different implementations or additional steps. For example, ransomware variants like Maze perform files scanning, registry information, and data theft before data encryption.

A successful ransomware attack can have various impacts on a business. Some of the most common risks include:

- Ransomware attacks are designed to force their victims to pay a ransom. Additionally, companies can lose money due to the costs of remediating the infection, lost business, and potential legal fees.
- Some ransomware attacks encrypt data as part of their extortion efforts. Often, this can result in data loss, even if the company pays the ransom and receives a decryptor.
- Ransomware groups are increasingly pivoting to double or triple extortion attacks. These attacks incorporate data theft and potential exposure alongside data encryption.
- Ransomware attacks can harm an organization's reputation with customers and partners. This is especially true if customer data is breached or they receive ransom demands as well.
- Ransomware attacks may be enabled by security negligence and may include the breach of sensitive data. This may open up a company to lawsuits or penalties being levied by regulators.

Taking the following best practices can reduce an organization's exposure to ransomware and minimize its impacts:

Cyber Awareness Training and Education: Ransomware is often spread using phishing emails. Training users on how to identify and avoid potential ransomware attacks is crucial. As many of the current cyber-attacks start with a targeted email that does not even contain malware, but only a socially-engineered message that encourages the user to click on a malicious link, user education is often considered as one of the most important defenses an organization can deploy.

Continuous data backups: Ransomware's definition says that it is malware designed to make it so that paying a ransom is the only way to restore access to the encrypted data. Automated, protected data backups enable an organization to recover from an attack with a minimum of data loss and without paying a ransom. Maintaining regular backups of data as a routine process is a very important practice to prevent losing data, and to be able to recover it in the event of corruption or disk hardware malfunction. Functional backups can also help organizations to recover from ransomware attacks.

Patching: Patching is a critical component in defending against ransomware attacks as cyber-criminals will often look for the latest uncovered exploits in the patches made available and then target systems that are not yet patched. As such, it is critical that organizations ensure that all systems have the latest patches applied to them, as this reduces the number of potential vulnerabilities within the business for an attacker to exploit.

User Authentication: Accessing services like RDP with stolen user credentials is a favourite technique of ransomware attackers. The use of strong user authentication can make it harder for an attacker to make use of a guessed or stolen password.

1 What is the significance of the WannaCry outbreak in the context of ransomware?

2 How did the COVID-19 pandemic influence the frequency of ransomware attacks?

3 In which way do ransomware operators utilise Remote Desktop Protocol(RDP) as an infection vector?

4 What measures do some ransomware variants take to hinder recovery efforts after encryption has occurred?

5 How do ransomware operators typically communicate their ransom demands to victims?

6 What are the potential outcomes that a company may face due to a ransomware attack?

7 What are the key components of an effective cybersecurity training program aimed at preventing ransomware attacks?

8 What is the importance of maintaining continuous data backups in ransomware attacks. How do they help organisations?

9 Why is patching considered a critical component in defending against ransomware attacks?

B Find in the text words having a similar meaning to the following definitions.

1 a factor that motivates or has a driving force upon someone to do something .....

2 shocking, or surprising that it is difficult to believe .....

3 the act of getting something, especially money, by threats .....

4 imposed or charged by official authorities .....

1-

2 - The covid 19 pandemic led to remote work, creating gaps in cyber defences that cybercriminals exploited these vulnerabilities.

3-

8 Listening: Is the cloud secure?

Listen and complete the following extract with the missing words.

We all know that cloud-based platforms like Microsoft Office 365 and Google GSuite can be great for collaboration and efficiency, but have you ever considered that in the wrong hands your cloud account can also be a **1** ..weapon..... .

A cyberattacker who takes over your cloud account has **2** ...free...reign.... over all the sensitive data you have access to. Anyone who controls your email account can exploit everyone who trusts it. Once your cloud account is **3**..hijacked....., it can lead to **4**...mis...fraud....., data breaches and more. Attackers target all sorts of accounts: you might expect some targets such as executives but there are many other more desirable targets like **5**...privileged.....users, users with access to **6**..regulated..data....., finance departments, and service accounts that access valuable information.

How do attackers get into a cloud account in the first place? Here are the most common ways:

Attackers can get your credentials in the **7**..data..breach..... or they can trick you in the providing account logging details through a **8**...credential...phishing... . In a **9** ..brute ...force...attacks....., they try hundreds of thousands of character and word combinations until they find your password. It's a bad practice, but many people use the same passwords for different accounts.
In a **10** ..credential...stuffing..., the attacker will try a large set of stolen passwords to see if any would **11**....get....them.....in..... .
We all love add-ons that give us new features **12** ..in.....our...apps....., but attackers can create seemingly helpful add-ons to **13**...compromise....your...app...and give them access to your cloud account. Cyberattackers are increasingly focusing on people not infrastructure.

9 Error correction: Smartphone security tips

Find and correct the mistakes in the following extract using the correction code below.
T(tense), Pr(preposition), Gr(grammar), P(punctuation), WO (word order), WW(wrong word), SM(something missing)

A smartphone is the most widely used electronic device in daily life for many of us. The days of mobile phones being used mainly to call someone or send a text message is long gone – now, they operate as portable computers, with a big array of apps for everything from social networking to online banking. The extent on which we rely on our phones, plus the amount of data they contain, means that phone security is crucial. If you want to know how to protect your phone, here are some essential smartphone security musts:

Keep your phone locked
If your device is stolen, the thief could obtain access to your personal information. To prevent this, it's important to have a lock on your screen. As long as this is a passcode, pattern, fingerprint, or face recognition depends on your preferences and your device's. You can usually specify how much the phone can be idle before locking when enabling a lock screen. Choose the shorter amount of time to increase your phone security. You are protected because the screen locks automatically while you forget to lock it yourself. It will also open up your battery because the screen goes dark after a set period of inactivity.

