Awareness Raising Quizzes Templates

November 08

Targeting Parents, End-users and SMEs

enisa

European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on information security awareness raising matters please use the following details:

E-mail: KJELL KALMELID, Expert Awareness Raising — kjell.kalmelid@enisa.europa.eu
Internet: http://www.enisa.europa.eu

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Acknowledgments

Kjell Kalmelid, Expert Awareness Raising, ENISA and coordinator of this document, wishes to acknowledge and warmly thank the four authors of the AR Community, who together wrote and compiled the quiz templates:

- Anna Rywczyńska, NASK, Poland
- Pierre-Luc Refalo, Hapsis Education, France
- Claudio Telmon, CLUSIT, Italy
- Johannes Wiele, Konradin IT-Verlag and Ludwig-Maximilians-Universität Munich, Germany

A special thank goes to Peter Pfeifhofer, Seconded National Expert, ENISA and Wendy Goucher, Idrach Ltd., the UK and Member of the AR Community for reviewing the templates and providing feedback.

Table of Contents

Preface

About this document

This document is the result of a joint work of four members of the ENISA AR Community. The purpose of this document is to provide information security awareness raising content in the form of a number of quiz templates.

About the AR Community

The AR Community is a subscription free community open to professionals working in the field of information security. It was launched in 2008 by ENISA in an effort to create an information security-focused community; particularly targeting professionals with an interest in security awareness raising matters.

Even though the AR Community primarily aims at attracting members in Europe, it has several members from countries outside Europe who all share the same idea; raising security awareness among people is key in order to achieve a true state of information security in any organization.

Introduction

Scope

The purpose of this document is to provide information security awareness raising content in the form of a number of quiz templates. The target audience of this document are organizations wishing to raise information security awareness among their target groups.

Objective

These quizzes should not be perceived as comprehensive self-tests of individuals current level of awareness and knowledge. The objective is merely to give the respondent a hint on their level of awareness and hopefully serve as a tool to encourage further interest in the values and risks of using computers and utilizing online services on the Internet.

How to use the templates

The templates can be used either as a printed hardcopy together with a response sheet or implemented as a web quiz. Each quiz comes with an *Introduction text* that should be kept or, if implemented as a web quiz, included on the same page of the questions.

IMPORTANT

In addition to the information provided in the Response columns, please provide local/national sources of information that you deem important, e.g. links, contact information to hotlines and local/national authorities. In certain questions, this is indicated with brackets for example [INSERT RELEVANT CONTACT POINT].

Overview of the quizzes

All in all, there are three quizzes, each targeting a particular target group; Parents, End-users and executive managers of small and medium-sized enterprises (SMEs).

Each template consists of a number of *themes* that are broken down into *questions*, which in turn are followed by a *response*. In some quizzes, the response provides correct and wrong answers together with some informational text and sometimes only a brief feedback.

Parents

Theme	Questions	Response
PC Usage of your kid	1. Online activities 2. Communication 3. PC usage 4. Internet and risks 5. Internet understanding	Lets the parent know to what extent their kid should use the computer and for what activities.
Privacy & Social networks	6. Using Social Networking sites 7. Creating safe profiles 8. Disclosing information	Lets the parent you know how to create safe profiles, do you know if your child has an online profile, what information shouldn't your child put online

Illegal content	9. Reporting illegal content 10. Encountering illegal content	Filtering software – do you know how to use it?
File sharing	11. Using peer-to-peer technology	Kids download multimedia. Do parents know about Copyright laws? What is allowed and not?
Cyberbullying	12. Handling cyberbullying	What is the effect of submitting false information and/or bullying somebody on the Internet?

