МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ГУМОВСЬКА Ірина Миколаївна

МАТЕРІАЛИ ДО ПРАКТИЧНИХ РОБІТ

З ДИСЦИПЛІНИ «ЛІНГВІСТИЧНІ АСПЕКТИ ІНТЕРНЕТ-КОМУНІКАЦІЇ»

ДЛЯ СТУДЕНТІВ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

«БІЗНЕС-КОМУНІКАЦІЇ ТА ПЕРЕКЛАД»

Тернопіль – 2023

Матеріали до практичних робіт з дисципліни «Лінгвістичні аспекти інтернет-комунікацій» для студентів освітньо-професійної програми «Бізнес-комунікації та переклад». Укладач: І.М. Гумовська. Тернопіль, 2023. 35с.

Рецензенти:

Бєлінська Ірина Дем'янівна – кандидат філологічних наук, доцент, доцент кафедри іноземних мов та інформаційно-комунікаційних технологій ЗУНУ;

Кебало Микола Степанович –кандидат філологічних наук, доцент кафедри німецької філології та методики викладання німецької мови Тернопільського національного педагогічного університету ім. В.Гнатюка.

Затверджено на засіданні кафедри іноземних мов та інформаційно-комунікаційних технологій, № 4 від 14 листопада 2023 року.

Відповідальний за випуск:

Крайняк Л.К. – кандидат філологічних наук, доцент, завідувач кафедри іноземних мов та інформаційно-комунікаційних технологій Західноукраїнського національного університету.

Зміст

WHAT DOES 143 MEAN?

143 means "I love you." It is a common way to express love in texts or messaging apps. The individual numbers in "143" represent the number of letters in the words.

- "I" = 1
- "love" = 4
- "you" = 3

Of course, using numbers in this way helps with brevity, but, nowadays, this is not the main reason terms like 143 are used. Specifically, 143 tends to be used for three reasons. Firstly, it allows the sender to say "I love you" without suffering the embarrassment of saying those "three magic words." Secondly, it is still a secretive way of expressing love, and, thirdly, it is a fun and modern way to take the edge of otherwise poignant words.

The Origin of 143

According to popular belief[1], the association of "143" with "I love you" is rooted back in 1894, when a new flashing lantern was installed in Minot's Ledge lighthouse off the coast of Massachusetts (near Boston Harbor). The lighthouse flash sequence was 1-4-3. Some years later (circa 1915), when Winfield Scott Thompson was the lighthouse keeper at Minot's Ledge, his wife told their children, who could see the lighthouse flashing at night, that it was the "I love you" flash. She told them it was their father's way of saying he loved them. The tale has proven so popular that the Minot's Ledge lighthouse is still nicknamed the "I Love You Lighthouse."

143 Before the Internet

143 was used as digital shorthand for "I love you" long before the spread of the internet and messaging apps. In the late 1980s, many people carried text-enabled pagers, which were small handheld devices that used the fledgling analogue-radio, mobile telephone network to send short text messages. Compiling a message on a pager was fiddly and the character count was brutally restrictive. As a result, users quickly invented brevity codes to save time and space. 143 was the code for "I love you" on pagers, and this was its first use in the "digital" era.

143 in a Conversation

Here is an example of 143 and other numeronyms in a conversation:

- Toni: 143.
- Jo: 1422.
- Toni: I think you meant 1432 (I love you too.)
- Jo: No, I meant 1422 (I love me too!)

143 Is a Numeronym

When used like this, numbers like 143 are known as "numeronyms," which are effectively abbreviations using numbers. Using numeronyms in this way is still highly popular in internet slang, despite the rise of emojis. Other common ways of expressing love with numbers include:

- 381 = I Love You (3 words, 8 letters, 1 meaning).
- 721 = Love You (7 letters, 2 words, 1 meaning).
- 831 = I Love You (8 letters, 3 words, 1 meaning).
- 1437 = I Love You Forever (number of letters in each word).
- 14344 = I Love You Very Much (number of letters in each word).

A-Z GLOSSARY OF TERMS RELATED TO ARTIFICIAL INTELLIGENCE

The emergence of artificial Intelligence (AI) has given rise to lots of new terms and abbreviations. AI also includes other aspects like Robotics, Computer Vision, Speech Recognition, Sentiment Analysis, Expert Systems, Fuzzy Systems, and Evolutionary Computation, each with its own set of abbreviations and terminologies. Here is a complete glossary of AI-related terms.

AI Artificial Intelligence	Computer systems able to perform tasks that usually require human intelligence.
AI/MLaaS Artificial Intelligence/Machine Learning as a Service	The offering of AI and ML capabilities as part of cloud computing services.
AGI Artificial General Intelligence	Highly autonomous systems that outperform humans at most economically valuable work.
ANN Artificial Neural Networks	Computing systems inspired by the human brain's neural networks. They are a key component of Deep Learning (DL).
AutoML Automated Machine Learning	The process of automating the end-to-end process of applying machine learning to real-world problems.
CNN Convolutional Neural Networks	A class of DNN, most commonly applied to analyzing visual imagery.
DL Deep Learning	A subset of ML that structures algorithms in layers to create an artificial neural network that can learn and make intelligent decisions on its own.