Turn off Wi-Fi and Bluetooth when not in use
When you let Wi-Fi and Bluetooth active, hackers can see what networks you have connected to before, spoof them and deceive your phone into connecting to Wi-Fi and Bluetooth devices that hackers carry out. Once connected to your phone, hackers can attack your device

with malware, steal data, spy on you – without you necessarily notice. Therefore, it's good to turn off Wi-Fi and Bluetooth when you don't need them.

Don't jailbreak or root your phone
Jailbreaking or rooting your phone is the process of unlocking your phone and removing the safeguards that manufacturers had put in place so you can access anything you want. Users jailbreak or root their phones to access app stores other than the official ones, but this carries risk. The apps on stores have not been vetted which means they can spy on your phone and steal sensitive information.

Enable remote wiping of your phone
If your phone is lost or stolen, you can clear remotely your personal data from its memory. Provided you have previously backed up your data to the cloud, you needn't to worry about losing that data.

10 Improve your vocabulary: CONFUSING WORDS

Choose the correct word in each sentence below.

1. My limited vocabulary **prevented/ avoided** me from getting a good grade in the test .
2. If you learn the vocabulary in this book, you have a better **chance/ possibility** of passing the exam.
3. I like working here. It's a good **job/ work** .
4. It's important to teach children not to **tell/say** lies.
5. 7. Words with the same dictionary meaning may have very different **connotative/ denotative** meanings.
6. 2. I have become tired of your **continual/continuous** email messages.
7. 3. If he were to study before tests, he could possibly work **farther/further** towards a scholarship.
8. Based upon all of the facts presented to them, the students **implied/inferred** that the experiment was a success.
9. Do you want to **lose/ loose** your high grade because of one poor test score?
10. The scientist is interested in the **oral/verbal** annotations contained in the study.
11. She made an astute **observance / observation** about the assignment.
12. If you have a more **ingenious / ingenuous** idea than what has already been presented at the conference, please voice it now.

11 Reading 3: Companies wrestle with growing cyber security threat: their own employees

A 🕮 Read the following article and then answer the questions.

Businesses deploy analytic tools to monitor staff as remote working increases data breach risk.

1 As cyber criminals and hackers ramp up their attacks on businesses amid coronavirus-related disruption, companies are also facing another equally grave security threat: their own employees.

2 Companies are increasingly turning to Big Brother-style surveillance tools to stop staff from leaking or stealing sensitive data, as millions work away from the watchful eyes of their bosses and waves of job cuts leave some workers disgruntled.

3 In particular, a brisk market has sprung up for cyber security groups that wield machine learning and analytics to crunch data on employees' activity and proactively flag worrying behaviours.

4 "We're seeing people say, 'I need better visibility into what my employees are doing with all of our data at home'," said Joe Payne, chief executive of cloud security group Code42, which tracks and analyses employees' activity on work devices. The group examines factors including when an employee typically works, what files they access and how much data they download.

5 "[Employers can ask] — if we have 10,000 employees, can you tell us who the most high-risk people are?" he said, adding that his company was handling a rise in cases of data theft among clients.

Insider threats

6 According to Mordor Intelligence, the $1.2bn data loss prevention market is set to balloon to $3.8bn by 2025, as many businesses migrate their data to the cloud.

7 So-called insider threats encompass employees unintentionally sharing private data outside of workplace networks, but also the deliberate stealing of data, typically motivated by financial opportunity or a grudge against an employer. Rarer, but a growing issue, is intellectual property theft and espionage on behalf of foreign governments.

8 Already more than a third of data breaches involve internal actors, according to a 2019 Verizon analysis of more than 40,000 incidents. At an exclusive meeting of top corporate cyber security heads at RSA, one of the largest cyber security conferences earlier this year, delegates labelled insider threats as their number one concern, according to one person in attendance — above nation state activity and threats from cyber criminals.

9 Traditionally, groups such as McAfee have offered tools that detect and block the exfiltration of sensitive data automatically. But there are also newer groups that seek to proactively alert employers to anomalous activity through behavioural analysis of data — which can involve screenshots and keystroke logging — and then place the onus on those employers to act in a way they see fit.

10 Falling under this category, Code42, Teramind, Behavox and InterGuard all told the Financial Times that they were seeing a rise in interest from potential clients under lockdown.

11 "There is an increase [during this pandemic] in people trying to steal intellectual property — reports or valuable HR data, client lists," said Erkin Adylov, chief executive of artificial intelligence group Behavox, which in February raised $100m from SoftBank's Vision Fund 2.

12 Its software analyses 150 data types to produce insights about employees' behaviour, including using natural language processing of email and workplace chats to assess "employee sentiment", he said. "Maybe there is uncertainty about [whether] the people are going to [keep] their job," Mr Adylov added.

13 The market is moving very fast. I would say it's probably growing at a clip of 100 per cent a year. The demand is outstripping supply," he said.

State adversaries

14 The risk of nation states opportunistically grooming employees for cyber espionage purposes is also a growing threat, several experts said. The issue was thrust into the spotlight recently when US officials last year charged two Twitter employees with mining data from the company's internal systems to send to Saudi Arabia.

15 "If I were a nation state actor [involved in cyber espionage] . . . certainly this is an opportunity to exploit some realities that exist. This is a heightened environment," said Homayun Yaqub, a senior security strategist at cyber group Forcepoint.

16 Executives at Strider Technologies, which wields proprietary data sets and human intelligence to help companies combat economic espionage, said it was seeing more recruitment of foreign spies, particularly by China, take place online under lockdown, rather

than at events and conferences. "We're providing [customers] with the capability to respond to that [changing] adversary tactic," said chief executive Greg Levesque.

17 Nevertheless, critics argue that the technology is still nascent and further investment is needed to develop a more accurate understanding of what risky patterns of behaviour look like.

18 And while employers have long been able to legally monitor emails and web activity for signs of external cyber security threats, for some there is a discomfort about the privacy and trust implications of using such tools on staff.

19 "It's intrusive, it's not very culturally palatable," said former US army intelligence sergeant and former Palantir executive Greg Barbaccia. "To me, the insider threat is a cultural human problem.

20 ." Omer Tene, vice-president of the International Association of Privacy Professionals, said: "Data breaches have been a huge issue. It's understandable why businesses would want to protect against that. I wouldn't be alarmist.