End-users

Theme	Questions	Response
Threats on the Internet	1. Attached files in emails 2. Anti-virus applications and Firewalls 3. Patching/Security updates 4. Passwords	Does the respondent know about different threats and how to protect oneself from them?
Phishing	5. Secure online shopping 6. Understanding phishing	Does the respondent know about secure online shopping and the threat of phishing attacks?
Protecting information	7. Backup 8. USB flash drives 9. Understanding encryption	Does the respondent know about the importance of backing up valuable information, risks and disadvantages with USB flash drives, and encryption to protect information?
Legal aspects/Copyright	10. Downloading files	How does the Internet compare to the real world? Downloading copyright material

SMEs

Theme	Questions	Response
Risk profile	1. Information assets 2. Threats	SMEs managers must identify critical information and potential threats
Legal and contractual issues	3. Privacy/Personal data 4. Software licences	SMEs managers must be aware of such legal respon-

Quiz Templates

Theme	Questions	Response
	5. Contract management	sibilities.
Human and organizational aspects	6. Password management 7. Email 8. Internet surfing 9. Social engineering 10. Mobile devices	A few behaviours must be adopted to reduce risks related to access and communications. Managers are to be examples for their employees.
Security tools	11. Back up 12. Anti-virus/spyware 13. Secure remote access 14. Encryption	A few technologies are mandatory to protect IS and sensitive data. SMEs Managers should understand the security baseline to be implemented

Parents Quiz

Parents Quiz

Introduction text to the Parents Quiz Profile

Welcome to the ENISA AR Quiz for parents!

The aim of this quiz is to provide a means for you as a parent to test your awareness and knowledge on a number of topics concerning your child's use of the computer and online services on the Internet.

The Internet is a fantastic resource that offers an abundance of valuable information and services. However, it also comes with risks and as a parent, you should be aware of them.

This quiz should not be perceived as a comprehensive self-test of your current level of awareness and knowledge. The objective is merely to give you a hint on your level of awareness and hopefully serve as a tool to encourage further interest in the values and risks of having your child using the Internet. We also hope you will find the sources of information provided on this website valuable and useful.

Quiz Templates

No.	Question	Answers	Response
1	What are the online activities of your child?	a) Chatting or emailing b) Blogging or using social networking sites c) Playing online computer games d) Searching information on the Internet for school reports or for homework e) All of the above more or less f) Don’t know	f) It is generally recommended that parents stay in touch with what their children are doing online. Ask your children what they are doing and have them show you how different functions, games or other online activities work! This way, your child will understand that you are genuinely interested in what he/she is doing. This is also important in order for you to know if your child is involved in activities you consider off-limits. a)-e). It seems your child is active in taking advantage of the benefits of IT. This is good! You also seem to know what your child is doing while using the computer (apparently, there more boxes you checked the more you know). **Basic tips** Keep your home computer(s) in easily viewable places, such as a family room or kitchen so that you can easily monitor your child’s activities.
2	Do you discuss with your child about his/her activities on the Internet?	a) Yes b) No c) Sometimes	a) and c) It is very good you discuss these things with your child. Continue doing this on a regular basis.

No.	Question	Answers	Response
			b) It's very important to regularly discussing these issues with your child. It's basically the only way for you to actually learn about your child's activities on-line and being able to understand the possible risks. **Basic tips** Trust is key. Keep the communication open so that your children are open with their activities online and at the same time feel they have your confidence to explore the Internet responsibly.
3	In average, how much time does your child spend using the computer?	a) More than 3 hours/day b) 2-3 hours/day c) 1-2 hours/day d) As much time as he/she needs to spend e) Don't know f) Less than 1 hour/day	a) – e) Make sure you are aware of the amount of time your child is spending in front of the computer. Don't forget your child also needs to do sports or any other physical activities. f) Less than 1 hour/day shouldn't signal any concern from your side. **Basic tips** Excessive playing of games or use of online services, especially in the night, should be a signal for you as a parent to consider restricting your child's use.
4	Do you believe the internet to be	a) No, risks are overestimated	a) Indeed, sometimes risks are overesti-

