КАЗАНСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

ИНСТИТУТ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ, ИСТОРИИ И ВОСТОКОВЕДЕНИЯ

Кафедра английского языка в сфере высоких технологий

Г.Ф. ВАЛИЕВА, Д.А. ЯРУЛЛИНА

ENGLISH FOR INFORMATION SECURITY

Учебное пособие

Казань – 2015

Принято на заседании кафедры английского языка
в сфере высоких технологий
Протокол № 1 от 17 сентября 2015 года

Рецензенты:
кандидат филолологических наук,
доцент кафедры английского языка в сфере высоких технологий КФУ
Д.Ф. Хакимзянова;
кандидат филолологических наук,
начальник управления международных связей КГЭУ,
доцент **Г.Т. Нежметдинова**

Валиева Г.Ф., Яруллина Д.А.
English for Information Security / Г.Ф. Валиева, Д.А. Яруллина. – Казань: Казан. ун-т, 2015. – 120с.

Данное пособие предназначено для студентов, обучающихся по специальности «Информационная безопасность» (10.03.10, 10.03.01), и содержит задания формата IELTS, что позволяет подготовиться к сдаче международного экзамена на базе профессионально-ориентированного материала, отработку четырех аспектов (Чтение, Аудирование, Говорение и Письмо), аутентичные тексты и аудиоматериалы, направленные на углубление и расширение профессиональной лексики.

© Валиева Г.Ф., Яруллина Д.А., 2015
© Казанский университет, 2015

INTRODUCTION

This textbook is dedicated to students of the Information Security specialization.

The purpose of the textbook is to form profession-oriented competences of students, enlarge their professional vocabulary and prepare for IELTS exam.

“English for Information Security” consists of 7 units, each of them contains all 4 aspects that are Speaking, Reading, Listening and Writing. As well as these aspects, there is a range of material which can be used according to students’ needs and time available. One can find useful vocabulary with definitions and transcriptions to practice pronunciation. Also some useful tips are presented to help fulfil the IELTS tasks. Students are given useful language to keep changing the phrases they use to express their opinion, agreement, disagreement, to hold and take part in a meeting and to make presentations.

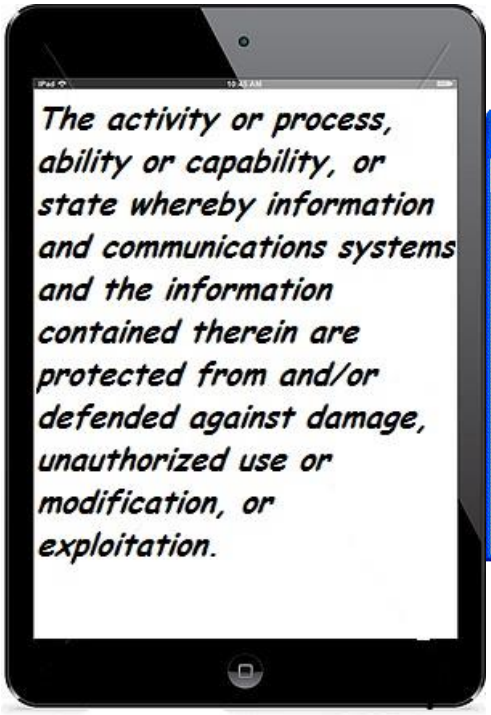
All texts are adapted from scientific articles and refer to students’ specialization. All recordings for Listening are taken from interviews with representatives of such organizations as Kaspersky Lab.

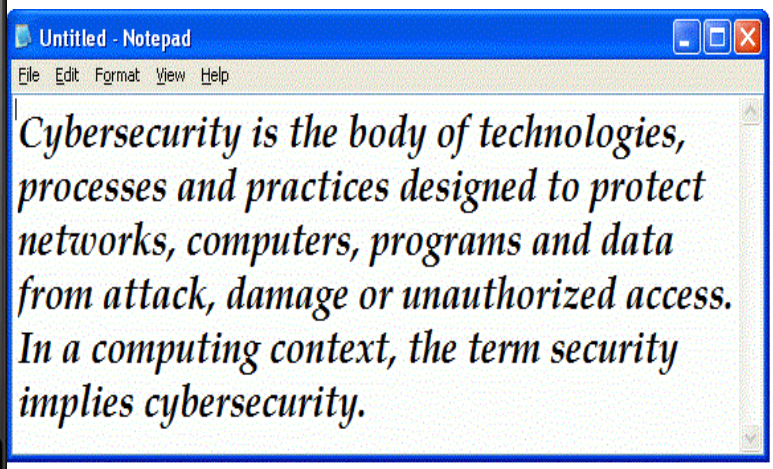
CONTENT

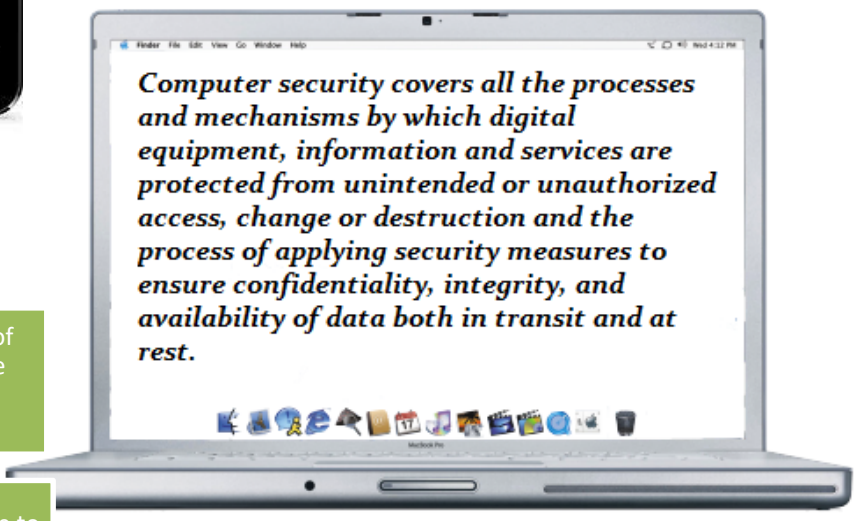
UNIT 1 CYBERSECURITY CAREER

Speaking

1. What is cybersecurity? Try to work out your definition using key words in the picture.
2. Choose the best definition for cybersecurity. Which one is similar to yours?







3. Discuss the topics:

a. 10 pluses of working in the sphere of cybersecurity

b. 10 minuses of working in the sphere of cybersecurity

c. What traces of character should a good specialist have?

d. Would you like to work in the field of cyber secuirity?

4. Imagine that you are working for the big company as a network security manager. Try to decribe your simple working day.

to be your own boss	a dead-end job	to do a job-share	a good team player	full-time	a heavy workload
a high-powered job	holiday entitlement	job satisfaction	manual work	maternity leave	to meet a deadline
a nine-to-five job	one of the perks of the job	part-time	to run your own business	to be self-employed	sick leave
to be stuck behind a desk	to be/get stuck in a rut	to take early retirement	temporary work	voluntary work	to be well paid
		working conditions	to work with your hands		

Reading 1 Vocabulary and Pronunciation

1. What are the main principles of cybersecurity career?

Note: Words in tasks are given in initial form!

2. Match the following transcriptions, **A-Q**, with the highlighted words and pronounce them.

A /ˈækjʊmən/

B /ˈmɪtɪgeɪt/

How to prepare for a cybersecurity

Cybersecurity breaches affect businesses large and small, and the annual cost of **computer- and network-based crimes** worldwide is estimated to be more than $400 billion. As organizations increasingly use data networks for business, commerce and the transfer of sensitive information, the risks multiply, as do the needs for qualified cybersecurity professionals.

(ISC)² Foundation and University of Phoenix set out to develop actionable

C /ˈkɒmɜːs/

D /dʌb/

E /əˌkrɛdɪˈteɪʃ(ə)n/

F /kɔ̃petɑ̃s/

G /ˈkruːʃ(ə)l/

H /ˈwɜːkfɔːs/

I /ˈvʌln(ə)rəb(ə)l/

J /əbˈteɪn/

K /ˈpɑːθweɪ/

L/ˈsteɪkˌhəʊldə/

M /ˌraʊndˈteɪb(ə)l/

N /ɪnˈtɜːnʃɪp/

O /ˌsaɪbəsɪˈkjʊərətɪ/

P /kəˈrɪkjʊləm/

Q /ʃɪft/

3. Read the article once. Try to work out the meaning of the highlighted words. Then match them with their definitions a-r.

a._____ *noun* ways of protecting computer systems against threats such as viruses.

b._____ *noun* a track that a person can walk along

c._____ *noun* the activities involved in buying and selling things.

recommendations to prepare students for cybersecurity careers-delivering a report on it, dubbed Cybersecurity Workforce Competencies: Preparing Tomorrow's Risk-Ready Professionals.

The research identifies three education-to-workforce gaps that leave employers and organizations particularly vulnerable: competency, professional experience and education speed-to-market.

The report is based on a year of research, including analysis of industry competency models and labor statistics, which led to a national focus group, followed by the roundtable with industry leaders.

"The growing frequency, sophistication, and costs of cyberattacks threaten business continuity for organizations of all sizes," said Julie Peeler, director of the (ISC)² Foundation, in a statement. "Preparing and attracting the next generation of cybersecurity professionals is critical to the health of the economy and businesses globally."

Roundtable participants say the following actions by industry and education leaders can have the most immediate impact on closing the gaps:

1. Encouraging problem-based learning via case studies and labs;

d._____ *noun* a period of time during which someone works for a company or organization in order to get experience of a particular type of work

e._____ *verb* to get something, especially by asking for it, buying it, working for it, or producing it from something else

f._____ *noun* the subjects studied in a school, college, etc. and what each subject includes

g._____ *verb* to give something or someone a particular name, especially describing what you think of it, him, or her

h._____ *noun* an important skill that is needed to do a job

i._____ *noun* a person such as an employee, customer, or citizen who is involved with an organization, society, etc. and therefore has responsibilities towards it and an interest in its success

2. Offering meaningful internships for cybersecurity degree completion; and
3. Developing curriculum and career resources that are informed by cybersecurity employers.

"The multi-faceted cybersecurity field demands a strong workforce comprised of individuals who can adapt to constant shifts in the sector," said Dennis Bonilla, executive dean of University of Phoenix College of Information Systems and Technology, in a statement. "The industry increasingly needs professionals who possess both technical skills and strong business acumen, and curriculum is shifting to reflect these dynamics. Relevant education and training aligned to industry requirements are crucial to protecting and growing business infrastructure in the US and globally."

"Having qualified cybersecurity professionals is critical in all industries," added Peeler. "Employers must act quickly to close workforce gaps and mitigate the risks that threaten enterprises. The roundtable report by the (ISC)² Foundation and University of Phoenix provides practical recommendations to key stakeholder groups that must work together to build the cybersecurity talent pipeline."

The report offers the following tips for

j._____ *noun* a group of workers who do a job for a period of time during the day or night, or the period of time itself

k._____ *noun* skill in making correct decisions and judgments in a particular subject, such as business or politics

l._____ *adj* extremely important or necessary

m._____ *noun* the group of people who work in a company, industry, country, etc.

n._____ *adj* able to be easily physically, emotionally, or mentally hurt, influenced, or attacked

o._____ *noun* involving several people who talk about something as equals

p._____ *verb* to make something less harmful, unpleasant, or bad

q._____ *verb* to get something

students interested in cybersecurity careers, and for employers struggling to fill job openings:

For Students

1. _____Obtain the relevant certifications that can help enhance employability.
2. _____Many jobs in this field may require a security clearance. Be mindful that past actions could affect your eligibility.
3. _____Demonstrate interest in the field by developing professional relationships. Stay abreast of industry trends by joining an association.
4. _____Seek opportunities to demonstrate your expertise by co-presenting at industry conferences and completing relevant projects.
5. _____Look for ways to obtain professional experience through internships, job shadowing or work-study jobs.

For Employers:

6. _____Offer internships and participate in higher education curriculum advisory boards.
7. _____Partner with middle schools and high schools to increase awareness of cybersecurity career opportunities.
8. _____Remove barriers to entry-

4. Read the article again and choose the most suitable topic sentence, i-xi, for each paragraph, 1-11, from the list below.

i Champion cybersecurity careers.
ii Get certified.
iii Hire interns.
iv Understand clearance requirements.
v Encourage professional experience.
vi Steer clear of clearances.
vii Promote partnerships.
viii Get involved.
ix Build a portfolio.
x Seek opportunities.
xi Engage with educators.

level jobs by decoupling tasks that require a security clearance. Many applicants, such as non-U.S. citizens, may be unable to obtain a security clearance readily.

9. _____Develop partnerships with higher education institutions to support curriculum development, career networking, and internships.

10. _____Develop and fund programs that provide industry experience to students. Ensure programs meet the National Security Agency's Centers of Academic Excellence accreditation requirements, and seek accreditation approval for such programs.

11. _____Internships are a viable step to employment and demonstrate the value of entry-level experience as a pathway to a career.

(adapted from http://www.infosecurity-magazine.com)

Listening and Speaking

1. What kind of IT professions do you know?
2. You are going to listen to a part of a TV program about cybersecurity.

Questions 1-5

Complete the notes below.

Write **NO MORE THAN THREE WORDS** for each answer:

Before you listen, try to predict what the answer will be

1. Almost any movie today dealing with national security includes a dramatic _____ scene.
2. It's growing importance, because now we are having _____
3. A lot of our confidential data we _____, they wouldn't be able to_____ it.

The recording will be played ONCE only!

4. Students who graduated computer science program are well prepared to _____ and _____.
5. They need to get _____, they need to get training, and they even have to get certificates.

Questions 6-10

Choose the correct letter **A**, **B**, **C** or **D**.

The words you read will probably not be the same as the ones you hear, so be prepared to listen to synonyms or paraphrases.

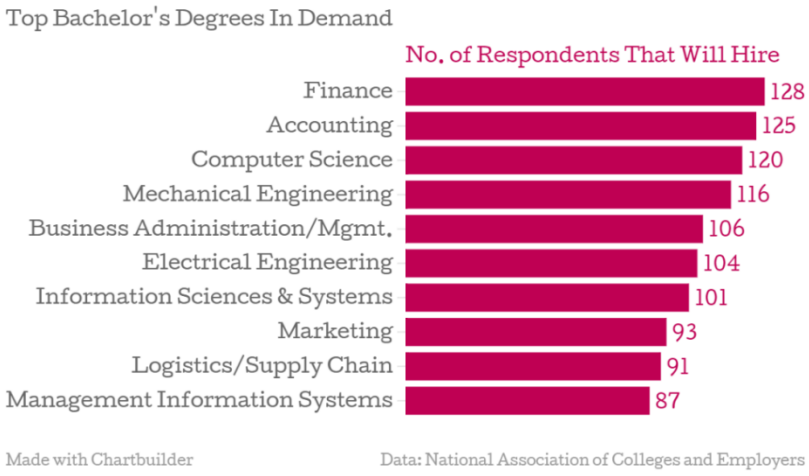
6. Why is cybersecurity so important?
   - **A.** It's fashionable
   - **B.** It's interesting for people
   - **C.** It's necessary because people use technological devices
   - **D.** It's necessary for proper office work
7. Why is information being decrypted?
   - **A.** To gain access to it
   - **B.** To delete it
   - **C.** Not to be able to read it
   - **D.** To make its usage easier.

Glossary:

High drama *noun* High drama usually refers to acting in an overly dramatic way.
Flow through *verb* to affect someone or something
Encrypt *verb* To alter (data) using a mathematical algorithm so as to make the data unintelligible to unauthorized users while allowing a user with a key or password to convert the altered data back to its original state.

8. What did Professor Ming do for cybersecurity?
   A. He opened special courses
   B. He opened IT university
   C. He invented new program
   D. He invented artificial intelligence
9. Who usually tends to get higher job offers?
   A. Postgraduates in computer science
   B. Students of computer science
   C. People who work in office
   D. People who have PhD
10. How many students choose technical major at university?
   A. A lot
   B. Not much
   C. A half
   D. None

3. Look at the graph. Do you agree with it? Make analysis based on the graph, try to answer the following questions:



A. Why do you think jobs in Finance are more demanded?

B. Analyze your country. Does this graph suit for it?

4. Divide into groups. Each group is to choose one degree in the chart. You are to decide why people need your job. Practice using “Useful language”.

Useful language	I see your point, but I think…
In our opinion…	Yes, I understand, but my opinion is that…
We (don’t) think that…	That’s all very interesting, but the problem is that…
The way we see it…	I’m afraid I can’t quite agree with your point…
If you want our honest opinion…	I think I’ve got your point, now let me respond to it…
According to the other side/our opponents…	We can see what you’re saying. Here’s my reply…
As far as I'm concerned…	
Our position is the following…	

Reading and Speaking 2

Do you think there is any difference between cybersecurity and information security? Prove your point of view.

Questions 1-6

Do the following statements agree with the information given in the text? Write **T**(true), **F**(false), **NG**(not given) next to the sentences 1-6.

Cybersecurity vs. Information Security.

Hollywood exerts influence over many areas of modern life, even down to how people think about and refer to different types of work. Movies and television shows often depict the professionals who deal with computer security as Cybersecurity or information security specialists. These terms are often used in the entertainment industry in a way that implies that they are identical, which can create confusion for those who are interested in pursuing a career in one of these exciting and growing fields. Prospective

1. Cybersecurity is a term made by Hollywood movies
2. Cybersecurity and information security are different things
3. Cybersecurity implies searching information in the internet
4. There is only one job in cybersecurity field.
5. It's not important to distinguish information and cyber security.
6. There is similarity between information and cyber security.

Questions 7-12

Choose **NO MORE THAN THREE WORDS** from the passage for each answer.

7. Student has to distinguish information and cyber

students need to be able to distinguish between these two professions in order to determine which career path is the best fit.

Cybersecurity

Cybersecurity is the use of various technologies and processes to protect networks, computers, programs and data from attack, damage or unauthorized access. Since all computer systems rely on operating systems and networks to function, those areas are often targeted for attack and are the main sources of many security vulnerabilities.

Cybersecurity jobs require strong technical skills and most require a technical degree in Cybersecurity, computer science, information technology or engineering. Cybersecurity degree courses often offer classes in:

Computer forensics

Advanced computer security issues and practices

General computer topics.

Cybersecurity jobs might include information systems security professional, senior system manager and system administrator.

Information Security

Information security involves protecting information from unauthorized access, use, disruption, modification or destruction, regardless of whether the information is stored electronically or physically. Cybersecurity is a

security to make a proper choice of his _____

8. Viruses, cyber-attacks, spies are one of many _____ that network can face with.
9. Information security deals with protecting information whether it stored _____
10. Information security students are also trying to take such courses as _____
11. By understanding differences between _____ ___ students can choose their future career path.
12. If you know differences between cybersecurity and information security, you are able to select

subset of the larger area of information security. Similar to Cybersecurity jobs, information security jobs also rely on strong technical skills since most information is stored digitally. A solid background in networking, system administration, software development and data integrity and security is an asset to those looking to enter this field. Prospective students should also consider supplementing technical courses with general communication and business courses. Information security jobs include security systems administrator, security auditor and security analyst.

Understanding technology and security issues is critical for any Cybersecurity or information security professional, regardless of the specific field of specialization. By understanding the differences between these two related but distinct fields, individuals choose the most appropriate educational options that will best prepare them for a career that matches their goals and interests.

The Bottom Line

When deciding on one of these computer security-related career paths, it is critical to be clear and detailed about exactly what it is you're looking for in a career. Cybersecurity and Information Security are two similar fields which offer a great variety of job options, but

profession that best matches you

_____

Try to find as many pluses and minuses of both professions as possible. Which one would you like to choose? Explain your point.

they are distinct career choices.

By fully understanding the differences and similarities between these two fields of study, individuals will better be able to select the educational path that best matches their skills, interests and career goals. By researching potential professions carefully, you'll be able to discern the differences and similarities between several possible programs of study. Gathering data about your prospective field and evaluating it carefully will allow you to make an informed choice about the best career path for you.

(adapted from http://www.floridatechonline.com)

Writing

1. Complete the letter by filling the gaps with a word from the box below.

Differences between CV and resume.

A resume is a one or two page summary of your skills, experience, and education. While a resume is brief and concise - no more than a page or two - a curriculum vitae is longer (at least two pages) and provides a more detailed synopsis.