21 "But you need to be aware as a business and a technology of the creepy line," he added. " you doing anything unexpected that will trigger backlash?"

1. Why are companies particularly worried about their employees under lockdown?
2. What does the writer predict will happen to the cyber security industry?
3. How do newer data protection groups alert employers to unusual activity?
4. What kind of intellectual property are people trying to steal during the pandemic?
5. What, in particular, has increased during the pandemic?
6. What problem does Greg Barbaccia highlight?

B Find the words or phrases in the article that match the definitions below.

1. to increase the rate or level of something .....
2. telling private or secret information to journalists or to the public leaking...
3. to mention something so that people know about it to flag.....
4. a feeling of anger towards someone because they have done something to you that does not seem right or fair ...grudge.....
5. to do something in order to stop something bad from happening or a bad situation from becoming worse ...to...combat
6. beginning or formed recently ...nascent.....
7. becoming involved in something in a way that is not welcome intrusive.....
8. acceptable ...palatable....
9. a strong, negative and often angry reaction to something that has happened .backlash

11 Writing

What precautions can you take to avoid becoming a victim of internet crimes?

6 Cloze test: "What are deepfake videos?"

Complete the following extract with the missing words. The first letter is given.

Deepfake videos are a type of manipulated media that utilize artificial intelligence and machine learning techniques to create highly realistic, **1 f.**fabricated..... content. These videos can be pre-recorded or **2 g**enerated..... in real-time with a GPU and fake webcam, and typically involve the **3 s.**ubstitution..... or superimposition of one person's face onto another person's body, allowing for the creation of highly convincing fake **4 f.**~~ace~~.....footage.

Deep fake videos are created by **5 t.**raining.....deep learning models on large datasets of images and videos of the target individual whose face is to be manipulated. These models learn to **6 a.**analyse.....facial features, expressions, and movements, and then generate new video frames that **7 s.**eamlessly..... blend the target face onto the source body. The result is a video that appears authentic, with the target person convincingly **8 m.**icking mimicking .....the actions and expressions of the original source.

The advancements in deepfake technology have raised **9 c.**oncerns..... due to their potential for misuse. Deepfake videos can be used to spread misinformation, **10 d.**eceive..... viewers, manipulate public opinion, or **11 d.**efame..... individuals. They have the potential to be employed in various contexts, such as politics, entertainment, social media, and even **12 f.**raud..... attempts.

It's important to note that not all manipulated videos are deepfakes. There are other types of manipulated videos, such as cheap fakes or shallow fakes, which involve simpler **13 e**diting techniques and are typically easier to **14 d.**etect..... . Deepfakes, however, stand out for their highly realistic and **15 s**ophisticated..... nature, making them a more significant **16 c**~~o~~ombined challenge.... to identify and combat.

As deepfake technology continues to **17 e.**volve....., it becomes increasingly important for individuals, businesses, and platforms to **18 i.**mplement..... robust detection methods and tools to combat the potential risks associated with deepfake videos. **19 P**~~re~~ventive.....Proactive measures, such as advanced AI algorithms, biometric verification, and facial analysis, are crucial for detecting and **20 m.**itigating.....the harmful effects of deepfake content.

7 Reading 2: Examining how AI can alleviate loneliness and its associated risks

A Read the following article and then choose the appropriate option from the subsequent statements.

Artificial intelligence and human relationships are often portrayed by Hollywood as dangerous and rife with ethical implications. The concept of substituting a human for a robot to have as a

companion is controversial. Many would view it as a depressing symptom of isolated modern day living, and a breakdown of our communities.

Some scientists, however, suggest that there may be more nuance to this issue, claiming that it is no different from having a pet or children who own inanimate dolls. People on the brink of social isolation could use AI technology to help hone their social skills, building their confidence for real-world human interactions. The technology could also be used to prevent major depressive disorders and help stabilize patients going through a mental health crisis.

Loneliness is not just a social state, but a damning comorbidity that wreaks havoc on a person's physical and mental well-being. Some scientists estimate that for elderly isolated individuals, the damaging effects of loneliness are equivalent to smoking 15 cigarettes a day. Being lonely can often lead to a rapid deterioration into deeper depression. As self-esteem continues to plummet, it can discourage individuals from attempting to interact with others, further diminishing their chances of recovery and social engagement. AI could intervene in this downward spiral, providing companionship to help build feelings of self-worth and foster positive emotional states.

Chatbots in their current primitive state have a limited scope to address loneliness in a positive manner. While a minority of people use them, the lack of safeguards and regulation means they can become addictive. Additionally, their inability to respond in a sophisticated and personalized manner limits their widespread application. Chatbots from the last few years also struggle to understand concepts beyond basic phrases, often providing bizarre or irrelevant answers in response to natural language. Anyone who has interacted with customer service text lobbies in recent years can relate to the frustration of trying to find solutions for even the most basic issues.

Despite this, technology is rapidly improving, and soon it will be able to detect nuance, learn personalities, and understand humor on a level never seen before. It is vital that when this happens, adequate safeguards are in place if they are indeed to be used in a constructive manner to help the isolated. AI chatbots must have built-in protection to ensure they do not exacerbate unhealthy behaviors and attitudes. Users are likely to develop close bonds with such AI companions, making it extremely important that user privacy is protected and secure from outside malicious exploitation.

The concern that users will choose the instant gratification of AI interaction over a genuine human bond is valid. To prevent addiction, AI companions must not merely provide simple on-demand positive affirmations to users. Human relationships require effort and trust built up over time to create familiarity. Programs that mimic this complex process will be difficult to achieve but will undoubtedly provide a much healthier tool for isolated individuals to improve their well-being.

Applications are not limited to just lonely people. Scientists are exploring the possibility of using AI chatbots to help children with autism develop social skills. Programs with exercises that simulate eye contact and environmental noises can assist neurodivergent individuals in building social proficiency, ultimately enhancing their relationships and quality of life.