No.	Question	Answers	Response
	a risky environment?	b) Yes, very much c) There are risks, but also valuable information, services and communication tools d) I don't know	mated, but it is also hard to assess risks as new services and functions are constantly introduced at the Internet. b) and c) It's good you are aware that the Internet can be dangerous for your child however don't forget that it indeed provides valuable information, services and functions as a communication tool. d) The best you can do is to try to learn as much as possible about the risks of Internet and, as a start, follow the safety recommendations of your service provider and at this website.
5	To what extent do you feel that you know how to use the Internet?	a) Better than my child does b) About the same as my child does c) Worse than my child does d) Don't know	a) and c) It's good you are aware of your level of knowledge compared to your child. Once again, what is important is that you try to learn more about risks online and how to mitigate them. c) Don't be taken aback by the fact that your child seem to know a lot more about the Internet and its services than you do. Many parents have the same experience. d) If you don't know, a recommendation is to sit down with your child from time to time and join him/her in browsing the web.

No.	Question	Answers	Response
			That will soon give you the answer.
6	What information is it all right for your child to disclose while using social networking sites?	a) The real first name and only last initial b) The name of the school your child goes to c) The favourite colour d) The real names of the parents, but not their own names e) The date of birth, but not their name f) Names of friends or relatives g) Their nickname	a), b), d), e) and f) – Wrong. You should explain to your child never to disclose any information on the Internet that could help someone else to identify her/him in real life. c) and g) Correct. A nickname or a favourite colour is safe information to put on the Internet.
7	Has your child created a safe profile on the social networking site he/she uses?	a) Yes b) No c) Don't know d) My child doesn't use social networking sites	a) Good! However, check if your child knows how to use Social Networking sites in a safe way. Make sure your child's safe profile meet the basic recommendations below. b) Follow the basic tips below on how to create a safe profile for your child. c) Not knowing how to use Social Networking sites safely can violate your child's privacy. d) Social networking sites are extremely popular among children and teens. They can be a valuable tool and offer great fun, for instance when chatting with friends all over the world. **Basic tips for creating safe profiles are:** 1. Set your profile as private allowing

No.	Question	Answers	Response
			other users to only see your child's username and be restrictive to disclose other information, for example a picture of your child. Only let the friends of your child access additional information. Make sure you know who your child's friends are. 2. Never make private data available on-line your such as real name, address, picture or phone numbers 3. Be selective with photos. Once available online, they remain on the Internet for-ever. Respect other's privacy – don't let your child upload somebody else's photo without asking for permission. 4. Tell your child to encourage their friends to create safe profiles. Don't hesitate to discuss these topics with the parents of your child's friends.
8	What information can you disclose if you want to create a safe profile on social networking sites?	a) I can disclose my phone number but not my email address b) I can disclose my postal address but not my phone number c) I can tell people I meet online where I'm working or which school I'm going to d) I can disclose any personal information to	a) – c) These pieces of information are all examples of private data. You should never make personal information available on-line. However if you decide to do so, make sure this data is accessible only to trusted users

No.	Question	Answers	Response
		people I trust e) I can upload a picture of myself as long as I don't reveal any personal information about myself	d) You should never make personal information available on-line. Make your profile "private" and provide access to private data only to people you know and trust. You can use your nickname on social networking sites, provided you don't add any other information that can reveal your identity. e) A picture of you is personal information.
9	Do you know to whom you should report illegal content found on the Internet? One or more answers are correct.	a) Yes, to the Police b) Yes, to the [NAME OF INTERNET SERVICE PROVIDER] (the company providing you an Internet connection) c) Yes, to the [NAME OF HOTLINE], a team qualified to receiving and reacting to notifications relating to the occurrence of illegal contents on the Internet d) No, I never report I just close the site	a) – c) Yes, you are right. Remember not to be indifferent to the illegal content found on the Internet. Such content as child pornography, racism or xenophobia should be reported to the hotline operating in your country, to the Police or the Internet Service Provider d) Remember that what the Internet is like also depends on you. Don't be indifferent to the illegal content you happen to come across on the net
10	Have your child ever encountered harmful or illegal content on the Internet?	a) Yes, many times b) Yes, once c) No, never d) I don't know	a) and b) To protect your child from contact with harmful or illegal content you must have filtering software installed on your computer. This is not a guarantee for protection, but it reduces the risks of being exposed to such content.