CV	**post**	**department**	**developer**
interview	**experience**	**qualified**	**closing**
skills	**salary**		

Dear Sir/Madam,

I am writing to apply for the **.....** of Software Development Manager advertised on February 9th on the University of Kent vacancy database. I have been working for the past ten years as a senior **.....** in a

Curriculum vitae includes a summary of your educational and academic backgrounds as well as teaching and research experience, publications, presentations, awards, honors, affiliations, and other details.
In Europe, the Middle East, Africa, or Asia, employers may expect to receive curriculum vitae. In the United States curriculum vitae is used primarily when applying for academic, education, scientific, or research positions. It is also applicable when applying for fellowships or grants.

telecommunication company in the IT **.....** I think now is the right time to apply for a better position as I believe I have gained relevant **.....** and skills.
As you can see from my enclosed **.....**, I am a **.....** engineer and believe I have excellent technical and management **.....**. My current **.....** is $55,000 a year.
I realize that the **.....** date for applications was last Saturday, but I hope you will still consider my application. I will be available for **.....** at any time, apart from the 12 - 24 March when I arranged a holiday in Italy.
I look forward to hearing from you soon.
Yours faithfully,
John Smith.

2. Write your own CV using the following tips. Write at least 150 words.

1. Use a confident tone and positive language.
2. Concentrate on your achievements not your responsibilities. This means listing things you have done - such as products launched, sales increase, awards won - not rewriting your job description. Quote figures whenever possible.
3. Make your most relevant experience and skills prominent to encourage the employer to read on.

4. Keep it to the point and concentrate on the quality of your achievements, not the quantity
5. List other skills that could raise you above the competition such as languages and IT skills
6. Your CV can be far longer than the normal 2 pages of a non-academic CV but your first page should include all the best bits.
7. Check thoroughly for correct spelling and grammar - spotting errors is a quick and easy way of weeding out weaker candidates when faced with a mountain of CVs to read.
8. Appeal to your online audience; ensure you have relevant keywords in your CV.
9. Capture immediate attention. Prioritize the content and detail the most relevant information first.
10. Make sure that you include all Education and prizes awarded, research interest, funding awarded for research projects, other research experience and your publications.

Notice:

British / American English

There are sometimes differences between British and American English and conventions. Here is a guide to some of the most important differences for your CV/resume and covering letter. But remember, this is a guide only - there are no strict rules. For example, some British people like to use "American" words, and some American people like to use "British" words.

British	**American**
CV/curriculum vitae	Resumé
covering letter	cover letter
Standard paper size: A4 (210 x 297 millimetres)	Standard paper size: Letter (8 1/2 x 11 inches)
Mrs	Ms
Dear Sirs	Gentlemen
Yours faithfully	Yours truly
Yours sincerely	Sincerely Sincerely yours Yours truly
Managing Director (MD)	Chief Executive Officer (CEO) General Manager
date format: DD/MM/YY example: 30/12/15 30 December 2015	date format: MM/DD/YY example: 12/30/15 December 31st, 2015
labour	labor

UNIT 1 CYBERSECURITY CAREER Revise and Check

CAN YOU:

…pronounce and give definition of:

commerce

dub

competence

workforce

vulnerable

roundtable

internships

curriculum

shift

acumen

crucial

mitigate

stakeholder

obtain

accreditation

pathway

…give definition of

Cybersecurity

…speak about:

Cybersecurity

Choosing career

Debating about job

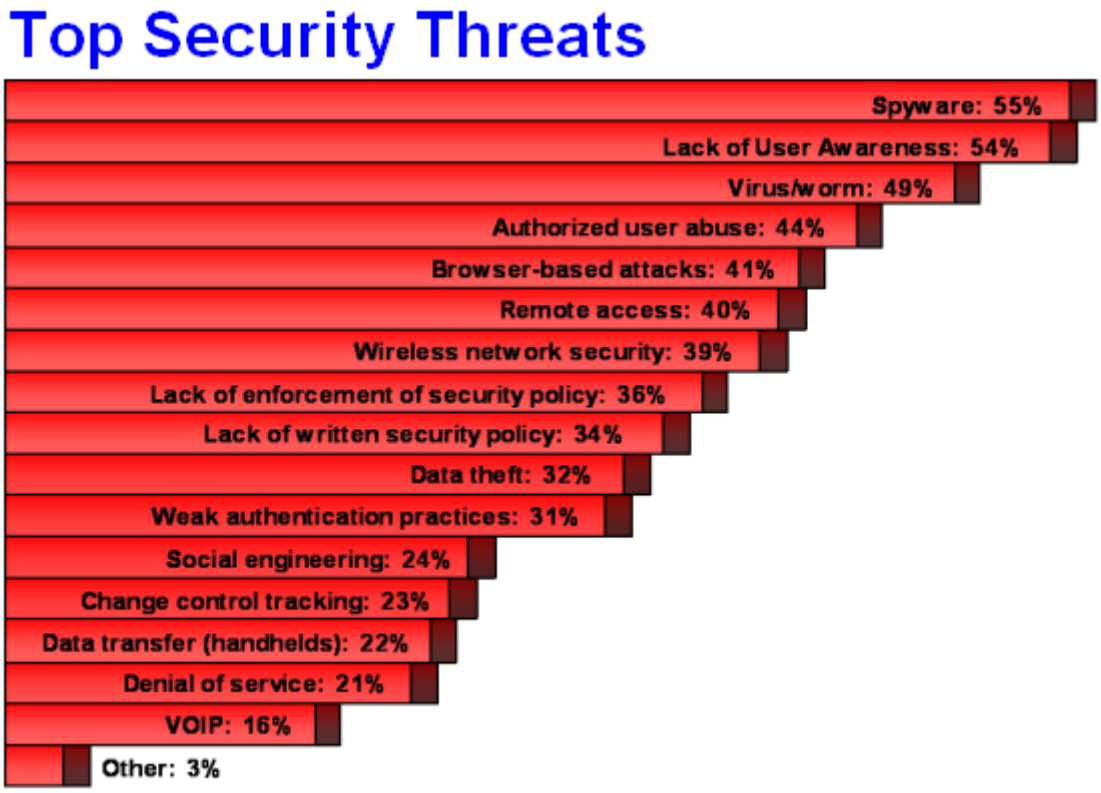
…write:

Curriculum Vitae

UNIT 2 SECURITY THREATS

Speaking

1. What kind of threats can you face? Discuss the threats given in the chart.



2. In pairs write down the description of the chart. Read the following tips first. Practice using "Useful language". You should spend about 10 minutes on this task. Present your description to your groupmates. Discuss and correct all mistakes together.

- ✓ Spend one or two minutes studying the chart;
- ✓ Explain what the chart is describing in introduction;
- ✓ Then identify two or three main features. Don't describe everything you see. Look for any interesting features, especially surprising or contrasting information;
- ✓ Start with an overall information and then move on to use details to support your main points. Remember to use expressions to link your ideas;
- ✓ Make conclusion. Just sum up. Do not explain anything and do not give new information.
- ✓ Write at least 150 words.
- ✓ Remember to check your work before the end.

Useful language	It/There is/are twice as…as
The chart	over … %
shows/illustrates/provides a clear	nearly/about/around … %
overview of/gives information…	is nearly the same as… } that of…
According to…	is a little more than… } the amount/
It can be seen…	is double… number/
It would appear from the chart…	percentage of…
One of the first things to note is…	relatively small percentage…
Another thing which stands out in	much more…than…
this chart is…	slightly more…
However…	a great deal…
Although…	The majority of…
It should be noted that…	A minority of…
A final point to note is…	compared with…
Overall, …	whereas/while…
To conclude…	As well as…it also shows…
It is clear from the data above	not only…but also…
that…	
The data clearly indicates…	

3. Can you add any other threats that were not mentioned in the chart?

Listening

Vocabulary and Pronunciation

You are going to listen to the speech by David Emm, Senior Security Researcher, Kaspersky Lab.

Section 1 Different types of Malware

Questions 1-17

Always read through the tasks very carefully before you listen to get an idea what you are listening for.

Complete the sentences below. Write down ***NO MORE THAN THREE WORDS*** for each answer.

1._____ is a collective term for all kinds of threats.

The most popular threat is 2. _____.

Virus infects the object on a disk by 3. _____ and travels

4. _____ from computer to computer.

Network Worms require 5. _____ to spread while 6. _____ do not.

You will hear a lot of information, but you don't need to understand it all. You should always look ahead to the next question so that you don't miss hearing the answer to a question.

Trojans are masqueraded with some useful function but perform 7. _____ on the computer.

If the code infects the computer when the victim views the webpage it is 8. _____.

Comparing Trojans with Viruses and Worms they don't 9. _____.

Backdoor Trojans allow 10. _____ of a system where

11. _____ records every key pressed.

Banking Trojans' aim is to steal money from a 12. _____.

Trojan downloaders download 13. _____ to the computer.

You will only hear each section **ONCE!**

14._____ combine the functionality of a virus, worm and Trojan in one package.

As soon as cybercriminals are able to control your computer they will connect it with other infected computers – create 15. _____ or botnet.

Now they can do anything from sending out 16. _____ to loading 17. _____ on organizations.

Be ready to listen for a paraphrase!

Write down the words exactly as you hear them!

Remember to write down the **speaker's** answer not your own one!

Check that your answers are spelt correctly, grammatically relevant and make sense in relation to the question.

Section 2 How malware evolves

Questions 18-33

Questions 18-22

Answer the questions below. Write down ***NO MORE THAN THREE WORDS*** for each answer.

18. What do damage with no financial gain such as deletion of files, renaming the data, erasing the data storage media refer to?

19. What machine can be unintended side effect of malware?

20. What kind of machine is of no value to cybercriminals?

21. What is an infected machine for cybercriminals?

22. The number of what is growing?

Questions 23-27

Choose the correct letter **A**, **B** or **C**.

23. Which motive of attacks wasn't mentioned?

A ruin reputation

B disrupt the work of a company

C steal money

24. What gives opportunity to access corporate system?

A confidential data

B disclosing information

C sensitive information

25. Cybercrime is effectively the use of malware for

_____.

A making money

B profit

C stealing data

26. What doesn't refer to identity theft?

A password

B intellectual property

C online banking logging

27. Which way of using victim's online credentials wasn't mentioned?

A laundering money

B accessing accounts

C selling to criminals

Be aware that some of the answers may come quickly one after the other!

Use shorthand to improve the speed at which you write down your answers (to write down the answers more quickly, write only the first two or three letters of the answer that you hear) or use your own system of note-taking

Questions 28-33

Do the following statements agree with the speaker?

Write **T**, **F**, **NG** on lines 28-33.

28. Encrypting the data with the password and making pay money to decrypt it is called ransomware.

29. Ransomware is very profitable.

30. Fake Anti-Virus scam indicates the presence of malware on victim's computer and asks for money to remove it.

31. Criminals can manipulate social networks.

32. When you pay for removal of malware criminals get your password.

33. Two malware mentioned above refer to extortion of money.

The questions are always in the order the answers occur in listening

Section 3 ***Questions 34-47***

How malware spreads and how to stay protected

Questions 34-38

Make sure you write NO MORE than the maximum number of words given in instructions!

Complete the summary below. Write down ***NO MORE THAN THREE WORDS*** for each answer.

Malware spreads via:

a. 34. _____. Having found the 35. _____ in web service criminals hide the code there. Computers can be infected while victims visit the pages;
b. e-mail 36. _____ or links;
c. social network;
d. 37. _____ that is physical media;
e. 38. _____ known as vulnerabilities or bugs.

Don't forget to listen for each answer **in turn**. If you miss one go on to the next question or you may miss that too.

Kaspersky analyses modifications of existing viruses that are 39. _____. It searches for 40. _____ of none viruses or signatures. Kaspersky provides a range of 41. _____: heuristic analysis, sandboxing, 42. _____, behavioral analysis etc. It has 43. _____ called Kaspersky Security Network. It provides 44. _____ protection as they can 45. _____ even unknown virus without the signature. Kaspersky can offer 46. _____, accurate and comprehensive analysis by applying 47. _____ of detection.

Always give an answer – you won't lose marks if it is wrong!

Pronounce and give definitions of the following words:

malware /ˈmæl.weər/
virus /ˈvaɪərəs/
worm /wɜːm/
e-mail worm /ˈiːmeɪl wɜːm/
network worm /ˈnetwɜːk wɜːm/
Trojan /ˌtrəʊ.dʒən/
homegrown application /ˌhəʊmˈgrəʊn ˌæplɪˈkeɪʃən/
drive-by download /ˈdraɪvbaɪ ˌdaʊnˈləʊd/
self-replicate /self ˈreplɪkeɪt/
backdoor Trojan /bækdɔːr ˌtrəʊ.dʒən/
banking Trojan /ˈbæŋkɪŋ ˌtrəʊ.dʒən/
Trojan downloaders /ˌtrəʊ.dʒən ˌdaʊnˈləʊdez/
hydrid threat /ˈhaɪbrɪd θret/
keylogger /kiːlɑː.gəʳ/
botnet /ˈbɒt.net/
spam /spæm/
target attack /ˈtɑːgɪt əˈtæk/
cyber vandalism /saɪbər ˈvændəlɪzəm/
sluggish /ˈslʌgɪʃ/
disclosing information /dɪsˈkləʊzɪŋ ˌɪnfəˈmeɪʃən/
cybercrime /ˈsaɪ.bə.kraɪm/
identity theft /aɪˈdentəti θeft/
laundering money /ˈlɔːndərɪŋ ˈmʌni/
ransomware /ˈrænsəm.weər/
lucrative /ˈluːkrətɪv/
fake anti-virus scam /feɪk ˌæntiˈvaɪərəs skæm/
extortion /ɪkˈstɔːʃən/
loophole /ˈluːphəʊl/
vulnerability /ˌvʌlnərəˈbɪləti/
bug /bʌg/
variants /ˈveəriənts/
snippet /ˈsnɪpɪt/
signatures /ˈsɪgnətʃərz/
sandbox /sænd bɒks/

Pronounce the following malware types that were not mentioned by the speaker and match them with their definitions. What do you know about them?

Malware	Definition
1. Bot /bɒt/	**A** will redirect your normal search activity and give you the results the developers want you to see. Its

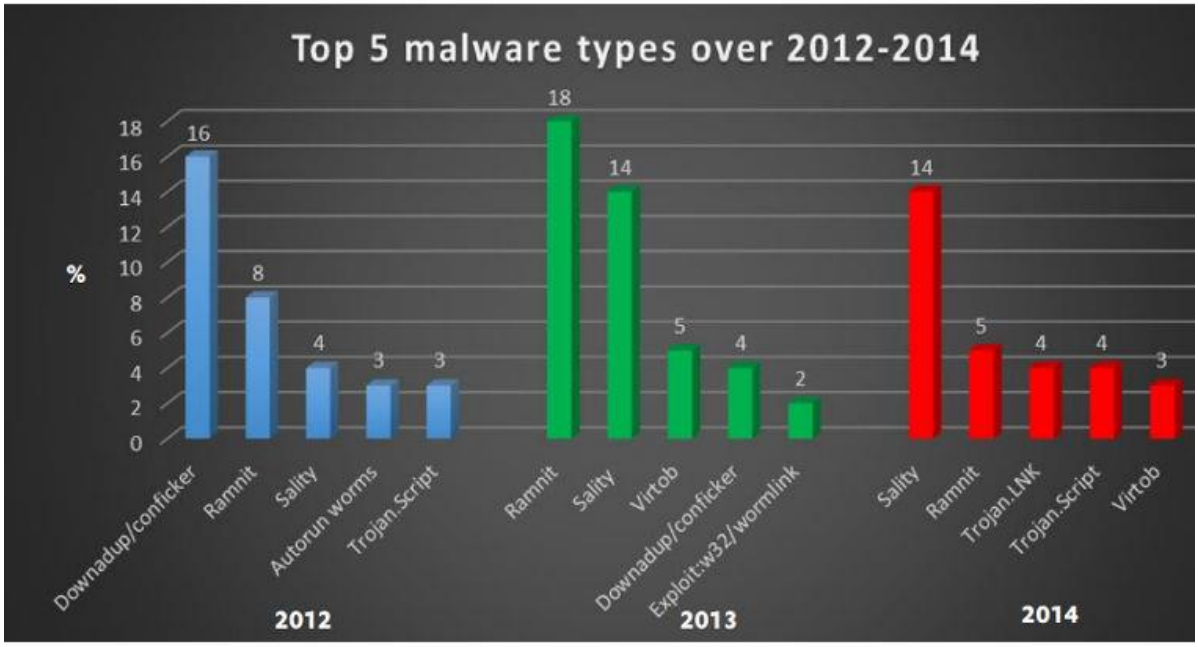
	intention is to make money off your web surfing.
2. Rootkit /ruːtkɪt/	**B** is one that can transform based on the ability to translate, edit and rewrite its own code.
3. Backdoors /ˈbækˌdɔː(r)z/	**C** is the name given to legitimate programs that can cause damage if they are exploited by malicious users – in order to delete, block, modify or copy data, and disrupt the performance of computers or networks.
4. Browser Hijacker /ˈbraʊzər ˈhaɪdʒækər/	**D** is the name given to programs that are designed to display advertisements on your computer, redirect your search requests to advertising websites and collect marketing-type data about you.
5. A stealth virus /stelθ ˈvaɪərəs/	**E** is derived from the word "robot" and is an automated process that interacts with other network services.
6. A metamorphic virus /ˌmet.əˈmɔː.fɪk ˈvaɪərəs/	**F** is complex malware that hides itself after infecting a computer and copies information from uninfected data onto itself and relays this to antivirus software during a scan.
7. A macro virus /mækrəʊ ˈvaɪərəs/	**G** provide a network connection for hackers or other Malware to enter or for viruses or SPAM to be sent.
8. Spyware /ˈspaɪ.weər/	**H** alters or replaces a macro, which is a set of commands used by programs to perform common actions.
9. Adware /ˈædweər/	**I** works in a similar way to spyware but does not usually collect information from the computer. Instead, it just sits there waiting for commands from a command-and-control server controlled by the

	attacker.
10.Riskware **/ˈrɪsk weər/**	**J** is designed to permit the other information gathering Malware to get the identity information from your computer without you realizing anything is going on.
11.Zombie **/ˈzɒmbi/**	**K** is a type of malware that surreptitiously gathers information and transmits it to interested parties.

Writing

You should spend about 20 min on this task. Write at least 150 words.

The chart shows 5 top malware types over 2012-2014 . Summarize the information by selecting and reporting the main features, and make comparisons where relevant.



- If the chart includes time references (dates, years) you will need a range of past and present tenses. If it has no past time reference, you will need to use present simple tense only.
- It is important not to offer your opinion on the chart or to try to give reasons for the figures mentioned.
- Paraphrase the figures in the chart. Use just under half of, a third…
- You need to compare information as well as describe it. Use phrases from Speaking of this unit (useful language) and the following ones:

to shoot up
to soar
to boom
to jump
to surge
to skyrocket to

amount of +uncountable noun
number of + countable noun
five (number) per cent of…
the percentage of (noun)…

to increase/an increase of 20%, in obesity
to rise/a rise
to go up
to grow
to climb
to double

dramatically/dramatic
steeply/steep
sharply/sharp
rapidly/rapid
significantly/significant
drastically

to reach a peak/a peak
to reach a high/a high
to hit record levels

clearly
undoubtedly
surprisingly
obviously
statistically
unbelievably
probably
luckily
disappointingly

to hold/remain steady
to remain/be stable/constant/unchanged
to flatten out
no change
to level off/a levelling off

to fluctuate/a fluctuation
to zigzag
to move up and down

gradually/gradual
steadily/steady
constantly/constant
slightly/slight
slowly/slow

to fall/a fall
to decline/a decline
to decrease/a decrease
to dip/a dip
to go down

Time expressions
in 2015
between 2013 and 2015
for 5 years
for the period
since 2013

to drop/a drop by
to plunge
to plummet by
to dive-take a nosedive

to bottom out
to fall/hit to a low point/a low point

Reading Vocabulary and Pronunciation

Social Engineering: an underestimated danger

What is Social Engineering? Does it really turn out to be one of the most dangerous threats?

Match the following transcriptions, **A-L**, with the highlighted words and pronounce them.

