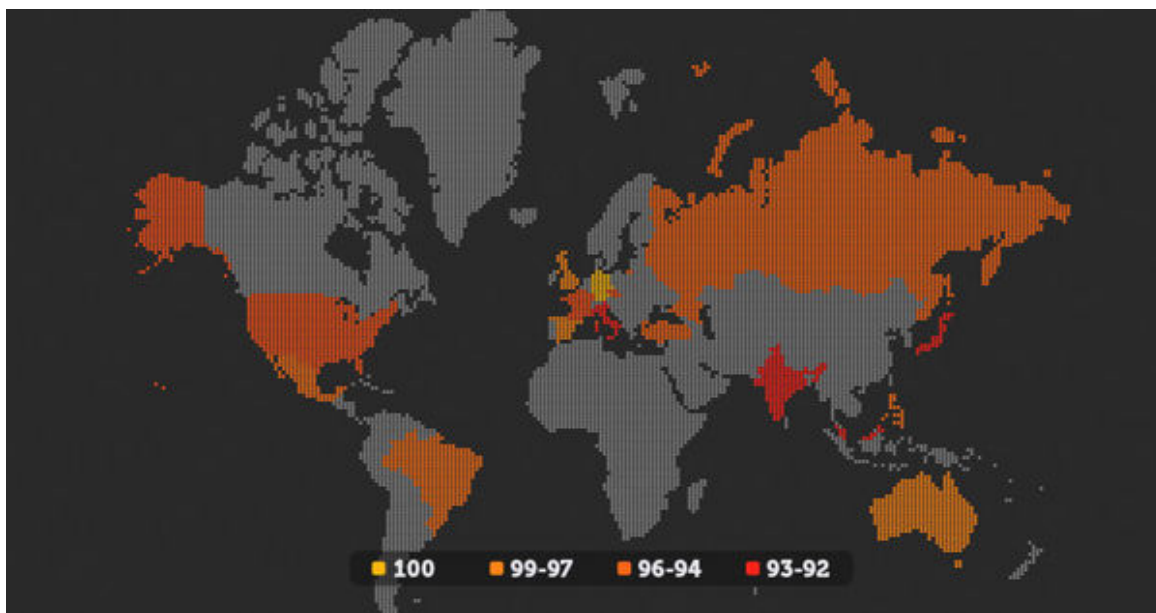


Are you cyber savvy?

The Internet, like the physical world, may be safe or unsafe, depending on your habits. You are safe in the street if you use crosswalks and obey traffic lights, but we don't recommend that you stroll around late at night with a wad of cash sticking out of your pocket. Life on the Internet comes with a few rules that are equally obvious, but not everyone is familiar with them. By taking this test, you will discover the degree of risk that you are exposed to when you are online and how likely you are to lose your valuable files, sensitive data, and even money by using the Internet in the way you currently do.

Your score is 130 points out of 150. Only 11% of test participants demonstrated the same level of cyber savviness as you. Congratulations! Your risk level is at a medium. Don't be alarmed this is a good result. Like many other users, you make some mistakes, but on the whole your online behavior is cautious and you take care to avoid falling for online fraudsters' tricks. Unfortunately, certain gaps in your cyber-literacy may threaten your personal privacy or even your money. Be sure to improve your knowledge of online threats and use security solutions. If you want to stay current on the latest news on online threats and tips and tricks to stay safe online, be sure to check out Kaspersky Daily: <https://blog.kaspersky.com/tag/cybersavvy> and Think Security Guide: <http://thinksecurityguide.com>. If you want to see if your devices have been compromised with malware, you can scan with these free tools <http://free.kaspersky.com/> and protect them with our range of products <http://www.kaspersky.com/trials>.



55

2

6

0

0

 Facebook Google+ LinkedIn Reddit Twitter

Safe answers

Question #5: On which of the pages below would you enter your credentials without hesitation?

This is a test of whether you can identify a phishing page, that is, a fake page designed to steal your credentials. The only correct answer is No. 4. The remaining three choices are screenshots of phishing pages detected by Kaspersky Lab experts in the expanse of the Internet. By entering data on these pages, you are handing that data over to cybercriminals.

Question #6: You have received an email with an attached Word file named “Overdue fines”. What will you do?