P8

Good friends are essential for maintaining health. They can be there to celebrate the good times and also help youth rough life's tougher moments. They prevent feelings of isolation and loneliness and help avert addictive behaviours such as drug use, gambling, or lack of exercise. Human beings are sociable creatures and need other people in their lives to function naturally. Without companionship, physical and mental health suffer dramatically. Using AI to help facilitate a return to sociability and to numb the pain of isolation is a novel concept that does hold some

promise. However, fully replacing a human relationship with AI remains risky, and applying this concept safely must be done with caution.

Written by Barry He / Updated: 2024-06-04

1. **What underlying social phenomenon does the passage suggest could threaten genuine human bonds in favour of AI interactions?**
   A) Urbanization leading to increased isolation
   B) The immediacy of technological solutions promoting convenience over depth
   C) Growing distrust in human capabilities
   D) Shifts in cultural values prioritizing individualism

2. **In what way does the passage characterize the effectiveness of AI companions for individuals who are lonely or socially isolated?**
   A) They are seen as a means to replace the need for real human contact.
   B) They hold potential but must evolve to avoid superficial interactions that lack emotional depth.
   C) They are primarily useful for entertainment, with limited therapeutic value.
   D) They are most effective when used in conjunction with traditional therapy methods.

3. **Which analogy used in the passage most effectively highlights the detrimental impact of loneliness on elderly individuals?**
   A) Loneliness is akin to enduring chronic pain without relief.
   B) Being alone is similar to the social disconnection experienced in virtual reality environments.
   C) The effects of loneliness mirror those of a lifestyle choice as harmful as smoking 15 cigarettes daily.
   D) Experiencing loneliness is as damaging as prolonged exposure to environmental toxins.

4. **What critical limitation of AI chatbots does the passage identify that could hinder their role in fostering genuine relationships?**
   A) Their reliance on user data leading to concerns over privacy violations.
   B) A tendency to generate responses that lack contextual understanding or emotional nuance.
   C) Insufficient accessibility for diverse populations, particularly in developing countries.
   D) An over emphasis on repetitive affirmations rather than substantive interaction.

5. **What essential precaution does the passage suggest must accompany advancements in AI technology in order to safeguard users?**
   A) Continuous market research to better tailor AI services to consumer demands.
   B) Implementing robust ethical guidelines to govern AI interactions and protect user well-being.
   C) Limiting the development of AI technology to prevent it from replacing human relationships.
   D) Encouraging widespread education on the psychological implications of AI companionship.

6. **How does the passage articulate the importance of effort in human relationships compared to interactions with AI?**
   A) Genuine connections thrive on shared experiences and mutual vulnerability, unlike AI interactions which are transactional.
   B) Relationships with AI are more efficient and less emotionally taxing than those with humans.

C) Human relationships inherently require less time investment than AI interactions.
D) Effort in human relationships is detrimental, as it can lead to dependency.

7. **What innovative application of AI technology for aiding children with autism is proposed in the passage?**
A) Utilizing AI to simulate peer interactions without external supervision.
B) Developing programs that train caregivers on how to manage autism symptoms effectively.
C) Creating interactive environments that help children practice social cues and responses in a controlled manner.
D) Using AI solely for academic support, ensuring no overlap with social skills training.

8. **What critical perspective on the use of AI companions is implied regarding their limitations in emotional support?**
A) They often perpetuate negative coping mechanisms rather than addressing underlying emotional issues.
B) The lack of human empathy in AI leads to a deeper sense of loneliness over time.
C) AI companions can effectively replace traditional forms of therapy if properly designed.
D) They are recommended only for short-term companionship, with no long-term benefits.

9. **What potential societal consequence of using AI as companions does the passage allude to?**
A) An increase in mental health issues due to reliance on technology over face-to-face interactions.
B) A broader acceptance of AI as a substitute for all forms of personal relationships.
C) A decline in the development of emotional intelligence among younger generations.
D) Enhanced feelings of fulfillment and happiness from using technology as a companion.

10. **In light of the passage, what conclusion can be drawn about the balance between AI companionship and human relationships?**
A) AI should be viewed as a superior alternative to human relationships in times of distress.
B) While AI can provide valuable support, it cannot replicate the depth and resilience of human interactions.
C) Human relationships are becoming obsolete due to technological advancements in AI.
D) AI companions can fulfill all the emotional needs previously met only by humans.

B Find in the article words that are similar in meaning to the following definitions.

1 Something that is widespread or prevalent particularly in a negative sense .....rife (§1 line 1)

2 Refine or improve something through practice or exercise .....hone (§2 line 3)

3 The simultaneous presence of two or more conditions in a person ....comorbidity (§3 line 1)

4 Prevent or avoid something undesirable .....avert (§8 line 3)

5 To lessen or dull emotional pain or distress .....numb (§9 last line)

8 Listening 2: How Chat GPT 5 Will Change The World Forever?

1. What underlying principle drives the anticipated advancements in GPT-5 according to the speaker?

A) The necessity for AI to process data at unprecedented speeds

B) The intention to replicate human emotional intelligence more accurately

C) The objective to create a fully autonomous AI that requires no human input

D) The emphasis on integrating diverse AI modalities beyond text

2. In what way does the speaker suggest GPT-5 will improve its creativity compared to previous models?

A) By utilizing a larger dataset that includes more unconventional literature

B) Through collaboration with human users during the content creation process

C) By implementing sophisticated neural networks that mimic artistic processes

D) By limiting the predefined structures that guide its outputs

3. According to the passage, what societal impact does the speaker foresee as a result of GPT-5's advancements?

A) A complete transformation of traditional educational systems

B) The cultivation of greater distrust in AI-generated content

C) A potential shift in how humans engage with technology in daily life

D) The obsolescence of human roles in creative industries

4. What type of feedback loop does the speaker describe as crucial for improving GPT-5's performance over time?

A) Regular surveys for user satisfaction after each interaction

B) Continuous model training on newly gathered conversation data

C) Mandatory monthly updates to the system's core algorithms

D) User-generated content that is submitted for analysis

5. Which factor does the speaker identify as a limitation of existing AI technologies that GPT-5 aims to overcome?

A) The inability to understand cultural references in human communication

B) The reliance on excessive computational resources for simple tasks

C) The lack of multi-modal capabilities across different media types

D) The frequent occurrence of biased outputs based on training data

6. How does the speaker envision the role of user data in shaping GPT-5's capabilities?

A) User data will serve solely to improve system security and privacy controls.