A /daɪər/
B /ˌræʃəˈnɑːl/
C /daɪˈvʌldʒ/
D /ˌpenɪˈtreɪʃən ˈtes.tər/
E /nɪˈglekt/
F /blægɪŋ/
G /ədˈhɪər/
H /səˈseptəbl/
I /ɪkˈsplɔɪtit/
J /geɪn/
K /tæp/
L /fəˈsɪlɪteɪt/

Read the article once. Try to work out the meaning of the highlighted words.

There is always a lot of concern about how we protect IT systems against sophisticated attacks by super intelligent hackers whilst completely neglecting the risks posed by staff not adhering to policies and procedures or their vulnerability to being socially engineered to give away information. The poor implementation of data protection rules can pose a major threat to information security. Vulnerabilities may also emerge where people are lazy, or do not understand the potential consequences of failing to meet policy standards. However, there are also lots of ways people might be manipulated through social engineering into giving away information that would facilitate an attack, and this risk is often overlooked.

Social engineering is the act of manipulating people into performing actions that compromise security or divulging confidential information. Perhaps the most well- known means of social engineering is **phishing** – the act of creating a legitimate looking email or letter from an institution or a person in a position of authority with the aim of gaining access to personal or confidential information.

Whilst phishing attacks are clumsy and easy to spot, a great number of emails sent, combined with the

Then match them with their definitions, a-l.

a._____ *verb*
to use part of a large supply of something for your own advantage

b._____ *verb*
to make something possible or easier

c._____ *adj*
very serious or bad

d._____ *verb*
to obey a rule or principle

e._____ *noun*
someone whose job is to attack computer systems in order to find security weaknesses that can then be fixed

f._____ *adj*
easily influenced or harmed by something

fact we all still receive them, suggests that the senders are achieving some level of success. Furthermore, some groups of people are singled out by social engineers as they are seen as more susceptible to phishing scams. Take for example the pyramid schemes that commonly target elderly people who are perceived to have the money to invest and time on their hands, and may be lonely and starving for attention. Another example is the recent money laundering scam targeting students, unemployed people, and foreign nationals. The targets effectively launder the criminals' money through their own bank account and take a percentage as "payment" for their services. This is, of course, illegal and can have dire consequences for the victims who may end up with a criminal record and/or being denied banking services. There are also examples of individuals working in large firms being specifically targeted with official looking emails issuing them with a subpoena and informing them they need to appear in court (in the USA). These emails, of course, had malicious links embedded within them. The targeted nature of such attacks has given rise to the term "**spear phishing**". Although phishing is perhaps the most well-known social engineering tactic, it is not the only one. There are numerous other ways a social engineer can persuade people to part with confidential information or permit them to access places they shouldn't be allowed to. For example:

g._____ *verb* to not give enough care or attention to something or someone

h._____ *noun* a group of reasons for a decision or belief

i._____ *verb* to get something useful

j._____ *noun* the practice of pretending to be someone else in order to get personal information about them

k._____ *verb* to give secret or private information to someone

l._____ *adj* be treated unfairly in order to get some benefit from you

Questions 1-8

Read the article again and choose the most suitable

1_____– This is one of the best tactics when you are trying to make it appear perfectly normal to everyone that you should be there. For example, pretend to be an employee to gain access – identity cards can be stolen or mimicked and uniforms can be purchased. Combined with poor access control procedures, this makes it easy to gain the necessary information for the social engineer.

2_____– the social engineer will create and use an invented scenario to engage the target in a way that increases their chances of divulging information or acting in a different way. This is also known as blagging.

3_____– the social engineer persuades the person responsible for a legitimate delivery that the consignment is requested elsewhere and steals the contents.

4_____– the real-world Trojan horse. This relies on the curiosity and greed of the victim by offering "too-good-to-be-true" investment opportunities. It can be in a form of music or movie download or a USB flash drive with a company logo left out in the open for you to find.

5_____– this is a common tactic used by social engineers. In emails, they will claim to be a peer/prince, a law enforcement agent, or anyone else that could be perceived as an authority figure. In person, an air of confidence and the ability to lie convincingly can gain a social engineer access to all

topic sentence, i-xii, for each paragraph, **1-8**, from the list below.

i **Vishing**
ii **Tailgating**
iii **Diversion theft**
iv **Unfriendly behaviour**
v **Impersonating someone in a position of authority**
vi **Quid pro quo**
vii **Familiarity exploit**
viii **Win-win deal**
ix **Reading body language**
x **Baiting**
xi **Hostility**
xii **Pretexting**

Questions 9-18

Complete the summary below with words from the article. Write **NO MORE THAN THREE WORDS** for each answer.

It's quite difficult to keep your system safe from 9. _____ attacks if sorts of places.

6_____– it is surprisingly easy to follow people into secure restricted area or system. The polite practice of holding doors open is a social engineer's dream. To be honest, most people hate confrontation and are unlikely to challenge you anyway.

7_____– drawing attention by being very unfriendly. This is because people just want to get rid of angry people and they are much more likely to obey your wishes when you are angry, so it works well when asking people to open doors for you or provide information on the location of things. A good real-world example of this is to start an argument with someone as you approach a checkpoint (e.g. if you are trying to sneak alcohol into a festival) and security staff may be more likely to wave you through instead of searching you.

8_____– this is where a social engineer will offer something for something else in return. For example, disgruntled employees may be approached to provide information in exchange for cash.

There are lots of techniques and approaches that the social engineer can access to facilitate their work. For example:

• **Surveillance** – identifying the targets' routine helps determine the best way to approach them. However, the approach does not always need to be direct. Take for example a scenario where a group

your employees don't 10. _____ the rules. The main purpose of social engineering is to make people 11. _____ confidential data. The most popular way is to send 12. _____ letter. For example, social engineers can easily 13. _____ money with the help of this method. But there are some other ways to 14. _____ access to confidential information. One of them is 15. _____ when social engineers go in path with you to enter necessary place. Another one is 16. _____ when they use something victims can be interested in to attract their attention. Also another 17. _____ can be used to 18. _____ the work.

of employees regularly go to the same pub on a Friday night. Conversations after a few alcohol beverages can lead to sharing of confidential information.

• **Maximizing on naivety** –for example, when the victim pays a bill over the phone in public place. By the time she gets through to payment services the social engineer can have a pen and notepad ready and will be able to write down all of her credit card information (including the 3 digit security code on the back of the card!).

• **Using social networks** – LinkedIn, Facebook, Twitter and other social networks contain a mountain of information. It is surprising how much personal data you can access about someone from their social media profiles. Knowing this kind of information could allow strangers to strike up a conversation with you under the pretense that they know you. Once your barriers are down, they can start asking more confidential questions to gain the key information that they want. Some people also post where they are at a given time and even information on when they are going on holiday!

• **New technology** – it is now easier to fake identity cards. There are also all sorts of tiny cameras and microphones on the market which help the social engineer gather information.

• **Services** – any service that involves geotagging will tell a social engineer where you are if they can tap into it. There are also very unethical telephone

Questions 19-25

Complete each of the following sentences, 5-10, with the best ending, **A-N**, from the list of endings below.

19. If you get an e-mail, …
20. If you are an employee, …
21. If you are an employer, …
22. If you use different protection policies, …
23. Try to give your employees access to …
24. Try to use special people to …
25. If you employ white hat hackers, …

call centre services available who will masquerade as someone on your behalf. Picture the scene – you have stolen a credit card from an elderly lady and you want to purchase expensive items with it. To achieve this you want to change the billing address for the credit card. Problem – you are not an elderly lady, nor you can mimic one, so calling the bank yourself is out of the question. If you don't have a friend who can call for you, you can actually purchase the service. Believe it or not, there are companies out there that will charge you around $7-15 to make the call to the bank on your behalf if you provide them with enough information to pass the security questions.

Everyone is at risk of being targeted by a social engineer. Even if social engineers don't think they can get access to you directly, they may try to target you through your friends, family, or colleagues. For example, they may hack into your friends' email account and send a message inviting you to click on a link. Because you trust your friend, you are more likely to click the link.

Tips for reducing risk

If you are unsure about the authenticity of an email or a letter, use contact information you have sourced independently (rather than that provided) to verify it.

As an employee of a company, you need to ensure that you are not exploited to give away trade secrets. In this instance, increasing your knowledge of how

A give information to your staff about accounts.
B keep it in secret.
C say the employees about your decision.
D contact the given source.
E inform your staff about them.
F be sure in security of your company.
G don't share information with people you are not sure about.
H challenge your colleagues.
I give recommendations.
J teach your employees how protect the data.
K check your company's security.
L you should check its authenticity.
M information they really need.
N necessary accounts.

social engineers operate and adopting a questioning nature will help – i.e. if someone you don't really know asks you something confidential, don't be afraid to challenge them. If in doubt, seek confirmation that you can share the information with that person from a trusted source before proceeding. Also, follow the data protection policy – e.g. if you have been told not to access personal email at work, don't just assume your employer is being unreasonable, because there may be a very good reason for the policy.

As an employer or business, remember that it is all good and well to spend money on technical protection systems, but if you don't train your staff to avoid social engineering attempts and teach them good data protection practices, your system is still vulnerable. It is important to explain to staff why you have certain policies in place. For example, if you block access to personal email accounts to help minimize the risk of malware being downloaded, then inform staff about this rationale.

You might also want to consider adopting the "least privilege" principle, which means providing users with access only to specific places - basically, the need-to-know translated into a need-to-access. The bottom line is that if the person cannot access the system, they cannot abuse it (either intentionally or unintentionally).

You might also want to employ penetration testers who can test the effectiveness of your security

procedures by trying to socially engineer their way into your business. They can test whichever security measures you want and will report back with recommendations for improvement.

Penetration tests can be physical (e.g. someone trying to get past building security) or through the IT systems (e.g. white hat hackers will attempt to breach your IT security systems). Don't warn your staff that a penetration tester is coming – it undermines the whole operation!

Social engineering will never go away. In fact, the more technologically advanced we become, the more necessary it is to use social engineering to gain access to IT systems. The methods are unlikely to change – social engineers have been using the same basic tricks (e.g. familiarity exploits) for years and there is no reason for them to change now.

The only difference is that new technology provides different ways of achieving their aim (e.g. allowing them to improve or automate their attacks).

Secondly, social engineering attacks are likely to continue to become more sophisticated and targeted. As people become more aware of social engineering tactics, it is necessary for them to up their game to ensure continued success (e.g. the development and use of social engineering services).

Finally, remember the birth of social media has acted as an enabler to social engineering, so be careful what you post. (adapted from www.insecuremag.com issue 37)

Questions 26-28

Do the following statements agree with the article? Write **T**, **F**, **NG** on lines 26-28.

26. Social engineering will be more popular.
27. Social engineers will use modern tactics in future.
28. Social engineers will use social networks.

Underline the sentence or part of the text that gives you the answer.

Speaking

You are going to have a conference dedicated to Security Threats. Choose any type of threat and prepare 7 min presentation about it. Be sure to speak about: history of this threat, how it works, how to avoid it and actions to be taken to remove it. Use the following plan and phrases or you'll lose your marks.

Greeting the audience Good morning (afternoon, evening) ladies and gentlemen (everyone). It's a pleasure to be with you here today. Shall we begin? (I think we can begin now)	**Introducing each section** So, let's start with… Now let's move on to… Let's turn our attention to… This leads me to…
Introducing yourself (your company) Let me introduce myself first (I'd like to introduce myself; Before I begin let me tell you a little about myself). I'm… I study… I work for…	**Referring backward and forwards** I mentioned earlier… I'll say more about it later. We'll come back to this point later.
Giving a short introduction Today (this morning) I'm going to (I'd like to) talk about (describe)… The aim (purpose) of my presentation today is… My talk today will deal with… My presentation today will concern primarily… This morning I'd like to cover the topic of…	**Checking understanding** Is that clear? Are there any questions? **Referring to visual information** This screen shows… If you look at this graph you can see… I'd like to draw your attention to…

The overview -presenting the structure	Concluding. Calling for questions
I've divided my presentation into (My talk will be in) … parts. First of all (to begin with, to start with, first), I'll present (give an overview)… Second (then, next, later, after that), I'll discuss (consider, talk about, look at, explain, analyze, explain, describe, focus on, move on, deal with, compare, review, outline, highlight, go over)… Finally (last of all, in the final part), I'll try to forecast…	That concludes my talk. That brings me to the end of my presentation. Thank you for being such an attentive audience (Thank you for your attention) If you have any questions, I'll be pleased (do my best, be happy) to answer them. I hope that was clear. If there are any questions, please don't hesitate to ask them. This is a complex subject. There are probably many things that are still not clear. I welcome any questions you may have. If you would like to have some points clarified, please feel free.
Referring to questions	**Dealing with questions**
Feel free to interrupt me if there's anything you don't understand. If you don't mind, we'll leave questions till the end.	I'm glad you asked that question. I'm sorry I'm not sure I understand. Could you repeat your question, please? If I understand you correctly, what you want to know is… Your question leads to an area which could be the subject of another presentation. I'm afraid I'm not the right person to answer that.

CAN YOU…

…speak about

different types of threats and malware

how malware evolves and spreads

how to stay protected

social engineering: tactics, approaches, tips to avoid

make presentation

…describe bar charts

…pronounce and give definition of

malware
virus
worm
e-mail worm
network worm
Trojan
homegrown application
drive-by download
self-replicate
backdoor Trojan
banking Trojan
Trojan downloaders
hydrid threat
keylogger
botnet
spam
target attack
cyber vandalism
sluggish
disclosing information
cybercrime
identity theft
laundering money
ransomware
lucrative
fake anti-virus scam
extortion
loophole
vulnerability
bug
variants
snippet
signatures
sandbox
bot
rootkit
backdoors
browser hijacker
a stealth virus
a metamorphic virus
a macro virus
spyware
adware
riskware
zombie
social engineering
phishing
spear phishing
neglect
familiarity exploit
adhere to
pretexting
facilitate
blagging
gain
diversion theft
divulge
baiting
penetration tester
tailgating
be exploited
hostility
tap into
dire
quid pro quo
susceptible
rationale
white hat hacker
sophisticated

UNIT 3 COMPUTER SYSTEM SECURITY

Speaking

What Makes a System Secure?

Discuss the following methods.

Which one is the most important?

Taking advantage of basic hardware and software security characteristics; for example, using a system architecture that's able to segment memory, thus isolating privileges processes from nonprivileged processes.

Performing the offline procedures that make or break a secure system - by clearly delineating system administrator responsibilities, by training users appropriately, and by monitoring users to make sure that security policies are observed. Also more global security management as figuring out what security threats dace your system and what it will cost to protect against it.

Monitoring who can access what data, and for what purpose. Your system might support discretionary access controls; with these, you determine whether other people can read or change your data. Your system might also have support mandatory access controls; with these, the system determines access rules based on the security levels of the people, the files, and the other objects in your system.

Ensuring that unauthorized users don't get into the system, and by encouraging authorized users to be security-conscious.

What is the difference between identification and authentication?

Reading 1 Vocabulary and Pronunciation

What kinds of Authentication do you know? Can you give any examples? Which ones do you use and why?

Pronounce the following words from the text with the help of given transcriptions.

authentication
noun /ɔːˌθen.tɪˈkeɪ.ʃən/
technique
noun /tekˈniːk/
biometric
adj /ˌbaɪəʊˈmetrɪk/
measurable
adj /ˈmeʒərəbl/
identification
noun /aɪˌdentɪfɪˈkeɪʃən/
enrollment
noun /ɪnˈrəʊlment/
geometry
noun /dʒiˈɒmɪtri/
iris
noun /ˈaɪərɪs/

Authentication is the process to allow users to confirm his or her identity to a Web application. Human factors are often considered the weakest link in a computer security system. Point out that there are three major areas where human-computer interaction is important: authentication, security operations, and developing secure systems.

Current authentication methods can be divided into three main areas:

• Token based authentication
• Biometric based authentication
• Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security.

Biometrics offer automated methods of identity verification or identification on the principle of measurable physiological or behavioral characteristics such as a fingerprint or a voice sample. The characteristics are measurable and unique. These characteristics should not be duplicable, but it is unfortunately often possible to create a copy that is accepted by the biometric system as a true sample.

The process of the user's registration with the

facial
adj /ˈfeɪʃəl/
recognition
noun /ˌrekəgˈnɪʃən/
signature
noun /ˈsɪgnətʃər/
dynamics
noun /daɪˈnæmɪks/
rhythm
noun /ˈrɪðəm/
digitalization
noun /ˈdɪdʒɪtəlizeiʃn/
microphone
noun /ˈmaɪkrəfəʊn/
amateur
adj /ˈæmətər/

Match the following transcriptions, **A**-**Z**, with the highlighted words and pronounce them.

A /kjuː/
B /raʊnd/
C /ˈvɜːtʃuəli/
D /ˈaɪgənˌfeis/
E /əbˈzɔːb/
F /ˈretɪnə/
G /ˈprɒpəli/

biometric system is called *enrollment*. Biometric systems can be used in two different modes. Identity *verification* occurs when the user claims to be already enrolled in the system (presents an ID card or login name); in this case the biometric data obtained from the user is compared to the user's data already stored in the database. *Identification* (also called *search*) occurs when the identity of the user is a priori unknown. In this case the user's biometric data is matched against all the records in the database as the user can be anywhere in the database or he/she actually does not have to be there at all. It is evident that identification is technically more challenging and costly.

There are lots of biometric techniques available nowadays. A few of them are in the stage of the research only (e.g. the odor analysis), but a significant number of technologies is already mature and commercially available (at least ten different types of biometrics are commercially available nowadays: fingerprint, finger geometry, hand geometry, palm print, iris pattern, retina pattern, facial recognition, voice comparison, signature dynamics and typing rhythm).

Fingerprint identification is perhaps the oldest of all the biometric techniques. The live fingerprint readers are most commonly based on optical, thermal, silicon or ultrasonic principles.

The iris is the colored ring of textured tissue that

H /ɪnˈveɪ.sɪv/
I /ˌsɪməlˈteɪniəsli/
J /ˌɪnfrəˈred/
K /ɪnˈtruːsɪv/
L /ˈkaʊn.təˌmeʒ.ər/
M /ˈkæptʃər/
N /dɪˈstɪŋgwɪʃ/
O /ɪnˈtrenʃt/
P /grɪd/
Q /gliːn/
R /səˈfɪstɪkeɪtɪd/
S /ˈækjərəsi/
T /strəʊk/
U /ˈtɪʃuː/
V /ˈsiːkwəns/
W /ˈkjuːmjələtɪv/
X /ˈvɜːsətaɪl/
Y /ˈdiːkɔɪ/
Z /pəˈmjuːtid/

Read the article once. Try to work out the meaning of the highlighted words. Then match them with their definitions, a-z.

a._____ *verb*
to become part of something

surrounds the pupil of the eye. Even twins have different iris patterns and everyone's left and right iris is different, too. Research shows that the matching accuracy of iris identification is greater than of the DNA testing. The iris pattern is taken by a special gray-scale camera in the distance of 10–40 cm from the camera. The camera is hidden behind a mirror, the user looks into the mirror so that he/she can see his/her own eye, then also the camera can "see" the eye. Once the eye is stable (not moving too fast) and the camera has focused properly, the image of the eye is captured.

Retina scan is based on the blood vessel pattern in the retina of the eye. Retina scan technology is older than the iris scan technology that also uses a part of the eye. The main drawback of the retina scan is its intrusiveness. The method of obtaining a retina scan is personally invasive. A laser light must be directed through the cornea of the eye. Also the operation of the retina scanner is not easy. A skilled operator is required and the person being scanned has to follow his/her directions.

Hand geometry is based on the fact that nearly every person's hand is shaped differently and that the shape of a person's hand does not change after certain age. Hand geometry systems produce estimates of certain measurements of the hand such as the length and the width of fingers. Various methods are used to measure the hand.

b._____ *verb*
to recognize the differences between two people, ideas, or things

c._____ *adj*
moving into all areas of something and difficult to stop

d._____ *noun*
a part at the back of the eye, which is affected by light and sends messages to the brain

e._____ *noun*
a movement that you make against something with your hand, a pen, brush, etc

f._____ *adj*
useful for doing a lot of different things

g._____ *verb*
to discover information slowly or with difficulty

These methods are most commonly based either on mechanical or optical principle. A few hand geometry scanners produce only the video signal with the hand shape. Image digitalization and processing is then done in the computer. On the other side there exist very sophisticated and automated scanners that do everything by themselves including the enrollment, data storage, verification and even simple networking with a master device and multiple slave scanners.