DNN Deep Neural Networks	A type of ANN with multiple layers between the input and output layers.
GAN Generative Adversarial Networks	A class of AI algorithms used in unsupervised machine learning, implemented by a system of two neural networks contesting with each other.
GRU Gated Recurrent Unit	A type of RNN that simplifies learning in sequential tasks. It uses gating mechanisms to control information flow.
IoT Internet of Things	The network of physical objects (i.e., "things") that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.
LSTM Long Short-Term Memory	A type of RNN that can remember long sequences of data, improving performance in tasks like speech recognition.
ML Machine Learning	A subset of AI that involves the practice of using algorithms to parse data, learn from it, and then make a determination or prediction.
NARROW AI Narrow Artificial Intelligence	AI systems designed to perform specific tasks, operating under a limited set of constraints. (Also known as "Weak AI".)
NLP Natural Language Processing	A branch of AI that helps computers understand, interpret, and manipulate human language.
RL Reinforcement Learning	A type of ML where an agent learns to behave in an environment, by performing actions and seeing the results.

RNN Recurrent Neural Networks	A type of ANN designed to recognize patterns in sequences of data, such as text, genomes, handwriting, or spoken word.
SUPERINTELLIGENT AI Superintelligent Artificial Intelligence	AI systems that surpass human intelligence in practically every field.
WEAK AI Weak Artificial Intelligence	AI systems designed to perform specific tasks, operating under a limited set of constraints. (More commonly known as "Narrow AI".)

EMOJI CATEGORIES

-  Face Emojis
-  Heart & Love Emojis
-  Food Emojis
-  Animal Emojis
-  Weather Emojis
-  Hand & Body Parts Emojis
-  Nature Emojis
-  Astrology Emojis
-  Astronomy Emojis
-  Party & Holiday Emojis
-  Music Emojis
-  Sport Emojis
-  Travel & Transport Emojis
-  Building Emojis
-  Sign Emojis
-  Shapes & Shades Emojis
-  Clothing & Accessories Emojis
-  Family Emojis
-  Fantasy Emojis
-  Money Emojis
-  Technology Emojis
-  Security Emojis
-  Tool Emojis
-  Time Emojis
-  Miscellaneous Emojis
-  Eight Ways to Insert an Emoji

LIST OF SPANISH "TEXT SPEAK" SLANG AND ABBREVIATIONS

Do you speak a bit of Spanish? Do you have Spanish-speaking friends? Why not surprise them by including some slang terms that Spanish speakers use in your next message?

Abbreviation or Slang Term	Meaning in Spanish and English
+ o -	mas o menos (Spanish for "more or less")
100pre	siempre (Spanish for "always")
aki	aqui (Spanish for "here")
alv	a la verga (Spanish for "go to hell")
amig@s	amigos or amigas (Spanish for "friends")
b	beso or bien (Spanish for "kiss" or "good")
beso	beso (Spanish for "kiss")
bs	besos (Spanish for "kisses")
c	sí (Spanish for "yes")
chich@s	chicos or chicas (Spanish for "guys")
da =	me da igual (Spanish for "I don"t mind")
dtb	Dios te bendiga (Spanish for "God bless you")
fin d	fin de semana (Spanish for "the weekend")
gnl	genial (Spanish for "great")

grax	gracias (Spanish for "thank you")
hla	hola (Spanish for "hello")
jaja	laughing (Spanish for sounds like ha ha)
Jiji	laughing (Spanish for sounds like he he)
k	que (Spanish for "how" or "what")
k acs	que haces (Spanish for "what are you doing")
k risa	que risa (Spanish for "that is so funny")
k tl	que tal (Spanish for "how are you?")
kiero	quiero (Spanish for "I want" or "I love")
klk	que lo que (Spanish for "what's up")
kls	clase (Spanish for "class")
kn	quien (Spanish for "who")
ktl	que tal (Spanish for "how are you?")
kyat	callate (Spanish for "shut up")
md=	me da igual (Spanish for "I don"t mind")
mdi	me da igual (Spanish for "I don"t mind")
me da =	me da igual (Spanish for "I don"t mind")

mxo	mucho (Spanish for "much" or "a lot")
npn	no pasa nada (Spanish for "nothing is happening")
ong	organizacion no gubernamental (Spanish for "non-governmental organization" (NGO))
pti	para tu informacion (Spanish for "for your information")
q	que (Spanish for "how" or "what")
q acs	que haces (Spanish for "What are you doing")
q tl	que tal (Spanish for "how are you?")
qtl	que tal (Spanish for "how are you?")
re100	recien (Spanish for "recently")
salu2	saludos (Spanish for "greetings")
ta	esta (Spanish for "is")
ta b	esta bien (Spanish for "it is good" or "is it good?".)
tam	te amo mucho (Spanish for "I love you a lot")
tki	tengo que irme (Spanish for "I have to go")
tkm	te quiero mucho (Spanish for "I love you a lot")
toy	estoy (Spanish for "you are")
tqi	tengo que irme (Spanish for "I have to go")

tqm	te quiero mucho (Spanish for "I love you a lot")
vns	venis (Spanish for "are you coming")
x	por (Spanish for "for" or "times")
xa	para (Spanish for "for")
xa k	para que (Spanish for "why")
xa q	para que (Spanish for "why")
xau	chau (Spanish for "good bye")
xfa	por favor (Spanish for "please")
xk	porque or por que (Spanish for "because" or "why")
xq	Porque or por que (Spanish for "because" or "why")
yo tb	yo tambien (Spanish for "me too")
ytb	yo tambien (Spanish for "me too")

WHAT DOES * MEAN?