B) User preferences will dictate the types of creative outputs generated by GPT-5.

C) Data collected over time will refine the AI's predictive abilities and response accuracy.

D) Data will primarily be used to limit user interactions based on algorithmic efficiency.

7. What challenge does the speaker imply is associated with GPT-5's interaction improvements?

A) The risk of developing dependence on AI for emotional support

B) The potential for users to manipulate the AI for deceptive purposes

C) The complexity of programming creative algorithms for varied outputs

D) The difficulty in measuring the effectiveness of AI-human interaction

8. Which of the following does the speaker suggest will be a significant milestone for GPT-5 in a conversational context?

A) Achieving full autonomy in generating discussion topics

B) Demonstrating the ability to change conversational styles based on user mood

C) Competing with human experts in niche subjects without failing

D) Providing real-time translations in multiple languages seamlessly

9. What potential risk does the speaker acknowledge regarding GPT-5's contextual understanding?

A) The possibility of misinterpretations leading to harmful advice

B) The unintended spread of misinformation through unverified content

C) The challenge of bias in outputs reflecting user data

D) The complexity of maintaining privacy in contextual data use

10. What criteria does the speaker propose should guide the ethical development of GPT-5?

A) Solely focusing on enhancing user engagement regardless of risk

B) Balancing technological advancement with social responsibility

C) Maximizing profit while minimizing development costs

D) Prioritizing speed and efficiency above all other concerns

U.S.T.H.B

Computer Science Faculty

Master 2

UNIT 2

Artificial Intelligence

1 Speaking

1 How would you define Artificial Intelligence?

2 What activities are computers better at than humans now?

3 What are the various areas where AI can be used?

2 Listening: What is artificial intelligence (or machine learning)?

Listen to the audio and choose the correct option.

Part A

1.What is the primary point the speaker makes regarding Artificial intelligence?
a) AI is a dangerous technology that will soon take over the world.
b) AI is already a part of our lives, even if we don't realise it.
c) AI is a complex concept that only experts can understand.
d) AI is a technology that is still in its early stages of development.

2. What is the primary reason for the recent surge in AI development and adoption?
a) Increased government funding for AI research.
b) Greater public awareness of AI's potential.
c) The availability of vast amounts of data and improved processing power.
d) The emergence of new AI algorithms.

3. what was the main goal of the original AI research project proposed by John McCarthy?
a) To create machines that could think and act like humans.
b) To develop AI applications for practical use.
c) To understand the limits of human intelligence.
d) To explore the potential of artificial intelligence for solving complex problems.

4. How does the speaker use the analogy of an exponential curve to describe AI development?
a) To highlight the slow and steady progress of AI development.
b) To illustrate the rapid acceleration of AI development.
c) To emphasize the unpredictability of AI development.
d) To explain the limitations of AI development.

5. What is the speaker's main point in this sentence: "Very soon, AI will become a little less artificial, and a lot more intelligent."?
a) AI is becoming increasingly sophisticated and capable.
b) AI is becoming more like human intelligence.
c) AI is becoming more accessible and user-friendly.
d) AI is becoming more widely adopted in society.

Part B

6. What is the main difference between Artificial intelligence and a robot?
a) AI is much more complex than robots.

b) AI is powered by software, while robots are powered by electricity.
c) AI is software that can be embodied in many different forms, including robots.
d) AI is more intelligent than robots.

7. What is a limitation of text-based bots, like weather bots?
a) They cannot understand complex commands.
b) They can only access information from specific data sources.
c) They cannot speak in human language.
d) They are not as powerful as other types of AI.

8. How do machine learning programs learn?
a) By being programmed with specific rules.
b) By analyzing thousands of examples and adjusting their algorithms.
c) By observing and imitating human behaviour.
d) By accessing vast amounts of data.

9. What is one of the key advantages of machine learning compared to human cognition?
a) Machines can experience emotions
b) Machines do not suffer from memory loss or distractions
c) Machines can think creatively
d) Machines require sleep to function

10. What is the most pressing concern about Artificial intelligence?
a) The potential for AI to become too powerful.
b) The possibility of AI being used for malicious purposes.
c) The impact of AI on the job market.
d) The ethical implications of AI development.

3 Reading 1: "Everything to know about Artificial Intelligence"

📖 A Read the following article and answer the questions below.

Hear the term artificial intelligence (AI) and you might think of self-driving cars, robots, ChatGPT or other AI chatbots, and artificially created images. But it's also important to look behind the outputs of AI and understand how the technology works and its impacts for this and future generations.

AI is a concept that has been around, formally, since the 1950s, when it was defined as a machine's ability to perform a task that would've previously required human intelligence. This is quite a broad definition and one that has been modified over decades of research and technological advancements.

When you consider assigning intelligence to a machine, such as a computer, it makes sense to start by defining the term 'intelligence' -- especially when you want to determine if an artificial system is truly deserving of it.

Our level of intelligence sets us apart from other living beings and is essential to the human experience. Some experts define intelligence as the ability to adapt, solve problems, plan, improvise in new situations, and learn new things.

With intelligence sometimes seen as the foundation for human experience, it's perhaps no surprise that we'd try and recreate it artificially in scientific endeavors. And today's AI systems might demonstrate some traits of human intelligence, including learning, problem-solving, perception, and even a limited spectrum of creativity and social intelligence.

AI comes in different forms that have become widely available in everyday life. The smart speakers on your mantle with Alexa or Google voice assistant built-in are two great examples of AI. Other good examples are popular AI chatbots, such as ChatGPT, the new Bing Chat, and Google Bard. When you ask ChatGPT for the capital of a country or you ask Alexa to give you an update on the weather, you'll get responses that are the result of machine-learning algorithms.
Though these systems aren't a replacement for human intelligence or social interaction, they have the ability to use their training to adapt and learn new skills for tasks that they weren't explicitly programmed to perform.