The signature dynamics recognition is based on the dynamics of making the signature, rather than a direct comparison of the signature itself afterwards. The dynamics is measured as a means of the pressure, direction, acceleration and the length of the strokes, number of strokes and their duration. The most obvious and important advantage of this is that a fraudster cannot glean any information on how to write the signature by simply looking at one that has been previously written.

Facial recognition is the most natural means of biometric identification. The method of distinguishing one individual from another is an ability of virtually every human. The better the image source (i.e. camera or scanner) is the more accurate results we get. The facial recognition systems usually use only the grayscale information. Colors (if available) are used as a help in locating the face in the image only. The

h._____ *noun* how correct or exact something is

i._____ *adverb* almost

j._____ *noun* the name given to a set of eigenvectors when they are used in the computer vision problem of human face recognition

k._____ *verb* to get control of a place with force

l._____ *adj* so fixed or have existed for so long that they cannot be changed

m._____ *noun* a series of related events or things that have a particular order

lighting conditions required are mainly dependent on the quality of the camera used. Facial recognition technology has recently developed into two areas: *facial metrics* and *eigenfaces*. Facial metrics technology relies on the measurement of the specific facial features (the systems usually look for the positioning of the eyes, nose and mouth and the distances between these features). The method is based on categorizing faces according to the degree of fit with a fixed set of 150 master eigenfaces. This technique is in fact similar to the police method of creating a portrait, but the image processing is automated and based on a real picture here. Better results can be achieved if the operator is able to tell the system exactly where the eyes are positioned. The systems also have problems to distinguish very similar persons like twins and any significant change in hair or beard style requires re enrollment. Glasses can also cause additional difficulties. The face recognition system does not require any contact with the person and can be fooled with a picture if no countermeasures are active. The liveness detection is based most commonly on facial mimics. The user is asked to blink or smile. If the image changes properly then the person is considered “live”. A few systems can simultaneously process images from two cameras, from two different viewpoints. The use

n._____ *adj*
light that feels warm but cannot be seen

o._____ *noun*
a group of events that is part of a series

p._____ *adj*
very advanced and works in a clever way

q._____
adverb correctly, or in a satisfactory way

r._____ *noun*
an action taken against an unwanted action or situation

s._____ *adj*
reached by gradually adding one thing after another

t._____ *noun*
someone or something used to lead a person or

of two cameras can also avoid fooling the system with a simple picture.

The principle of speaker verification is to analyze the voice of the user in order to store a voiceprint that is later used for identification/verification.

Speaker verification and speech recognition are two different tasks. The aim of speech recognition is to find *what* has been told while the aim of the speaker verification is *who* told that. Speaker verification focuses on the vocal characteristics that produce speech and not on the sound or the pronunciation of the speech itself.

The greatest advantage of speaker verification systems is that they do not require any special and expensive hardware. A microphone is a standard accessory of any multimedia computer, speaker verification can also be used remotely via phone line. A high sampling rate is not required, but the background (or network) noise causes a significant problem that decreases the accuracy. The speaker verification is not intrusive for users and is easy to use.

Palmprint verification is a slightly different implementation of the fingerprint technology. Palmprint scanning uses optical readers that are very similar to those used for fingerprint scanning, their size is, however, much bigger and this is a limiting factor for the use in workstations or mobile devices.

Hand vein geometry is based on the fact that the

animal to a place so that they can be caught

u._____ *adj* interrupting a peaceful situation, becoming involved in something in a way that is not welcome

v._____ *adverb* happening or existing at the same time

w._____ *noun* a pattern or structure made from horizontal and vertical lines crossing each other to form squares

x._____ *adj* changed sequence of

y._____ *noun* the material that animals and plants are made of

z._____ *verb* to give someone a signal to do something

vein pattern is distinctive for various individuals. The veins under the skin absorb infrared light and thus have a darker pattern on the image of the hand taken by an infrared camera. The hand vein geometry is still in the stage of research and development.

DNA sampling is rather intrusive at present and requires a form of tissue, blood or other bodily sample. This method of capture still has to be refined. So far the DNA analysis has not been sufficiently automatic to rank the DNA analysis as a biometric technology. The analysis of human DNA is now possible within 10 minutes. At present DNA is very entrenched in crime detection and so will remain in the law enforcement area for the time being.

Thermal imaging is similar to the hand vein geometry. It also uses an infrared source of light and camera to produce an image of the vein pattern in the face or in the wrist.

Identifying individuals by the ear shape is used in law enforcement applications where ear markings are found at crime scenes. An ear shape verifier (Optophone) is produced by a French company ART Techniques. It is a telephone-type handset within which is a lighting unit and cameras which capture two images of the ear.

The body odor biometrics is based on the fact that virtually each human smell is unique. The smell is captured by sensors that are capable to

Questions 1-10

Read the text again and match characteristics, 1-10, with suitable type of authentication, **A**-**O**.

1. Based on the process, the way you make it
2. Better than the DNA
3. Has recently started to be used as it took much time before
4. Needs no contact with people
5. You need to follow instructions
6. You will need to choose from pictures
7. Can be used remotely

obtain the odor from non-intrusive parts of the body such as the back of the hand.

Keystroke dynamics is a method of verifying the identity of an individual by their typing rhythm which can cope with trained typists as well as the amateur two-finger typist. Systems can verify the user at the log-on stage or they can continually monitor the typist. These systems should be cheap to install as all that is needed is a software package.

The US company AIMS is developing a system which scans the dermal structure under the fingernail.

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. Although there are different types of authentication techniques available alphanumeric passwords are the widely used because they are versatile and it is easy to implement and use. ***The text based*** passwords need to satisfy two contradictory requirements. That is it should be easily remembered by the user and it should be hard to guess by an attacker. So these text passwords are vulnerable to dictionary attacks and brute force attacks.

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). They can be classified into three

8. Is supposed to be cheap
9. Based on optical and mechanical principle
10. Easy to use and carry out

A token based
B fingerprint
C finger geometry
D hand geometry
E palm print
F iris pattern
G retina pattern
H facial recognition
I signature dynamics
J speaker verification
K hand vein geometry
L DNA sampling
M keystroke dynamics
N text based passwords
O graphical passwords

categories according to the task involved in memorizing and entering passwords: recognition, recall, and cued recall.

A *recognition-based* scheme requires identifying among decoys the visual objects belonging to a password portfolio. A typical scheme is Passfaces wherein a user selects a portfolio of faces from a database in creating a password. During authentication, a panel of candidate faces is presented for the user to select the face belonging to her portfolio. This process is repeated several rounds, each round with a different panel. A successful login requires correct selection in each round. The set of images in a panel remains the same between logins, but their locations are permuted. Story is similar to Passfaces but the images in the portfolio are ordered, and a user must identify her portfolio images in the correct order. Déjà Vu is also similar but uses a large set of computer generated "random-art" images. Cognitive Authentication requires a user to generate a path through a panel of images as follows: starting from the top-left image, moving down if the image is in her portfolio, or right otherwise. The user identifies among decoys the row or column label that the path ends. This process is repeated, each time with a different panel. A successful login requires that the cumulative probability that correct answers were not entered by chance exceeds a threshold within

a given number of rounds.

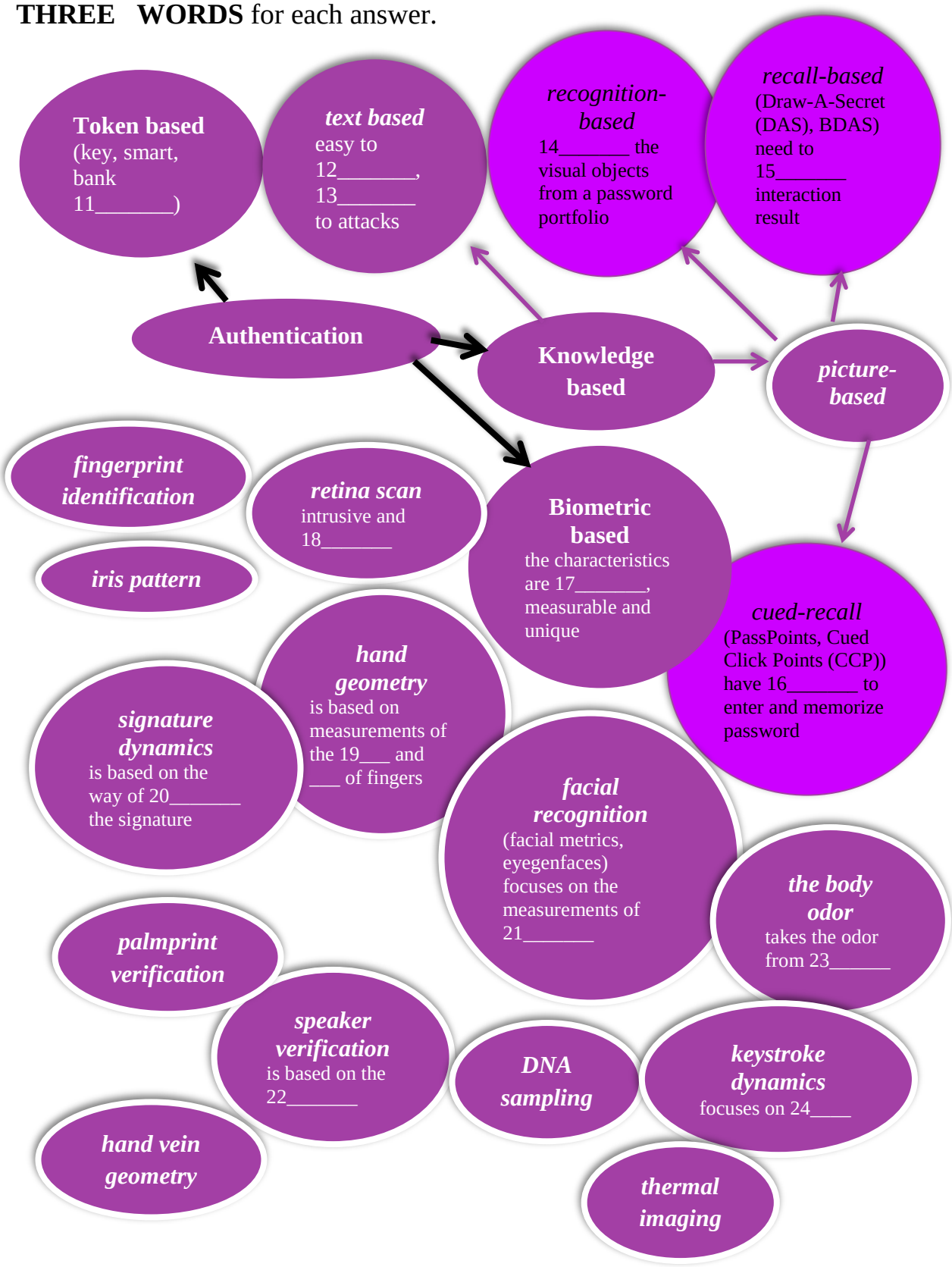
A *recall-based* scheme requires a user to regenerate the same interaction result without cueing. Draw-A-Secret (DAS) was the first recall-based scheme proposed. A user draws her password on a 2D grid. The system encodes the sequence of grid cells along the drawing path as a userdrawn password. Pass-Go improves DAS's usability by encoding the grid intersection points rather than the grid cells. BDAS adds background images to DAS to encourage users to create more complex passwords.

In a *cued-recall* scheme, an external cue is provided to help memorize and enter a password. PassPoints is a widely studied click-based cued-recall scheme wherein a user clicks a sequence of points anywhere on an image in creating a password, and re-clicks the same sequence during authentication. Cued Click Points (CCP) is similar to PassPoints but uses one image per click, with the next image selected by a deterministic function. Persuasive Cued Click Points (PCCP) extends CCP by requiring a user to select a point inside a randomly positioned viewport when creating a password, resulting in more randomly distributed click-points in a password.

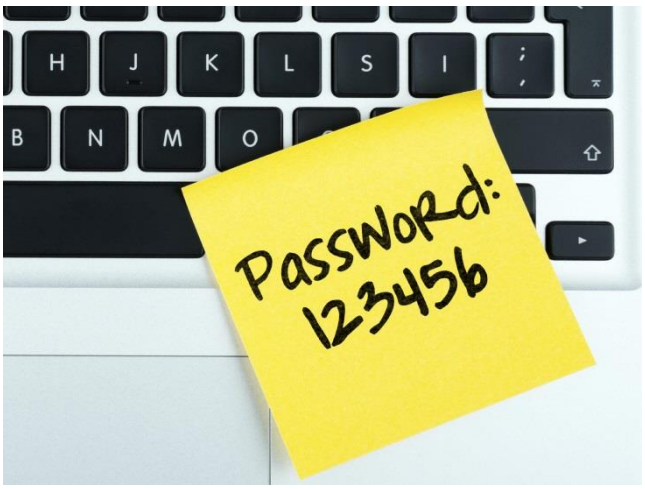
(adapted from www.ijcsit.com Vol.6 (1), research.microsoft.com ITonIFaS Vol 9, arxiv.org IJSPTM Vol 2, ai.pku.edu.cn)

Questions 11-25

Complete the chart below with words from the text. Write **NO MORE THAN THREE WORDS** for each answer.



Listening



"A password should be like a toothbrush. Use it every day; change it regularly; and DON'T share it with friends."

You are going to listen to the interview with David Emm, a Senior Security Researcher at Kaspersky, UK Global Research and Analysis Team.

What are the advantages and disadvantages of passwords?

Can you recommend any ways to protect passwords? Do you agree with the hints presented below?

Questions 1-17

Questions 1-2

Choose the correct 2 letters **A**, **B** or **C**.

1. What are the most dangerous mistakes people make?

A one password for all accounts

B writing password everywhere

C recycling passwords

2.What should people do?

A have a key word

B have ways to create a unique password

C realize that password is your identity

Hints for protecting passwords:

- Don't allow any logins without passwords (every account must have a password).
- Don't keep passwords that may have come with your system.
- Don't ever let anyone use your password.
- Don't write your password down.
- Don't type a password while anyone is watching.
- Don't record your password online or send it via e-mail.
- Don't keep the same password indefinitely.

What is a strong password? How to create it?

Questions 3-6

Complete the table below. Write down ***NO MORE THAN THREE WORDS*** for each answer.

How to create a unique password:

a. use the words that are not in the 3. _____.
b. try not to use the words that are 4. _____.
c. mix up letters, numbers and 5. _____ to 6. _____.

Question 7

Choose the correct 2 letters **A**, **B** or **C**.

7. What should people do to memorize their passwords?

A create their own formula

B have favourite passphrase

C have the same part in all passwords

Questions 8-11

Complete the flow chart below. Write down ***NO MORE THAN THREE WORDS*** for each answer.

Step process of creating formula

take 8. _____ of the word and move it to the end

↓

put 9. _____ after the third character

↓

10. _____ the fifth character

↓

Glossary:

jumble
verb /ˈdʒʌmbl/ (also jumble up)
to mix things together in an untidy way

reverse
verb /rɪˈvɜːs/
to change a situation or change the order of things so that it becomes the opposite

scramble
verb /ˈskræmbl/
to move or climb quickly but with difficulty, often using your hands

enterprise
noun /ˈentəpraɪz/
a business or organization

vendor
noun /ˈvendɔːr/
someone who sells something outside

take another character and
11. _____ in that string

Questions 12-17

Complete the sentences below. Write down ***NO MORE THAN THREE WORDS*** for each answer.

12. If you lose your password there is a _____ to reset it.
13. This _____ feature is a great advantage for potential attackers to apply to reset the password.
14. You should pick things for questions that are not easy to _____ from social networks.
15. Kaspersky Lab offers an _____ producing unique passwords.
16. There is the risk in business that some third party can look a password over _____.
17. One should be careful and keep the password in a _____.

Speaking

Imagine you are members of the department responsible for security of the company. You are supposed to present the best ways of protecting the data to the CEO. So you are to have a **meeting** to discuss pros and cons of each type of authentication to choose the best one that can meet the company's security need. Choose the chairperson first. Practice using "Useful language".

Asking for opinions What are your views? How do you feel about? Do you think…? Do we all agree?	**Giving opinions** In my opinion… From a … point of view… Personally I think… I really do think… I'm inclined to think… I'm quite sure…
Agreeing I agree completely. Yes, that's an important point. Yes, definitely. Yes, … is right. Yes, I'd go along with that. Yes, I agree with that.	**Disagreeing** I'm afraid I can't agree with that idea. I don't think so. Sorry, but I don't agree. **Expressing reservations** You could be right, but… Maybe, but…
The Chair Person: **Opening** Shall we start? **Starting objectives** The aim of the meeting is to… **Beginning of the discussion** …, would you like to start? **Interrupting** Just a minute, … , could I just ask something? Before you go on could I say something? **Asking for clarification** Sorry, I don't quite follow you. Could you explain what you mean by… **Checking agreement** Do we all agree then? **Moving on**	

Let’s move on to the next topic.

Concluding

Well, I think that’s everything. Is there anything else you want to discuss?

Summarizing

So, to sum up, we’ve agreed that…

Closing

Good. Let’s call it a day, then.

Reading 2 Vocabulary and Pronunciation

What is Encryption?

Can you give definition of Cryptography?

What kinds of Encryption do you know?

What are their positive and negative sides?

What is the difference between them?

Read the article once. Find definitions of the following words and pronounce them:

Cryptography /krɪpˈtɒg.rə.fi/

Cipher /ˈsaɪ.fər/

Encryption

Although there are many ways to protect information from undesired access, including various physical security techniques that prevent any access from unintended receivers, it is most useful to safeguard data so that it can be transmitted over insecure networks, such as the Internet, without fear of compromise. Since the time of the ancient Egyptians, cryptography, or the art of secret writing, has been employed to keep key information private. Encryption algorithms or *ciphers* are mathematical formulas or functions applied to data to transform the unprotected information, or *plaintext* or *cleartext,* into an unrecognizable format commonly referred to as *ciphertext.* There are generally two inputs to an encryption algorithm: a *key* and the plaintext itself.[3] In some cases the ciphertext is larger than its associated plaintext or the same size. The goal is to make the time it would take to recover or *decipher* the plaintext, having only the ciphertext and not the key, so long as to greatly exceed the time-value of the

Plaintext /ˈpleɪnˌtɛkst/
Ciphertext
A key /kiː/
Decipher /dɪˈsaɪfər/
Brute-force methods /bruːt- fɔːs ˈmeθəd/
Symmetric encryption /sɪˈmetrɪk ɪnˈkrɪpʃən/
A one-time pad /ˈwʌntaɪm pæd/
Substitution ciphers /ˌsʌbstɪˈtjuːʃən/
Transposition ciphers /ˌtræn.spəˈzɪʃ.ən/
Diffusion ciphers /dɪˈfju·ʒən/
The Avalanche effect /ˈævəlɑːnʃ ɪˈfekt/
Block ciphers /blɒk/
Stream ciphers /striːm/
Public key encryption
Sender non-repudiation /rɪˈpjuːdieɪʃən/
A digital signature /ˈdɪdʒɪtəl ˈsɪgnətʃər/

Match the following transcriptions, **A**-**I**, with the highlighted words and pronounce them.

plaintext. Ideally, a strong algorithm and key combination should take at least millions of years to break, based on mathematical predictions. Naturally, if an interloper manages to somehow obtain the ciphertext and the key, deciphering the information is as straightforward as it is for the intended receiver, and therefore all security is lost.

Much of security is predicated on strong methods of keeping encryption keys sacrosanct, in order to force attackers to use *brute-force* methods, such as trying every possible key combination with the use of fast computers. The ideal algorithm is strong, meaning that the algorithm itself is relatively impervious to direct attack, leaving attempts to derive or guess the key as the only practical avenue to breaking the encryption. The ideal encryption algorithm creates unique ciphertext from the same plaintext for each key permutation, among other traits.