The asterisk (*) is a small and seemingly simple symbol, but don't be fooled. It has an impressive array of uses. It features in mathematics, computer programming, texting, university dissertations, and normal language, where is helps with handling sensitive language. Here are seven common uses of asterisk:

(1) Spelling Correction

When a texter's fingers work faster than their eyes and produce a typo or their autocorrect inserts the wrong word, the texter can use an asterisk in the next message to show a correction. For example:

- Jo: I am seeing doctor Singh tomorrow for my anal exam.
- Jo: *annual!
- Sam: LOL

(2) Censoring Swear Words

Asterisks are commonly used in writing to obscure swear words or offensive language. Asterisks allow writers to convey swear words without spelling them out fully. This helps them to maintain a level of propriety while still communicating the intended message.

- Traffic warden: You can't threaten me.
- Driver: I just f*cking did, mate.
- Traffic warden: I'm not removing the ticket. You're parked illegally.
- Driver: Get a f*cking real job. You can suck my d*ck.
- Traffic warden: You're being filmed. And, no thanks.

When it's appropriate to cite the swear words verbatim, an asterisk can help writers distance themselves from the crudity.

(3) Placeholder or Wildcard Character

In computing and search queries, an asterisk can be used as a wildcard character, which represents any string of characters in searches. For example, if you search for "bo*t" it might find "boat", "bolt", "boot", and "bout."

(4) Obscuring Characters

An asterisk is commonly used to obscure certain characters in a string of text, such as in passwords or sensitive information. For instance, a hidden password might appear as "******".

(5) Emphasizing Text

In some texting apps (e.g., WhatsApp), asterisks are used for bolding text. For example:

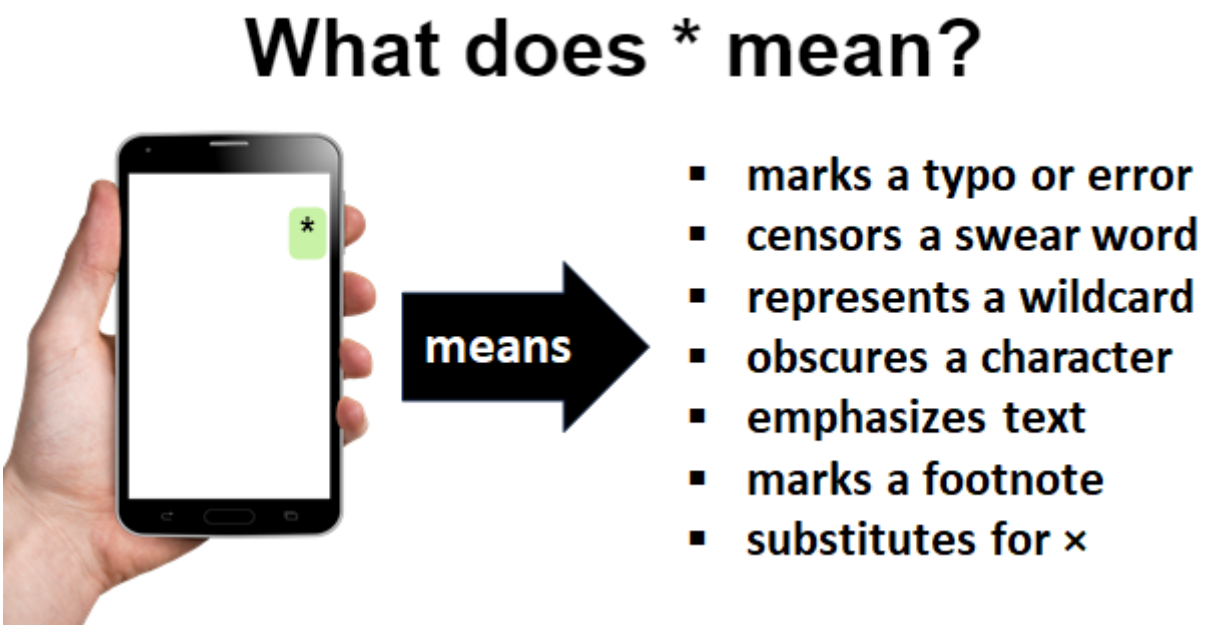
- I need an answer *today* please.
  (This displays **today** in bold.)

(6) Textual Reference or Footnote

In written documents, an asterisk is often used to indicate a footnote or a reference point. If an additional explanation or a citation is needed, an asterisk is placed at the end of word to be explained, and the corresponding text or citation is placed at the bottom of the page.

(7) Mathematical Operations

In mathematical operations, especially in computer programming and on calculator keypads, an asterisk is used as the symbol for multiplication. For example, **5 * 6** means "5 multiplied by 6". Incidentally, we have the codes for a proper times symbol (×) if you don't want to use an asterisk or a lowercase x.