When receiving a message with an attachment, especially from an unknown sender, it is always a good idea to check that it is not spam. Some spam, for instance, is embedded with malware disguised as a safe format. Even if you have been waiting, impatiently, for something like a fine notice from the tax inspector, it is best to scan the attachment for malware before opening it. Deleting the message is also quite safe – particularly if you do not feel like reading incoming emails.

Question #7: The file you need is on a file-sharing site (a site where people upload files and from which other people can download them). When you click to download it, you are given the choice whether to download at low speed or try the high-speed mode for free. Which option will you choose?

When choosing the high-speed download option, a user is often asked to click on some advertising links, enter a phone number, or perform similar actions that are fraught with the risk of device infection or loss of confidential data. As they say, it is better to be safe than sorry.

Question #8: You are creating a new account on a website. How will you create a password?

Of course, it is always best to come up with a new, complicated password. Firstly, a complicated password with a large number of characters, including upper and lower case letters, digits and punctuation marks, is much harder to crack. Secondly, if you always use the same password, or variations of it, and one of your passwords is intercepted, cybercriminals will gain access to several, rather than one, of your online services.

Question #9: A website requires you to have a more complicated password. How will you save it?

The safest options are to remember your password or use a special program. Anything written down on a piece of paper, in the browser, on the computer or on your phone can be stolen and used to compromise your account (for example, on a social network).

Question #10: To create a temporary account on a website (for example, to order a one-time delivery), you need to specify your email. Which address will you provide?

If you only have one email address and you provide it every time, this is not safe. Firstly, it means that all your services and messengers are linked to one email address. By cracking that email account, an attacker will immediately gain access to the rest of your accounts. Secondly, if you write your main email address everywhere, even for temporary accounts, you are more likely to become a favorite target for spam and phishing emails.

Question #11: You have entered your login and password on a webmail site. The browser offers you the option to save your credentials so that they can be used for automatic form completion in the future. What will you do?

What is wrong with saving your password in the browser? Even if this is your personal device to which no one else has access, there is malware designed to look for your passwords in everyday places like autocomplete forms.

Question #12: Your digital pictures and videos take up too much space but you don't want to delete them. What will you do?

The safest option is to encrypt the folder with your photos and move it to the cloud. Due to the encryption, there is no risk that someone will be able to gain unauthorized access to your files. At the same time, storing photos in the cloud means you don't need to worry about your data being lost if your hard drive is broken or stolen – in this respect, cloud storage is really more reliable than a hard disk.

Question #13: Do you create backup copies of your files so you can restore them to your device should you need to?

Perhaps creating backup copies of all your files every day is too much of a good thing. However, if you do not want to lose, say, your documents or photos on a broken, lost or infected device, backing them up once in a while makes sense.

Question #14: From what sources do you usually download files such as applications, movies, books, games?

Of course, it is best practice not to download anything, but this rarely happens in the age of the Internet, right? To minimize your chances of coming across an infected page or malicious application disguised as a legitimate one, be careful about choosing your sources. The best option is to choose licensed products from well-known online shops and app stores.

Question #15: You want to download Yesterday by The Beatles and there are a few options in the Internet. Which of the files you would download?

If you chose any of the options except “Betles-Yesturday.wma”, you have been taken in by cybercriminals. It turns out that good spelling was not among the strengths of the user who made the file available, but at least you can be sure that that user did not try to make you install malware with the extension of a screensaver (Yesterday-Beatles-Song.scr) or executable file (Beatles_Yesterday.mp3.exe) on your device instead of an audio recording.

Question #16: You want to make a purchase online. The payment system requires you to enter your credit card details. What precautions will you take to ensure a safe transaction?

Even if you use the sites of large and proven companies, it is very important to take precautions. In most cases, financial data is intercepted on the user's – that is, your – device, not on the website. If it is not a fake (i.e., phishing) site, of course. This means that you should be sure to check the address bar (whether you got the address right) and the contents of the page – has anything changed, are there any extra data entry fields? Entering data using a virtual keyboard is also a good idea, because it helps to prevent

characters entered using the regular keyboard from being intercepted by malware designed for this purpose. Unfortunately, the incognito mode of the browser and anonymizers are useless against financial data theft.

Question #17: When dining out, you want to pay by credit or debit card. Which scenario would you prefer?

Another widespread type of financial fraud is copying a bank card illegally. This is why you should never lose sight of your card – and never give your account information to another person, even if that person is a very good waiter.

Question #18: You are authorizing on a banking website (let's say Money Bank). Which address looks safe to you?