So what exactly is a key? A key is simply a number with a predetermined length. Keys can be created or generated in many ways, but computers commonly generate them. Ideally, each key is truly random, meaning that any possible key combination is equally likely and that keys are not generated in a predictable fashion. A random number generator (RNG) or a pseudo-random number generator (PRNG) is frequently used for this purpose. The difference between an RNG and a PRNG is that the RNG autonomously generates random numbers, whereas a PRNG is computer-based and creates a somewhat

A /siːd/
B /ɪnˈvaɪə.lə.bl̩/
C /beər/
D /ˈsækrəʊsæŋkt/
E /bʌlk/
F /daɪˈvʌldʒ/
G /ˌfiːzəˈbɪləti/
H /sjuːdəʊ-/
I /ˈbʌndl/

Read the article again. Try to work out the meaning of the highlighted words. Then match them with their definitions, a-i.

a._____
verb to give secret or private information to someone

b._____
verb to carry something

c._____ *adj* too important to be changed or destroyed

random number based on *seed* values that are readily available within the computer. A significant threat to any PRNG is the feasibility of regenerating the key if one can determine the seed values.

Encryption algorithms are divided into two families based on the key type: symmetric or secret key, and asymmetric or public key encryption. In symmetric key encryption both the sender (encrypter) and receiver (decrypter) use the same secret key, so named because the strength of the system relies on the key being known only to the sender and receiver. In asymmetric key encryption, the sender and receiver each have distinct but mathematically related keys.

Symmetric encryption is the oldest form of encryption and has been used to safeguard communications for over three thousand years. All secret key algorithms or systems require that the party generating the key share or transfer it to the other party in a secure manner. If the key is not transferred by some means that prevents its interception by unintended receivers and attackers, whatever strength is inherent in the algorithm is compromised and the confidentiality of data encrypted with the key cannot be guaranteed. Thus, when considering a symmetric key encryption scheme, it is equally important to evaluate the key transfer mechanism.

Figure 1 illustrates the encryption process using a symmetric key cipher. Sometimes other values are provided to the encryption algorithm for initialization purposes. The resulting ciphertext will bear no

d._____
noun a number of things that are tied together

e._____
noun possibility to do

f._____ *adj* the source, beginning, random

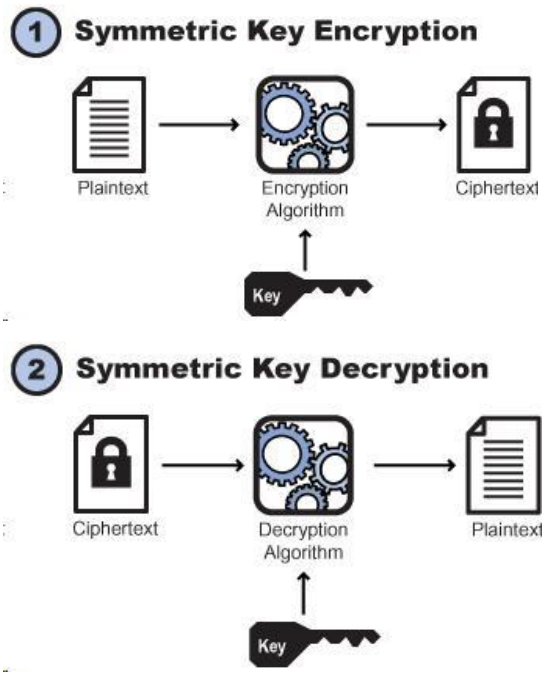
g._____
noun the large size of something or someone

h._____
false

i._____ *adj* that must be respected and not removed or ignored

Can you read the following acronyms: RNG, PRNG, RSA?

relation to the plaintext. Figure 2 shows how decryption is accomplished by reversing the process. If values other than the key were used to initialize the encryption operation, they are required inputs to the decryption algorithm. The resulting plaintext will be a faithful reproduction of the original plaintext. Using the wrong key in the decryption process, even if different from the correct key by just one bit, results in meaningless output.



Along the way, it was also determined that if the key was only used once then destroyed, the resulting system, called a *one-time pad,* is mathematically proven to be unbreakable through cryptanalysis. Naturally, a lot more keys have to be transferred when using a one-time pad and the keys still need to be distributed in a secure manner, so this is not commercially feasible.

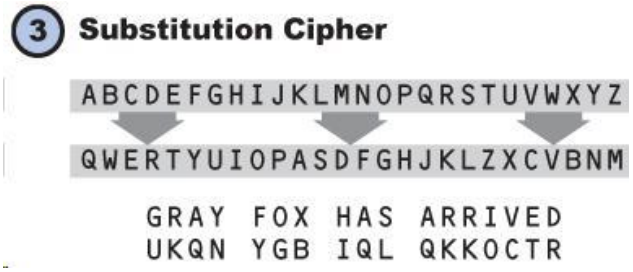
Symmetric encryption algorithms are primarily used for bulk encryption of data, such as an entire file,

The following are the secret key algorithms listed in chronological order of their inception.

Data Encryption Standard (DES)
DES is a standardized and published encryption algorithm, approved by the U.S. Government in 1977 after considerable analysis. The genesis of DES is traced back to a cipher termed Lucifer, invented by Horst Feistel of IBM. It uses a 56-bit key, which is sometimes stored with additional parity[7] bits, extending its length to 64 bits. DES is a block cipher and encrypts and decrypts 64-bit data blocks. Although at the time of its inception, the effort to crack a 56-bit key was considered so enormous as to prevent brute-force attacks, it is now considered insecure, and all government agencies must use algorithms with longer keys, as discussed below. Despite the obsolescence of DES due to its key length, it is quite elegant and the most cryptanalyzed algorithm in the world, withstanding all attacks on the algorithm itself.

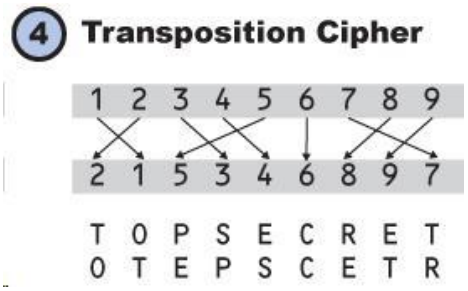
RC4
RC4 is a stream cipher, also created in 1987, and its only complexity is in the generation of the keystream, which is potentially an infinitely long sequence of key values, which start with a 40- or 128-bit key, and a 24-bit initialization vector

document, or bundle of transaction data. The two fundamental symmetric encryption techniques are *substitution* and *transposition.* Substitution ciphers are simple and operate by *replacing* each character with another character, for example, the letter 'a' would be substituted for the letter 'g' every place it occurs. Substitution ciphers are rarely used today due to the ease in breaking them with frequency cryptanalysis, in which the frequency of encrypted characters in the ciphertext is used to derive the plaintext. Figure 3 is an example of a substitution cipher.



In contrast, transposition ciphers operate by moving plaintext characters to new locations in the ciphertext, rather than by substituting individual characters. An example of a simple transposition cipher is the word jumble or cryptogram in a newspaper. All the characters found in the plaintext are in the ciphertext, but in different relative positions. Unlike a word jumble, which is a random transposition, transposition-based encryption works by moving characters around in a definite pattern that is reversed to decrypt the ciphertext. Pure transposition ciphers are not used in modern cryptography because of the ease of computer-based cryptanalysis. Figure 4 is an

example of a transposition cipher. The key for such a cipher is a representation for the character replacement scheme.



The principles of substitution and transposition are, however, combined into *diffusion ciphers*, which are used for all modern symmetric key ciphers. Diffusion algorithms not only substitute differing values for the plaintext characters, but also spread the characters throughout the ciphertext. A significant strength of many diffusion-based algorithms is that the same character will actually be encrypted into a different symbol based on its location in the plaintext and the data that precedes it.

The best secret key algorithms possess a property known as *the Avalanche effect*, in which even a one-bit change in the plaintext results in changes in approximately one-half of all the ciphertext bits. Symmetric ciphers are fast and typically compact in terms of their computer code size and memory requirements, which is important as encryption capabilities are extended to devices like PDAs and smart phones that have power, processor, and memory limitations.

Symmetric algorithms can be further divided into *block* and *stream* ciphers. Block algorithms encrypt

The actual encryption step is very simple; the keystream is combined with the plaintext in an XOR (XOR stands for 'exclusive OR' and is a standard logical operation performed on two values on a bit-wise basis. If one value is '0' and the other '1,' the XOR output is '1,' whereas the XOR output is '0' if either both inputs are '0' or '1.' The XOR operation is not only extremely fast, but has the useful property of being symmetric. For example, if the first four bits of the keystream and plaintext are, respectively, '1011' and '0010,' the result of XORing them is '1001,' the ciphertext. Notice how decryption works: the keystream is identical, so '1011' and '1001' are XORed, resulting in '0010,' the original plaintext) operation. Using the same key and IV, the keystream is totally reproducible, so in practice the sender and receiver using this algorithm will each be generating an identical keystream. RC4 is ten times faster than DES.

and decrypt a fixed-size block of cleartext and ciphertext, respectively, usually a multiple of 64 bits. Stream ciphers, on the other hand, continuously encrypt any amount of data as it is presented, usually by mathematically combining the data with a *keystream*, an infinitely long key sequence that is generated based on a finite key starting value.

Public Key Encryption

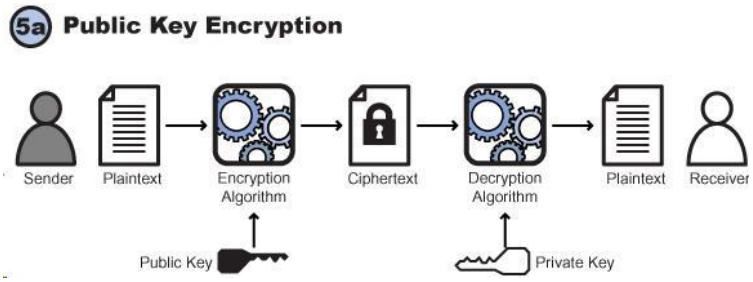
It was made by Ronald Rivest, Ari Shamir and Leonard Adleman, all researchers at MIT and inventors of the public key encryption algorithm called RSA. RSA not only eliminated the need to transfer secret keys, but also facilitated convenient and efficient encryption by removing the Diffie-Hellman requirement of exchanging values back and forth.

Figure 5a demonstrates how RSA works. Note that the public and private keys referenced in the figure are part of the receiver's *key pair*. When the sender wishes to encrypt information that only the receiver can decrypt, she uses the receiver's public key to encrypt. The public key, as the name suggests, can be freely distributed in the clear. It can be sent via electronic or postal mail, posted on a billboard, or spoken over the telephone without sacrificing any security. It is essential, however, that the private key be kept inviolable and never shared or divulged to anyone.

RC5
RC5 is a fast, parameterized block cipher, with a variable block size (32, 64 and 128 bits), variable key size (0 to 2040 bits), and a variable number of rounds (0 to 255), or individual encryption steps.RC5 is patented by RSA. It can be used as a drop-in replacement for DES, with the block size set to 64 bits and the key size set to 56 bits.

Triple DES (3DES)
Triple DES is simply three successive encryptions with DES.It is possible to use either 2 or 3 distinct keys with 3DES. Thus, for the three-key case, one obtains the benefit of a 168-bit key space with the known strength of the DES algorithm. Performed correctly, 3DES is as unbreakable a secret-key algorithm as any known, but it is slow. 3DES is defined as ANSI standard X9.52.

Advanced Encryption Standard (AES)
The National Institute of Standards and Technology (NIST) selected an algorithm called "Rjindael" on October 2, 2000 as the AES in a multi-year competition. AES replaced DES. AES is projected to provide secure encryption of sensitive but unclassified government information until 2020. Rjindael is a fast block cipher, with variable key length and block sizes (each can be independently set to 128, 192 or 256 bits). AES became an official U.S. Government standard in 2002. Like DES before it, AES is now widely used for commercial and private encryption purposes. One significant benefit of AES is that the algorithm is public, and its use is unrestricted, with no royalties or license fees owed to the inventors or the government.
RSA is the undisputed leader in public key encryption. The algorithm's one-way function is based on the *intractability,* or mathematical difficulty, of factoring the product of two prime numbers. In RSA, the product of the prime numbers is the public key, and the two prime numbers make up the private key. If an attacker can factor the public key, the private key is thus compromised, and it is possible to decrypt information encrypted with the public key.



Note the fundamental differences between asymmetric and symmetric key encryption. When using secret key ciphers, there is a different secret key for each pair of parties communicating. In the public key case, there is just one key pair for each receiver, because the public key can be distributed to everyone who wants to send encrypted data to the receiver. Having the public key allows senders to encrypt data, but without the private key, they are unable to use the public key to decrypt communications from anyone else using the same key pair.

Equally important as the advantages inherent in public key encryption is the support for the properties of *authentication* (identification of the sender) and *sender non-repudiation* (the inability of a sender to refute that they signed something encrypted with their private key). Since anyone with the sender's public key can decrypt a message encrypted by the sender's private key, this type of encryption, called a *digital signature,* does not protect the confidentiality of the message. The sender is prevented, however, from denying that he was the originator of the information thus signed, unless the private key was compromised. (adapted from http://www.infosectoday.com)

Writing

- Make a plan;
- Make sure you have an introduction, 2-3 paragraphs giving reasons and examples, and a conclusion;
- Check for errors – spelling, grammar, punctuation and appropriate (formal) language;
- Make sure you answered all parts of the question;
- Check you have written enough (not more than about 290).

You should spend about 40 minutes on this task. Write at least 250 words.

Write about the following topic:

The importance of computers and networks and the information they store and communicate to society today are equaled only by the threats to them. The recent departure of Google from mainland China over a widely-publicized attack there on its e-mail system is an ominous reminder of the growing attacks on data and communication networks. The encryption algorithms are in many instances the only protection between our critical information and those who seek to compromise and exploit it.

To what extend do you agree or disagree with this statement. Give reasons for your answer and include any relevant examples from your own knowledge or experience.

- ✓ Don’t repeat the question in your introduction. Try to paraphrase it;
- ✓ avoid repeating the same words, keep changing phrases to show flexibility. Improve your written work by using a variety of connecting words: though, unfortunately, consequently, in addition (to), therefore, in fact, despite (the fact that), however, although, also, what is more, more over, as a result (of)…
- ✓ try to vary the sentence structures you use, different grammar constructions like gerund, conditional sentences, passive voice:
  Many people believe that… – It is commonly believed that…, Some people think that…- It is often thought that…,
  It is considered by many that…
  It is argued by some that…
  Some people support the opinion that…;
- ✓ write complex sentences joining some sentences using sequencing words and relative pronounce (which, that, where, when). Be careful with punctuation (defining, non-defining clauses);
- ✓ include opinions, reasons and examples to extend your answer: for example/instance…; to illustrate…; as an illustration,…; to give a clear example,…; this can be seen by..;
- ✓ conclusion is a short paragraph which summarises your arguments. Don’t introduce new ideas!

UNIT 3 COMPUTER SYSTEM SECURITY

Revise and Check

CAN YOU…

…speak about

Authentication and its types: token based, biometrics, knowledge based

Passwords: cons and pros, hints to protect and create

Cryptography

Encryption and its types (symmetric, public), their positive and negative sides and difference between them

…hold and take part in a meeting

…write an essay

…pronounce and give definition of

Authentication
biometric
identification
enrollment
iris
retina
accuracy
properly
capture
intrusiveness
invasive
sophisticated
strokes
glean
distinguishing
eigenfaces
Countermeasures
Simultaneously
Distinctive
Absorb
Infrared
Tissue
Entrenched
Virtually
Versatile
Decoys
Rounds
Permuted
Cumulative
Cue
Grid
Sequence
jumble
reverse
scramble
enterprise
vendor
Cryptography
Cipher
Plaintext
Ciphertext
A key
Decipher
Brute-force
methods
Symmetric
encryption
A one-time pad
Substitution
ciphers
Transposition
ciphers
Diffusion
ciphers
The Avalanche
effect
Block ciphers
Stream ciphers
Public key
encryption
Sender non-
repudiation
A digital
signature
Sacrosanct
Pseudo
Seed
Feasibility
Bear
Bulk
Bundle
Inviolable
Divulge

UNIT 4 NETWORK SECURITY

Speaking and Vocabulary

1. Choose the most relevant definition of Network Security. Prove your choice.

Network security is protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system

The authorization of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password that allows them access to information and programs within their authority.

Network security is an over-arching term that describes that the policies and procedures implemented by a network administrator to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources.
This means that a well-implemented network security blocks viruses, malware, hackers, etc. from accessing or altering secure information.

2. Study the following words. Work out definition for each.

Adware	Back up	Denial of Service	Bot
Compromised	Configure	Validation	Botnet
computer	Extended	Flash drives	Drive-by
Encryption	Firewall	Mobile device	download
Firmware	Malware	Spyware	Instant

Key logger	Software	Vulnerability	messaging
Phishing	patches	Payment	Peer-to-peer
URL	Virus	Data stewards	(P2P)
	Credit Card		Trojan
			Worm
			Processing

3. Now work out definition for network security. Try to use words from exercise 2. Explain how each of the word is connected with network security.

4. Fill in the gaps. Use words given in exercise 2.
   a. _____ a portable, wireless computing device that is small enough to be used while held in the hand.
   b. _____ widespread or extensive
   c. _____ software that is installed surreptitiously and gathers information about an Internet user's browsing habits, intercepts the user's personal data, etc., transmitting this information to a third party:
   d. _____ a person responsible for the management of data elements
   e. _____ to try to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one.
   f. _____ to put together by supplying, arranging, or connecting a specific set of internal or external components:
   g. _____ the process of converting data to an unrecognizable form.

h. _____ a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules.
i. _____ to give official sanction, confirmation, or approval to, as elected officials, election procedures, documents.
j. _____ a continuous action, operation, or series of changes taking place in a definite manner.
k. _____ any malicious computer program which misrepresents itself as useful, routine, or interesting in order to persuade a victim to install it.
l. _____ capable of or susceptible to being wounded or hurt, as by a weapon
m. _____ software that displays advertisements and is integrated into another program offered at no charge or at low cost.

5. Write 10 different sentences using words from exercise 2.

Reading

What are the main principles of network security? Try to work them out without reading the text.

Note: The order of question might differ from the text order.

WHAT IS NETWORK SECURITY?

Network Security is an organization's strategy and provisions for ensuring the security of its assets and of all network traffic. Network security is manifested in an implementation of security policy, hardware, and software. For the purposes of this discussion, the following approach is adopted in an effort to view network security in its entirety:

Now read the text. Are those principles the same with yours?

Do the following statements agree with the information given in the text? Write **T**(true), **F**(false), **NG**(not given) next to the sentences 1-7.

1. To understand what network security is we must take into account such things as: policy, enforcement, auditing.
2. The main goal of network security is to save information
3. Network security is high-cost service.
4. Firewall is not important in the process of network security.
5. Policy management can be simplified by CIA.
6. CIA is complexity, identity and availability.

Policy

Enforcement

Auditing

The IT Security Policy is the principle document for network security. Its goal is to outline the rules for ensuring the security of organizational assets. Employees today utilize several tools and applications to conduct business productively. Policy that is driven from the organization's culture supports these routines and focuses on the safe enablement of these tools to its employees. The enforcement and auditing procedures for any regulatory compliance an organization is required to meet must be mapped out in the policy as well.

Enforcement

Most definitions of network security are narrowed to the enforcement mechanism. Enforcement concerns analyzing all network traffic flows and should aim to preserve the confidentiality, integrity, and availability of all systems and information on the network. These three principles compose the CIA triad:

Confidentiality - involves the protection of assets from unauthorized entities

Integrity - ensuring the modification of assets is handled in a specified and authorized manner

Availability - a state of the system in which

7. Additional services for network security are now available as add-ons.

Choose the correct letter, **A, B, C** or **D**.

8. One of following terms is not used in terms of network security:
   A. Enforcement
   B. Policy
   C. Detection
   D. Protection

9. Which of those is the layer for controlling network:
   A. Authentication
   B. Decryption
   C. Adware
   D. confidentiality

10. Auditing gives company:
    A. opportunity to fire people
    B. a chance to work out new criteria for network security
    C. to save time and

authorized users have continuous access to said assets.

Strong enforcement strives to provide CIA to network traffic flows. This begins with a classification of traffic flows by application, user, and content. As the vehicle for content, all applications must first be identified by the firewall regardless of port, protocol, evasive tactic, or SSL. Proper application identification allows for full visibility of the content it carries. Policy management can be simplified by identifying applications and mapping their use to a user identity while inspecting the content at all times for the preservation of CIA.

