**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**

**“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”**

**Методичні вказівки з англійської мови**

**для самостійної роботи студентів 2 року навчання спеціальності**

**Кібербезпека**

**Cybersecurity: Methodological instructions in the English language**

**for 2nd year students’ self-study**

 Затверджено редакційно-видавничою

 радою університету,

 протокол № 2 від 28.06.2023 р.

Харків

НТУ “ХПІ”

2023

Методичні вказівки з англійської мови для самостійної роботи студентів 2 року навчання спеціальності Кібербезпека = Cybersecurity: Methodological instructions in the English language for 2nd year students’ self-study / уклад. Т.Є.Гончаренко, В.В. Гращенкова, А.В. Саламатіна, М.Є.Тихонова. Харків: НТУ „ХПІ”, 2023. 40 c.

Укладачі: Т.Є. Гончаренко

В.В. Гращенкова

А.В. Саламатіна

М.Є. Тихонова

Рецензент: О.Я. Лазарева

 Кафедра іноземних мов

**ВСТУП**

Методичні вказівки з англійської мови призначені для самостійного опрацювання студентами матеріалів пов’язаних з професійною діяльністю у сфері Кібербезпеки та відповідають вимогам, що висуваються програмою мовної підготовки для студентів технічних ВНЗ.

Основна мета методичних вказівок - надання специфічних професійно-орієнтованих матеріалів для вивчення, опрацювання та закріплення граматичних та лексичних тем, що призначені для оволодіння спеціалізованою лексикою, розвитку навичок читання та професійної комунікації англійською мовою.

Методичні вказівки складаються з 12 автентичних текстів та 2 відеоматеріалів, тематика яких пов’язана з новими тенденціями розвитку кібербезпеки, типами атак на інформаційні системи, розробкою, реалізацією, впровадженням та управлінням комплексними програмно-технічними системами захисту інформації на підприємствах та створенням комп'ютерних систем, що впливають на безпеку транспортних, енергетичних, медичних та інших комплексів. Робота з текстами сприятиме розвитку навичок переглядового читання, яке націлює студентів на швидкий пошук основної тематичної лінії тексту та формулювання його основної ідеї; ознайомчого виду читання, що передбачає вдосконалення вміння студента знаходити й розуміти основну інформацію тексту, вміння відокремити головне від другорядного та дослідницького читання, призначеного для вироблення вмінь і навичок отримувати повну інформацію з тексту, аналізувати викладені в ньому факти, порівнювати їх, узагальнювати і робити власні висновки.

Методичні вказівки містять завдання у вигляді лексичних та граматичних вправ, що сприятимуть розширенню активного словникового запасу за фахом, формуванню навичок говоріння, розвитку монологічного мовлення, ведення дискусій на професійні теми. При підборі матеріалу використовувалась автентична література, оригінальні науково-популярні тексти, а також сучасні Iнтернет ресурси та відеоматеріали.



**Warm up**

**SPEAKING**

* **1.1 Read the text given below. What trends in the development of cyber security are currently the most necessary? Give your reasons.**
* **1.2 What are the advantages and disadvantages of using smart medical devices.**

**READING**

**Text 1. Cybersecurity Threats and Trends for 2023**

**Phishing Gets More Sophisticated —**[Phishing attacks](https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/), in which carefully targeted digital messages are transmitted to fool people into clicking on a link that can then install malware or expose sensitive data, are becoming more sophisticated.

Now that employees at most organizations are more aware of the dangers of email phishing or of clicking on suspicious-looking links, hackers are upping the ante — for example, using machine learning to much more quickly craft and distribute convincing fake messages in the hopes that recipients will unwittingly compromise their organization’s networks and systems. Such attacks enable hackers to steal user logins, credit card credentials and other types of personal financial information, as well as gain access to private databases.

**Ransomware Strategies Evolve —**[Ransomware attacks](https://www.webroot.com/blog/2019/02/28/the-ransomware-threat-isnt-over-its-evolving/) are believed to cost victims billions of dollars every year, as hackers deploy technologies that enable them to literally kidnap an individual or organization’s databases and hold all of the information for ransom. The rise of cryptocurrencies like Bitcoin is credited with helping to fuel ransomware attacks by allowing ransom demands to be paid anonymously.

As companies continue to focus on building stronger defenses to guard against ransomware breaches, some experts believe hackers will increasingly target other potentially profitable ransomware victims such as high-net-worth individuals.

**Cryptojacking —** The cryptocurrency movement also affects cybersecurity in other ways. For example, [cryptojacking](https://hackernoon.com/cryptojacking-in-2019-is-not-dead-its-evolving-984b97346d16%22%20%5Ct%20%22_blank) is a trend that involves cyber criminals hijacking third-party home or work computers to “mine” for cryptocurrency. Because mining for cryptocurrency (like Bitcoin, for example) requires immense amounts of computer processing power, hackers can make money by secretly piggybacking on someone else’s systems. For businesses, cryptojacked systems can cause serious performance issues and costly down time as IT works to track down and resolve the issue.

**Cyber-Physical Attacks —** The same technology that has enabled us to modernize and computerize critical infrastructure also brings risk. The ongoing threat of hacks targeting electrical grids, transportation systems, water treatment facilities, etc., represent a major vulnerability going forward. According to a recent report in The New York Times, even [America’s multibillion-dollar military systems are at risk](https://www.nytimes.com/2018/10/10/us/politics/hackers-pentagon-weapons-systems.html) of high-tech foul play.

**State-Sponsored Attacks**

State-sponsored attacks (SSA) are carried out by cyber criminals directly linked to a nation-state. Their goals are threefold:

* Identify and exploit national infrastructure vulnerabilities.
* Gather intelligence.
* Exploit systems and people for money.

Cybercrime today is a major threat not just for the private sector and for individuals but for the government and the nation as a whole. As we move into 2023, state-sponsored attacks are expected to increase, with attacks on critical infrastructure of particular concern.

**IoT** **Attacks —**The Internet of Things is becoming more ubiquitous by the day (according to [Statista.com](https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/), the number of devices connected to the IoT is expected to reach 75 billion by 2025). It includes laptops and tablets, of course, but also routers, webcams, household appliances, smart watches, medical devices, manufacturing equipment, automobiles and even home security systems.

Connected devices are handy for consumers and many companies now use them to save money by gathering immense amounts of insightful data and streamlining businesses processes. However, more connected devices mean greater risk, making IoT networks more vulnerable to cyber invasions and infections. Once controlled by hackers, IoT devices can be used to create havoc, overload networks or lock down essential equipment for financial gain.

IoT security threats and risks are represented by the following:

- Botnets

- Ransomware

- Convergence

- Invisibility

- Unencrypted Data

- Rogue Devices.

**Smart Medical Devices and Electronic Medical Records (EMRs) —**The health care industry is still going through a major evolution as most patient medical records have now moved online, and medical professionals realize the benefits of advancements in smart medical devices. However, as the health care industry adapts to the digital age, there are a number of concerns around privacy, safety and cybersecurity threats.