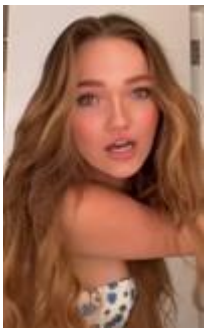
WHAT DOES POV MEAN?

POV means "Point of View." It is often seen on social media (especially TikTok) as #pov. There are two main ways that #POV is used:

POV = In My Opinion

In comment sections, discussion boards, and in general text-based chat, POV means "this is my point of view" or "in my opinion." In this context, it is essentially a caveat to reduce the number of comments from haters. It highlights the right of the poster to say what they feel, even if it might offend some. For example:

- Meat is murder! #POV.
- Lettuce lives matter too! #POV.



Here is a real example. TikTok user **Alyssa McKay (@alyssamckayyy)** received over five million likes for her video "wear your masks." Her video was a satirical observation of how rich girls partied during the Coronavirus pandemic. The introduction of her video carried the #pov caveat, letting viewers know that this was simply her opinion. In essence, her POV meant "I am entitled to my opinion, and here it is." It was included for its connotation of "I'm **not** telling **you** what to think. I am simply expressing what **I** think." This use of POV is designed to disarm dissenters who might otherwise contest a poster's observation. Most dissenters know that they cannot contest someone's right to express an opinion.

POV = What Is Seen From the Perspective of the Camera or Main Protagonist

In this context, POV is usually used as an adjective (e.g., POV camera). It describes either a first-person perspective (the view of the narrator) or a third-person perspective (the view of the main character)[1]. It is particularly common in sports broadcasting. For example, during sports matches (such as football, hockey, soccer, etc.), the POV camera shows the game from the perspective of a particular player. In Formula 1 motor racing, viewers can see the race from a driver's dashboard camera, which gives a third-person POV experience.

First Person or Third Person POV? With a driver's dashboard camera, if the driver were also the race commentator, the camera view would be a first-person POV. However, as is the norm, the commentator is track side. This means the camera shot is a third-person POV. The third-person POV aspect is also used in the film industry, when a scene is filmed so the viewer experiences events through the eyes a certain character. This is often mistakenly called the first-person perspective, but it is only the first-person perspective if the person through whose "eyes" you are seeing events is

also the narrator. The porn industry is one sector of the film industry that does use first-person POV cameras.

WHAT DOES IB MEAN?

IB means "Inspired By" and "International Baccalaureate." Here is more information about each of these definitions of IB.

Inspired By

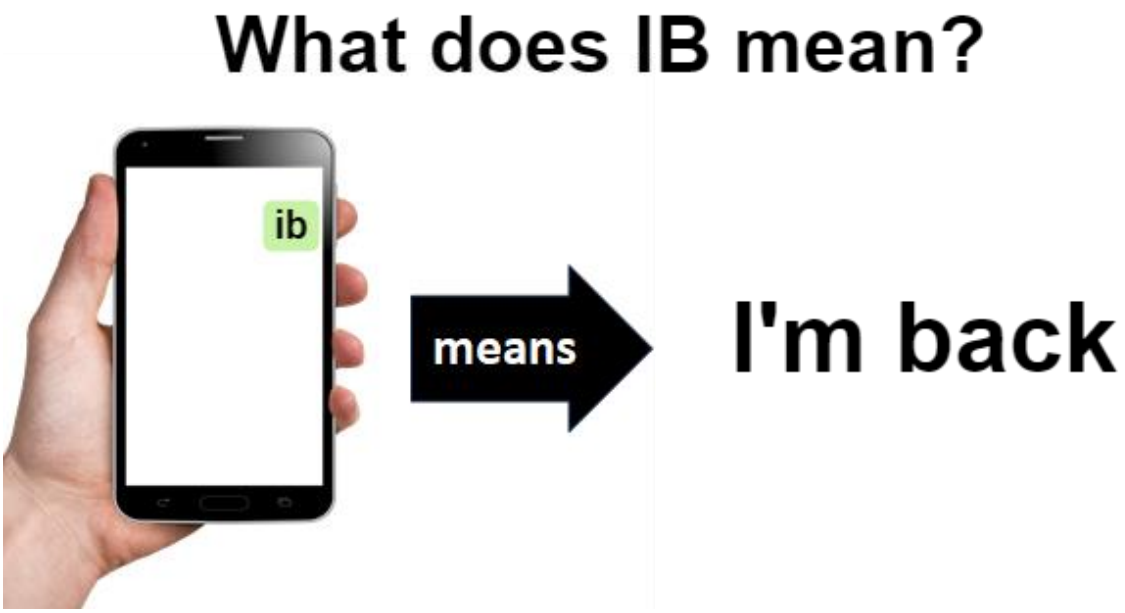
On social media apps such as TikTok, IB usually means "Inspired By." It is used to tag and give credit to another user or trend that has inspired the poster to make their own video.

IB is used similarly to DC, when DC means "dance credit."

International Baccalaureate

IB is also used to refer to the International Baccalaureate, a full-time education programme for students aged 16 to 18 years that takes two years to complete. IB students take six subjects, plus a "Theory of Knowledge" course. They must also write an "Extended Essay."