The concept of defense in depth is observed as a best practice in network security, prescribing for the network to be secured in layers. These layers apply an assortment of security controls to sift out threats trying to enter the network:

Access control
Identification
Authentication
Malware detection
Encryption
File type filtering
URL filtering

These layers are built through the deployment of firewalls, intrusion prevention systems (IPS), and antivirus components. Among the

money

D. to start a new project.

11. Next generation firewall gives opportunity to:

A. download content easily

B. to surf the internet

C. to observe the traffic coming from all ports.

D. to build up our own computer.

components for enforcement, the firewall (an access control mechanism) is the foundation of network security.

Providing CIA of network traffic flows was difficult to accomplish with previous technologies. Traditional firewalls were plagued by controls that relied on port/protocol to identify applications—which have since developed evasive characteristics to bypass the controls—and the assumption that IP address equates to a user's identity. The next generation firewall retains an access control mission, but reengineers the technology; it observes all traffic across all ports, can classify applications and their content, and identifies employees as users. This enables access controls nuanced enough to enforce the IT security policy as it applies to each employee of the organization, with no compromise to security.

Additional services for layering network security to implement a defense in depth strategy have been incorporated to the traditional model as add-on components. Intrusion prevention systems (IPS) and antivirus, for example, are effective tools for scanning content and preventing malware attacks. However, organizations must be cautious of the complexity and cost that additional components may add to its network

Glossary:

Enforcement The act of compelling observance of or compliance with a law, rule, or obligation.

Integrity The condition of being unified or sound in construction.

Authentication The process or action of proving or showing something to be true, genuine, or valid.

Malware Software which is specifically designed to disrupt or damage a computer system.

security, and more importantly, not depend on these additional components to do the core job of the firewall.

Auditing

The auditing process of network security requires checking back on enforcement measures to determine how well they have aligned with the security policy. Auditing encourages continuous improvement by requiring organizations to reflect on the implementation of their policy on a consistent basis. This gives organizations the opportunity to adjust their policy and enforcement strategy in areas of evolving need.

(adapted from https://www.paloaltonetworks.com)

Listening and Speaking

1. Do you know what social engineering is? Try to guess and work out meaning of it.

2. Now read the definition of social engineering. Were you right? Write down 5 main principles of social engineering.

Listen to a security expert James Lyne. How can you safe yourself from social engineering?

Questions 1-6

Complete the notes below.
Write **NO MORE THAN THREE WORDS** for each answer:

1. It is getting harder to crack the

The recording will be played ONCE only!

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.
The term "social engineering" as an act of psychological manipulation is also associated with the social sciences, but its usage has caught on among computer and information security professionals.

program because programmers learn lessons about how

_____

2. Criminals have to move to new way that is called as

_____

3. This way is based on _____ the things they shouldn't or _____ the information away.
4. First way of social engineering is

_____

5. _____ is one of the main principles of avoiding social engineering attacks.
6. Create _____. The more controls your implement much more luck you can avoid attacks on your computer.

Questions 7-11

Choose the correct letter **A, B, C** or **D**.

7. New ways of cheating are emerging because:

A. people are getting more stupid

B. people learn their mistakes

C. people are trying something new

D. just for fun

Glossary:

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Gmail- short for google mail.

Intercept - To gain possession of (an opponent's pass), as in football or basketball.

Awareness- the state or condition of being aware; having knowledge; consciousness

8. The main principle of social engineering is:

   A. to push person to press link and give information away

   B. to steal information

   C. to get information by asking people he or she knows

   D. to guess the password

9. One of the methods based on tricking person on sending him e-mail. It's called:

   A. Fishing

   B. Phishing

   C. Cheating

   D. Validating

10. James show how to:

    A. Steal passwords

    B. Play game

    C. Make up e-mail

    D. Buy a product

11. E-mail's home page was looking:

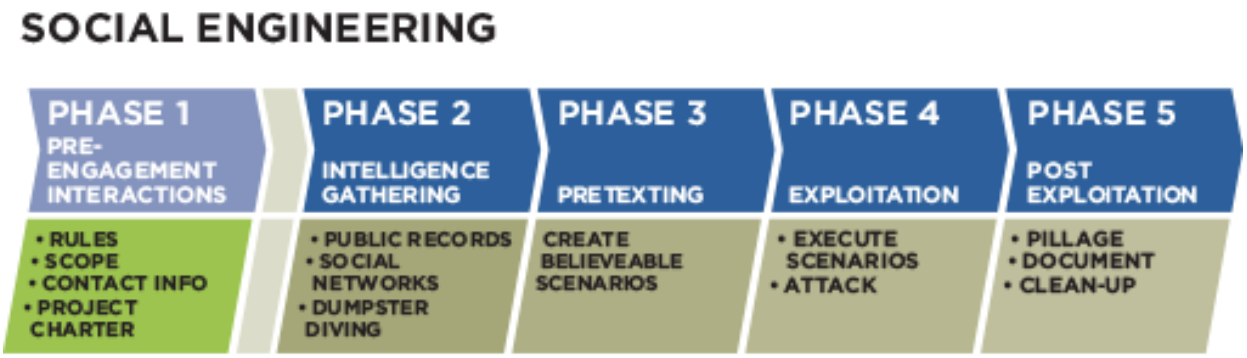
    A. Pretty normal

    B. Unusual

    C. Like new one

    D. Strange

3. You can see the graph below. It shows typical social engineering scheme. Try to think over different scenarios that can be connected with this graph.



Writing

You should spend about 20 min on this task. Write at least 150 words.

This chart shows the distribution of malicious traffic sources detected inside healthcare networks. Notice that the fourth largest source is “radiology imaging software.”

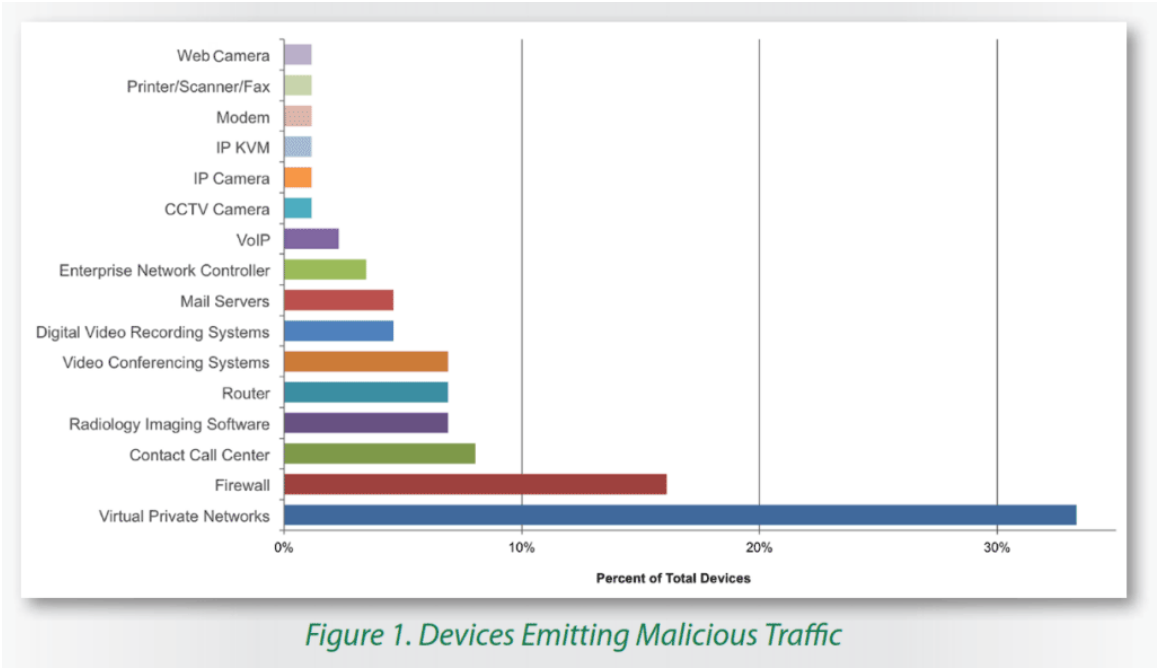


Figure 1. Devices Emitting Malicious Traffic

How many healthcare providers even realize that medical devices and radiology software can be hacked? HIPAA network security requirements suggest these systems should be locked-down. Write our own way of solving this problem by discribing a chart.

Useful vocabulary

Increases:	a slight / notable / significant decrease in ...
a slight/constant/marked/substantial/increase in sales	the downturn began in (month)
an increase of about/roughly/approximately/in the region of ... %	the situation began to deteriorate in (month)
a little over/above what we predicted	the number has continued to fall
the recovery/upturn began in	**Fluctuations:**
an overall increase in .	a slow start developed into steady progress in sales
an upward trend in the demand for ...	an initial upward trend was followed by ...
sales reached record levels / reached a peak in	we note slight fluctuations through the year
a strong surge in the sales of ..	normal seasonal variations are the cause of occasional downward trend
by (month), the figure had risen to ...	sales have been (rather) irregular
Decreases:	the level / the rate has been unstable since ...
just under our target	you will note a certain instability in the rate of

CAN YOU:

…pronounce and give definition of:

Adware

Compromised computer

Encryption

Firmware

Key logger

Phishing

URL

Back up

Configure

Extended

Firewall

Malware

Software patches

Virus

Credit Card

Denial of Service

Validation

Flash drives

Mobile device

…give definition of

Network security

…speak about:

Network security

Phishing

Social engineering

…describe:

bar charts

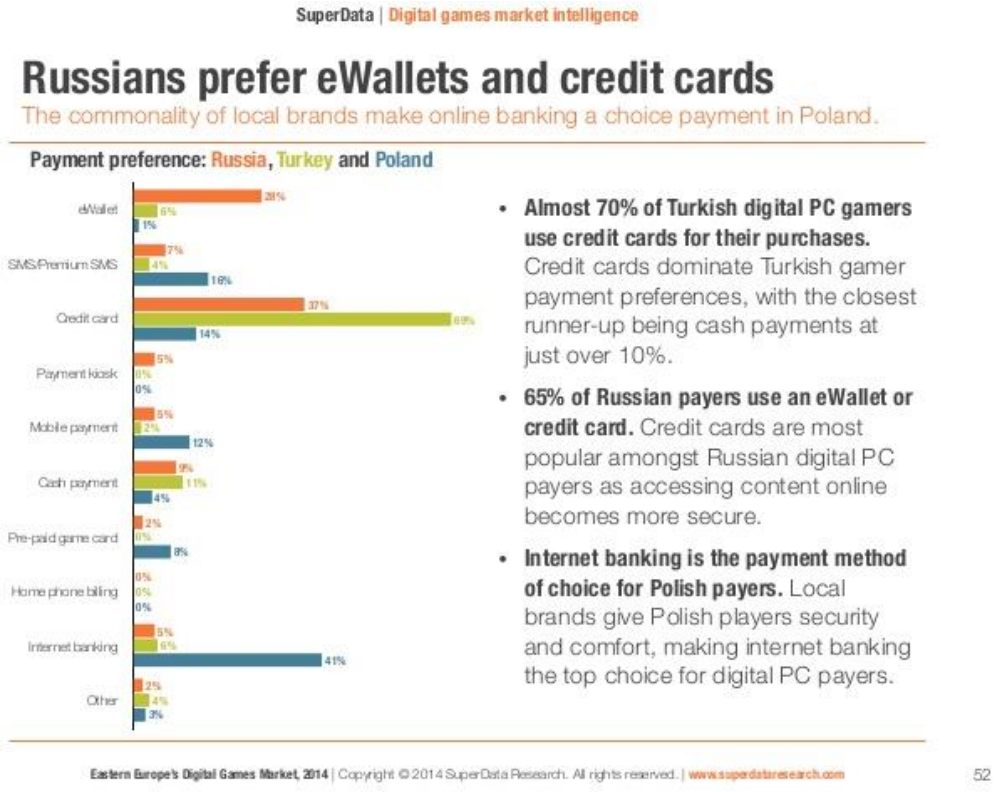
UNIT 5 ONLINE BANKING SECURITY

Speaking

1. Give the definition of online banking.
2. Study the main threats while using the internet. Give example of each when using online banking systems.

- viruses and worms: programmes that self-replicate or are sent over the internet by e-mail and can damage your PC;
- Trojans: programmes that, unbeknown to the user, compromise computer security by intercepting passwords, for example;
- phishing: using a false name, website or address for fraudulent purposes;
- pharming: redirecting users to a fraudulent server;
- rootkits: malicious software giving unauthorised administrator-level access without the real administrator noticing; they share certain features with trojans;
- hacking: unauthorised access to a PC via the internet.

3. Study the given graph. Give brief analysis of it. Use tips from the previous units.



Reading Vocabulary and Pronunciation

Do you use online banking systems in everyday life?

Write pluses and minuses of it.

Questions 1- 5

Complete the sentences below. Write down **NO MORE THAN THREE WORDS** for each answer.

1. US government concerned with the use of _____ because they are to be controlled by military technology.
2. Businesses concerns are usually connected

Concerns About Electronic Banking

Since Electronic Banking is a new technology that has many capabilities and also many potential problems, users are hesitant to use the system. The use of Electronic Banking has brought many concerns from different perspectives: government, businesses, banks, individuals and technology.

Government

From a government point of view, the Electronic Banking system poses a threat to the Antitrust laws. Electronic Banking also arouse concerns about the reserve requirements of banks, deposit insurance and the consumer protection laws associated with electronic transfer of money. The US government is concerned with the use of high quality of encryption algorithms because encryption algorithms are a controlled military technology.

Businesses

Businesses also raise concerns about this new media of interaction. Since most large transfer of money is done by businesses, these businesses are concern about the security of their money. At the same time, these businesses also consider the potential savings in time and financial charges (making cash deposits and withdrawals which some banks charge money for these processes) associated with this system. Another businesses concern is connected to the customer. Businesses ponder the thought that there

with _____.

3. Investing between time of deposit and the time of withdrawal is called _____.
4. Individuals are concerned about _____ access to their account and _____ of their personal information.
5. Keys areas in technology accepts are: Security, _____.

Questions 6-10

Do the following statements agree with the information given in the

are enough potential customers who would not make a purchase because the business did not offer a particular payment system (e.g. electronic cash and electronic check). This would result in a loss of sales. On the other side of the coin, if this system becomes wide spread, this would allow more buying power to the consumer which puts pressure on businesses to allow consumers to use electronic transfer of money.

Banks

Banks are pressured from other financial institutions to provide a wide range of financial services to their customers. Banks also profit from handling financial transactions, both by charging fees to one or more participants in a transaction and by investing the funds they hold between the time of deposit and the time of withdrawal, also known as the "spread". With more financial transactions being processed by their central computer systems, banks are also concern about the security of their system.

Individuals

Individuals are mainly concern with the security of the system, in particular with the unwarranted access to their accounts. In addition, individuals are also concern with the secrecy of their personal information. 82% of American poled expressed concern over privacy of computerized data. As more and more people are exposed to the

text? Write **T**(true), **F**(false), **NG**(not given) next to the sentences 6-10.

6. Privacy section is not so important in aspect of security.

7. Authentication is one of the ways to cheat on person.

8. Online banking is one of the most safest ways to safe money.

9. Main concern of people is privacy of their personal information.

10. The lack of security can seriosly damage banking system.

information superhighway, privacy of information and the security that goes hand and hand with this information is crucial to the growth of electronic transactions. Some privacy technologies related to the electronic banking industry are electronic cash and electronic checks which will be discussed in the software solution section.

Technology

In order to provide effective and secure banking transactions, there are four technology issues needed to be resolved. The key areas are:

1. Security

Security of the transactions is the primary concern of the Internet-based industries. The lack of security may result in serious damages such as the example of Citibank illustrated in the earlier section.

The security issue will be further discussed in the next section along with the possible attacks due to the insufficient protections. The examples of potential hazards of the electronic banking system are during on-line transactions, transferring funds, and minting electric currency, etc.

2. Anonymity (Privacy)

Generally speaking, the privacy issue is a subset of the security issue and thus will be discussed in the Privacy Technology section later. By strengthening the privacy technology, this will ensure the secrecy of sender's personal information and further enhance the security of the transactions. The

examples of the private information relating to the banking industry are: the amount of the transaction, the date and time of the transaction, and the name of the merchant where the transaction is taking place.

3. Authentication

Encryption may help make the transactions more secure, but there is also a need to guarantee that no one alters the data at either end of the transaction. There are two possible ways to verify the integrity of the message. One form of verification is the secure Hash algorithm which is "a check that protects data against most modification." The sender transmits the Hash algorithm generated data. The recipient performs the same calculation and compares the two to make sure everything arrived correctly.

If the two results are different, a change has occurred in the message. The other form of verification is through a third party called Certification Authority (CA) with the trust of both the sender and the receiver to verify that the electronic currency or the digital signature that they received is real.

4. Divisibility

Electronic money may be divisible into different units of currency, similar to real money. For example, electronic money needs to account for pennies and nickels.

(adapted from http://csrc.nist.gov/)

Match the following transcriptions, **A-P**, with the highlighted words and pronounce them.

A. [ɪkˈspəʊz]
B. [ˈhɛzɪt(ə)nt]
C. [ˈmɜːtʃ(ə)nt]
D. [ˌvɛrɪfɪˈkeɪʃ(ə)n]
E. [ʌnˈwɒrəntɪd]
F. [kənˈsɜːn]
G. [trænˈzækʃ(ə)n]
H. [θrɛt]
I. [dɪˌvɪzɪˈbɪlɪtɪ]
J. [ɪnˈʃʊ(ə)rəns]
K. [ˌɪnsəˈfɪʃ(ə)nt]
L. [ɔːˌθɛntɪˈkeɪʃ(ə)n]
M. [ˈs(j)uːpəˌhaɪweɪ]
N. [ˌɪntəˈrækʃ(ə)n]
O. [wɪðˈdrɔːəl]
P. [ˈpɒndə]

Try to work out the meaning of the highlighted words. Then match them with their definitions, a-p.

a. _____ *noun* a statement saying you will be harmed if you do not do what someone wants you to do

b. _____ *verb* to relate to (something or someone) : to be about (something or someone)

c. _____ *noun* the capacity of being divided.

d. _____ *verb* think about or consider (something) carefully

e. _____ *noun* evidence that establishes or confirms the accuracy or truth of something:

f. _____ *noun* the process of determining whether someone or something is, in fact, who or what it is declared to be.

g. _____ *noun* An agreement between a buyer and a seller to exchange goods, services or financial instruments.

h. _____ *noun* a person who buys and sells commodities for profit; dealer; trader.

i. _____ *adj*. slow to act or speak especially because you are nervous or unsure about what to do

j. _____ *noun* mutual or reciprocal action or influence

k. _____ *adj*. lacking in what is necessary or required

l. _____ *noun* any very fast route or course

m. _____ *verb* to lay open to danger, attack, harm, etc.

n. _____ *adj*. Having no justification; groundless

o. _____ *noun* an agreement in which a person makes regular payments to a company and the company promises to pay money if the person is injured or dies, or to pay money equal to the value of something (such as a house or car) if it is damaged, lost, or stolen

p. _____ *noun* the act of taking money out of a bank account

Writing and Speaking

You should spend about 20 min on this task. Write at least 150 words.

Think over main principles of online banking. Do you agree with them?

The annual survey of 1,000 consumers was conducted for the ABA by Ipsos-Reid, an independent market research firm, Aug. 14 to 16. A list of questions asked was designed to take a snapshot of current consumer trends. You can see this graph below. Make an analysis.

What is your preferred banking method? Discuss pros and cons of them. Practice using "Useful language".

Useful language	On the other hand, we can
Many people think…	observe/notice/see that …

Let us consider what are the advantages and disadvantages of …

Let us start by considering the facts.

It is generally agreed today that…

The first thing that needs to be said is …

First of all, let us try to understand …

In conclusion, I can say that although ..

To draw the conclusion, one can say that …

The arguments we have presented … suggest that … / prove that … / would indicate that …

From these arguments one must … / could… / might … conclude that …

The other side of the coin is that …

Another way of looking at this question is to …

One should, nevertheless, consider the problem from another angle.