According to the Software Engineering Institute of Carnegie Mellon University, “As more devices are connected to hospital and clinic networks, patient data and information will be increasingly vulnerable. Even more concerning is the risk of remote compromise of a device directly connected to a patient. An attacker could theoretically increase or decrease dosages, send electrical signals to a patient or disable vital sign monitoring.”

With hospitals and medical facilities still adapting to the digitalization of patient medical records, hackers are exploiting the many vulnerabilities in their security defenses. And now that patient medical records are almost entirely online, they are a prime target for hackers due to the sensitive information they contain.

**Clickjacking**

Clickjacking attacks typically feature a webpage that has a button inviting you to click it to win something, such as a free vacation. When you click the button, you’re actually clicking on a hidden button contained in an invisible layer beneath or above the button you can see. The invisible button performs a malicious function, such as downloading malware to your computer.

**Social Engineering** **—** Hackers are continually becoming more and more sophisticated not only in their use of technology, but also psychology. Tripwire describes [social engineers](https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/) as “hackers who exploit the one weakness that is found in each and every organization: human psychology. Using a variety of media, including phone calls and social media, these attackers trick people into offering them access to sensitive information.”

**1.3 According to the text decide if the statements below are *TRUE* or *FALSE***. **Write**

|  |  |
| --- | --- |
| ***TRUE*** | *if the statement agrees with the information* |
| ***FALSE*** | *if the statement contradicts the information* |

1. Cyber attacks target computer systems, accessing sensitive data from a targeted computer and then usually either disabling or extracting it.
2. Fake messages are crafted and distributed by using machine learning.
3. [Ransomware attacks](https://www.webroot.com/blog/2019/02/28/the-ransomware-threat-isnt-over-its-evolving/) steal credit card credentials.
4. Organizations and individuals can become ransomware victims.
5. Private computers can be used to “mine” for cryptocurrency.

** 1.4** **Match the following terms with their proper definitions. Find these words in the text. Which of them weren’t mentioned in the text above.**

|  |  |
| --- | --- |
| **1.** Ransomware | **a.** is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online. |
| **2.** A backdoor | **b.** is a type of malware from crypto virology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off. |
| **3.** Phishing | **c.** is a form of social engineering where attackers deceive people into revealing sensitive information or installing malware such as ransomware. |
| **4.** A cyber-physical attack | **d.** is an online threat that hides on a computer or mobile device and uses the machine’s resources to “mine” forms of online currency known as cryptocurrencies. |
| **5.** Cryptojacking | **e.** refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access on a computer system, network, or software application. |
| **6.** Social engineering | **f.** is a security breach that impacts operations and damages property. |
| **7.** Clickjacking | **g.** unlike most other forms of cyberattacks, involves human interaction. This attack is a form of con artistry that plays on people’s helpful or curious nature to get them to hand over personal information. |

 **Task 1.5 Sсan the recommendations given below and determine what type of cyberattack** **is meant in the text.**

**How to prepare for the possibility of a highly sophisticated, targeted, and well-funded attack:**

Firstly, the fundamentals should be in place, including antivirus, patch management, encryption, backup, disaster recovery plan, and more.

Secondly, organizations should embed security awareness in the company culture by performing regular phishing assessments and social engineering training: the fewer human vulnerabilities, the fewer entry points into your systems.

Third, organizations should isolate critical IT systems and sensitive data stores from the internet and the general intranet. This added layer of security makes it considerably more difficult for attackers to steal information or disrupt operations.

Fourth, evaluate your technology supply chain for current hardware and software vulnerabilities. Conducting an audit will provide insight into potential backdoors for malicious actors. It isn’t paranoia; it’s risk management.

Fifth, stay active in the community to learn about relevant threats. Likewise, share what you know and help build a more robust culture of industry awareness.

**Grammar**

|  |
| --- |
| **PASSIVE VOICE** |
| **Remember!** The sentence having **intransitive** verbs cannot be changed into passive voice. |
| **Remember!** Exceptions:1. Use preposition “**with**” instead of “**by**”

For the sentences with “**pleased, impressed, charmed, disgusted** etc.” as the main verbs.1. Use preposition “**to**” instead of “**by**”

For the sentences with “**known, married, obliged**” as the main verbs.1. Use preposition “**at**” instead of “**by**”

For the sentences with “**surprised, shocked, disappointed, annoyed, laughed, alarmed, displeased, distressed, astonished**” as main verb.1. Use preposition “**in”** instead of “**by”**

For the sentences with “**interested, consisted, absorbed, contained**, etc.”as the main verbs.1. Use of ‘**when’**

For the sentences with “**feel, smell, taste**, etc.” as the main verbs. |

* **Task 1.6 Write out from Text 1. Cybersecurity Threats and Trends for 2023 all the verbs in the passive voice.**
* **Task 1.7 Make up make passive sentences using prepositional constructions from the table above.**
* **Task 1.8 Change these sentences into the passive voice where it’s possible.**

1. I understand the difficulty of your situation, but people should share with others what they feel in such situations.

2. We frequently encounter such situations in our school and take some precautions to ensure discipline.

 3. Our work was really successful, but we could not prevent a small error at the end of the work. It was very sad for everyone to experience this situation.

4. If you think there is any problem with this issue, you can contact me. If you can use communication tools such as e-mail, telephone or fax for this, I can provide you with faster feedback.

5. The information we share about our daily life on the Internet often violates the privacy of personal life. In short, it makes us naked on the Internet.

**READING**

**Text 2. Common Types of** **Cyber-Physical Attacks**

**2.1 Skim the article, decide which type of cyber-physical attack is described, fill in the gaps and title each part of the text.**

**a. Side-Channel Attacks**

**b. Zero-day attacks**

**c. Eavesdropping attacks**

**d. Replay attacks**

**e. Data Injection attacks**

**f. Denial of Service attacks**

The most common types of cyber-physical attacks can be summarized as follows:

**1.** … attacks target a security vulnerability that has not yet been disclosed publicly. Since such a vulnerability has not been disclosed publicly, there’s a high probability that knowledge thereof is merely possessed by a specific few individuals who have somehow managed to find such a vulnerability.

The implications of such an attack on an industrial scale could be disastrous, particularly if it involves a production line being compromised with malicious software that is powerful enough to resist the installation of any security patch that would disable it.

**2.** Attackers can illegally gain access to confidential and sensitive information by launching an eavesdropping attack on communication channels used by individuals or institutions to share such critical information.

When information that contains sensitive content relating to how a certain system or production process operates is shared on an insecure communication channel, it presents an opportunity for an attacker to eavesdrop on such information and plan a devastating attack on the system.

**3**. … attacks aim to bring down the systems by denying them access to any form of computational resources so that the process controlled by the targeted system falls under the control of the attacker. For example, the communication between an industrial server and other lower-level industrial control systems can be disrupted by a DoS attack that can deny these systems access to the server network.