No.	Question	Answers	Response
			c) That's good to hear. If you haven't yet installed filtering software on your computer, do so. d) Talk to your child and ask if he/she ever has encountered any content upsetting him/her. If you haven't yet installed filtering software on your computer, do so.
11	What should your child know when using peer-to-peer technology?	a) It is practically impossible to receive viruses on your computer b) It can be illegal to download certain files c) It can include illegal or harmful content d) Sharing files is safer when you have a firewall	a) Wrong. Unfortunately, it is just as likely to get your computer infected with viruses through peer-to-peer technology as it is from the web or by email. Be careful when you download content via peer-to-peer technology and make sure you always run the file through an anti-virus programme before opening (executing) it. b) Correct. Copyright material, like music, movies or software, which you download from the Internet, will generally be protected in the same way as material in other media. In many countries, it is illegal to download copyright protected material. You should explain to your child that before downloading any material that oth-

No.	Question	Answers	Response
			ers have placed on the Internet, you should ensure that they have the permission of the owners of rights in the material unless copyright exceptions or defences apply. c) Correct. Unfortunately, peer-to-peer technology is also used for distributing illegal or harmful content. d) Correct. With a firewall installed on your computer you at least reduce the risk of having it infected by viruses. A firewall is like a filter that can screen out malware that tries to reach your computer over the internet and search for vulnerabilities and then try to break in at a weak point.
12	What should I as a parent do if my child is being cyberbullied while chatting on the Internet? One or more answers are correct.	a) Encourage your child not to respond to the cyberbullying b) Immediately delete any messages or pictures received by email that are upsetting your child. c) See to that your child is only using moderated chat rooms d) Encourage your child to talk with you about the situation e) Tell your child to stop emailing and chatting to avoid cyber bullies	Cyberbullying is the latest form of bullying that takes place online while using Internet or cellular phones. a) Correct. Responding will likely not stop the bullying. On the contrary, by responding the bullies might be encouraged to continue their bullying. b) Wrong. Never delete messages or pictures received by email. Save these as evidence. c) Correct. In moderated chat rooms an adult is monitor the correspondence be-

No.	Question	Answers	Response
		f) Contact [INSERT RELEVANT CONTACT POINT]	tween participants. e) Wrong. If you do so, your child becomes deprived of the fantastic opportunities of the Internet. f) Correct. Contact [INSERT RELEVANT CONTACT POINT]. They help children and youth who face threats when using the Internet and mobile phones **Basic tips** • Always encourage your child to talk to you if something upsetting or frightening happens to her/him on the Internet. • Monitor the online activity of your child to ensure that he/she is not communicating with bullies. • Teach your child to protect their privacy online • Teach your child not to respond to harassment of any kind such as negative emails and aggressive or attacking chat messages. If your child is being cyberbullied report it to [INSERT ONE OR MORE RELEVANT CONTACT POINTS].

End-user Quiz

End-user Quiz

Introduction text to the end-users Quiz Profile

Welcome to the ENISA AR Quiz for end-users!

The aim of this quiz is to provide a means for you as an end-user to test your awareness and knowledge on a number of topics concerning your use of the computer and online services on the Internet.

The Internet is a fantastic resource that offers an abundance of valuable information and services. However, it also comes with risks and therefore you should be aware of them.

This quiz should not be perceived as a comprehensive self-test of your current level of awareness and knowledge. The objective is merely to give you a hint on your level of awareness and hopefully serve as a tool to encourage further interest in the values and risks of using the Internet. We also hope you will find the sources of information provided on this website valuable and useful.