One should, however, not forget that …

On the other hand, …

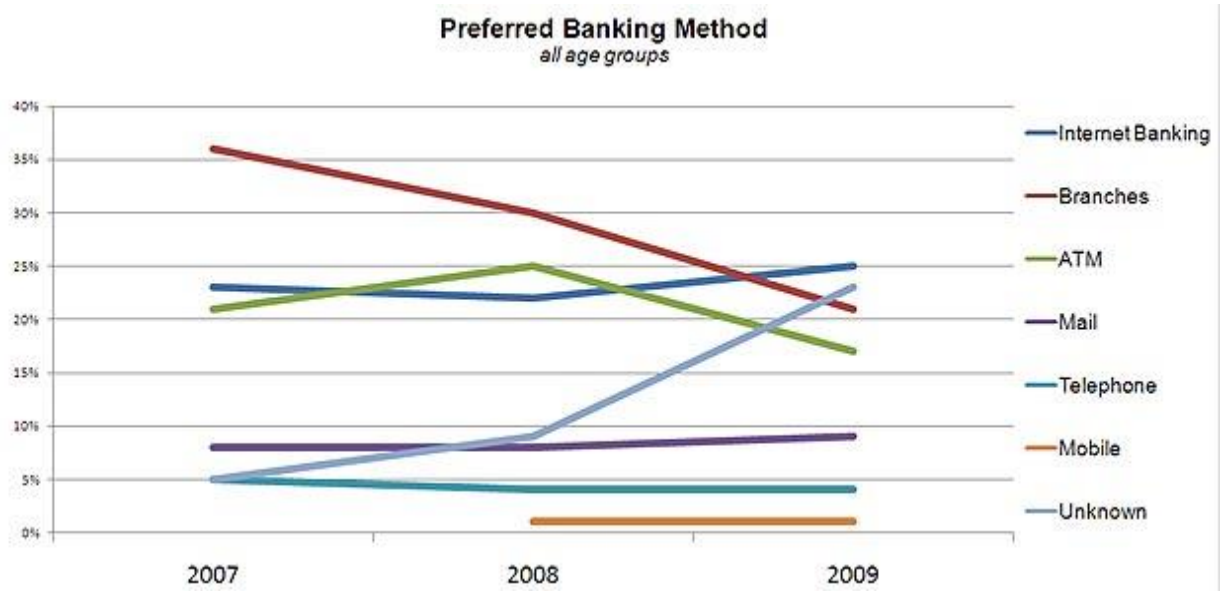
Although …

Perhaps, we should also point out the fact that …

One must admit that …

We cannot ignore the fact that …

Thus, … / Therefore,…



Listening

Write down minuses and pluses of online banking. Check up your opinion with Barbara's.

You are going to listen to a financial expert Barbara Shaw who explains how online banking can save you both time and money.

You will only hear each section ONCE!

Questions 1- 7

Complete the sentences below. Write down **NO MORE THAN THREE WORDS** for each answer.

Before you listen, try to predict what the answer will be

1. For many people _____ and _____ provided by online banking are the best part.
2. By online banking system you can make a _____ and check_____.
3. Many people spend much time sitting in front of the kitchen table going over _____, writing up_____ and putting them into _____.
4. _____ reduces the time you spend on banking.
5. Online banking is easy way to_____.
6. Online banking can help us save _____ and _____.
7. With bill service you can _____ to your bills.

Questions can be given in paraphrased forms!

UNIT 5 ONLINE BANKING SECURITY

Revise and Check

CAN YOU:

…pronounce and give definition of

hesitant

concern

threat

insurance

interaction

withdrawal

ponder

transactions

unwarranted

exposed

superhighway

insufficient

Authentication

merchant

verification

Divisibility

…describe

graphs

…speak about:

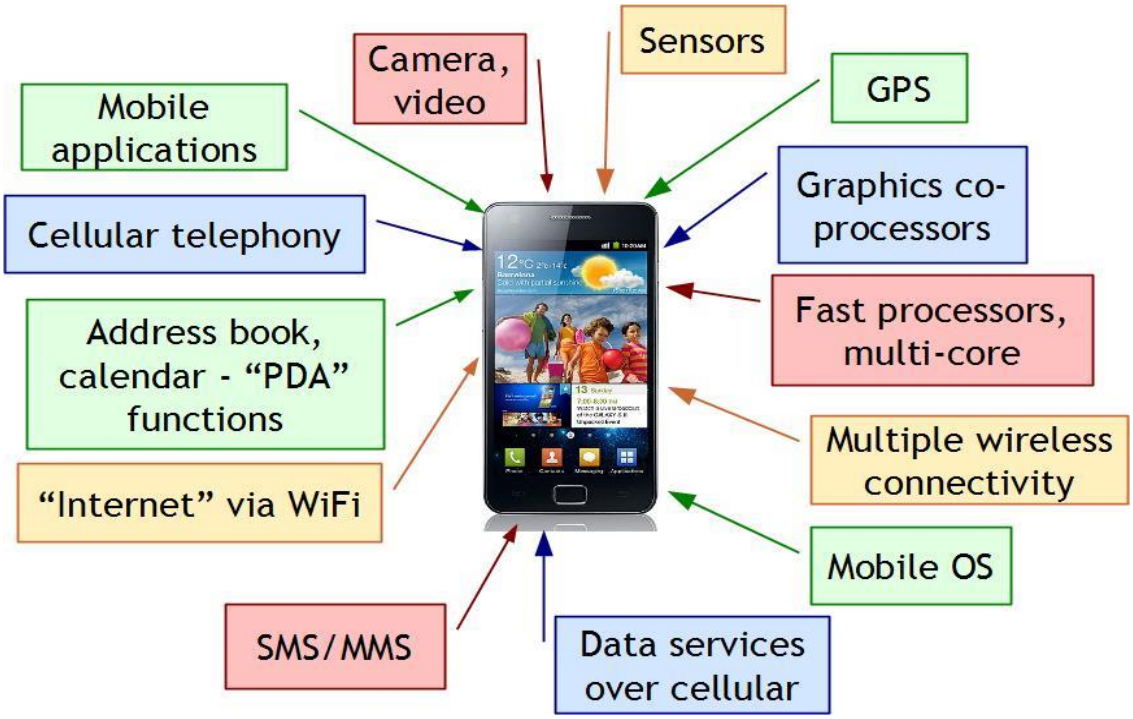
Online banking

UNIT 6 MOBILE DEVICES SECURITY

Speaking

1. Study the graph. Give short analysis for it. Do you think that this graph is right for nowadays?

2. Now work in pairs. Take a look at your partner's cell phone. Explain what type of phone is that. Use the chart below to help you.



Reading Vocabulary and Pronunciation

1. Do you think that mobile security is important in nowadays? Why? Prove your point.

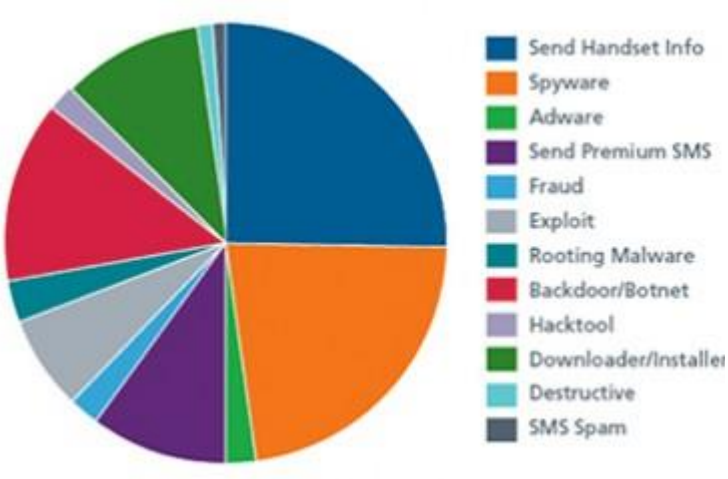
2. Match the following transcriptions, **A-L**, with the highlighted words and pronounce them.

   A. [səˈfɪstɪkeɪtɪd]
   B. [ˈluːkrətɪv]
   C. [kənˈviːnɪənt]
   D. [ʌn liːʃ]
   E. [ˈmɔltɪtjuːd]
   F. [prɒkˈsɪmɪtɪ]
   G. [prəˈtɛkʃ(ə)n]
   H. [dɪˈsɛmɪneɪt]
   I. [skæm]
   J. [prəˈlɪfəreɪt]
   K. [frɔːd]
   L. [ˈmælwɛə]
   M. [ˈvaɪtl]

3. Read the article once. Try to work out the meaning of the highlighted words. Then

Cybercriminals developing complex hacks of mobile devices

What's the future of cybercrime? In short, it's mobile devices. That's the new target for cybercriminals, and their attacks are getting more sophisticated. One of the biggest innovations in mobile technology is mobile banking, and cybercriminals are right on top of it with new ways to get into your account and hack other vital information, says a new report from McAfee Labs.



"In today's digital world, we use our smartphones for just about everything, so the idea of paying with your mobile device sounds fun and convenient. That is until a cybercriminal unleashes a near field communication (NFC) hack while you're sitting on the bus on the way to work or standing in line at an amusement park," says Lianne Caetano, director of mobility product marketing

match them with their definitions, a-k.

a. _____ *adj*. of or relating to life
b. _____ *verb* to _____ *adj*. altered by education, experience, etc., so as to be worldly-wise
c. abandon control of
d. _____*adj*. suitable or agreeable to the needs or purpose; well-suited with respect to facility or ease in use; favorable, easy, or comfortable for use.
e. _____ *verb* to scatter or spread widely, as though sowing seed; promulgate extensively; broadcast; disperse
f. _____ *noun* software intended to damage a computer, mobile device, computer system, or

at McAfee, in a post about the report. "An NFC attack deploys viruses that disseminate through proximity to quickly spread malware through a crowd, a process the McAfee Labs team calls 'bump and infect.' Once the malware infects a device, the scammer collects the details associated with your digital wallet account and secretly reuses these credentials to steal your money."

Caetano said NFC attacks are just one of several types of mobile scams that are expected to proliferate in 2013. As the smartphone market explodes, and the devices become capable of more important transactions, the hacks are becoming more sophisticated, destructive and difficult to spot.

In its newly released Mobile Security: McAfee Consumer Trends Report, McAfee Labs identified and analyzed a variety of mobile security threats. Here are two of the most common.

Bad Apps. Cybercriminals are going to great lengths to insert bad apps into trusted sources such as Google Play, and using them as the gateway to a multitude of mobile hacks. McAfee Labs found that 75 percent of the malware-infected apps downloaded by McAfee Mobile Security users were housed in the Google Play store, and the average consumer has a one-in-six chance of downloading a risky

computer network, or to take partial control over its operation.

g. _____ *noun* nearness in place, time, order, occurrence, or relation.

h. _____ *noun* the act of protecting or the state of being protected; preservation from injury or harm.

i. _____ *noun* a confidence game or other fraudulent scheme, especially for making a quick profit; swindle.

j. _____ *verb* to increase in number or spread rapidly and often excessively

k. _____ *noun* deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair

app. About a quarter of these risky apps contain both malware and a suspicious URL capable of generating click fraud or phishing schemes for personal information.

Complex malware. McAfee Labs found that 40 percent of malware misbehaves in more than one way. A complex attack helps criminals achieve success because they are hard to detect and they often take advantage of the specific technologies or vulnerabilities of a mobile device. Malware poses a real threat to consumers and can be very lucrative for criminals.

The chart above shows a broad range of malicious or potentially undesirable attack methods associated with Android malware families from 2007 through 2012. About half of all malicious behaviors are related to either spying, which could mean a criminal is browsing your text message history, or sending handset information, said Caetano.

Caetano said it makes sense to pay attention to the permissions requested by an app and keep an eye on monthly bills to catch premium content fraud quickly. Also, look carefully at the URL or address bar of all websites and apps, as attackers will lure users in by building a web page or link with the common misspelling of a popular page or app. For example, if you're searching for "example.com" a criminal might

or dishonest advantage

4.Explain the graph given in the text. Try to combine it with the information given in the text. Use the following tips to make a good speech.

build an attack around “exemple.com.”

“The moral of this mobile security story is that it’s time that we all take mobile protection a little bit more seriously,” said Caetano. (adapted from http://www.sv411.com/)

Does the report have a suitable structure?
Does it have an introduction, body and conclusion?
Does it include connective words to make the writing cohesive within sentences and paragraphs?
Does the report use suitable grammar and vocabulary?
Does it include a variety of sentence structures?
Does it include a range of appropriate vocabulary?
Does the report meet the requirements of the task?
Does it meet the word limit requirements?
Does it describe the whole graph adequately?
Does it focus on the important trends presented in the graphic information?

Listening

You are going to listen to a part of a program “How it works”.

Questions 1- 7

Complete the sentences below. Write down **NO MORE THAN THREE WORDS** for each answer.

You will only hear each section ONCE!

Before you listen, try to predict what the answer will be

1. Today our life is full of mobile devices, some of the people check their phones _____ times a day.
2. As mobile technology becomes more _____ so do the security attacks.
3. _____ is masquerading information as a trusted source.
4. He downloads the version that already is bounded with _____.
5. Malware is short for _____.
6. Tapping into personal network is called _____.
7. The maker of real app is also unaware how their app is being _____.

Questions can be given in paraphrased forms!

Questions 8-10

Answer the questions below. Write down **NO MORE THAN THREE WORDS** for each answer.

Tasks are not always given in the same order as the text

8. What is SDK?
9. What kind of processes does mobile security have?
10. What is the most important thing we carry about?

Questions 11-15

Do the following statements agree with the information given in the recording? Write **T**(true), **F**(false), **NG**(not given) next to the sentences 11-15.

11. It’s not important to check up mobile app before using it.
12. Personal data is usually stored in safest place on the phone
13. Phising is one of the hacking ways to get your personal data
14. Malware is always to hurt a device.
15. Social engineering is tapping into your own network.

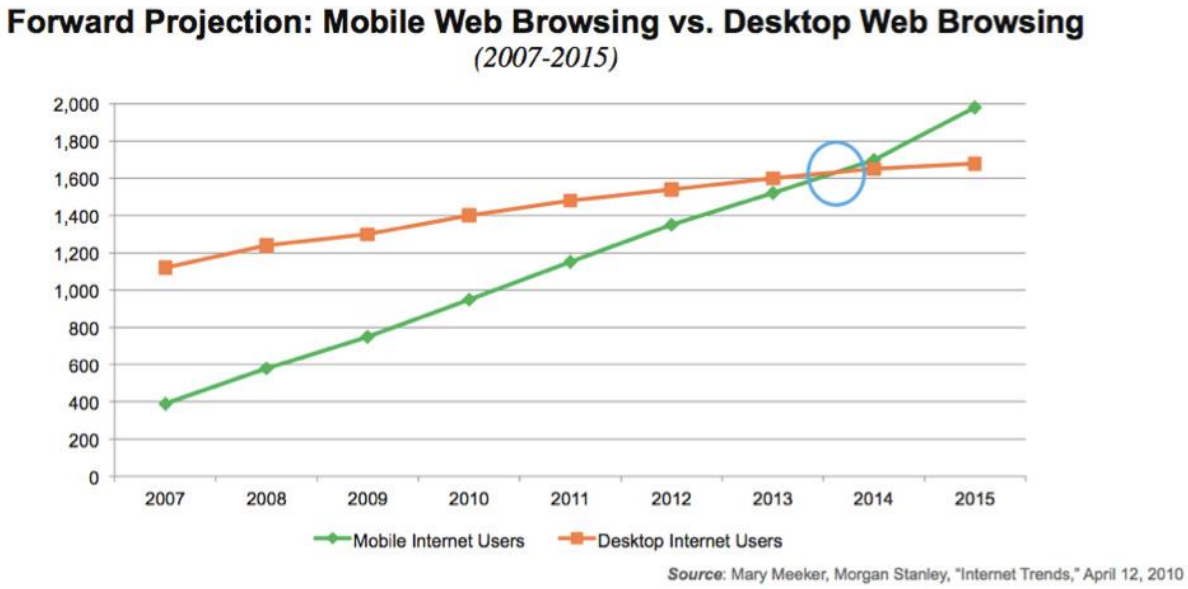
Writing

You should spend about 20 min on this task. Write at least 150 words.

Analyze this graph and work out how life changed during this period?

The green line on this chart represents mobile devices
The orange line is viewing on desktop and notebook screens.

Mobile Web Usage Growing



Read these sentences. They come from websites. Use the words you have learned to help you choose the correct answers. Study new words. Use them in your writing task.

1. Please choose a username/security code/house number. It can be the same as your email address.
2. The receipt / address / password you entered is incorrect. Please try again.
3. You can find the security code / password / payment on the back of your card.
4. Please enter your name / security code / card number carefully, without any spaces.
5. Select your card's expiry date / account / receipt by using the drop down menu.
6. Please print your expiry date / postcode / receipt and keep it for your records.
7. To make online payments you need to set up a card number / account / computer.
8. You can add to or empty your account / payment / basket at any time.
9. When you are ready to pay you should proceed to the checkout / password /security code.
10. Please select a date from the expiry date / account / drop down menu.

Revise and Check

CAN YOU:

…pronounce and give definition of

Sophisticated

Vital

Unleash

Convenient

Disseminate

proximity

scammer

proliferate

multitude

fraud

malware

lucrative

protection

describe

pie charts

line charts

…speak about:

Smartphones

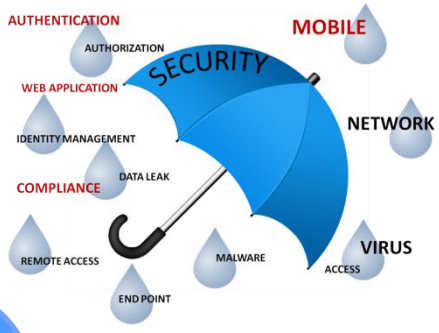
Online payments

Hacks of mobile devices

UNIT 7 CLOUD SECURITY

Speaking

1. Choose the most relevant definition of Cloud Computing. Prove your choice.



Cloud computing is the latest approach to provide computing infrastructure, with the purpose to shift the location of the computing infrastructure to the network in order to reduce the cost of management and maintenance of hardware and software resources.

Cloud computing is defined as a type of computing that relies on *sharing computing resources* rather than having local servers or personal devices to handle applications.

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"

2. Give your own definition of Cloud Computing using information from the previous ones.

3. In small groups talk about…

a. Service Models. Can you give any examples?

b. Three Deployment Models of Cloud. What is the difference between them?

4. In pairs write down as many benefits of Cloud Computing as you can. Discuss them with your groupmates to find out who has written more. Prove your ideas. Practice using "Useful language".

Useful language	Another good thing about it is that…
It is true that / clear that / noticeable that…	One argument in support of…
One should note here that…	Firstly / Secondly / Finally…
It is undeniable that…	What is more…
It is a well-known fact that…	Besides /because it is…
Doubtless…	Moreover…
One cannot deny that…	In addition to…
Nevertheless, one should accept that…	Furthermore, one should not forget that…

Reading Part 1 Vocabulary and Pronunciation

1. What kind of challenges can you face dealing with Cloud Computing?
2. Match the following

The Security, Privacy and Trust Challenges of Cloud Computing

Security, Privacy and Trust are the three major concerns about cloud computing. In the cloud computing world the virtual environment lets user access computing power. To enter this

transcriptions, **A-O**, with the highlighted words and pronounce them.

A /ˌʌndəˈlaɪŋ/
B /kəmˈplaɪəns/
C /ɪnˈtegrəti/
D /ˈæset/
E /kənˈsent/
F /ɪnˈhɑːns/
G /nɒn-rɪˌpjuːdiˈeɪʃən/
H /əˌkaʊntəˈbɪləti/
I /əˌveɪləˈbɪləti/
J /trænˈspærənsi/
K/ˌɪmplɪmenˈteɪʃən/
L /ˈliː.kɪdʒ/
M /kəˈmɪtmənt/
N /ˈkɒnsɪkwəns/
O /ˈækses/

3. Read the article once. Try to work out the meaning of the highlighted words. Then match them with their definitions, a-o.

virtual environment a user is required to transfer data throughout the cloud. Consequently several security concerns arise. Before assessing Security concerns of Cloud Computing let's define the Security, Privacy and Trust.

• **Security** is all about the maintenance of the confidentiality, availability and integrity of data or information. Security may also include authentication, reliability, non-repudiation and accountability. The fundamental property of security is the information or data must be closed to any unauthorized person.

• **Privacy** is a fundamental human right which concerns the expression of various legal and non-legal norms regarding the right to private life. Privacy also talks about the protection and appropriate use of the personal data. Organizations manage the privacy using application of laws, polices, standards and processes. The globally accepted privacy principles: consent, purpose restriction, legitimacy, transparency, data security and data subject participation.