**4**. False … inject harmful code and commands into control systems networks that are not fortified with efficient authentication mechanisms. Such attacks can range from commanding industrial control systems to performing actions that are outside of safe operating margins, to completely reconfiguring the control systems’ equipment to perform differently from the way they are meant to function.

**5**. Even though authentication mechanisms can help prevent harmful commands from being executed by targeted equipment, an authenticated data packet modified with malicious instructions can be retransmitted. This can prove quite dangerous because such an altered data packet appears to be from a legitimate origin. Electronic equipment that such packets are transmitted have no clue that this is actually malicious content in the disguise of a legitimate data packet.

**6**. … attacks are characterized by the illegal collection of data through information leakage in industrial equipment. For example, attackers can obtain sensitive information on the working of a system by fluctuations tracing the variations in the power usage while processing data. In-depth monitoring of industrial manufacturing equipment during the production process can give away critical information that can help create an almost precise reproduction of the product produced by the compromised machine.

The threat of cyber-physical attacks is real and had often resulted in the loss of millions of dollars. A more worrisome fact is that attacks on cyber-physical systems may even lead to loss of human life (for example, an attack on a nuclear power plant system). Understanding the threat landscape and implementing stringent security measures is imperative for industries where CPS is used extensively.

**LISTENING**

**Video 1. “Cyberattacks increase during Holidays. How to protect yourself and your business.”**

* **1. Watch the video** **“Cyberattacks increase during Holidays. How to protect yourself and your business.”**
* **2. Answer the following questions.**

<https://www.youtube.com/watch?v=Cn5qAIQlOOY>



1. Why do users click on malicious links more often during winter holidays?

2. What kind of information are these hackers looking for?

3. What pieces of advice were given by a presenter in order to avoid a cyber attack?

4. Why are the holidays so appealing for the cyber criminals?

5. How many people had taken alcohol before they had to handle a cyber attack during holidays according to a study conducted by a cyber security company?

6. What common techniques are used by hackers during winter holidays?

7. Which companies are the primary targets of cyberattacks?

8. What can organizations do in order to stay protected?

**Warm up**

**SPEAKING**

* 1. How can the human factor increase the cybersecurity risk?
	2. Can conducting security training for employees outside of the IT department affect the security of the company?

**READING**

**Check your answers and read the text about “Types of Cybersecurity”**

**Text 3. Types of Cybersecurity**

Cybersecurity can be categorized into five distinct types:

* Critical infrastructure security
* Application security
* Network security
* Cloud security
* Internet of Things (IoT) security

To cover all of its bases, an organization should develop a comprehensive plan that includes not only these five types of cybersecurity, but also the three components that play active roles in a cybersecurity posture: people, processes and technology.

* 1. **People**

Let’s face it, no matter what precautions you put into place, if people don’t follow the rules, you’re still at risk. The saying “you’re only as strong as your weakest link” comes to mind. In most cases, human error is just that – a mistake.

Most people aren’t intentionally bypassing security protocol – they either aren’t trained to do so, or they aren’t educated about the significance of their actions. Conducting security awareness training and reinforcing the most basic cybersecurity principles with employees outside of the IT department can make a big difference in company’s security posture.

Here are five ways the human factor can increase your cybersecurity risk:

1. **Suspicious URLs and Emails:** Explain to employees that if something looks strange – it probably is! Encourage staff to [pay attention to URLS](https://www.comptia.org/blog/security-awareness-training-how-to-detect-phishing-attacks), [delete emails](https://www.comptia.org/blog/security-awareness-training-what-does-a-phishing-email-look-like) that don’t have content or look like they are coming from a spoofed address, and stress the importance of guarding personal information. As the IT professional, it’s your responsibility to raise awareness of potential cybersecurity threats.
2. **Password Idleness:** We know that holding on to the same password for ages isn’t a great idea. But, Bob in finance may not understand that. Educate employees [about the importance of frequently changing passwords](https://www.comptia.org/blog/security-awareness-training-passwords) and using strong combinations. We all carry a plethora of passwords and since it’s a best practice not to duplicate your passwords, it’s understandable that some of us need to write them down somewhere. Provide suggestions on where to store passwords.
3. **Personally Identifiable Information:** Most employees should understand the need to keep personal browsing, like shopping and banking tasks, to their own devices. But everybody does a bit of browsing for work, right? Emphasize the importance of keeping an eye on what websites may lead to others. And, that includes social media. Karen in customer service may not realize that sharing too much on Facebook, Twitter, Instagram, etc. (like personally identifiable information) is just one way hackers can gather intel.
4. **Backups and Updates:** It’s fairly easy for an unsavvy tech consumer to go about their daily business without backing up their data regularly and updating their system’s anti-virus. This is a job for the IT department. The biggest challenge here is getting employees to understand when they need your help with these items.
5. **Physical Security for Devices:** Think about how many people in your office leave their desk for meetings, gatherings and lunch breaks. Are they locking their devices? Highlight the need to protect information each and every time a device is left unattended. You can use the airport analogy. Airport staff are constantly telling us to keep track of our bags and never leave them unattended. Why? Well, because you just don’t know who is walking by. Encourage employees to protect their devices with as much care as they protect their baggage.
	1. **Processes**

When employees outside of the IT department are trained, IT pros can focus on process. The processes by which cybersecurity professionals go about protecting confidential data are multi-faceted. In short, these IT pros are tasked with detecting and identifying threats, protecting information and responding to incidents as well as recovering from them.

Putting processes into place not only ensures each of these buckets are being continuously monitored, but if [cybersecurity attacks](https://www.comptia.org/blog/types-of-cyber-attacks) happen, referencing a well-documented process can save your company time, money and the trust of your most valuable asset – your customers.

The National Institute of Standards and Technology (NIST) under the U.S. Commerce Department has developed the [Cybersecurity Framework](https://www.nist.gov/cyberframework) for private-sector companies to use as a guide in creating their own best practices. The standards were compiled by NIST after former U.S. President Barack Obama signed an executive order in 2014. It’s a great resource to use as you work to combat your cybersecurity risk.

* 1. **Technology**

Once you have frameworks and processes in place, it’s time to think about the tools you have at your disposal to start implementation.

Technology has a dual meaning when it comes to your toolbox:

* The technology you’ll use to prevent and combat cybersecurity attacks, like DNS filtering, malware protection, antivirus software, firewalls and email security solutions.
* The technology your data lives on that needs your protection, like computers, [smart devices](https://www.comptia.org/blog/the-internet-of-things-%28iot%29-and-technical-debt-why-it-matters), routers, [networks](https://www.comptia.org/blog/security-awareness-training-network-segmentation) and the [cloud](https://www.comptia.org/blog/your-cloud-solutions-deserve-zero-trust-networking).