When I write **IB**, I mean this:



TOP CYBERSECURITY TERMS TO LEARN

1. Authentication

The process of identifying a user's identity, making sure that they can have access to the system and/or files. This can be accomplished either by a password, retina scan, or fingerprint scan, sometimes even a combination of the above.

2. Botnet

A combination of the words "robot" and "network", a botnet is a network of computers that have been infected with a virus, and now are working continuously in order to create security breaches. These attacks come in the form of Bitcoin mining, sending spam e-mails, and DDoS attacks (see below).

3. Data Breach

The result of a hacker successfully breaking into a system, gaining control of its network and exposing its data, usually personal data covering items such as credit card numbers, bank account numbers, Social Security numbers, and more.

4. DDoS

The acronym stands for Distributed Denial of Service and is a favorite Black Hat tool. Using multiple hosts and users, hackers bombard a website with a tidal wave of requests to such an extent that it locks up the system and forces it to temporarily shut down.

5. Domain

A series of computers and associated peripherals (routers, printers, scanners), that are all connected as one entity.

6. Encryption

Coding used to protect your information from hackers. Think of it like the code cipher used to send a top-secret coded spy message.

7. Exploit

A means of attack on a computer system, either a series of commands, malicious software, or piece of infected data. Note that in this context, "exploit" is a noun, not a verb, as in "The hacker used a malware exploit to gain access to the credit card's server."

8. Firewall

Any technology, be it software or hardware, used to keep intruders out.

9. Hacker, Black Hat

Any hacker who attempts to gain unauthorized access to a system with the intent to cause mischief, damage, or theft. They can be motivated by greed, a political agenda, or simply boredom.

10. Hacker, White Hat

A hacker who is invited to test out computer systems and servers, looking for vulnerabilities, for the purposes of informing the host of where security needs to be buffed up. They are benign hackers, personifying the old axiom "It takes a thief to catch a thief". Sometimes called "ethical hackers."

11. Malware

A portmanteau of "malicious" and "software", describing a wide variety of bad software used to infect and/or damage a system. Ransomware, worms, viruses, and trojans are all considered malware. It most often delivered via spam emails.

11. Man in the Middle Attack

An attack on the "middleman", in this case, defined as the Wi-Fi system that connects users to the Internet. Hackers who commit Man in the Middle Attacks can break the Wi-Fi's encryption and use this as a means of stealing your personal data because they're now in the system.

12. Phishing

A scam where a hacker poses as a legitimate business or organization (especially credit card companies, banks, charities, Internet providers, other utilities) in order to fool the victim into giving them sensitive personal information or inducing them to click a link or attachment that ends up delivering malware. Some of these schemes are extremely well done, others are sloppy and amateurish and can be spotted with just a little extra vigilance.

13. Ransomware

A form of malware that hijacks your system and encrypts your files, denying you access to them until you send money to unlock everything. In other words, it kidnaps your computer and holds it for ransom, hence the clever name.

14. Spoofing

Sadly, this has nothing to do with Weird Al Yankovic doing a parody version of a popular song. Rather, it's when a hacker changes the IP address of an email so that it seems to come from a trusted source.

15. Spyware

A form of malware used by hackers to spy on you and your computer activities. If a mobile device such as a smartphone is infected with spyware, a hacker can read your text messages, redirect your phone calls, and even track down where you are physically located!

16. Trojan Horse

Yet another form of malware, this one a misleading computer program that looks innocent, but in fact allows the hacker into your system via a back door, allowing them to control your computer.

17. Virus

Malware which changes, corrupts, or destroys information, and is then passed on to other systems, usually by otherwise benign means (e.g. sending an email). In some cases, a virus can actually cause physical damage.

18. VPN

An acronym standing for Virtual Private Network, a VPN is a method of connecting a series of computers and devices in a private encrypted network, with each user's IP address being replaced by the VPN's IP address. Users get Internet anonymity, making it difficult for hackers to attack.

19. Worm

Malware that can reproduce itself for the purposes of spreading itself to other computers in the network. Particularly nasty, worms can either be simply a means of slowing down a system by eating up resources, or by committing exploits such as installing back doors or stealing data.

20. Cloud

You already utilize cloud computing if you use Gmail for email, Google Drive for document storage, or Netflix to stream your favorite movies. These services are all built

on the cloud. cloud computing is providing on-demand services over the internet.If you want to run a business and you need to keep user data and you decide to do it on a hard drive, you will need a lot of storage space and a tech staff for it.Cloud service providers like Microsoft Azure, AWS, and Google Cloud, which offer on-demand services and are both cost-effective and low-risk in terms of security, make this procedure simple.

21. Software

It is a group of applications that instruct a computer to carry out a task. In which Users can download and use a package that contains these instructions.A hard drive or magnetic diskette are common examples of external long-term memory devices where software is often kept. When it is in use the computer reads the program from the storage device and temporarily stores the instructions in random access memory (RAM). Google Chrome is one such example of application software.

22. IP Address

The world IP stands for Internet Protocol. An IP address is a series of numbers allocated to computers routers servers, and pretty much anything connected to the Internet, including websites. It functions very similarly to a standard address, allowing users to find any system or device on the global network by specifying its location

23. Rootkit

A rootkit is a collection of programs or software tools that allow hackers to remotely access and control a computer or network. Although rootkits do not directly damage users, they have been used for other purposes that are legal, such as remote end-user support. However, the majority of rootkits either leverage the system for additional network security attacks or open a backdoor on the targeted systems for the introduction of malware, viruses, and ransomware. Typically, a rootkit is installed without the victim's knowledge via a stolen password or by taking advantage of system flaws. In order to avoid being picked up by endpoint antivirus software, rootkits are typically employed in conjunction with other malware.