• **Trust** can be defined as " *a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another".* It revolves around 'assurance' and confidence that people, data, entities, information or processes will function or behave in expected ways. Trust may be human to human, machine to machine, human to machine,

a._____ *noun* something that you must do that takes your time, obligation

b._____ *noun* making known secret information

c._____ *noun* an obligation or willingness to accept responsibility and perform periodic checks to be certain that the policy is being followed

d._____ *noun* a realization of a technical specification or algorithm as a program, software component, or other computer system through computer programming and deployment

e._____ *noun* not being able to refuse, the verification of the identities of individuals or companies

or machine to human. Trust can be regarded as a consequence of progress towards security or privacy objectives.

Challenges of Cloud Computing due its Underlying Technologies

By the definition of cloud computing (by NIST), a number of challenges for security, privacy and trust from the underlying technologies (virtualization technology, grid computing, web services, service-orientated architectures, web application frameworks and encryption) of cloud computing are:

Area/ Technology	**Security**	**Privacy**	**Trust**
Virtualization	Integrity	Segregation of personal data on shared infrastructure	Compromised virtual machines/ hypervisors permit loss of trust
Grid technology	Availability		Interoperability
Web services	Integrity and confidentiality	Security and confidentiality	Interoperability
Service-orientated architectures	Integrity		The reliance of distributed systems on different security credentials

f._____ *verb*
to raise to a higher degree

g._____ *noun*
clarity

h._____ *noun*
the result of an action or situation

i._____ *noun*
the component of information assurance that focuses upon providing immediate access to mission critical data when it is needed for decision making

j._____ *noun*
ways of controlling who can see or enter information on a computer system, to obtain or retrieve (information) from a storage device

Web application frameworks	Integrity and availability		Trust across distributed environments
Encryption in the cloud context	Confidentiality	Security and Confidentiality	

Security challenges of Cloud computing:

Cloud computing is not secure by nature. The Security risks depend on the cloud services and deployment model. The security challenges related to Cloud computing are:

Users control over Cloud resources - Cloud users typically have no control over the Cloud resources. There is a risk of data exposure to third parties on the Cloud or the Cloud provider itself. From a security perspective, data keepers of the Cloud computing have to ensure that each user can control over his data or information.

Data secrecy & confidentiality - Encrypting data is a common practice to protect secrecy and confidentiality of data. End-users may hold the decryption keys that still leads to some technical challenges.

Access control and use of the data - The cloud computing requires the identity and access control management measures. When data are trusted to a third party for handling or storage within a common user environment, precaution must be taken to ensure uninterrupted and full control of

k._____ *noun*
the state of being whole and not divided, the assurance that information can only be accessed or modified by those authorized to do so

l._____ *noun*
an item of value owned; any data, device, or other component of the environment that supports information-related activities

m._____ *noun*
permission, approval, or agreement

n._____ *noun*
the practice of obeying rules or requests made by people in authority
procedures that must be followed

o._____ *adj*
basic, fundamental

the data.

Application & Platform Security - The application, which was developed for internal use, is now being used in cloud computing environment without addressing the risks of new technology. Migration to Cloud computing (the secure development lifecycle of the organization) needs to be changed to accommodate the Cloud computing risk context.

Privacy challenges of Cloud computing:

In the Cloud-computing environment Cloud providers can host or store important data, files and records of Cloud users. It is difficult for companies and private users to control the information or data all times they entrust to Cloud suppliers. Some key privacy challenges particular to the Cloud-computing are:

A_____ - Any type of information can be hosted or managed by the Cloud providers. The information may be highly confidential or extremely valuable as company asset. Then entrusting this information to a Cloud increases the risk because there is a possibility of cloud platform sharing by the competitors.

B_____ - The users of the same Cloud share the server of data processing and the data storage facilities, they are exposed to the risk of data or information leakage, either by accident or intentionally.

Data transfers to different locations - If the data

4. Read the article again and choose the most suitable topic sentence, I-X, for each paragraph, **A**-**E**, from the list below.

I. Management problems
II. Sensitivity of information
III. Users' possibility to access the data
IV. Trust in Cloud Providers
V. Confidentiality of information
VI. Data privacy
VII. Leak of the data
VIII. Trust enhancement through assurance mechanisms
IX. Continuity and Provider Dependency
X. Privacy preservation

on the Cloud change the location regularly or reside on multiple locations, it becomes complicated to watch the data flows. Data transfers to other countries require arrangements to be placed. It will be complicated to fulfill these arrangements if data locations are not stable.

C_____ - Companies engaging in Cloud computing expect that the privacy commitments they have made towards their customers, employees or other third parties will continue to be carried out by the Cloud computer provider. **Trust challenges of Cloud computing:**

Trust is critical barrier that must be passed. Cloud customers must trust the cloud providers. Providers must trust customers with access to the services which may lead to security issue. If Cloud providers succeed in providing the solutions to Security and Privacy, they achieve success in the trustworthy services in cloud computing. They can enhance user's confidence in the application of Cloud computing and would build the trust in the market of Cloud services.

Joining the Cloud by users/resources dynamically – In cloud computing environment many users or resources join and leave cloud dynamically. Users, resources and the cloud should establish the trustful relationships with each other and they should take into account the change which is happening dynamically.

Different Security policies – The cloud environment consists of distributed users and resources from different local systems that may have different security policies. This situation brings up the question how to build a suitable relationship between them?

D_____ - The complexity of Cloud architectures and the lack of transparency will increase the security risk. In many Cloud implementations, the centralized management and control introduces several single points of failure. These could threaten the availability of Cloud users' data or computing capabilities indirectly.

Compliance with applicable regulations and good practices - Once the applicable law to a Cloud service is determined, the provider will need to comply with other regulations such as privacy, General civil law and contract law, Consumer protection law, etc.,

E_____ - The Cloud-computing concept cannot guarantee full, continuous and complete control of the Cloud users over their assets. For these reasons, the establishment of appropriate "checks and controls" to ascertain that Cloud providers meet their obligations becomes very relevant for Cloud users.

Do not expect the topic sentence or heading to use the same words as the text. They will probably be paraphrased.

Listening and Speaking

What kind of risks can you take dealing with Cloud Computing?

You are going to listen to the interview with Kristin Lovejoy, Vice President IBM Security Strategy, Richard Cocchiara, CTO/IBM Business Continuity and Resiliency Services, and RicTelford, Vice President IBM Cloud Services.

The recording will be played **ONCE** only!

Section 1 ***Questions 1-10***

Questions 1-3

What do responders worry about?

Write the correct letter, **A-F**, next to question 1-3.

Before you listen, try to predict what the answer will be.

A Uptime/business continuity
B The data leakage
C Inability to customize applications
D Reducing the strength of corporate network security
E Data privacy
F Keeping safe your privacy

The words you read will probably not be the same as the ones you hear, so be prepared to listen to synonyms or paraphrases.

1. 77% _____
2. 50% _____
3. 23% _____

Questions 4- 9

Choose 6 great security threats in Cloud Computing, **A-K**.

A Handling over sensitive data to a 3rd person

B Complying with the law

C Loss of governance

D Lock in

Glossary:
breach *noun* the act or a result of breaking;
tenant *noun* a group of users who share a common access with specific privileges to the software instance;
back up *verb* to make a copy of information on your computer;
SLA Service level agreement

E Accessibility of the data

F Insider full of malice

G Failure of isolation

H Insecure Interfaces

I Deletion of the data

J Infrastructure failure

K Management Interfaces

Question 10

Which threat does Richard Cocchiara agree with?

Choose 1 letter, **A-K**.

Which threats are the most and least dangerous from your point of view?

Prove your ideas. Practice using "Useful language".

Useful language	It seems to me…
I strongly believe that …	As far as I'm concerned…
In my opinion…	I'd like to point out that…
Personally, I think…	I consider…
I'd say that…	To my mind…
I'd suggest that…	I'm inclined to think that…

Section 2

Questions 11-14

Choose the correct letter **A**, **B**, **C** or **D**.

11. What does centrally managed mean?

Try to give an answer for all the questions. Multiple Choice questions in particular are worth trying to answer, as you have a chance of guessing the correct one.

A apply the policy equally

B push the policy down

C well managed Cloud environment

D apply a policy from the top and push it down

12. Why can't enterprises perform logging and auditing themselves?

A too expensive

B hard to combine

C impossible to combine

D difficult to implement

13. What is compelling statement about Cloud?

A updating

B patching

C delivering immediate control to all assets

D the ability to deliver security control

Skip any questions you are not sure about, rather than wasting too much time on a particular question. You can come back to these questions later.

14. What wasn't mentioned by Kristin Lovejoy?

Cloud can offer better benefit with:

A right SLA

B understanding of security architecture

C being centrally managed

D right provider

Section 3

Questions 15-23

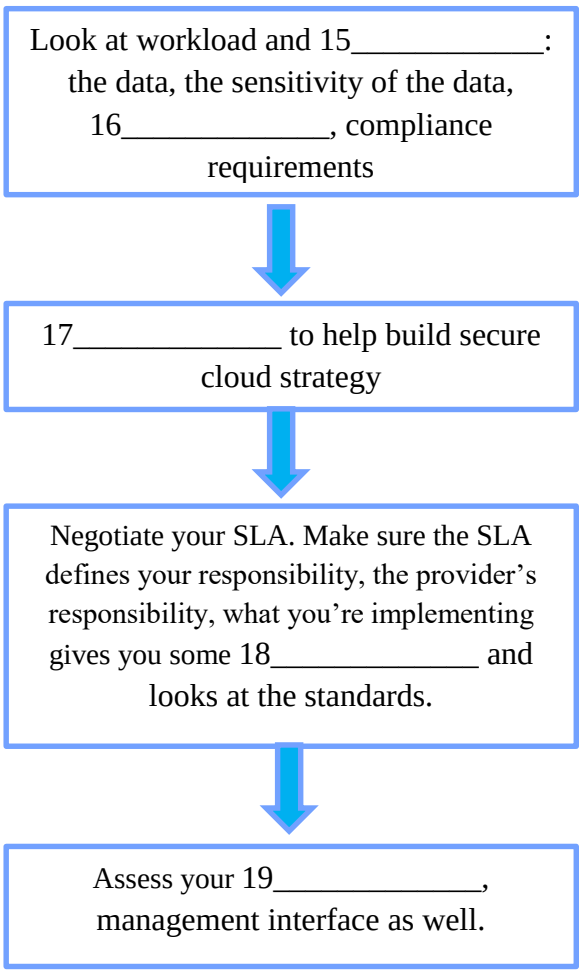
Questions 15-19

Complete the flow chart below. Write down ***NO MORE THAN THREE WORDS*** for each answer.

Some of the answers you hear may be very close in recording. Always be ready to listen for the answer!

How to get started in developing and executing Cloud Security Strategy

The information you need to answer the questions is in the same order as it is on the recording.



You may know the answers due to your knowledge, but your answers cannot depend on that: you will need to listen for to what the **speakers** say to identify the answer.

Questions 20-22

Do the following statements agree with the interviewers? Write **T**, **F**, **NG** on lines 20-22.

20. Creating an architecture make sure yours combines with the cloud provider's.

21. The Cloud Provider should manage all your risks.

22. Your strategy must be entire and cover all aspects.

If you have to complete the chart, always write the words you hear on the recording; do not use your own words.

Question 23

Which aspects weren't mentioned? Choose 3 letters, **A-K**.

A physical security

B platform security

C application security

D data security

E network policy

F compliance requirements

G network

H access control

I data privacy

J identity management

K centralized policy

Reading Part 2 and Speaking

Questions 1-4

Choose the most suitable threat, **A**-**H**, for each paragraph, 1-4, from the list below.

A Shared Technology issues

B Isolation Failure

C Data loss or leakage

D Protecting data policy

E Compliance risk

F Account or Service Hijacking

G Abuse and illegal use of cloud computing

PROPOSED SOLUTIONS TO CLOUD COMPUTING SECURITY, PRIVACY AND TRUST CHALLENGES

For the above specified Cloud Computing Security, Privacy and Trust Challenges, the following measures need to be considered.

The steps to be considered when moving to Cloud environment

Adapting a few guidelines will help protect users on the cloud environment. Cloud security mechanisms can be of two different categories: Partner-based (Security for SaaS, PaaS, IaaS) or Userbased (client based).

- **Strategically plan your cloud security –** Considering security during the initial

H Management Interfaces

Questions 5-10

Complete each of the following sentences, 5-10, with the best ending, **A-L**, from the list of endings below.

Try to predict how each sentence will end before looking at the list of endings.

5. Before choosing cloud provider…
6. Determine responsibilities and roles…
7. Implement strong access control and authentification…
8. Implement strong API access control..

planning phase creates solid foundation. Careful considerations must be taken how corporate workloads should be delivered to end users.

- **Select the Cloud provider –** It is crucial to choose a cloud provider who can protect your sensitive information or data. Before selecting cloud provider check whether they have experience in both IT and security services for their strategic service performance assurances.
- **Find the written document about security measures provided by the cloud provider –** This means getting assurances from the cloud provider written into the contract. The document must include applications, infrastructure, configurations, policies, rules and regulations.
- **Find out who will monitor your data –** Find out who will access to data and why and when they are accessing it.
- **Have a plan for Security issues –** What responsibility the cloud provider is promising, and what actions he will take during and after the security issue must be checked.
- **Verify the access controls being used –** Verify the access controls imposed on the data to ensure that the third parties cannot access the data. It is important to clearly define roles and responsibilities to ensure that even

9. Security policy refers to …
10. Integrity and confidentiality of the data are maintained by …

A to prevent account hijacking.
B authentication.
C to be sure that no one can access the data.
D encryption.
E to prevent isolation failure.
F identification.
G to prevent insecure interfaces.
H find out what experience he has.
I to ensure that others can monitor data.
J check what documents he has.
K to prevent data breach.
L authorization.

privileged users cannot skip auditing, monitoring and testing, unless authorized.

- **Monitoring system –** Cloud provider must continuously monitor data in the cloud. Establish cloud performance objectives and test regularly.

Measures to be taken for the top threats identified in the Cloud Computing

For 1_____

- Care must be taken in Initial registration and Validation process.
- To use credit card in Cloud computing an Enhanced fraud monitoring system must be implemented.
- Monitoring public blacklists for one's own network blocks.

For ***Insecure Interfaces and APIs***

- Cloud providers interfaces security model must be analyzed properly.
- Strong authentication and access controls must be implemented.
- Understand the dependency chain associated with the APIs.

For ***Malicious Insiders***

- Identify the human resources requirements as a part of legal contracts.
- Information security, management practices require transparency.
- Decide Security breaches.
- Conduct survey on comprehensive supplier

Questions 11-16

Complete the abstract below with words from the text. Write **NO MORE THAN ONE WORD** for each answer.

Try to predict what kinds of words may be missing by using your knowledge of **grammar**. Your answers need to be grammatically correct.

Cloud Computing has emerged as a new paradigm of computing, that is built on the foundations of Distributed Computing, Grid Computing, and Virtualization.

assessment and implement strict supply chain management.

In case of 2_____

- Best Security practices must be implemented for installation or System configuration.
- Unauthorized activities must be monitored.
- Service level agreements must be enforced.
- Configuration audits and vulnerability scanning must be conducted.
- Strong authentication and access control administrative access.

For 3_____

- Implement strong API access control.
- Specify backup and retention mechanisms
- Analyze data protection at both design and run time.
- Necessary measures must be taken for strong key generation, storage, and destruction practices.

With respect to 4_____

- Implement strong monitory system to detect unauthorized activity.
- Sharing of account details between users and services must be avoided.
- Read and understand properly cloud security policies.

Security requirements need to be considered with respect to service models and cloud deployment models

A cloud customer needs to check the security

state of the cloud model before selecting cloud provider. For this an assessment must be performed in terms of security requirements. The following table gives six security requirements with respect to Cloud Service Models and Cloud Deployment Models.

Security Requirements	Cloud Deployment models								
	Public Cloud			Private cloud			Hybrid Cloud		
Identification & Authentication	√	*	√	√	*	√	*	*	√
Authorization	√	√	√	*	*	√	*	*	√
Confidentiality	*	*	√	*	√	√	*	*	√
Integrity	√	*	√	*	√	√	√	√	√
Non-repudiation	*	*	√	*	*	√	*	*	*
Availability	√	√	*	√	√	√	*	*	*
	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS
	Cloud Service Models								

(A Check mark (√) indicates requirement in the Cloud Service Models and Deployment models, while the asterisk (*) indicates optional)

Cloud computing has grown to provide a promising business concept for computing infrastructure, where 11_____ are beginning to grow about how safe an environment is. Security is one of the major 12_____ in cloud computing 13_____. The aim of this article is to address the security, privacy and trust

Identification and authentication methods include passwords, smartcards and biometrics. Authorization or access control refers to a set of security policies which defines users' permissions to access the resources in the cloud. Depending on the way that the security policies are specified, access control can be categorized into different models. Encryption is a core mechanism for maintaining the confidentiality of all data, whether it consists of business, personal or sensitive information, and it can also be used to establish the integrity of various transactions, code and data. Encryption is considered as a security control on maintaining confidentiality

14_____ of cloud computing and we 15_____ some solutions by analyzing the technological, operational and legal 16_____ of cloud computing taking into consideration cloud customers.

and integrity. The uses of encryption in accessing services in the cloud are similar to data protection as conventional technologies. Many public offered services are provided via an HTTPS-protocol connection to a web service, which works on the concept of Secure Socket Layer (SSL) protection. (adapted from International Journal of Computer Science and Information Technologies www.ijcsi.com)

Do you agree with solutions proposed by the authors of this article? Practice using “Useful language”.

Useful language	I don't agree with…
I agree with…	I'm sorry to disagree with…
That's true that…	I'm afraid I have to disagree…
I'd go along with…	I'm not so sure about…

Writing

You should spend about 20 min on this task. Write at least 150 words.

The table from Reading Part 2 gives six security requirements with respect to Cloud Service Models and Cloud Deployment Models.

Summarize the information by selecting and reporting the main features, and make comparisons where relevant.

When you write about a chart or table you will receive marks for organizing and describing all the information. You will not receive marks for giving reasons for the information or giving your opinion about the information (but you will not lose marks if you do this). As you have limited time and number of words, write about the information only.

CAN YOU…


…give definition of
Cloud computing
…pronounce and give definition of
availability
integrity
non-repudiation
accountability
consent
transparency
consequence
underlying
access
asset
leakage
commitments
implementations
compliance
enhance
tenant
…speak about
Service models
Deployment models
Cloud Computing challenges
Security threats in CC
Benefits of CC
Security strategy steps
Proposed solutions and measures to be taken
…describe tables

BIBLIOGRAPHY

1.Annelli Williams Writing for IELTS. – Collins, 2011.

2.Authentication - http://arxiv.org

3.Biometrics - http://ai.pku.edu.cn

4.Captcha - http://research.microsoft.com

5.Concerns About Electronic Banking - http://csrc.nist.gov/

6.Cybercriminals developing complex hacks of mobile devices - http://www.sv411.com/

7.Cybersecurity vs. Information Security - www.floridatechonline.com

8.Deborah Russell, G.T. Gangemi Computer Security Basics

9.Els Van Geyte Reading for IELTS. - Collins, 2011.

10.Garry Adams and Terry Peck 101 helpful hints for IELTS Academic Module

11.How to prepare for a cybersecurity www.infosecurity-magazine.com

12.Introduction to Cryptography http://www.infosectoday.com

13.Martha Grand A short guide to oral presentation in English. - ENSIEG

14.Michael Black, Wendy Sharp Cambridge Objective IELTS

15.Pauline Cullen Cambridge Vocabulary for IELTS Advanced

16.Passwords Security http://www.youtube.com/

17.Richard Hallows, Martin Lisboa, Mark Unwin IELTS Express Intermediate Course book. - Thomson tm, 2006.

18.Social Engineering: an underestimated danger www.insecuremag.com

19.The Security, Privacy and Trust Challenges of Cloud Computing www.ijcsit.com

20.What is Network Security www.paloaltonetworks.com

21.http://itlaw.wikia.com

22.http://dictionary.cambridge.org

23.http://www.collinsdictionary.com

24.http://www.macmillandictionary.com

25.http://www.ielts-exam.net/

26.http://www.net-security.org