Back in the day, cybersecurity initiatives focused on defensive measures inside the boundaries of traditional tech. But today, policies like Bring Your Own Device (BYOD) have blurred those lines and handed hackers a much broader realm to penetrate. Remembering cybersecurity basics like locking all of your doors, windows, elevators and skylights will keep you from joining the cyber-crime statistics.

**READING**

**VOCABULARY**

* **4.1 Read the text and fill in the gaps with the words from the vocabulary given in the box:**

|  |
| --- |
| widespread, sensitive, cryptography tools, solid foundation, to avoid, code breakers, revealing, deciphering, entrust, estimates |

**Text 4. Cryptography in the Modern Era**

With the 1\_\_\_\_\_\_\_use of online and digital communication systems, 2\_\_\_\_\_\_\_\_\_information is transmitted around the world every day. Cryptography has become essential for protecting information online.

Cyber security professionals need a good understanding of cryptography and 3\_\_\_\_\_\_\_\_\_\_ to set up and run secure computer systems and networks. An [online master’s degree in cyber security](https://onlinedegrees.und.edu/masters-cyber-security/) can offer a 4\_\_\_\_\_\_\_\_\_\_in the cryptography tools that students seeking a career in the field will need.

In World War II, German submarines lurking below the surface of the North Atlantic preyed on Allied ships carrying supplies to England from the United States. The ships, not knowing the locations of submarines, could do little 5\_\_\_\_\_\_\_\_the attacks.

Enter British mathematician Alan Turing and a team of 6\_\_\_\_\_\_\_\_. Using the cryptography tools available at the time, they cracked codes generated by Germany’s sophisticated Enigma machine, 7\_\_\_\_\_\_\_\_German communications with the submarines. This allowed the Allies to route their ships to avoid the submarines.

8\_\_\_\_\_\_\_\_\_\_the German codes was one of the more significant achievements in cryptography, a field almost as old as human communication.

Today, cryptography is a key tool in the battle to keep computer systems and networks secure and private.

There’s a lot to protect. Individuals 9\_\_\_\_\_\_\_\_personal, financial, medical and other information to companies, government agencies and other organizations that store it digitally. Hardly a month goes by without news of a data breach that exposes millions of accounts.

Research firm Gartner 10\_\_\_\_\_\_\_\_that more than 80% of companies encrypted their web traffic in 2021. That percentage is likely to grow as more companies seek to protect their data as well as meet stricter regulations governing security and privacy.

**GRAMMAR**

* **Choose the correct form of the verb.**

**Text 5. Five Powerful Cryptography Tools for Cyber Security Professionals**

Multiple cryptography tools **can use/can be used/must be used** to build and fortify their computer system defenses by cyber security professionals. Here’s a look at five key tools that cyber security specialists can **integrate/to integrate/be integrated** into their strategies.

**Security Tokens**

A security token **has been/is/was** a physical device that holds information that authenticates a person’s identity. The owner plugs the security token into a system — via a computer’s USB port, for example — **gained/will gain/to gain** access to a network service. It’s like swiping a security card to get into an office. A bank might issue security tokens to customers to use as an extra layer of security when they logging/**log/will log** in to their accounts.

**Key-Based Authentication**

Key-based authentication is a method that **is employed/ employed/employs** asymmetric algorithms to confirm a client’s identity and can be an effective substitute for using passwords to verify a client. The key factors at play in key-based authentication are public and private keys that **confirm/confirms/confirming** identity.

In public key authentication, each user **give/gives/is given** a pair of asymmetric keys. Users store their public keys in each system they want access to, while the private keys **safely maintain/safely maintained/are safely maintained** on the device with which the user **is** **connected/connects/will be connected** to the secured systems.

When **connecting/connected/having connected**, the server authenticates the user with the public key and asks the user to decrypt it **used/using/uses** the corresponding private key.

**Docker**

The Docker software platform builds applications based on containers: small self-contained environments that share an operating system kernel but otherwise run in isolation from one another. By their nature, Docker containers are secure. More security can **add/be added/to be added** by enabling one of several applications that fortify the system.

**Java Cryptography Architecture**

The popular Java programming language has built-in cryptographic functions. The Java Cryptography Architecture (JCA) **has integrated/integrates/is** **integrated** with the core Java application programming interface (API). The JCA contains APIs that handle security functions that **include/includes/has included** encryption, managing keys, generating random numbers securely and validating certificates. These APIs provide a way for developers to build security into application code.

**SignTool**

Another security tool embedded in an operating system is Microsoft SignTool (SignTool.exe). A command-line tool, SignTool can digitally **sign/to sign/be signed** and time-stamp files and verify signatures in files. It **is automatically installed/** **has automatically installed/** **has been automatically installed** with Microsoft Visual Studio, a software development environment. SignTool allows software developers to certify that the code they developed is theirs and that it **has been tampered/hasn’t been tampered/hasn’t tampered /** with since it was published.

**READING**

**Warm up**

**SPEAKING**

* **6.1 What modern trends in cryptography do you know?**

**6.2 Skim the text given below to compare your ideas with the information.**

**6.3 Search the Internet and add some information about other treds in cryptography.**

**Text 6. Trends in Cryptography**

Cryptography tools constantly evolve as cryptographers and hackers leapfrog each other in building defenses and overcoming them. Several trends on the horizon point to new directions in cryptography.

**Quantum Computers and Cryptography**

The emerging technology of quantum computing promises great leaps in power and speed. Companies such as Google and IBM are racing to develop quantum computers, which could make some kinds of computing problems easier to solve than with today’s conventional computers.

One such problem area is the encryption protocols for today’s computing systems. The computing power of a quantum computer, experts say, could shred current security defenses. Security experts are developing systems that could protect against quantum systems.

**Cloud Computing**

When a company stores data on someone else’s servers, such as in a public cloud, the company loses control over securing the data. To solve that problem, some companies encrypt the data before storing it on a cloud system, giving the company a measure of control over the encryption. Another approach is to use cloud services that encrypt information when it enters the cloud environment, which protects it as it is stored or transmitted.

**Blockchain**

Blockchain is a distributed ledger that underlies digital currencies such as bitcoin. A blockchain is a series of data or transactions (the blocks) connected by cryptographic signatures stored in shared ledgers and supported by nodes, which form a network of processes. Nodes maintain a copy of the entire chain and are continually updated and kept in sync.

Companies have deployed blockchain technologies for secure transactions with customers as well as for storing data such as medical records.

**GRAMMAR**

* **Choose the correct form of the verb.**

**Text 7. Why is cloud security important?**

In modern-day enterprises, there **1.** **is/was/has been** a growing transition to cloud-based environments and IaaS, Paas, or SaaS computing models. The dynamic nature of infrastructure management, especially in scaling applications and services, can bring a number of challenges to enterprises when adequately resourcing their departments. These as-a-service models **2.** **are given/give/will give** organizations the ability to offload many of the time-consuming, IT-related tasks.