24. BYOD (Bring Your Own Device)

Bring Your Own Device (BYOD) is a company policy that permits, encourages, or mandates employees to access enterprise systems and data using their own personal devices, such as laptops, tablets, and smartphones, for work-related activities.

25. Pen-testing

An approach to security evaluation where manual exploitations and automated techniques are used by attack and security professionals. Only environments with a solid security infrastructure should employ this advanced kind of security evaluation with a mature security infrastructure. Penetration tests can disrupt operations and harm systems because they employ the same equipment, procedures, and methodology as malicious hackers

26. Social Engineering

Instead of breaking in or utilizing technical hacking techniques, social engineering is a growingly popular way to access restricted resources. This strategy relies on user manipulation and human psychology. An employee might get an email from a social engineer purporting to be from the IT department in order to deceive him into disclosing private information rather than trying to uncover a software weakness in a company system. Spear phishing assaults are built on a foundation of social engineering.

27. Clickjacking

While someone is tricked into clicking on one object on a web page when they want to click on another, this practice is known as clickjacking. In this manner, the attacker is able to use the victim's click against them. Clickjacking can be used to enable the victim's webcam, install malware, or access one of their online accounts.

28. Deepfake

A piece of audio or video that has been altered and changed to make it seem authentic or credible. The most perilous aspect of the prevalence of deepfakes is that they can easily convince individuals into believing a particular tale or idea, which may lead to user behavior that has a greater impact on society at large, such as in the political or financial spheres.

29. Multi-Factor Authentication

Multi-factor authentication (MFA), also referred to as two-factor authentication, makes it more difficult for hackers to access your account by requiring you to provide at least two different credentials. MFA requires a second factor to confirm your identity in addition to your username and password, such as a one-time security code, a fingerprint scan, or a face recognition scan.

30. User Authentication

A technique to prevent unauthorized users from accessing sensitive data is user authentication. For instance, User A can only see data that is relevant and cannot view User B's sensitive information.

31. Antivirus

The newest virus detection technology is integrated into anti-virus systems to shield users against viruses, spyware, trojans, and worms that can damage computer hardware through email or web browsing.

32. Ethical Hacking

With the owner's permission, breaches the network to obtain sensitive information—completely legal. Typically, this technique is used to check for infrastructure weaknesses.

33. Cyber Attack

Any attempt to breach a logical environment's security boundary. An attack may concentrate on intelligence gathering, disrupting company operations, exploiting weaknesses, keeping track of targets, stopping work, obtaining value, harming logical or physical assets, or leveraging system resources to enable assaults against other targets.

34. Network

Two or more computers connected together to share resources (such printers and CDs), exchange files, or enable electronic communications make up a network. A network's connections to its computers can be made by cables, phone lines, radio waves, satellites, or infrared laser beams.

35. Internet of Things

The phrase "Internet of Things" (IoT) refers to commonplace items that are connected to the internet and are capable of autonomously collecting and transferring

data without requiring human input. Any physical thing that can be given an IP address and can transport data is considered to be a part of the Internet of Things, which also includes traditional computers, vehicles, CCTV cameras, household appliances, and even people.

36. Penetration Test

A penetration test, commonly referred to as a pen test, simulates a cyberattack on your computer system to look for weaknesses that could be exploited.Pen testing involves attempting to get into any number of application systems (such as frontend/backend servers, APIs, etc.) in order to find security holes like unsanitized inputs that are vulnerable to code injection attacks.

KEY CYBER ACRONYMS TO KNOW

With all the technical aspects of cybersecurity, some cybersecurity terms and acronyms might seem like a foreign language. With some context, though, you may find that these acronyms are not only straightforward, but they're also necessary ingredients for your success.

Advanced persistent threat (APT)

An advanced persistent threat is a continuous, targeted cyberattack that uses sophisticated methods to carry out cybercrime or espionage. These attacks involve multiple phases and can remain undetected for long periods of time. APTs are different from traditional cyberattacks in that they can take up to years of planning and execution.

Given the complexity and extended planning involved in APTs, these attacks are often orchestrated by state-sponsored actors. This elevates APTs to among the most critical cybersecurity threats, especially for MSPs. Underestimating them would be a costly oversight, necessitating rigorous preventive measures.

Business email compromise (BEC)

Business email compromise is a form of email phishing that occurs when a threat actor poses as someone like a coworker. When successful, BEC can facilitate malicious activity like data theft or ransom schemes.

Unlike other cyberattacks that often rely on automated defenses, BEC necessitates tailored mitigation strategies, such as comprehensive user education. The best course of action involves training all users to identify the various forms BEC can take, thereby strengthening your organizational defenses.

Chief information security officer (CISO)

The chief information security officer is a senior-level executive responsible for an organization's data and information security. This role also involves realizing security goals in conjunction with digital transformation and business enablement. More recently, CISOs have taken up the responsibility of managing cyber risk.