Artificial intelligence can be divided into three widely accepted subcategories: narrow AI, general AI, and super AI.
Artificial narrow intelligence (ANI) is crucial to voice assistants, such as Siri, Alexa, and Google Assistant. This category includes intelligent systems that have been designed or trained to carry out specific tasks or solve particular problems, without being explicitly designed to do so. ANI might often be referred to as weak AI, as it doesn't possess general intelligence, but some examples of the power of narrow AI include the above voice assistants, and also image-recognition systems, technologies that respond to simple customer service requests, and tools that flag inappropriate content online. ChatGPT is an example of ANI, as it is programmed to perform a specific task, which is to generate text responses to the prompts it is given.

Artificial general intelligence (AGI), also known as strong AI, is still a hypothetical concept as it involves a machine understanding and performing vastly different tasks based on its accumulated experience. This type of intelligence is more on the level of human intellect, as AGI systems would be able to reason and think like a human. Like a human, AGI would potentially be able to understand any intellectual task, think abstractly, learn from its experiences, and use that knowledge to solve new problems. Essentially, we're talking about a system or machine capable of common sense, which is currently not achievable with any form of available AI. Developing a system with its own consciousness is still, presumably, a fair way in the distance, but it is the ultimate goal in AI research.

Artificial super intelligence (ASI) is a system that wouldn't only rock humankind to its core, but could also destroy it. If that sounds straight out of a science fiction novel, it's because it kind of is: ASI is a system where the intelligence of a machine surpasses all forms of human intelligence, in all aspects, and outperforms humans in every function.
An intelligent system that can learn and continuously improve itself is still a hypothetical concept. However, it's a system that, if applied effectively and ethically, could lead to extraordinary progress and achievements in medicine, technology, and more.

Overall, the most notable advancements in AI are the development and release of GPT 4. But there have been many other revolutionary achievements in artificial intelligence.

Adapted from: https://www.linkedin.com/pulse/what-artificial-intelligence-you-hear-term-ai-might-think-sns-njpfc

1 How has the definition of artificial intelligence (AI) evolved since its introduction in the 1950's?

2 Why is intelligence considered a foundational element of the human experience ?

3 What aspects of human intelligence might contemporary AI systems demonstrate?

4 How do machine-learning algorithms enable systems like ChatGPT and voice assistants to provide responses?

5 In which way artificial general intelligence is different from artificial narrow intelligence?

6 Why is developing a system with its own consciousness considered a distant goal in AI?

7 What factors distinguish super artificial intelligence from other forms of AI?

8 What are the potential implications of artificial intelligence?

B Find in the article words that are similar in meaning to the following definitions

1 a serious and determined effort or attempt to achieve a specific goal ...endeavors.....

2 a range of different but related qualities or activities .....spectrum.....

3 to mark or indicate something for attention or consideration .....Highlight....Flag

4 Language in use: Revising comparative form

Complete the following passage by filling in the blanks with the appropriate comparative form of the adjectives provided in brackets.

Artificial Intelligence (AI) is evolving rapidly and some researchers argue that it is changing our lives **1**(quick).....quicker..... we could have ever imagined. In recent years, machines have become **2** (intelligent).more.....intelligent.... they were before and their ability to learn and adapt has improved much **3** (good).....better..... over time. While AI is helping individuals and businesses alike, it is also causing some concerns. For instance, AI systems can make decisions **4** (thoughtlessly) more.....thoughtlessly..human beings, pushing the ethical boundaries even **5** (far).....further..... . AI systems can sometimes be **6**(fair)....fairer.....humans when making decisions. This can lead to outcomes that are not just or equitable. While some find AI to be a **7**(helpful).....more.....helpful assistant in their tasks, others argue that it can be **8** (risky)....riskier..... due to potential biases ingrained in algorithms. Moreover, some people believe that AI is working **9** (smart).....smarter.... in tasks that require immense computation, ultimately leading to outcomes that are **10** (satisfactory).. .....more.....satisfactory

Furthermore, the advancements in AI technology demonstrate how it is often adapted **11** (easy)....easier .....into various sectors. Industries such as healthcare and finance have integrated AI systems **12**(seamlessly).....more.....seamless..... traditional methods would allow. In these cases, AI processes data **13**(quickly).more..quickly. and with **14** (accuracy) .....more.....accuracy....., showcasing its capacity to enhance decision-making. However, it is crucial for us to remember that AI is not without its flaws. It can analyze information far **15** (efficiently).....more.....efficiently..... humans, but it still lacks empathy and understanding that comes naturally to people. As AI continues to develop, it is vital to approach its potential with caution. It is essential to ensure that the implementation of AI systems is done responsibly and **16** (thoughtfully)....more..... . Only then can we harness the full potential of artificial intelligence for a **17** (fulfilling)....more..... future.

Aya

5 Language in use 2: Double Comparative

A Defining Double Comparative

Double comparatives are phrases commonly used in English to express increasing or decreasing returns. Double comparatives are often employed to underline the importance of doing or not doing a certain activity. Here are some examples of double comparatives:

- *The more you study, the more you learn.*
- *The less furniture I buy, the less space I need.*

B Using Double Comparatives

1 As you can see from the above examples, the format of double comparatives is as follows:
The (more / less) + (noun / noun phrase) subject + verb , the (more / less) + (noun) subject + verb

2 Double comparatives with 'more' and 'less' can be used with adjectives in the same way. In this case, the structure places the comparative adjective first:
The + comparative adjective + (noun) + subject + verb , the + comparative adjective + it is + infinitive

- *The easier the test is, the longer students will wait to prepare.*
- *The more difficult the task is, the sweeter it is to succeed.*

3 These forms can be mixed up as well. For example, a double comparative might begin with a more / less plus a subject and then end in a comparative adjective plus the subject.