As companies continue **3.** **migrate/to migrate/to be migrated** to the cloud, **4.** **understanding/ understand/ understood** the security requirements for keeping data safe has become critical. While third-party cloud computing providers may take on the management of this infrastructure, the responsibility of data asset security and accountability **5.** **necessarily shift/don't necessarily shift/doesn't necessarily shift** along with it.

By default, most cloud providers follow best security practices and take active steps to protect the integrity of their servers. However, organizations need to make their own considerations when **6.** **protecting/protected/are protected** data, applications, and workloads running on the cloud.

Security threats **7.** **become/has become/have become/** more advanced as the digital landscape continues to evolve. These threats explicitly target cloud computing providers due to an organization's overall lack of visibility in data access and movement. Without taking active steps to improve their cloud security, organizations can face significant governance and compliance risks when managing client information, regardless of where it **8. was stored/is stored/stored.**

Cloud security should be an important topic of discussion regardless of the size of your enterprise.  Cloud infrastructure supports nearly all aspects of modern computing in all industries and across multiple verticals.

However, successful cloud adoption is dependent on putting in place adequate countermeasures to defend against modern-day cyberattacks. Regardless of whether your organization operates in a public, private, or hybrid cloud environment, cloud security solutions and best practices are a necessity when ensuring business continuity.

**Text 8. What are some cloud security challenges?**

**Lack of visibility**
It's easy to lose track of how your data **9.** **was accessed/is accessed/is being accessed** and by whom, since many cloud services are accessed outside of corporate networks and through third parties.

**Multitenancy**
Public cloud environments house multiple client infrastructures under the same umbrella, so it's possible your hosted services can **10.** **get compromised/ got compromised/compromised** by malicious attackers as collateral damage when **11.** **targeting/ targeted/are targeted** other businesses.

**Access management and shadow IT**
While enterprises may **12.** **be able to/can/ be able** successfully manage and restrict access points across on-premises systems, administering these same levels of restrictions can be challenging in cloud environments. This can be dangerous for organizations that **13.** **don't deploy/ doesn't deploy/ not to deploy** bring-your-own device (BYOD) policies and **14.** **be allowed/allow/allows** unfiltered access to cloud services from any device or geolocation.

**Compliance**
Regulatory compliance management is oftentimes a source of confusion for enterprises using public or hybrid cloud deployments. Overall accountability for data privacy and security still rests with the enterprise, and heavy reliance on third-party solutions to manage this component can lead to costly compliance issues.

**Misconfigurations**
Misconfigured assets accounted for 86% of breached records in 2019, **15. made/making/make** the inadvertent insider a key issue for cloud computing environments. Misconfigurations can include leaving default administrative passwords in place, or not creating appropriate privacy settings.

**Warm up**

**SPEAKING**

* **9.1 What types of network security protections do you know?**

**9.2 Skim the text given below to compare your ideas with the facts.**

**VOCABULARY**

**Text 9. Types of Network Security Protections**

* **9.3. Skim the text, pay attention to the following words and word combinations and explain their meaning in English:**

|  |
| --- |
| **vulnerability, blocking malware,** **application-layer attack, network segmentation, denying unsanctioned access, multi-factor authentication, granular access, compliance related data, security patch** |

**Firewall**

[Firewalls](https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/) control incoming and outgoing traffic on networks, with predetermined security rules. Firewalls keep out unfriendly traffic and is a necessary part of daily computing. Network Security relies heavily on Firewalls, and especially [Next Generation Firewalls](https://www.checkpoint.com/cyber-hub/network-security/what-is-network-segmentation/), which focus on blocking malware and application-layer attacks.

**Network Segmentation**

[Network segmentation](https://www.checkpoint.com/cyber-hub/network-security/what-is-network-segmentation/) defines boundaries between network segments where assets within the group have a common function, risk or role within an organization. For instance, the perimeter gateway segments a company network from the Internet. Potential threats outside the network are prevented, ensuring that an organization’s sensitive data remains inside. Organizations can go further by defining additional internal boundaries within their network, which can provide improved security and access control.

**What is Access Control?**

Access control defines the people or groups and the devices that have access to network applications and systems thereby denying unsanctioned access, and maybe threats. Integrations with Identity and Access Management (IAM) products can strongly identify the user and Role-based Access Control (RBAC) policies ensure the person and device are authorized access to the asset.

**Remote Access VPN**

[Remote access VPN](https://www.checkpoint.com/products/remote-access-vpn/) provides remote and secure access to a company network to individual hosts or clients, such as telecommuters, mobile users, and extranet consumers. Each host typically has VPN client software loaded or uses a web-based client. Privacy and integrity of sensitive information is ensured through multi-factor authentication, endpoint compliance scanning, and encryption of all transmitted data.

**Zero Trust Network Access (ZTNA)**

The zero trust security model states that a user should only have the access and permissions that they require to fulfill their role. This is a very different approach from that provided by traditional security solutions, like VPNs, that grant a user full access to the target network. [Zero trust network access (ZTNA)](https://www.checkpoint.com/cyber-hub/network-security/what-is-zero-trust-network-access-ztna/) also known as [software-defined perimeter](https://www.checkpoint.com/cyber-hub/network-security/what-is-software-defined-perimeter-sdp/) (SDP) solutions permits granular access to an organization’s applications from users who require that access to perform their duties.

**Email Security**

[Email security](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/) refers to any processes, products, and services designed to protect your email accounts and email content safe from external threats. Most email service providers have built-in email security features designed to keep you secure, but these may not be enough to stop cybercriminals from accessing your information.

**Data Loss Prevention (DLP)**

[Data loss prevention (DLP)](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-data-loss-prevention/) is a cybersecurity methodology that combines technology and best practices to prevent the exposure of sensitive information outside of an organization, especially regulated data such as personally identifiable information (PII) and compliance related data: HIPAA, SOX, PCI DSS, etc.

**Intrusion Prevention Systems (IPS)**

[IPS technologies](https://www.checkpoint.com/cyber-hub/network-security/what-is-ips/) can detect or prevent network security attacks such as brute force attacks, Denial of Service (DoS) attacks and exploits of known vulnerabilities. A vulnerability is a weakness for instance in a software system and an exploit is an attack that leverages that vulnerability to gain control of that system. When an exploit is announced, there is often a window of opportunity for attackers to exploit that vulnerability before the security patch is applied. An Intrusion Prevention System can be used in these cases to quickly block these attacks.

**Sandboxing**

[Sandboxing](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-sandboxing/) is a cybersecurity practice where you run code or open files in a safe, isolated environment on a host machine that mimics end-user operating environments. Sandboxing observes the files or code as they are opened and looks for malicious behavior to prevent threats from getting on the network. For example malware in files such as PDF, Microsoft Word, Excel and PowerPoint can be safely detected and blocked before the files reach an unsuspecting end user.

**Hyperscale Network Security**

[Hyperscale](https://www.checkpoint.com/cyber-hub/network-security/what-is-hyperscale/) is the ability of an architecture to scale appropriately, as increased demand is added to the system. This solution includes rapid deployment and scaling up or down to meet changes in network security demands. By tightly integrating networking and compute resources in a software-defined system, it is possible to fully utilize all hardware resources available in a clustering solution.