No.	Question	Answer	Response
1	***Attached files in emails*** Please select the answer below, which you believe corresponds best to the risks with email attachments. One or more answers may be correct:	1. Only attached files with the extension .EXE pose a real risk 2. All attached files are potentially harmful and may contain viruses 3. If I know and trust the sender I can always open the attachment 4. It is safe to open attachments if I have a firewall installed on the computer 5. An anti-virus programme will reduce the risk of being infected with viruses from email attachments	1. Wrong. There is a wide range and number of other extensions should be considered suspicious when received in email. You should not open such attachment unless you requested or expected it. 2. Correct. Unfortunately, this is true. That's why it's so important to have anti-virus software installed on your computer. 3. Wrong. Even if you know and trust the sender they might unknowingly and not deliberately send or forward you an attachment containing viruses. 4. Wrong. A firewall does not scan the content of email attachments. 5. Correct. Anti-virus software substantially reduces the risk of being infected by computer viruses. Even though it's not a guarantee against being infected, it is strongly recommended that you invest in anti-virus software.
2	***Anti-virus applications and Firewalls*** Check what you now about anti-virus software and firewalls.	1. Anti-virus software searches your hard drives for viruses and protects your private network 2. A firewall protects the resources of a private network from users from other networks 3. Anti-virus software should never be used	1. Wrong. Anti-virus software does not protect your private network. It only searches for viruses on your computer. 2. Correct. A firewall is a system between your computer network and the Internet. Firewalls analyze data entering and exiting the network and rejecting information from unsecured and

No.	Question	Answer	Response
		together with a firewall 4. A firewall searches your hard drives for viruses and protects the resources of a private network from users from other networks 5. Anti-virus software searches your hard drives for viruses	unknown locations. 3. Wrong. You should use both anti-virus software and firewall 4. Wrong. A firewall does not search for viruses. 5. Correct. Anti-virus software scans your hard drives and alerts you when viruses are found. Many anti-virus software also scan for spyware and adware.
3	***Patching/Security updates*** Which option/s best completes this sentence? "Patching your computer is important because . . ."	1. It makes your computer less vulnerable to virus attacks. 2. Patches remove viruses 3. It reduces spam in your inbox 4. It fix problems with a computer program or its supporting data 5. All of the above	1. Correct. Patching your computer closes vulnerabilities in your operative system or applications thereby making your computer less vulnerable to virus attacks. 2. Wrong. Patching your computer does not remove viruses on your computer. In order to remove viruses, you must install anti-virus software. 3. Wrong. A patch merely fixes a security hole in your operative system or your applications. It will not affect the type of information you receive by email. 4. Correct. A patch fix certain problems in the code of a computer program 5. Wrong.
4	***Passwords*** Which of the following should be included in a safe password?	1. Your name 2. Both upper and lower case letters 3. Your phone number 4. Your licence plate number spelled back-	1. Wrong. You should not use a word connected to you as an individual 2. Correct. By using both upper and lower case letters, the number of combinations increases

No.	Question	Answer	Response
		wards 5. Whatever letters or numbers as long as the password is five characters long 6. A combination of a certain number of alphanumeric characters	and so the strength of your password 3. Wrong. You should not use combinations of characters connected to you as an individual 4. Wrong. You should not use combinations of characters connected to you as an individual even if they are spelled backwards. 5. Wrong. A password of five characters only, is not considered safe enough. It should consist of at least seven, but preferably more, characters 6. Correct. A strong password consists of a combination of upper and lower case letters, characters and figures.
5	***Secure online shopping*** What indicates you are shopping online in a secure manner?	1. I know the company 2. They are selling quality goods of famous brands 3. There's a banner on the top of the page saying "Secure Website" 4. The URL/address of the web site starts with "https://..." 5. All of the above	1. Correct. Always shop with companies you know and sites you trust. 2. Wrong. The quality of the goods offered does not mean the merchant is serious and the site secure. 3. Wrong. You should never rely on a banner alone. Instead, you should try to have the security of the web site verified. For example, check that the company has indicated an address and phone number. If you have doubts about the company, call the phone number and ask questions to determine if the business is legitimate. You can also contact [INSERT NAME OF RELEVANT ORGANIZATION/ASSOCIATION/AUTHORITY] to check the legitimacy of the company.