CISOs can also act as "coaches" in the sense that they help organizations and educate users about how to manage cyber risk. The CISO role is crucial in an effective cybersecurity strategy, so any candidates you work with for this role should be thoroughly vetted.

Cyber threat intelligence (CTI)

Cyber threat intelligence is the collection, analysis, and integration of information about threats to an organization's digital infrastructure. To conduct CTI, you can source data from many types of intelligence, from human to open source.

Having CTI in place can help you avoid cyberattacks and even improve your cybersecurity management procedures. The more CTI is conducted, the more you know about the potential threats you're up against. ConnectWise's CRU (cyber research unit) is an example of a CTI resource MSPs can integrate to enhance their own offerings.

Distributed denial of service (DDoS)

Distributed denial of service is a type of cyber attack that overwhelms a server, network, or service with a flow of malicious traffic or data. That traffic can come from multiple sources, including botnets, and it can easily overwhelm a target.

DDoS attacks can stop operations in their tracks by leaving servers and networks unusable, so quick action is important in the case of a DDoS attack. Failing to act quickly may result in service denial or operational disruptions.

Data loss prevention (DLP)

Data loss prevention is a combination of technology and processes used to protect data by monitoring traffic. With cyberattacks more prevalent than ever, organizations need to keep a closer—and constant—eye on their data with DLP.

DLP keeps track of the flow of all data to identify sensitive information exiting the network, as a leak or attack can happen at any moment. When considering DLP for your organization, keep in mind that DLP should be easy to use and record information ranging from the people involved all the way to what actually happened. In addition, business continuity and disaster recovery (BCDR) is a set of solutions that can make sure that your clients' data is protected in a disaster or downtime scenario.

Endpoint detection and response (EDR)

Endpoint detection and response tools monitor, detect, and respond to irregular activity on any endpoint device. While irregular activity isn't always a sign of an attack, EDR provides visibility for more accurate analysis and threat mitigation in the case of suspicious activity.

EDR also improves firewall functionality, especially with many devices spread out away from a data center. The key is detecting these spread-out devices using EDR, which better protects them from cyberattacks. Combine this with other cybersecurity tools like a SOC, and you have a solid line of defense against cyberattacks.

Governance, risk management, and compliance (GRC)

Governance, risk management, and compliance (GRC) is not merely a strategy, but a holistic framework that helps organizations protect their data while operating efficiently and within the bounds of the law. The three components are interrelated yet distinct:

- Governance ensures that organizational activities align with business objectives and stakeholder expectations.
- Risk management involves identifying, assessing, and mitigating risks that could hinder the organization's operations.
- Compliance ensures adherence to both external regulations and internal policies.

Properly implemented GRC creates a comprehensive roadmap for cybersecurity and data management, offering organizations an integrated approach to protect their assets and maintain regulatory compliance. The framework becomes essential for organizations lacking the resources to continually monitor and protect their vast array of data.

Identity and access management (IAM)

Identity and access management refers to a framework of technologies and policies designed to grant access to resources. More specifically, IAM ensures only the appropriate users have access to sensitive resources. IAM does this by letting

organizations use zero-trust accounts in which employees can only access data necessary to their roles.

As remote work and SaaS become more common, granting access to individual users on an as-needed basis becomes necessary. Denying access is equally important—especially if you want to keep your data as secure as possible.

Incident response (IR)

Incident response is how an organization handles the aftermath of a cyberattack. Incident response is necessary for any organization, as attacks and security breaches can occur at any time. Proper IR can help you mitigate the impact of incidents like DDoS or phishing attacks or even events like a damaged device.

With IR, your goal should be to expect the unexpected, and an IR plan can help you stay prepared in the case of an incident. Managed incident response services can also help provide another line of defense and 24/7 real-time monitoring.

Managed detection and response (MDR)

Managed detection and response is an often outsourced service that employs experts and technology to find, monitor, and respond to threats. MDR can help reduce threats in your organization—without having to hire extra staff. MDR also lets you address threats quickly, monitoring potential problems in real time.

Managed security service provider (MSSP)

A managed security service provider (MSSP) specializes in overseeing and administering an organization's security measures such as VPNs, firewalls, and intrusion detection systems. Unlike a MSP, an MSSP has a focused expertise in security-related services.

As the threat landscape evolves, the MSSP's role grows increasingly critical in navigating complex cybersecurity challenges. These providers leverage threat intelligence reports to stay ahead of emerging cybersecurity trends and threats. Across various security layers, including Managed Detection and Response (MDR), MSSPs add substantial value to organizations dealing with intricate security needs. In some cases, MSPs can build an MSSP inside their own service as well to increase their ability to service clients.

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology officially promotes "U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." A major part of the NIST's reputation is its cybersecurity framework, which outlines how private companies should handle cyberattacks. The NIST cybersecurity framework is only the U.S.'s primary cyber framework, and there are different frameworks for different countries, such as the Essential Eight for Australia or Cyber Essentials for the U.K.

Open-source intelligence (OSINT)

Open-source intelligence is information from public data that an organization collects, analyzes, and reports on. Organizations can take what they learn from this intelligence analysis, parse the data, and apply it to their security protocol.