**Cloud Network Security**

Applications and workloads are no longer exclusively hosted on-premises in a local data center. Protecting the modern data center requires greater flexibility and innovation to keep pace with the migration of application workloads to the cloud. Software-defined Networking (SDN) and Software-defined Wide Area Network ([SD-WAN](https://www.checkpoint.com/cyber-hub/network-security/what-is-sd-wan/)) solutions enable network security solutions in private, public, hybrid and cloud-hosted [Firewall-as-a-Service](https://www.checkpoint.com/cyber-hub/network-security/firewall-as-a-service-fwaas/) (FWaaS) deployments.

**VOCABULARY**

* **10.1 Read the text and fill in the gaps with the words from the vocabulary given in the box:**

|  |
| --- |
| **security testing, software application code, firewalls, application security,** **vulnerability scanning, security standards, security testing, implement, authentication, firewalls, ways** |

**Text 10. What is Application Security?**

Application security aims to protect 1\_\_\_\_\_\_\_\_\_\_ and data against cyber threats. You can and should apply 2\_\_\_\_\_\_\_\_ during all phases of development, including design, development, and deployment.

Here are several 3\_\_\_\_\_\_\_\_to promote application security throughout the software development lifecycle (SDLC):

* Introduce 4\_\_\_\_\_\_\_\_and tools during design and application development phases. For example, include 5\_\_\_\_\_\_\_\_during early development.
* 6\_\_\_\_\_\_\_\_security procedures and systems to protect applications in production environments. For example, perform continuous 7\_\_\_\_\_\_\_\_.
* Implement strong 8\_\_\_\_\_\_\_\_\_for applications that contain sensitive data or are mission critical.
* Use security systems such as 9­\_\_\_\_\_\_\_\_\_, web application firewalls (WAF), and intrusion prevention systems (IPS).

**LISTENING 2**

**What are the main types of hackers?**

* **2.1 Watch the video attentively. What information from the video was new for you?**



<https://www.youtube.com/watch?v=JaWll6zqlj4>

** 2.2. Decide if the statements below are TRUE or FALSE.**

1. There are four classes of hacker.

2. There two malicious types of hackers.

3. Ethical hackers are lawful good wizards of the net.

**2.3. What type of hackers do the following statements refer to?**

1. Selling stolen credit card information is all in a day’s work.

2. They will try their best to find holes in the client’s security.

3. They don’t steal information on purpose

4. They offer penetration tests.

5. They use their knowledge for profit, for lulls or both.

6. They don’t damage anything on purpose

7. They are the bogeyman of the Internet.

8. They don’t care about consent.

9. All their options are illegal or immoral.

10. They go to great pains to ensure that whatever they do happens with the consent of everyone involved.

**READING**

**11.1 Read the text and compare the information. What information wasn’t given in the video above?**

**11.2 Tell the difference between white, black, and grey hat hackers.**

**Text 11. What are the three main types of hackers?**

Hackers fall into three general categories: black hat hackers, white hat hackers, and grey hat hackers. **Although hackers are often associated with exploiting vulnerabilities to gain unauthorized access to computers, systems, or networks, not all hacking is malicious or illegal.**

In its purest sense, [hacking](https://www.avast.com/c-hacker) is simply the application of computer skills to solve a particular problem. There are many different types of hackers, and a lot of hacking activities are beneficial, because they uncover programming weaknesses that help developers improve software products.

**Black hat hackers**

**Black hat hackers are**[**cybercriminals**](https://www.avast.com/c-cybercrime)**that illegally crack systems with malicious intent.** Seeking to gain unauthorized access to computer systems is the definition of black hat hacking. Once a black hat hacker finds a security vulnerability, they try to exploit it, often by implanting a [virus or other type of malware](https://www.avast.com/c-malware-vs-virus) such as a [trojan](https://www.avast.com/c-trojan).

[**Ransomware attacks**](https://www.avast.com/c-what-is-ransomware)**are another favored ploy that black hat hackers use to extort financial gains or**[**breach data systems**](https://www.avast.com/c-b-what-is-a-data-breach)**.**

**White hat hackers**

**Vulnerabilities are identified and fixed by white hat hackers who are ethical security hackers.** Hacking into systems with the permission of the organizations they hack into, white hat hackers try to uncover system weaknesses in order to fix them and help strengthen a system’s overall security.

**Many cybersecurity leaders**[**started out as white hat hackers**](https://blog.avast.com/how-to-become-a-white-hat-hacker?_ga=2.12892798.811119647.1665144727-1259669144.1665144727)**, but the vital role played by ethical hacking is still widely misunderstood, as made clear by a recent**[**ethical hacking case in Germany**](https://blog.avast.com/white-hat-hacking-and-cdu-avast?_ga=2.12892798.811119647.1665144727-1259669144.1665144727)**.**

**Grey hat hackers**

Grey hat hackers may not have the criminal or malicious intent of a black hat hacker, but they also don’t have the prior knowledge or consent of those whose systems they hack into. Nevertheless, when grey hat hackers uncover weaknesses such as [zero-day vulnerabilities](https://www.avast.com/c-zero-day), they report them rather than fully [exploiting](https://www.avast.com/c-exploits) them. But grey hat hackers may demand payment in exchange for providing full details of what they uncovered.

**Other types of hackers**

Although nearly all hackers fall into one of the three categories (black hat, white hat, or grey hat), there are other types and sub-types of hackers.

* **Green hat hackers:**Green hat hackers are “green” in the sense that they’re inexperienced and may lack the technical skills of more experienced hackers. Green hats may rely on [phishing](https://www.avast.com/c-phishing) and other [social engineering](https://www.avast.com/c-social-engineering) techniques to bypass security systems.
* **Blue hat hackers:** **Blue hat hackers are white hat hackers who are actually employed by an organization to help improve their security systems by conducting**[**penetration tests**](https://www.avast.com/c-penetration-testing)**.**
* **Red hat hackers:** Also known as vigilante hackers, red hat hackers are motivated by a desire to fight back against black hat hackers, but they do this by infiltrating black hat communities on the [dark web](https://www.avast.com/c-dark-web) and launching hacking attacks against their networks and devices.

**What’s the difference between white, black, and grey hat hackers?**

The main difference between white, black, and grey hat hackers is the motivation or intent that each type of hacker has when they break into computer systems. White hat hackers probe cybersecurity weaknesses to help organizations develop stronger security; black hat hackers are motivated by malicious intent; and Grey hat hackers operate in the nebulous area in between — they’re not malicious, but they’re not always ethical either.

