

SPAM IQ Test



The Spam IQ test is a simple and straightforward method to check your knowledge about spam. As you attempt the different questions, you will become more alert and conscious of the problem thereby preserving yourself more efficiently from spam. Thank you for your interest in the Spam IQ test.

Questions

Question 1

You receive an email from an organization asking that you "Verify your account information within 24 hours or your account will be frozen." This email requests your password, login name, National ID Number, credit card details or other personal information.

You know the organization and think that you may have subscribed to one of their services.

What do you do?

- a) You reply to the email asking them why they want this information
- b) You reply to the email with the information asked for.
- c) You delete the email.

Question 2

To reduce spam, you can:

- a) Use one email address for friends and family and instruct them never to supply that address to anyone else. Create a second address for trusted businesses.
- b) Create temporary "throw-away" email addresses that you use for specific purposes including newsgroup and newsletter subscriptions, message board postings and other online services that require an email address.
- c) c) Do both A and B

Question 3

To help minimize the amount of spam that you receive, turn off the preview pane — a window that allows you to preview the contents of an email message — in your email software.

- a) True
- b) False
- c) Good email software protection allows me use the preview pane without potentially harming my computer system.

Question 4

If you choose to post your email address to a website, can you choose a format that makes it more difficult for spammers to collect it?

- a) Yes
- b) No
- c) Spammers don't collect email addresses that way. They rent or buy email address lists.

Question 5

You have received an email message promoting a service that you never asked for. At the bottom of the message you find a phone number to call in order to be removed from this mailing list. You:

- a) Call the number and ask to be removed from this mailing list.
- b) Delete the email message.
- c) Reply to the email message asking to be removed from the mailing list.

Question 6

Is it worthwhile to create an "alphanumeric" address (an email address that combines both numbers and letters)?

- a) Yes
- b) No

Question 7

You have an easy to remember password and you use the same password everywhere, even for your bank account. You have heard that you should use different passwords for your accounts and change them regularly.

What should you really do?

- a) Continue using the same password.
- b) Create passwords made up of mixed characters and numbers (such as 43JAMP9), and change your account passwords once a month.
- c) Create three passwords based on your favourite names and rotate those between your accounts every three months.
- d) Keep a list of 20 short, easy to remember word passwords in a file on your computer. Then you can look them up and change your account passwords every six months.

Question 8

How often should you update your antivirus program and personal firewall?

- a) Never. Installing these programs is all that is required.
- b) Once a month
- c) Once a week
- d) Check as often as possible and use the auto-update feature if the software offers it.

Question 9

After checking your email, your computer starts behaving unusually. You:

- a) Install or update anti-virus and firewall software and run a full system scan.
- b) Configure your firewall so that it prompts you every time a program on your computer attempts to connect to the Internet.
- c) Check for any unauthorized use of your personal accounts including, banking, credit card, e-commerce, email, and any other password-protected account.
- d) A and B
- e) A, B and C

Question 10

There is no risk in opening email attachments from someone you don't know.

- a) True

- b) False
- c) You can open anything if you have anti-virus software installed on your computer system.

Question 11

It's generally safe to open an email attachment from someone you know, even if you weren't expecting it:

- a) Only if you check the Internet/Email header information (which identifies the route the email has taken to get to you) to confirm the sender's identity.
- b) Yes, it should be safe—you trust your friends not to present a spam threat.
- c) No, you should never do this.

Question 12

To protect your computer from attacks by spammers, you need to install:

- a) Anti-spam software
- b) Anti-virus software
- c) A personal firewall
- d) A, B and C
- e) A and C

Question 13

The best way to protect your computer is to disconnect from the Internet and turn it off when it's not in use.

- a) True—Turning my computer off assures total safety.
- b) False—I never have to disconnect because I get a good security package as part of my deal with my internet service provider (ISP). They constantly update it and it's always on, automatically.

Question 14

You receive an email message that says, "Click the link below to gain access to your account." You:

- a) Cut and paste the link into your web browser — the software application that enables web pages to be displayed.
- b) Delete the email message.
- c) Click on the link to safely access your account.

Question 15

It's always safe to open email messages that appear to come from you yourself.

- a) True
- b) False
- c) This is a trick question—you can't send an email to yourself!

Question 16

Does a web browser — the software application that enables web pages to be displayed — need to be updated regularly?

- a) Yes
- b) No

- c) There is no need for updates, unless the manufacturer recalls it and that's rare.

Question 17

Your best way of telling if an email message is suspicious is by looking at:

- a) The email address it is sent from.
- b) The Internet/email header.
- c) The email addresses of other recipients of the email.