- *The less you think about the problem, the more relaxed you feel.*
- *The more the students study for the test, the higher their scores will be.*

4 You can also reverse the above by beginning with a comparative adjective and ending with more / less plus a subject and verb or noun, subject and verb.

- *The richer the person is, the more privilege he enjoys.*
- *The older you are, the more experience you have.*

5 We can use comparative adverbs in the same way as adjectives. The structure is as follows:
The comparative + subject + verb , the comparative + subject + verb

- *The harder you study English, the more confidently you speak.*
- *The less carefully you plan, the worse the results will be.*

6 Double comparatives are often shortened in spoken English, especially in expressions ending in "**better**".

- *What sort of presentation should I prepare? The shorter, the better!*
- *What kind of laptop were you looking for? – I don't really care, the cheaper, the better.*

Use the following sentence segments to create double comparatives.

1 clicks/a lot of/ story/a /gets, money/make/revenue/through/a lot of/online publishers/advertising.
The more clicks a story gets, the more money online publishers make through advertising.
2 becomes/ intelligence/ advanced/ artificial, human/ takes/ a lot of/ it/ jobs/ over.
The more advanced artificial intelligence becomes, the more it takes over human jobs.
3 effort/ you/exhibit/ your/ remarkable/ studies/ in, will/ results/ obtain/ rapidly/ you.
The more effort you exhibit in your studies, the more remarkable results you will rapidly obtain.
4 materials/ from/a great deal/learn/ educational / you, from /help/ you/ little / others/ need.
The more educational materials u learn from, the less help u need from others.
5 something/ hurriedly/ done/ is, made /easily/are/ mistakes.
The more hurriedly something is done, the more easily mistakes made.
6 vocabulary/ learn / I/ try/ hard/ to, words/ unlikely/ / confused / I/ a lot/ remember/ the/ get/ / am/ / to/ I/ and.
The harder I try to learn vocabulary, the more confused I get words I remember and the less likely I am to get remember the words
7 take/ time/ a lot of/ you, the/ turn/ good/ in/ assignment/ you.
the more time u take, the better assignment u turn in.

exhibit = Expression

the more Unlikely = the less likely

8 possibilities/ there/ and/ a lot of/ opportunities/ are, to/ number/ systems/ attacks/ are/ a great/ subject/ of/ the.
The more possibilities and opportunities there are, the greater the number of the attacks.
9 from/ materials/ learn/ deal/ you/ educational/ a great, help/ others/ you/ from/ need/ little. systems are subject to.

10 data/ the/ receives/ a lot of/ computer, accurate/ its/ can/ predictions/ it/ very/ in/ be.
The more data a computer receives the more accurate its predictions can be.

6 Idioms

Read the following story. Underline all the idioms and expressions that you can find.

Keys to Success

John is an accomplished, successful businessman who is quite popular as a mentor. He enjoys showing young professionals the ropes. The first thing he says is that his career has not always been smooth sailing. In fact, he learned a number of lessons along the way. "First and foremost," John said, "don't believe that success is ever manna from heaven." He has met many people with similar rags-to-riches stories and learned that a lot of hard work went into their success.

John believes in hard work but also in recognizing the right opportunities:

"It's absolutely essential to never spread yourself too thin. If you have too many irons in the fire, you'll certainly miss out on real opportunity. I've seen people as busy as a bee who never really seem to do anything."

You'll probably agree that it's impossible to really concentrate if you have to worry about 50 different things. Another good lesson is that it's important to know which side your bread is buttered on and to give that activity your full attention. In other words, you need to ride the gravy train. Don't start looking for new challenges if everything is working out for the best.

The most important ability of any successful entrepreneur, John stressed, is to have the presence of mind not to simply take advantage of an opportunity but also to keep your eye on the ball. Some people are quick on the uptake, but then they get bored. It's important to be consistent and not spread yourself too thin. Finally, make sure never to show your hand to your opponents.

That's how to be successful, according to John.

1 Going from poor to rich ...rags...to...riches...
2 Be aware and be able to grasp an opportunity ...Presence...of...mind...
3 Understand very quickly ...quick...on...the...uptake...
4 An easy life with no problems ~~Concentrate on what's important~~ ...smooth...sailing...
5 Make money by doing something that has already proved to be successful ...ride...the gravy train
6 End with the best possible result ...work...out...for...the...best...
7 Show others the advantages you have in a situation ...show...your...hand...
8 Explain and show by example how something is done properly...show...someone...the ropes
9 Doing too many things at once ...spread...yourself...too...thin...
10 Understand what is most important to you ...know...which...side...your...bread is buttered
11 Doing too many things at the same time...have too many irons in the fire...
12 Very busy (also as busy as a beaver)...as...busy...as...a...bee...
13 Concentrate on what's important ...keep...your...eyes...on...the...ball...

BChoose the correct compound words in the following phrases.

1. a room for stores **a storeroom / a storesroom**
2. a tape for measuring up to 300 cms**a 300-cm tape measure /a 300-cm measure tape**
3. size of cables **cables size / cable size**
4. reduction in cost**reduction cost / cost reduction**
5. two periods of three months**two three-month periods /three two-month periods**
6. plugs with 3 pins **three-pin plugs / three-plug pins**
7. two steel boxes for tools**two steel-tool boxes / two steel toolboxes**
8. the assistant manager of the office **the assistant manager office**
the assistant office manager

CUsing the words in the box, form compound adjectives and then complete the following sentences.

driven	battery	oriented	free	powered	alone	menu
activated	Space	object	hands	stand	voice	saving

1 .....programming is based on objects and their effects on eachother, rather than on a series of instructions.

2 ..... PCs take up little desktop space.

3 A ..... program lets you select a command from a menu.

4 A ..... computer or business can operate on its own.

5 A ..... device doesn't require the hands for operation.

6 A ..... product is activated by the user's voice.

7 A ..... computer is a computer that runs on batteries.

D Replace the underlined parts of the following sentences with compound words.

