

<b>Software firewall is a program designed to:</b>		
<b>answer options</b>	<b>Response Percent</b>	<b>Response Count</b>
<b>Monitor network connections, control programs' internet activity and shield a computer from remote intruders and unwanted data.</b>	100.00%	43
Increase throughput of the current connection, optimize traffic and boost file download speeds.	0.00%	0
Improve reliability of data transfer and recover lost packets.	0.00%	0
Automate the procedure of managing access configuration and dynamically assign IP addresses for the joining hosts.	0.00%	0

<b>Q. What most precisely characterizes a computer virus?</b>		
<b>A. Viruses are characterized by being self-replicating. A program that hides itself and memorizes passwords is a keylogger.</b>		
<b>answer options</b>	<b>Response Percent</b>	<b>Response Count</b>
<b>A program that replicates by appending a piece of its code to an otherwise harmless executable file.</b>	74.42%	32
A file that instructs your computer to reboot following installation and adds its entry to the "Run" thread of the Windows Registry.	2.33%	1
A program that hides itself on a system and memorizes entered passwords which it later transfers to the perpetrator.	20.93%	9
A text file placed locally without your consent that records history of your browsing sessions for the purpose of customizing appearance and speeding up future access.	2.33%	1

**Q. Security updates are needed to:**

**A. Security updates are to resolve flaws and vulnerabilities in operating systems and installed applications.**

answer options	Response Percent	Response Count
Mitigate flaws in installed programs and host Operating Systems to resolve vulnerabilities.	83.72%	36
Improve program design and functionality.	16.28%	7
Make programs easier to use.	0.00%	0
To boost vendors' profits.	0.00%	0

**Q. Antivirus is a program that:**

**A. Antivirus applications only find/clean/remove files that are infected with a virus (or an obvious variant) known to that particular antivirus application. The antivirus software must generally have a signature in the database to identify a particular virus.**

answer options	Response Percent	Response Count
Will remove all kinds of malicious programs that exist.	20.93%	9
Removes only select categories of malware, depending upon how successfully it can identify any given threat.	69.77%	30
Will roll back all changes made since activation of malware, or prevent the activation in the first place to ensure total invincibility.	6.98%	3
Can be updated via Windows Update in order to obtain new signature definitions.	2.33%	1

**Q. Which of the following might be the consequence of botnet activity?**

**A. All of these are known uses of botnets.**

answer options	Response Percent	Response Count
Your computer will be commandeered and used to clandestinely to send spam and attack others.	2.38%	1
Your machine will act as a server by running backdoor software that accepts remote connections.	7.14%	3
Part of your Internet bandwidth will be hijacked and used to funnel malicious traffic.	4.76%	2
<b>All of the above.</b>	<b>85.71%</b>	<b>36</b>

**Q. What is the principle drawback of modern antiviruses?**

**A. The main drawback is that antivirus depends on knowing the signature for the virus you have received. If the virus is not previously known to the developers of the virus signature database, there can be a time window of several hours to several days where the virus will not be caught by the software.**

answer options	Response Percent	Response Count
<b>Reliance on antivirus signatures and immature Heuristics-based detection capabilities.</b>	38.10%	16
High price and the absence of free telephone support.	9.52%	4
Sometimes false positives occur, necessitating manual restoration of an erroneously removed object from the quarantine location.	30.95%	13
High memory, CPU and hard disk utilization.	21.43%	9

**Q. A friend has sent you a link to a file with an invitation to run it. He/she is not online right now so you can't check in with them. What should you do?**

**A. Always check with the sender before opening unexpected attachments or clicking unknown links. The sending address is easy to spoof and as noted above new viruses are not always caught by antivirus applications.**

answer options	Response Percent	Response Count
Trust my friend and click on the link.	0.00%	0
Save the file and run a virus scan on it. If the file is clean, it's probably ok to run it.	14.29%	6
<b>Do not click on the link, even if it's from a friend without checking with them first.</b>	83.33%	35
Trust your firewall to block the file if it's malicious.	2.38%	1

**It's December 20th and you have just received an email from your bank asking you to confirm your online activities by logging on to your account within a week. What is the best course of action to take?**

answer options	Response Percent	Response Count
<b>If possible, call your bank to confirm or otherwise, the authenticity of the email. If you can't reach your bank, don't click the link, but visit your account by manually entering the url of the bank (as you know it) into your browser.</b>	100.00%	42
Follow the link provided in the email and enter your login information - after all the email has your bank's logo and looks legitimate.	0.00%	0
Setup my antispam software to automatically purge messages received from people not listed in my contacts.	0.00%	0
I know it's phishing, so I'll just put false information in to fool the hackers. If it's not my information, they can't do anything to harm me.	0.00%	0

**Q. Which of the following activities could you probably do safely without fear of a malware infection?**

**A. Many of the flaws that are being utilized to infect systems now are within Microsoft Office applications rather than the operating system itself. Don't assume that application patches are any less important than operating system patches.**

answer options	Response Percent	Response Count
Running a screensaver downloaded from the internet.	0.00%	0
Not keeping up to date with Microsoft Word security patches and then double-clicking on a document that claims to come from someone you know.	2.38%	1
Allowing outlook to download and display graphics included in html emails.	2.38%	1
<b>None of the above.</b>	95.24%	40

**Q. How do you decrease the susceptibility of your computer to malware attacks?**

**A. While items 1 & 2 (and the encryption part of item 4) are good practices, they won't decrease your susceptibility to malware attacks. The second part of item 4 will be a problem for most folks, since we receive email from the public. Working under a restricted account will limit damage to files/system functions that can be accessed by that account. Many malware attacks will depend on the users current privileges being at the administrative level.**

answer options	Response Percent	Response Count
Perform incremental backups of your system.	9.52%	4
Set File and Printer Sharing permissions only to apply to hosts on your subnet.	9.52%	4
<b>Work under the Restricted User account.</b>	21.43%	9
Use encryption and have antispam automatically delete messages arriving from unknown senders.	59.52%	25