OSINT is helpful to any organization, partly because the information is free and easy to access as a member of the public. While other, less overt sources may suit your needs better at times, OSINT is a reliable source of information when you need to make a decision in a short amount of time.

Recovery time objective/recovery point objective (RTO/RPO)

Recovery time objective refers to the way an organization moves forward from an incident. More specifically, RTO is the amount of time it takes to recover affected systems and data after something like an attack or security breach. Your RTO goal should be the shortest amount of time possible, but just having an RTO and trying to adhere to it can help you avoid downtime or worse.

A recovery point objective is the point in time at which your organization needs to restore systems and data. Your RPO should take into account how much data your organization can afford to lose, and you should attempt to recover as much data as possible.

Secure access service edge (SASE)

Secure Access Service Edge is a unified cloud-native security framework that integrates network security functions with wide area networking (WAN) capabilities.

It offers a comprehensive solution to protect and manage data traffic for distributed, cloud-first organizations.

By providing security and networking through the cloud, SASE mitigates various security challenges and threats. It allows users to securely connect to an organization's devices and systems, irrespective of the tools in use or physical location.

One of the key advantages of SASE is its ability to enable secure access without adding extra risk to the organization. This framework is becoming increasingly crucial as business processes continue to shift towards cloud environments and as seemingly straightforward tasks grow in complexity.

Security information and event management (SIEM)

Security information and event management is a system or solution that aggregates large amounts of data regarding threat investigations. Because of this, SIEM is crucial for any organization looking to analyze and mitigate threats.

SIEM provides in-depth insights in real time, making it a powerful tool in any organization’s security arsenal. As far as detecting and responding to security events, you shouldn’t overlook SIEM to provide a centralized view of all security activity.

Security operations center (SOC)

A security operations center is a central location or team tasked with monitoring and responding to security threats and potential breaches. SOC teams use a variety of tools and intelligence to assess incidents and deal with them accordingly.

A SOC offers around-the-clock protection, so problems get resolved quickly, and recovery time doesn’t slow your organization to a halt. For a centralized security hub, you can’t do much better than an efficient, qualified SOC.

Single sign-on (SSO)

Single sign-on is a system that lets users authenticate themselves through multiple devices and applications using a single set of credentials. SSO streamlines the login process for all users and adds a layer of security.

So, not only is SSO faster than many other sign-on methods, but it’s also more secure. SSO often finds use alongside multi-factor authentication (MFA), increasing security in the event of a compromised SSO log-in.

Zero trust network architecture (ZTNA)

Zero trust network architecture refers to the practice of only granting network access to users who need it to complete a specific task. ZTNA also implies that network access doesn’t equate to full access and users can’t typically access the entire network.

PREPARE YOUR PROJECTS ON LINGUISTIC ASPECTS OF INTERNET COMMUNICATION

This test aims to assess your understanding of the linguistic features and conventions used in online communication. It covers various aspects.

1. Vocabulary and Register:

a) Identify the specific registers used in online communication platforms like social media, forums, and email;

b) explain the difference between formal and informal register and give examples of each in online communication;

c) define and provide examples of slang, jargon, and abbreviations commonly used online;

d) analyze how emojis, emoticons, and other nonverbal cues convey meaning online.

2. Syntax and Grammar:

a) identify the characteristic sentence structures and grammatical patterns used in online writing;

b) explain the use of fragmentation, ellipsis, and other non-standard grammatical features in online communication;

c) discuss the role of punctuation in conveying meaning and tone online;

d) analyze the impact of autocorrect and predictive text on online grammar and style.

3. Discourse and Pragmatics:

a) define and identify the different types of discourse markers used in online communication, like hedges, boosters, and stance markers;

b) explain how participants in online communication negotiate turn-taking and manage discourse coherence;

c) analyze how politeness strategies are employed in online communication to achieve social goals;

d) discuss the impact of anonymity and online disinhibition on online discourse behavior.

4. Sociolinguistics:

a) identify the different linguistic varieties (e.g., dialects, accents) used in online communication;

b) explain how language reflects social identity and group membership in online communities;

c) discuss the role of language in online power dynamics and social hierarchies;

d) analyze how language can be used for social exclusion and discrimination online.

5. Multilingualism and Global Communication:

a) describe the challenges and opportunities of online communication in a multilingual world;

b) explain how code-switching and code-mixing are used in online communication;

c) discuss the role of translation tools and technologies in online communication;

d) analyze the impact of globalization on online language usage and norms.

Instructions:

- Answer all questions to the best of your ability.
- Provide examples to support your answers.
- Use clear and concise language.
- You can use your own knowledge and research to answer the questions.

REFERENCES

1. Crystal, D. (2011). Internet linguistics: A student guide. Routledge.
2. Jones, R. (2013). The language of the internet. Cambridge University Press.
3. Baron, N. S. (2008). Always on: Language in an online and mobile world. Oxford University Press.
4. Danet, B., Herring, S. C., & Gergen, M. (Eds.). (2013). The Routledge handbook of language and social media. Routledge.
5. https://www.cyberdefinitions.com/definitions/123.html
6. https://www.connectwise.com/blog/cybersecurity/essential-cybersecurity-acronyms
7. https://www.simplilearn.com/top-cybersecurity-terms-you-need-to-know-article