0Users typically access social media services via technologies **(1)**that are relating the webon desktop computers or laptops, or download services that offer social media functionality to their devices **(2)**that are made for portability. When engaging with these services, users can create platforms **(3)**that allow Interaction to a high degree through which individuals, communities and organizations can share, co-create, discus and modify content **(4)**which is created by usersor **(5)**created in advance and posted online

5 CLOZE TEST

Complete the following passage about "Navigating Social Media in the Pandemic" with the missing words. The first letter is given.

The need for increased **(1)**c..... was clear at the start of the pandemic. Screenshots of Zoom parties and new challenges, like # see10 do10 pushup challenge, made it obvious that users wanted to stay **(2)** e..... as they coped with a new, shared reality. However, more than three years later, pandemic-related challenges have slowed down, and social media **(3)**f..... are swinging back to many of the same old pitfalls that have made them difficult for mental health for years, such as **(4)**m..... and heavily edited photos.

These unrealistic representations have an **(5)**i..... on users, especially those who are turning to social media more frequently. People **(6)** d..... with social anxiety, for example, are already **(7)** p..... experiencing the negative consequences of social media.

Originally, it was thought that people with social anxiety might **(8)**b ..... from social media use since it could serve as a stepping stone for social **(9)**i.....,. . In many cases, however, the **(10)**p..... of gaining more 'likes' or more 'friends,' has had the opposite effect. Instead of making people who feel socially **(11)** a..... more connected, it forces them to realisehow disconnected they are.

3 Language work: Revising compound words

A Find the missing words to form compounds in the following sentences.

1 Password..protected...sites are accessible only to users entering the correct password.

2 Cloud...-based.....services or resources made available to users on- demand via the internet from a cloud.

3 Cyber.....threats.....refers to malicious attempts to gain access to a computer network.

4 Human..powered.....search engines rely on human intervention to submit information.

5 Data...warehouse...is a large store of data accumulated from a wide range of sources used to guide management decisions.

B Read the following sentences, and then form compounds that refer to them.

1. A website which is designed in a good way. .....well-designed...website....independent
2. A software designed to work across multiple platforms. .....cross-platform...software
3. An operation which doesn't require hands. .....a..hands-free...operation.....
4. A computer which runs on batteries. .....a.....battery-powered.....computer.....
5. A hard drive which integrates two different technologies. .....a...hybrid...hard...drive.
6. A special file which redirects to another file or program. .....a...shortcut...file.....
7. A peripheral device which reads and writes flash memory. .....A flash...memory...reads
8. A file which can be retrieved and displayed, but not changed or deleted. .....read...only file
9. A content created by users of a service. .....User...generated...content.....
10. Strategies against malware. ...Anti-malware.....

4 Idioms

Read the following passage. Underline all the idioms and expressions that you can find.

Young and Free: Prerequisite for Success

Let's face it: In today's business world you need to be young and free of attachments to strike it rich. It's a dog eat dog world out there and you're going to have to work quite a lot. Of course, not only will you have to work quite a lot, you'll need to be flexible and ready to take advantage of anything. That's where the "free" part comes in.

I've got a young friend, he's only 25, but he fits the bill perfectly. He's single and he's hungry. He's willing to start from scratch and, best of all, he isn't afraid of putting his nose to the grindstone for those 80 hour weeks. He decided to take the bull by the horns by going starting up his own business. He found a software developer who knew the internet inside out. This young man was also very ambitious. He left his safe job at the drop of a hat. They were both reaching for pie in the sky, and they were ready.

They also were lucky. They founded a startup and got into the whole social networking business in 2018. In other words, they were early birds and they were willing to sink or swim. Probably the most important ingredient in their success was that they were willing to play things by ear. They kept their ears to the ground, moved full steam ahead and drove hard

bargains. Soon, their business was growing by leaps and bounds. Of course, they had some stumbling blocks along the way. Who doesn't? Still, they got the jump on the competition and by the year 2023, they were multi-millionaires. This sort of success for the young and free now has copycats around the world.

Now write one of the idiomatic expressions next to its definition below.

1 immediately =.....in.....a.....drop.....of.....a.....hat.....
2 very quickly (used with improvement) =.....by.....leaps.....and.....bounds.....
3 someone or a company who tries to do things like another person or company=.....a.....copycat
4 very competitive = ...dog.....eat.....dog.....
5 to make a business deal that is very advantageous for you =.....drive.....hard.....bargains
6 someone who takes early advantage of a situation =.....early.....birds.....
7 to have the right characteristics for something =.....fit.....to.....the.....bill.....
8 to continue with full commitment =.....full.....steam.....ahead.....
9 to get the advantage over someone by starting early =.....get.....the.....jump.....on.....someone
10 to pay attention to rumours, news, and industry insiders =.....keep.....their.....ears.....to.....the.....ground
11 to have expert knowledge about something =.....inside.....out.....
12 something very hard to achieve, a dream =.....pie.....in.....the.....sky.....

5 Internet crimes

Choose the right answer to identify the following internet crimes.

1 Which of the following refers to the forging of the return address on an email so that the email message appears to come from someone other than the actual sender.

a Spamming (b) Spoofing c Spooling d None of these

2 Which of the following is a fraudulent practice in which someone tries to trick you into giving them your private information via text message.

a Encrypting b Vishing (c) Smishing d Pretexting

3 In which type of malicious act, a hacker contacts you by phone or email and attempts to acquire your password.

a Defacing (b) Phishing c Bugging d None of these

4 Which of the following refers to any fraudulent business or scheme that take money or other goods from an unsuspecting person.

a Hacking b Spamming (c) Scamming d Pharming

5 Which of the following involves the repeated use of the Internet or other electronic means to harass, intimidate or frighten a person or group.

a Cyberbullying b Cyberslaking c Cyberstalking (d) Both a and c

6 Which of the following is a type of malware that is programmed to hide on a target computer or server and send back information to the master server, including login and password information, bank account information, and credit card numbers

a Spooling b Ransomware (c) Spyware d None of these

7 Which of the following is the art of manipulating people into giving up confidential information, usually through technology. It aims to take advantage of a potential victim's natural tendencies and emotional reactions.

a Pharming b Adware c Malvertising (d) None of these