Question 18

You hate receiving spam email messages and wish they would stop. To avoid spam or reduce the volume you receive you:

- a) Carefully follow the mailing list removal instructions provided by some emails.
- b) Reply to unwanted messages with a statement that you are not interested in receiving further emails, and ask or demand that the sender stop bothering you.
- c) Simply delete the offending messages and take no other action.
- d) A and B

Question 19

Is it true that it won't present a threat of spam if you forward email petitions that you receive to all of the contacts in your address book?

- a) Yes—I want to share the things I'm interested in, and get support for positions I agree with.
- b) No—I don't want to impose on my contacts by sending them unrequested material.

Question 20

You can manage spam by:

- a) Setting up filtering options in your email software that send spam directly to a junk mailbox.
- b) Use a spam filter provided by your ISP, so that recognized spam never reaches your computer.
- c) A and B

Answers

Answer to Question 1

c) You delete the email.

You should never respond to email messages asking for personal information. Reputable organizations do not request confidential information this way. Fraudsters often send authentic looking email messages that appear to come from legitimate and well-known companies.

These messages often inform the recipient of a problem with an account and request personal information, which is then used to commit identity theft and fraud. This type of fraud is commonly known as "phishing".

Links in these messages may also lead to fraudulent websites that look legitimate. Do not follow links provided in email messages of this type. If in doubt, phone the organization to verify the request. Do not use the contact information provided in the email message. It could be fraudulent as well.

Answer to Question 2

c) A and B

A and B both. It's a good idea to have one email address that is used exclusively for friends and family. These trusted people should be made aware that they are not to share this address with anyone, and should use it only to communicate with you directly. The more exposure an email address gets the more vulnerable it becomes to spam. Examples of how people may be exposing your email address to spam include:

- Including you on mass mailings such as jokes and chain emails,
- Using your email address on websites that offer "Send to a friend" or "Invite a friend" services, or
- Entering your email address on ballots and surveys (both online and paper-based).

A second address can be used for dealing with trusted businesses such as utility providers and banks. A third email address can be used for other activities such as newsgroup and newsletter subscriptions, message board postings and other online services that require an email address. These activities are more likely to expose your email address to spam.

Check with your Internet Service Provider (ISP) to find out how you can set-up additional email addresses. A number of free email services are also available on the Internet.

Answer to Question 3

a) True

Spam can often contain invisible programming code that allows spammers to confirm that an email address exists and is active. This programming code can be activated through the preview pane.

Active email addresses are more likely to generate a response from spam and therefore attract more of it.

Using the preview pane may also expose your computer to various types of viruses. Most email programs give you the option of turning off the preview pane. Consult your email program's documentation for additional information.

Answer to Question 4

a) Yes

Although spammers can rent or buy existing email address lists, many opt to use software known as "spambots" that extract email addresses from web pages.

However, if you post your email address in a format such as "jane AT myDomain DOT com", it can help prevent "spambots" from recognizing it.

Do not post your primary email address on websites. Doing so will only help attract spam to it. Create an email address specifically for this purpose that you can easily part with if spam becomes a problem.

Check with your Internet service provider (ISP) to find out how you can set-up additional email addresses. A number of free email services are also available on the Internet.

Answer to Question 5

b) Delete the email message.

Some spammers supply an offshore phone number in the email messages that they send. Calling these numbers can end up costing you a small fortune in long distance fees.

Responding to the message will confirm to the spammer that your email address is active and make it vulnerable to additional spam.

Remember, con artists will use any trick to get your money. Never call a number that you get through unsolicited email.

Answer to Question 6

a) Yes

Some spammers use programs that automatically generate commonly used email addresses such as myName@myDomain.com.

Therefore, it is better to use an email address that combines numbers and letters, such as Myname348xyz@myDomain.com. An alphanumeric email address is harder to guess and possibly less vulnerable to spam. But remember spammers may ultimately discover any email address.

Answer to Question 7

- b) Create passwords made up of mixed characters and numbers (such as 43JAMP9), and change your account passwords once a month.

The more complex a password is, the more difficult it is for others to figure out. Always create passwords of at least eight characters that combine numbers, letters and special characters when possible. Change your account passwords regularly to minimize the risk of them being discovered and to limit the damage caused if ever they are.

Storing passwords in a file on your computer is not safe. Your computer could be broken into or stolen. Memorizing them provides you with the best protection.

If you decide to write your passwords down on paper:

- Do not store your user name and passwords in the same place.
- Do not include obvious headings on the page such as "my password" or "my user names".
- Do not place this information near your computer.

Answer to Question 8

- d) Check as often as possible and use the auto-update feature if the software offers it.