**GRAMMAR**

**11. 3 Find sentences in the text above highlighted in bold. Which of the sentences are passive?**

**Warm up**

**SPEAKING**

* 1. **Who is the most gifted hacker** **in your opinion? Why do you think so?**
	2. **Skim the text, choose two the most notorious hackers out of ten and compare their hacking careers.**

**READING**

**Text 12. Top 10** **Most Notorious Hackers of All Time**



**What is hacking?**

Computer hacking is the act of identifying and exploiting system and network vulnerabilities in order to obtain unauthorized access to those systems. Not all hacking is malicious. White hat hackers may work in cyber security or as software engineers and testers seeking out vulnerabilities in order to fix them. Black hat hackers operate with malicious intent. That said, there is a large grey area populated by political activists and hackers who wear both hats.

Hacking costs companies and consumers trillions of dollars every year. According to [*CPO Magazine*](https://www.cpomagazine.com/tech/11-eye-opening-cyber-security-statistics-for-2019/), by 2021, hacking attacks will cost a total $6 trillion, up from $2 trillion in losses reported in 2019. Much of the [cyber crime](https://www.kaspersky.com/resource-center/threats/cybercrime) problem stems from the same features of the internet from which we all benefit. Even the most amateur hacker can easily find all the tools they need online at virtually no cost.

The hacker onslaught didn't occur overnight. It took decades of work by now-famous hackers to discover critical vulnerabilities and reveal the strategies that established the foundations of the internet and its free-for-all libertarianism. Here's a look at the top ten most notorious hackers of all time.

1. **Kevin Mitnick**

A seminal figure in American hacking, Kevin Mitnick got his career start as a teen. In 1981, he was charged with stealing computer manuals from Pacific Bell. In 1982, he hacked the North American Defense Command (NORAD), an achievement that inspired the 1983 film [*War Games*](https://www.imdb.com/title/tt0086567/?ref_=nv_sr_srsg_0). In 1989, he hacked Digital Equipment Corporation's (DEC) network and made copies of their software. Because DEC was a leading computer manufacturer at the time, this act put Mitnick on the map. He was later arrested, convicted and sent to prison. During his conditional release, he hacked Pacific Bell's voicemail systems.

Throughout his hacking career, Mitnick never exploited the access and data he obtained. It's widely believed that he once obtained full control of Pacific Bell's network simply to prove it could be done. A warrant was issued for his arrest for the Pacific Bell incident, but Mitnick fled and lived in hiding for more than two years. When caught, he served time in prison for multiple counts of wire fraud and computer fraud.

Although Mitnick ultimately went white hat, he may be part of the both-hats grey area. According to [Wired](https://www.wired.com/2014/09/kevin-mitnick-selling-zero-day-exploits/), in 2014, he launched "Mitnick's Absolute Zero Day Exploit Exchange," which sells unpatched, critical software exploits to the highest bidder.

1. **Anonymous**

Anonymous got its start in 2003 on [4chan message boards](https://en.wikipedia.org/wiki/4chan) in an unnamed forum. The group exhibits little organization and is loosely focused on the concept of social justice. For example, in 2008 the group took issue with the Church of Scientology and begin disabling their websites, thus negatively impacting their search rankings in Google and overwhelming its fax machines with all-black images. In March 2008, a group of "Anons" marched passed Scientology centers around the world wearing the now-famous Guy Fawkes mask. As noted by [The New Yorker](https://www.newyorker.com/magazine/2014/09/08/masked-avengers), while the FBI and other law enforcement agencies have tracked down some of the group's more prolific members, the lack of any real hierarchy makes it almost impossible to identify or eliminate Anonymous as a whole.

1. **Adrian Lamo**

In 2001, 20-year-old Adrian Lamo used an unprotected content management tool at Yahoo to modify a Reuters article and add a fake quote attributed to former Attorney General John Ashcroft. Lamo often hacked systems and then notified both the press and his victims. In some cases, he'd help clean up the mess to improve their security. As [Wired](http://www.wired.com/2010/05/lamo/) points out, however, Lamo took things too far in 2002, when he hacked The New York Times' intranet, added himself to the list of expert sources and began conducting research on high-profile public figures. Lamo earned the moniker "The Homeless Hacker" because he preferred to wander the streets with little more than a backpack and often had no fixed address.

1. **Albert Gonzalez**

According to the New York Daily News, Gonzalez, dubbed "soupnazi," got his start as the "troubled pack leader of computer nerds" at his Miami high school. He eventually became active on criminal commerce site Shadowcrew.com and was considered one of its best hackers and moderators. At 22, Gonzalez was arrested in New York for debit card fraud related to stealing data from millions of card accounts. To avoid jail time, he became an informant for the Secret Service, ultimately helping indict dozens of Shadowcrew members.

During his time as a paid informant, Gonzalez continued his in criminal activities. Along with a group of accomplices, Gonzalez stole more than 180 million payment card accounts from companies including OfficeMax, Dave and Buster's and Boston Market. [The New York Times Magazine](https://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html) notes that Gonzalez's 2005 attack on US retailer TJX was the first serial data breach of credit information. Using a basic SQL injection, this famous hacker and his team created back doors in several corporate networks, stealing an estimated $256 million from TJX alone. During his sentencing in 2015, the federal prosecutor called Gonzalez's human victimization "unparalleled."

1. **Matthew Bevan and Richard Pryce**

Matthew Bevan and Richard Pryce are a team of British hackers who hacked into multiple military networks in 1996, including Griffiss Air Force Base, the Defense Information System Agency and the Korean Atomic Research Institute (KARI). Bevan (Kuji) and Pryce (Datastream Cowboy) have been accused of nearly starting a third world war after they dumped KARI research onto American military systems. Bevan claims he was looking to prove a UFO conspiracy theory, and according to the [BBC](http://news.bbc.co.uk/2/hi/technology/4761985.stm), his case bears resemblance to that of Gary McKinnon. Malicious intent or not, Bevan and Pryce demonstrated that even military networks are vulnerable.

1. **Jeanson James Ancheta**

Jeanson James Ancheta had no interest in hacking systems for credit card data or crashing networks to deliver social justice. Instead, Ancheta was curious about the use of bots—software-based robots that can infect and ultimately control computer systems. Using a series of large-scale "[botnets](https://www.kaspersky.com/resource-center/threats/botnet-attacks)," he was able to compromise more than 400,000 computers in 2005. According to [Ars Technica](https://arstechnica.com/uncategorized/2006/05/6789-2/), he then rented these machines out to advertising companies and was also paid to directly install bots or [adware](https://www.kaspersky.com/resource-center/threats/adware-pornware-riskware) on specific systems. Ancheta was sentenced to 57 months in prison. This was the first time a hacker was sent to jail for the use of botnet technology.

1. **Michael Calce**

In February 2000, 15-year-old Michael Calce, also known as "Mafiaboy," discovered how to take over networks of university computers. He used their combined resources to disrupt the number-one search engine at the time: Yahoo. Within one week, he'd also brought down Dell, eBay, CNN and Amazon using a [distributed-denial-of-service (DDoS)](https://www.kaspersky.com/resource-center/threats/ddos-attacks) attack that overwhelmed corporate servers and caused their websites to crash. Calce's wake-up call was perhaps the most jarring for cyber crime investors and internet proponents. If the biggest websites in the world—valued at over $1 billion—could be so easily sidelined, was any online data truly safe? It's not an exaggeration to say that the development of cyber crime legislation suddenly became a top government priority thanks to Calce's hack.

