10 Quiz Questions about Computer Security

1. When should you postpone restarting your computer after installing a security update?

1. You can always postpone restarting your computer after a security update. That's why Windows lets you postpone the reboot.
2. You should never postpone restarting your computer after a security update. That reboot is really important to fully implement the patches you downloaded.
3. You should only postpone restarting your computer after a security update if you fully disconnect from the Internet first.
4. You should only postpone restarting your computer after a security update if you must keep your computer on to do important work which cannot wait.

Correct Answer: you can delay rebooting your computer if absolutely necessary, but you should not delay for any minor reason. The sooner you reboot your computer, the safer you will be. Disconnecting from the Internet after downloading the patches will protect you from new viruses getting on your computer, but it will not protect you from viruses you've already downloaded which can use the vulnerability before it gets patched during the next reboot.

2. Why should you ever turn off your firewall?

1. To install a new firewall or update your current firewall software.

2. You should never turn off your firewall.
3. When you go offline, the firewall isn't necessary, so you can turn it off to make your computer faster.
4. When you need every last bit of power your computer has, such as when you're trying to win at an online computer game.

Correct Answer: your firewall isn't necessary when you're disconnected from the Internet, but you should still not turn off your firewall even then. It's too easy to forget to turn the firewall back on when you do connect to the Internet and even one second connected to the Internet without a firewall can be enough time for a virus to infect your computer. You can install a new firewall without turning off your old firewall and your firewall uses so little processing power that turning it off makes almost no sense. Learn how to protect your computer.

3. How does turning off User Account Control (UAC) prompts in Windows Vista and Windows 7 make Windows less secure?

1. Disabling User Account Control lets anyone on your computer create new user accounts which they can use to install dangerous software.
2. Disabling User Account Control lets you enable dangerous settings in the Control Panel.
3. Disabling User Account Control lets viruses install themselves on your computer.
4. Disabling User Account Control does not make your computer less secure. It just gets rid of annoying pop-ups.

Correct Answer: viruses can install themselves on your computer much more easily if you disable User Account Control (UAC). UAC prevents programs from installing themselves without your permission, effectively blocking most viruses.

Run a Free PC Privacy Scan Now

4. Does the password to your Windows user account protect your files from other users on your computer?

1. No, the password only provides security against unskilled users who want to log into my Windows account.
2. Yes, the password does secure my files, but only if I enable folder encryption.
3. Yes, the password automatically protects my files from all other users on my computer.
4. Yes, the password does protect my files from other users, but only if I have the only Administrator account on the computer.

Correct Answer: Other users on your Windows computer can access your files directly through Windows without knowing your user password. Encryption which uses your user password can also be bypassed by skilled users. Not even administrator accounts get any special file safety. If you want to ensure your files can't be read by other users on your computer, you should use encryption not tied to your user password. Are you an unwitting cyber security terrorist?

5. What does a keylogger do?

1. It keeps track of your passwords (keys) for security and convenience.
2. It tracks your keystrokes to help you debug programs.
3. It tracks key statistics about your computer system to help Microsoft improve performance in the next version of Windows.
4. It tracks every key you press on your keyboard to help hackers figure out your passwords.

Correct Answer: keyloggers come in two forms: software keyloggers and hardware keyloggers. Viruses install software keyloggers on your computer which send every key you press on your keyboard back to the virus creator. He can then see what you typed immediately after you typed gmail.com—which will probably be your password. Advanced hackers install hardware keyloggers on computers to track their targets to get the same information or to get the contents of secure email and documents.

6. How do you know when you're connected to a secure website?

1. The web address (URL) starts with HTTPS and the address bar includes the color green.
2. There is a lock icon in the web address bar.
3. The web address (URL) starts with HTTPS and the address bar is red.
4. All websites today are secure websites.

Correct Answer: most modern browsers include the color green in the address bar when you visit a secure website. All secure websites also start with HTTPS (note the S), but some websites which start with HTTPS only encrypt part of their site, so they're not totally secure. (You can typically use these semi-secure websites for a credit card purchase, but you should be aware than hackers may know that you visited the site even though they can't see your credit card number.)

7. What are quarantined files?

1. Core system files which Windows will not let you change.
2. Files belonging to other users which Windows will not let you view.
3. Files in your Recycle Bin which have not yet been permanently deleted.
4. Files your anti-virus software thinks might contain a virus.

Correct Answer: many anti-virus programs will move files they think contain viruses to a special folder so you can examine them before deleting them. This folder is called a quarantine, although some programs give it a different name. For example, it's your Avast "Chest". You should not open files from the quarantine folder unless you know that they are safe.

8. Why should you use a brand name anti-virus program when you can use any old firewall?

1. You should use both a brand name anti-virus and a brand name firewall to ensure your security.
2. You don't need a brand name anti-virus or firewall; any anti-virus and firewall program will do a good job.
3. All firewalls use a simple system, but anti-viruses use a complex system, so anyone can make a good firewall, but only a company with a significant amount of resources can make a good anti-virus program.
4. Windows includes a firewall built by Microsoft, so you don't need a different firewall, but you do need anti-virus software and you should pay to get the best possible.

Correct Answer: even though recent versions of Windows do include a default firewall, all firewalls use a simple proactive defense system which any competent programmer can build, so all firewalls are effectively equal. Anti-virus programs use reactive defenses, so the faster the programmer reacts, the better your security. Only large anti-virus companies have enough programmers to react fast enough to major virus attacks.

9. Who can send email pretending to be you by using your email address?

1. Anyone on the Internet can put your email address in the form field.
2. Only your Internet Service Provide (ISP), such as GMail.com, can fake email from you.
3. Only hackers who break into your computer can fake email from you.
4. Nobody can fake email from you unless they get your username and password.

Correct Answer: anyone can fake email from you because anyone can put your email address in the form field. Spammers do this all the time in phishing attacks where they send a fake email claiming to be from PayPal, Google, and other trusted companies. You should never assume that an email comes from a particular person or company just because it uses their email address.

10. Can a computer running a good firewall and the latest anti-virus get infected with a virus?

1. Absolutely not; good security blocks 100% of infections.
2. Yes, but only if you manually run the virus from the quarantine folder.
3. Yes, but only if you download the virus manually and install it despite your virus software's warning.
4. Yes, you can still get viruses even if you have the best security software and use it properly.

Correct Answer: you can always get a virus no matter how great your security software. Anti-virus software, in particular, is reactive. Somebody has to get infected before the anti-virus programmer can write a rule to protect your computer, so if you're one of the first few hundred or thousand people to get a virus, your computer has no immunity against it and you will probably get infected. That's why good

security starts with good backups—you can't protect yourself against every virus, but you can protect yourself against data loss.