New viruses are discovered on a daily basis. You should check for updates for your anti-virus program and personal firewall as often as possible. Many software packages can even be configured to check for and install updates automatically (auto-update). Consult your software's documentation for additional information.

Answer to Question 9

- e) A, B and C

Spam often comes bundled with malicious programs such as viruses. If you notice that your computer is behaving unusually, it may have been infected.

Possible symptoms of infection are:

- Sluggish computer performance.
- Programs or files mysteriously appear or disappear.
- Someone tells you that they have received email messages from you, which you did not send.

Install anti-virus and firewall software, keep this software updated and scan your system for viruses on a daily basis. Most firewalls can be configured to prevent unknown programs from accessing the Internet. This can help minimize the damage caused by an infected system. See your firewall's documentation for details.

Answer to Question 10

- b) False

Never open attachments from someone you don't know. An attachment may contain software that could jeopardize your computer's performance and compromise your personal

information. While anti-virus software will protect you from some malicious programs, it is not fail proof.

Answer to Question 11

c) No

It's always best to check with the sender that an attachment has been included. Spammers may use a "spoofed" email address, so that email you receive appears to have been sent by someone that you know and trust. Even the information in the Internet/Email header (an option available on most email programs through the options menu) may have been spoofed. Spammers may in fact be sending you a malicious program through an email attachment, that will allow them to gain access to your computer and your personal information. If you receive an attachment that you weren't expecting, ALWAYS verify with the email sender before opening it.

Answer to Question 12

d) A, B and C

It is recommended that you use all three.

Anti-spam software can scan email before it is received and automatically dispose of known spam. Most Internet service providers (ISPs) offer this service, sometimes for a monthly fee. Many free email services also offer anti-spam services.

Anti-virus software can help protect your computer from infected spam. It can also help remove known viruses from an infected computer system. A personal firewall helps you control traffic to and from your computer. Make sure to choose a firewall that provides both incoming and outgoing protection.

Answer to Question 13

a) True

It's a good idea to disconnect from the Internet and shut down your computer when you're not using it. New spam programs and other threats can appear at any time, and no security package is totally safe—it's just too difficult for them to keep up with the fraudsters. Many spammers are using sophisticated programs which find and exploit unprotected computers that have been left turned on and connected to the Internet. If you turn off your computer you'll prevent malicious programs from accessing the Internet and your computer system. If you have any doubts or questions, consult your Internet service provider (ISP), or check your system's documentation.

Answer to Question 14

b) Delete the email message.

To be absolutely safe, simply delete any dubious email. If you have a legitimate account somewhere, you should be able to access it directly by typing the website's URL into your web browser's address bar. "Phishers" often insert misleading links into email messages; these lead to fraudulent websites designed to steal your personal information.

"Phishers" often insert misleading links into email messages that lead to fraudulent websites designed to steal your personal information.

Answer to Question 15

b) False

You can indeed send an email to yourself—and unless you're positive that you did so, do not open it. A technique known as email "spoofing" can allow a spammer to send messages that appear to be from you yourself. Unfortunately, you are probably not the only person receiving such an email, and if you open it, you might be playing into the hands of a fraudster. If you get an email that seems to come from yourself but doesn't, contact your ISP or computer support person.

Answer to Question 16

a) Yes

Make sure that you regularly check for updates to your web browser. The companies that design web browsers are always looking for ways to make their software safer in order to protect their customers.

Consult your web browser's documentation for additional information on how to keep it updated.

Answer to Question 17

b) The Internet/email header.

The Internet/email header can usually be accessed through an options menu and is an expansion of the main header (Often the From: or Subject: line of an email). It can tell you where a message originated from and what route it took to get to you. Although Internet/email headers can be difficult to understand, they are more reliable in determining where an email message actually came from. Educate yourself—an Internet search for "reading email headers" or "reading Internet headers" can provide links to many tutorials. Consult your email software's documentation for additional information about displaying header information.

Answer to Question 18

c) Just delete the message.

Spam can often contain invisible programming code that allows spammers to validate an email address when a message is previewed. A valid email address is more prone to spam than one whose authenticity has not been confirmed. However, if you've registered online with a legitimate organization, you may use their "unsubscribe" service. Legitimate organizations are happy to keep the amount of unwanted email down.

Answer to Question 19

b) No

Unless you are 100 percent sure about the origin of a petition, it would be wise to delete it. Mass-mailings like this constitute spam, and spammers will use any email addresses they get to send out even more spam.

Answer to Question 20

c) A and B

By setting up filtering options in your email software and by using the anti-spam services offered by many ISPs, you have a better chance of controlling the spam that you receive. You'll never get rid of all the spam, but a lot of it will be diverted before it gets to your inbox.