No.	Question	Answer	Response
			4. Correct. The "s" that is displayed after "http" indicates that Web site is secured with SSL (Secure Socket Layer), which is a way of securing the connection between you and the company's web server with encryption. In addition, you should look for a closed padlock displayed at the bottom of your screen. In case that lock is open, you should consider it as not a secure site. 5. Wrong. Only answer 1 and 4 are correct. **Basic tips** • Shop with companies you know • Make sure the connection is always secured via SSL • Read the web site's privacy and security policies to learn how the company handles sensitive information like credit card numbers and personal data. • Always print copies of your orders • Know your rights Your online transactions are governed by the law [ADD INFORMATION ON APPLICABLE LAWS, REGULATIONS ETC. PROTECTING THE USE OF CREDIT CARDS WHEN SHOPPING ONLINE]
6	***Phishing*** Check what you know about	1. The "From Field" appears to be from the legitimate company mentioned in the e-	1. Correct. Remember, it's very simple to change the "from" information in any e-mail client.

No.	Question	Answer	Response
	typical phishing attempts and how to protect you from them.	mail 2. If I use anti-virus software, I will not be at risk for phishing attempts 3. Typically, they ask for personal information such as usernames, passwords and credit card numbers 4. Emails containing links/URLs to web addresses are more dangerous than others 5. Typically, the sender requests that you reply within a few days 6. All of the above	2. Wrong. However, using anti-virus software reduces the risk of being infected by viruses and can warn if a message include links or attachments. 3. Correct. Remember, banks and legitimate companies never ask you for personal information via email or request you to change your credentials such as usernames or passwords. If you receive such a request, immediately delete the email from your inbox as well as from your trash box in your email client in order to avoid accidental clicks. 4. Correct. You should never ever click the links within the text of the e-mail. In a phishing attempt, the text of the link does not correspond to a legitimate website. However, be aware of any message requesting you to provide sensitive information. 5. Wrong. In most cases phishers want you to react immediately. See such requests as a warning. 6. Wrong. Only 1, 3 and 4 are correct. **Basic tips:** If you follow the LIST approach you will reduce the risk of being victim of a phishing attempt. Ask yourself these questions when receiving suspicious emails.

No.	Question	Answer	Response
			Legitimacy: Does the request seem legitimate and usual? For example, should you be asked for this information, and is this how you should normally provide it? **Importance**: What is the value of the information you are being asked to provide or the task that you are being asked to perform, and how might it be misused? **Source**: Are you confident that the source of the request is genuine? Can you find a way to check? **Timing**: Do you have to respond now? If you still have doubts, take time to make further checks or ask for help. If you receive an email you believe is a phishing attempt, please contact: [INSERT NAME OF RELEVANT ORGANIZATION/ASSOCIATION/AUTHORITY].
7	***Backup*** Check what you know about backing up data.	1. You should only backup photos you store on the computer. 2. Any information you deem important should be backed up. 3. Files I don't want change in the future only have to be backed up once. 4. You should never use CD-RW as external storage format 5. You should have your backup files in the	1. Wrong. You should backup any files that are of value to you 2. Correct. For example: • Photos • Software or music you've purchased and downloaded from the Internet • E-mail address book • E-mails and letters 3. Correct. However, the more backup copies you

No.	Question	Answer	Response
		same room where the original files are in case you need them	have, the better 4. Wrong. CD-RWs are excellent storage formats. They can store relatively large amounts of data and are quite inexpensive to buy. There are several other storage formats as well, each with their own advantages and disadvantages, for example: • External drives • USB flash drives • Online backup and storage 5. Wrong. It is always best to store your backup copies in a different room from that of your computer. Ideally, you should have several backup copies stored in separate locations. If you store important documents in a safe deposit box at your bank for example, you should store a backup of your files there as well.
8	***USB flash drives*** An increasingly popular storage format for data is USB flash drives. But are you aware of the risks and disadvantages with USB flash drives?	1. They are not suitable for storing photos 2. They may contain viruses 3. They are expensive in relation to storage capacity 4. They are easy to misplace or lose 5. They are a safe way of storing data because USB flash drives are encrypted	1. Wrong. You can store whatever files on a USB flash drive just like any hard drive. That's one of the advantages with USB flash drives. 2. Correct. Before using a USB flash drive for the first time, you should scan it for viruses. In addition, you should always do this after copying files from an un-trusted computer. 3. Wrong. One of the main advantages with USB flash drives is the relatively low price considering the high storage capacity. 4. Correct. The fact they are small is sometimes