1. **Kevin Poulsen**

In 1983, a 17-year-old Poulsen, using the alias Dark Dante, hacked into ARPANET, the Pentagon’s computer network. Although he was quickly caught, the government decided not to prosecute Poulsen, who was a minor at the time. Instead, he was let off with a warning.

Poulsen didn’t heed this warning and continued hacking. In 1988, Poulsen hacked a federal computer and dug into files pertaining to the deposed president of the Philippines, Ferdinand Marcos. When discovered by authorities, Poulsen went underground. While he was on the run, Poulsen kept busy, hacking government files and revealing secrets. According to his [own website](https://www.kingpin.cc/about/), in 1990, he hacked a radio station contest and ensured that he was the 102nd caller, winning a brand new Porsche, a vacation, and $20,000.

Poulsen was soon arrested and barred from using a computer for three years. He has since converted to white hat hacking and journalism, writing about cyber security and web-related socio-political causes for [Wired](https://www.wired.com/author/kevin-poulsen/), The Daily Beast and his own blog Threat Level. Paulson also teamed with other leading hackers to work on various projects dedicated to social justice and freedom of information. Perhaps most notably, working with Adam Swartz and Jim Dolan to develop the open-source software SecureDrop, initially known as DeadDrop. Eventually, Poulsen turned over the platform, which enabled secure communication between journalists and sources, to the Freedom of Press Foundation.

1. **Jonathan James**

Using the alias cOmrade, Jonathan James hacked several companies. According to the [New York Times](https://www.nytimes.com/2000/09/23/us/youth-sentenced-in-government-hacking-case.html), what really earned James attention was his hack into the computers of the United States Department of Defense. Even more impressive was the fact that James was only 15 at the time. In [an interview with PC Mag](https://www.pcmag.com/archive/qa-hackings-boy-wonder-212515), James admitted that he was partly inspired by the book *The Cuckoo’s Egg*, which details the hunt for a computer hacker in the 1980s. His hacking allowed him to access over 3,000 messages from government employees, usernames, passwords and other sensitive data.

James was arrested in 2000 and was sentenced to a six months house arrest and banned from recreational computer use. However, a probation violation caused him to serve six months in jail. Jonathan James became the youngest person to be convicted of violating cyber crime laws. In 2007, TJX, a department store, was hacked and many customer’s private information were compromised. Despite a lack of evidence, authorities suspect that James may have been involved.

In 2008, James committed suicide by gunshot. According to the [Daily Mail](https://www.dailymail.co.uk/news/article-2262831/Revealed-Aaron-Swartz-prosecutor-drove-hacker-suicide-2008-named-cyber-crime-case.html), his [suicide note](https://www.dailymail.co.uk/news/article-2262831/Revealed-Aaron-Swartz-prosecutor-drove-hacker-suicide-2008-named-cyber-crime-case.html) stated, “I have no faith in the 'justice' system. Perhaps my actions today, and this letter, will send a stronger message to the public. Either way, I have lost control over this situation, and this is my only way to regain control.”

1. **ASTRA**

This hacker differs from the others on this list in that he has never been publicly identified. However, according to [the Daily Mail](https://www.dailymail.co.uk/news/article-2262831/Revealed-Aaron-Swartz-prosecutor-drove-hacker-suicide-2008-named-cyber-crime-case.html), some information has been released about ASTRA. Namely that he was apprehended by authorities in 2008, and at that time he was identified as a 58-year-old Greek mathematician. Reportedly, he had been hacking into the Dassault Group, for almost half a decade. During that time, he stole cutting edge weapons technology software and data which he then sold to 250 individuals around the world. His hacking cost the Dassault Group $360 million in damages. No one knows why his complete identity has never been revealed, but the word 'ASTRA' is a Sanskrit word for 'weapon'.

 Some of these top hackers aimed to make the world a better place, others to prove UFO theories. Some wanted money and others hoped for fame. All these people played a critical role in the evolution of the internet and cyber security.

REFERENCES

1. Avast Academy. Oliver Buxton. Hacker Types: Black Hat, White Hat, and Gray Hat Hackers, 2023

URL: <https://www.avast.com/c-hacker-types>

1. Cambridge English Dictionary Online.

URL: <https://dictionary.cambridge.org> (reference date: December 25, 2022).

1. Collins English Dictionary Online.

 URL: <https://www.collinsdictionary.com/> (reference date: December 25, 2022).

1. CompTIA Tech Career Academy. Why Is Cybersecurity Important?, 2022

URL: <https://www.comptia.org/content/articles/what-is-cybersecurity>

1. Kaspersky. Top 10 Most Notorious Hackers of All Time, 2022

 URL: <https://www.kaspersky.com/resource-center/threats/top-ten-greatest-hackers>

1. Konverge Technologies. 6 Common Types of Cyber Physical Attacks, 2023

URL: <https://www.konverge.co.in/types-of-cyber-physical-attacks/>

1. Michelle Moore, PhD. Top Cybersecurity Threats in 2022, 2022

URL: <https://onlinedegrees.sandiego.edu/top-cyber-security-threats/>

1. Todd Barnum. The Cybersecurity Manager's Guide. O'Reilly Media, Inc., 2021. 176
2. University of North Dakota. 5 Powerful Cryptography Tools for Cyber Security Professionals. 2023

URL: <https://onlinedegrees.und.edu/blog/5-cryptography-tools/>

1. Virgilio Viegas, Oben Kuyucu. IT Security Controls. A Guide to Corporate Standards and Frameworks. Apress, 2022. 354

Навчальне видання

Методичні вказівки для

самостійної роботи студентів 2 року навчання спеціальності

Кібербезпека

 Укладачі: ГОНЧАРЕНКО Тетяна Євгеніївна

 ГРАЩЕНКОВА Вікторія Володимирівна

 САЛАМАТІНА Анна Володимирівна

 ТИХОНОВА Марина Євгеніївна

Англійською мовою

Відповідальний за випуск *Гончаренко Т.Є.*

Роботу до видання рекомендувала доц. Шеїна Л.О.

В авторській редакції

План 2023 р., поз.

Підп. до друку 03.06.2023. Формат 60×84 1/16. Папір офсетний.

Riso-друк. Гарнітура Times New Roman. Ум. друк. арк.1,5.

Наклад 50 прим. Ціна договірна.

Видавничий центр НТУ «ХПІ».

Свідоцтво про державну реєстрацію ДК № 5478 від 21.08.2017 р.

61002, Харків, вул. Кирпичова, 2

Друкарня «Мадрид», Харків, вул. Ольмінського, 11