The only correct answer choice here is <https://MoneyBank.com>. If an address starts with http rather than https, this means that the connection is not encrypted and the information sent over can be intercepted. If the site name has extra characters or contains a typo, this is a sure sign of phishing.

Question #19: Do you allow your browser to collect your website browsing history?

With technology everywhere, protecting your privacy is not easy. But at least you can do the necessary minimum – regularly purge your browsing history or not save it at all.

Question #20: Which channels do you use for private messaging?

Of course, the most secure answer in this case is, “I don't undertake private messaging online”. But if you do like to discuss private topics with the help of the latest technologies, your best bet is using your own protected devices and messengers that use encryption.

Question #21: How do you store information on your computer that you don't want anyone to see?

The safest answer is to encrypt your data or immediately delete it. Unfortunately, if your device has Internet access, using password protection or attempting to hide the device will not provide complete protection of your data against leaks.

Question #22: How do you usually install new applications on your computer?

If you install applications without carefully reading messages in the installation window, you can easily get a bunch of unwanted applications together with the program you want, as well as changes to the operating system that can be dangerous for you and your data.

Question #23: What is your attitude to websites that identify your location and display ads based on websites you visit and your search history?

Of course, you are entitled to appreciate the fact that large IT corporations and advertising companies know your habits, interests and secrets better than your closest friends do. But if this is not to your liking, you don't have to live with it. There are many useful tools that make tracking your online activity more difficult.

Question #24: You have received a message from a friend through a social network. The friend suggests that you click on a link and like some pictures. What will you do?

Following links sent by your friends on social networks without any questions is like playing Russian roulette. There is no telling what is in store for you – it can be photos, but it can also be annoying advertising or dangerous malware.

Question #25: Which of your personal details are available to everyone, not just your

friends, on social network websites?

The more personal information you display online, the greater the risk. Cybercriminals will take the trouble to look at your information. In fact, there are known cases of personal information from social network pages being used for real-world crimes, not just for guessing account passwords.

Question #26: What do you do when you receive a friend request from a person you don't know?

If you accept friend requests from anyone, or anyone with whom you have common friends, you are in the danger zone. Your friends might have added an unknown person to their friend lists – which means that somebody whose motives are unclear will have access to your friends' personal information – and yours as well. In the best possible scenario, that person may be doing this for advertising purposes.

Question #27: You are installing an application. What will you do when the License Agreement screen appears?

Few people like spending a few minutes of their lives on studying the vendor's guarantees and warnings before installing a program. However, carefully reading the terms could prevent unpleasant surprises like personal data leaks, financial losses and the like.

Question #28: What will you do with an application you haven't used for a long time?

Older and more popular applications have more vulnerabilities that are known to cybercriminals. A vulnerability is a convenient entryway for malware to get on your device. The fewer such entryways the better – which means that all unneeded applications should be removed.

Question #29: Which permissions do you grant to the applications on your mobile device?

If applications on your device are allowed to do too many things or something of which you are not aware – that is a threat to you. Can they access your contacts? Photos? Location? Messages? Can they send information found on your device to external servers? What do you really know about the activity of the applications on your device?

Question #30: The operating system has notified you about updates that need to be downloaded and installed. What will you do?

Why is it important to install updates sooner rather than later? Because updates provide patches to security 'holes' found in the system to date. Such 'holes' can be used by cybercriminals to take control of your device.

Question #31: You are choosing an antivirus/internet security solution for your device. Which features are the most important to you?

Of course, tastes do differ. But there is an important parameter that should be kept in mind, first and foremost, when selecting a solution: the quality of protection. The best source of information on this is professional tests carried out by independent labs. At the same time, whether the settings are easy to understand and how much a solution affects system resources is also important. Note that you received the smallest number of points if you chose options like "Good reviews from my friends and on the Internet", "Good interface design" and "Low price". These options have little to do with the quality of a security solution.

Question #32: In which cases do you run an antivirus scan?

For this question, all the options are optimal except “I never run scan tasks” and “I don’t use a security solution”. The more often you scan and the more thorough the scans, the lower the risk.

Question #33: What will you do if your antivirus does not allow you to install a program?

As a rule, security solutions do not object to ‘good’ applications being installed. Even if this is a program you know and trust, it is always best to play it safe. One thing is for certain: it is not safe to disable protection, even temporarily. Malware could be disguised as the application you need, or malicious code may be embedded in a legitimate program. In any event, making life easier for cybercriminals should not be an option.