No.	Question	Answer	Response
			an advantage, but inevitably make them easy to misplace or lose. 5. Wrong. Normally, USB flash drives do not come with encryption functionality. In order to protect the data you should encrypt files stored on USB flash drives using encryption hardware or software. If you lose it, no one else can retrieve the data. If you also have a separate backup of those files, you don't risk losing valuable information at all.
9	***Encryption*** Encryption is a means of protecting information, but how much do you know about encryption?	1. Encryption is expensive for home-users 2. Typically, encrypted files can not be disclosed to others 3. Not all data can be encrypted 4. E-mails do not have to be encrypted unless sent with attachments 5. Encryption protects the confidentiality of information	1. Wrong. Encryption software doesn't have to be expensive. There are even encryption freeware. When choosing encryption software, make sure the source code is publicly available. This allows programming and encryption experts to examine it and search for "back doors" and bugs. 2. Correct. The most popular file encryption software is using very strong algorithms that are virtually impossible to crack. 3. Wrong. All data can be encrypted. However, some encryption software is only for encrypting e-mails whereas other also provides file encryption and even hard disk encryption. 4. Wrong. What data is encrypted depend on what you decide to encrypt. 5. Correct. Encryption is a method to protect the unauthorized disclosing of information.

No.	Question	Answer	Response
10	***Downloading files*** The internet is a fantastic resource with all its information available a click away. But are you aware of the copyright aspects of downloading files?	1. It's illegal to download illegally published copyright-protected material 2. It's illegal to download any copyright-protected material 3. It's legal to download music as long as it's not MP3 format 4. It's illegal to share/upload illegally published copyright-protected material 5. Software is not copyright-protected material, only text, music, photos and films	[RESPONSES TO THIS QUESTION HAVE TO BE ADDED AND MUST BE MODIFIED TO COMPLY WITH LAWS APPLICABLE IN YOUR COUNTRY]. 1. 2. 3. 4. 5.

SME Quiz

SME Quiz

Introduction text to the SMEs Quiz

Welcome to the ENISA AR Quiz for SME Executives!

The aim of this quiz is to provide a means for you as an executive of a small or medium enterprise to test your awareness and knowledge on a number of topics concerning your use of computers and the Internet as tools to support your business activities. These tools are valuable to increase the ability for your company to communicate and compete in a European and global market. However, they also come with risks you should be aware of.

This quiz should not be perceived as a comprehensive self-test of your current level of awareness and readiness. The objective is merely to give you a hint on your level of awareness and hopefully serve as a tool to encourage further interest in the values and risks of using the Internet. We also hope you will find the sources of information provided on this website valuable and useful.

Risk profile

Networks and information security management is basically a risk management activity, and as such a requirement to identify the valuable assets of the enterprise that could be damaged through IT systems vulnerabilities. Besides production processes, information is a valuable asset that is commonly damaged by IT systems failures.

Valuable information comprises for example information databases of suppliers and customers address books (also on mobile devices), financial information, industrial models and business plans. Information is an asset and as such at risk to many threats like natural hazards, crime, system failures and human errors.

No.	Question	Answers	Response
1	Do you know which valuable information is processed on your IT systems, and where?	a) Yes, we have a detailed inventory of valuable information, that we use e.g. for backups b) Yes, we know that some systems are critical because they process highly valuable information c) No, we know that there is some valuable information on our systems, but we don't know exactly which and where d) No, we don't actually have highly valuable information in our systems e) I don't know	A detailed knowledge of the valuable information processed on IT systems is the basis for proper risk management. This knowledge is the basis for proper implementation of controls (e.g. protection mechanisms) and for efficient investments. Know your enemy. You will then be able to invest in the most appropriate countermeasures.
2	Which of the following represent the greatest threat to your business' information?	a) Competitors, because competition is very high this market b) Partners, because valuable data must be shared with multiple actors c) Criminals, because my company develops commercial activities for individuals	

No.	Question	Answers	Response
		d) Employees, because they might intentionally or unintentionally leak information e) None f) I don't know	

Legal and contractual issues

Any executive must abide to the law and comply with legal obligations. In the field of network and information security, several European and/or domestic laws must be taken into consideration and then applied in the company's business.
Are you aware of your legal responsibilities related to information security?

No.	Question	Answers	Response
3	Are you aware about privacy regulations applicable in your country / Europe (concerning customers' data)? Are you aware on the impact on IT management?	a) Yes, this process is under control b) No, we do not deal with such legal issue c) Partially, an improvement process has been implemented recently d) I don't know	Compliance related to network and information security legal issues tend to become more and more important. Executives must be aware of their legal responsibilities. Personal data protection and software licences management are key in this area. In the case of outsourcing, obligations of contractors should be clearly stated in contracts. This includes handling of sensitive data on information systems during maintenance activities.
4	Are you aware of copyright regulations applicable in your country / Europe (concerning software and digital contents)?	a) Yes, this process is under control b) No, we do not deal with such legal issues c) Partially, an improvement process has been implemented recently d) I don't know	
5	Do you have implemented contractual obligations to protect the network and information security when your systems are outsourced e.g. for	a) Yes, this process is under control b) No, we do not outsource c) Partially, an improvement process has been implemented recently	

No.	Question	Answers	Response
	maintenance?	d) I don't know	

Human and organizational aspects

Security tools are very useful to protect networks and information systems. Nevertheless, as for driving a car safely, only drivers' behaviour can seriously reduce accidents. So, your employees should have a basic awareness and understanding of how to handle information and computers.

How does your business' information security policy (explicit or implicit) reflect the matters below?

No.	Question	Answers	Response
6	Your password used to access your business data is known:	a) Only by you b) By a few colleagues c) By a system administrator d) By family members	A few basic attitudes and paying attention on a few risky situations can greatly reduce information security risks. Executives are important in the development of an Information Security Culture as they must act as good examples. The Internet is a new environment, like a foreign country: you need to develop the proper attitude that helps in avoiding frauds and risks. Start by defining security policy. You will find more information here: [ADD MORE INFORMATION AND/OR INSERT LINKS WHERE MORE INFO CAN BE FOUND]
7	Do you use your private web mail for professional purposes?	a) Never b) Sometimes c) Frequently d) Everyday	
8	Do you handle professional matters on Social Networks or newsgroups?	a) Never b) Sometimes c) Frequently d) Everyday	
9	How would you react if you receive a phone call or an e-mail asking for business information?	a) I never answer b) I answer the questions c) I ask for details before answering d) I ask a colleague or a friend for advice e) I don't know	
10	Are your mobiles devices (PDAs,	a) Yes	

No.	Question	Answers	Response
	laptops, USB keys) always under control and surveillance when not used?	b) No c) Sometimes d) I don't have such devices e) I don't know	

Security tools

Once information assets are identified, some basic techniques can protect them efficiently. Virus or spyware attacks, network intrusion or information theft/disclosure could impact business activities.

Are you aware of security tools aimed at protecting sensitive devices and information?

No.	Question	Answers	Response
11	Back up of sensitive data are implemented:	a) Daily b) Weekly c) Monthly d) Never e) I don't know	Some basic solutions are good enough to protect companies' information systems. Those cited in the questions are now easy to use and cost effective. Not using them will greatly increase the risk of system compromise and damage trough trivial means.
12	Anti-virus and anti spyware are installed and updated:	a) On PCs b) On laptops c) On file servers d) On e-mail servers e) I don't know	
13	Secure remote access are installed on PDAs and laptops (with VPN and strong authentication)	a) Yes b) No c) In progress d) I don't know	

No.	Question	Answers	Response
14	Encryption is used to encrypt:	a) Data on PCs b) Data on laptops, PDAs and other mobile devices c) Data on file servers d) E-mails e) I don't know	

enisa
European Network
and Information
Security Agency

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu