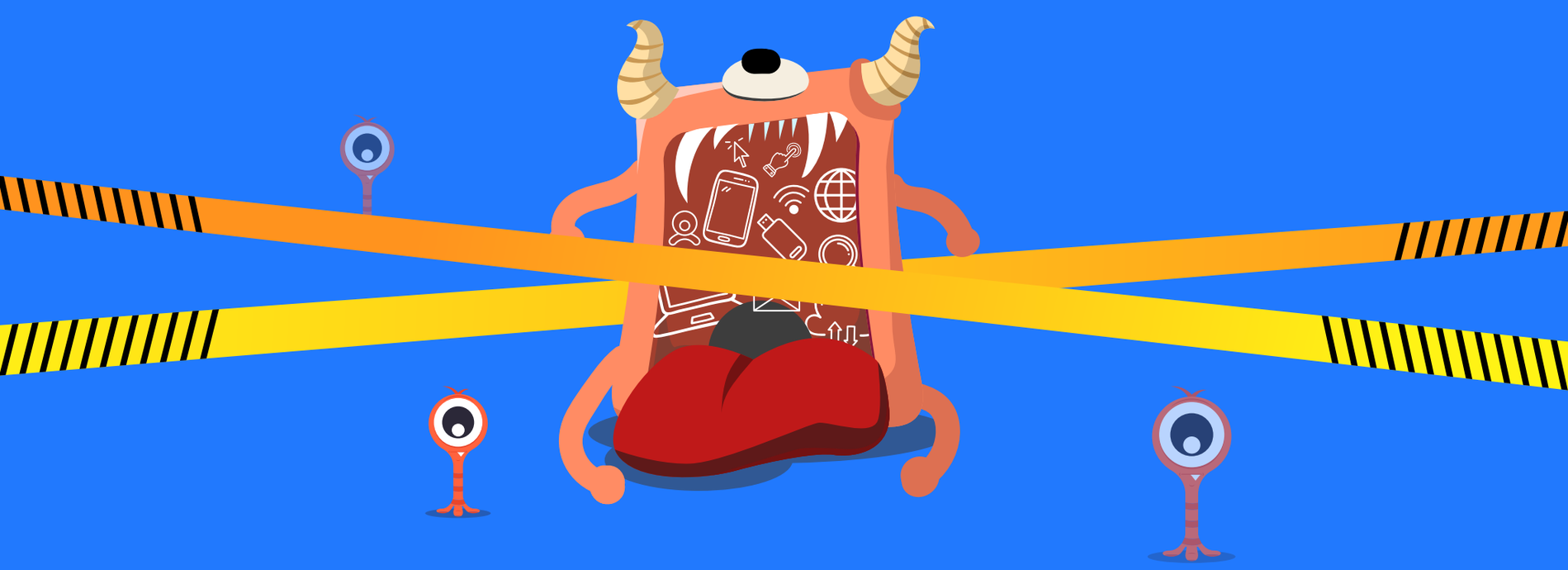
Antivirus REVIEWS

# 50 WAYS TO PROTECT YOUR DEVICES AGAINST ALL VIRUSES!



# Your computer and cellphone contain your entire life. Don’t believe us?

Where are the photographs of the amazing trip to Hawaii stored? Where do you access your bank account and pay your bills from?

How you call for those succulent pork dumplings from the Burmese place around the corner? Where do you access social media to post those gramworthy selfies from? With browsers that can remember passwords and autofill information, you have more of yourself on your computer and the Internet than you canimagine. You need to safeguard this more than ever now with online scams and thefts gaining ground. Thieves have gone high tech and you shouldn’t take that lightly.

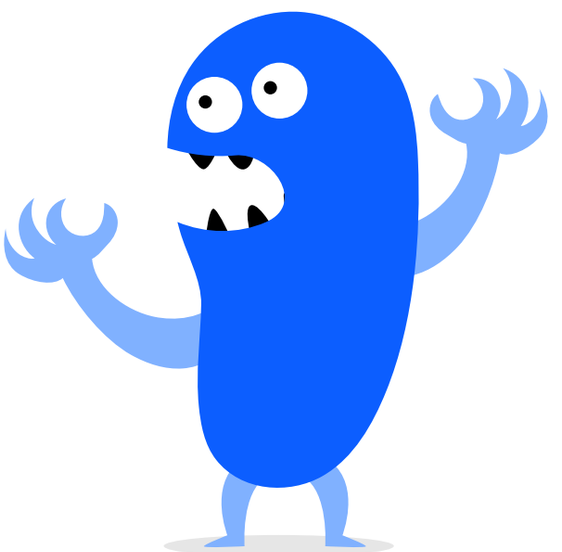
**Given here are  50 exhaustive ways you can ensure your PC is protected 24/7 even when you aren’t online.**

## 1 Update your OS regularly.

Software developers like Microsoft regularly release patches for flaws and it would behoove you to update these as and when they're released.

## 2 Update your antivirus on every rollout.

With new kinds of viruses, trojans, malware and spyware making their presence known every day, security companies release updates to their security suites on a regular basis. Update your antivirus software every time the company sends you an update notification.

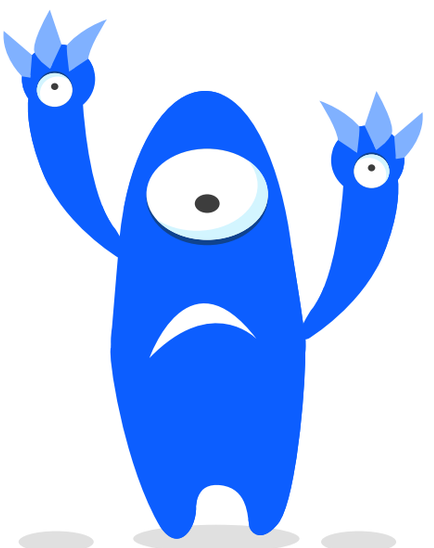


## 3 Choose a complicated password.

Your password is the final frontier to your data, so avoid using birthdays, anniversaries, names of family members or even pets. Use a different complex alpha numeric password for your router, PC, email accounts, bank and even shopping sites that can't be easily guessed. Use a password manager for ease of use.

## 4 Use the free antivirus inbuilt into your OS.

This is the basic security that comes inbuilt with the OS. Use this as the bare minimum if you aren't going to invest in paid security.

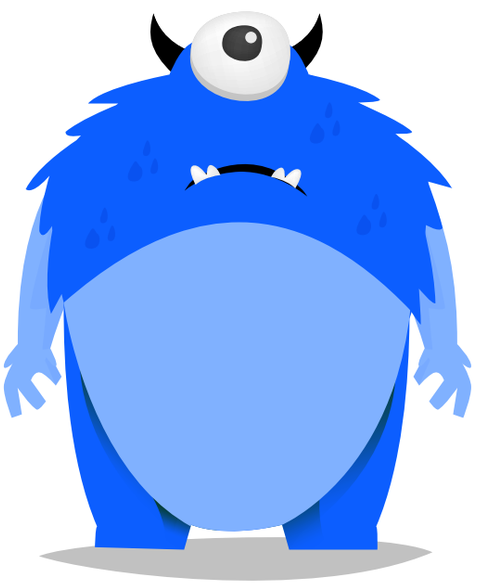


## 5 Ensure you turn on Windows firewall.

This protects your PC by preventing strangers from accessing your computer through the Internet or a network.

## 6 Use the latest version of your browser.

A web browser that is out of date could potentially have security vulnerabilities and you run the risk of having your computer compromised. Personal information, banking details, online purchases, photos and other sensitive data could be stolen, destroyed or worse - held for ransom.



## 7 When downloading software, use trusted sources.

Ensure that you download software only from reputable and trusted websites. Read the privacy policy and terms and conditions carefully before downloading anything. In particular, be wary of screensavers, games, P2P sites and browser add-ons.

## 8 Beware of phishing mails.

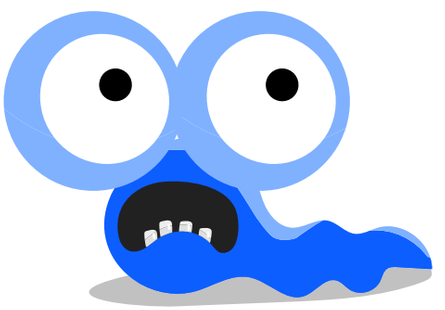
These mails attempt to relieve you of your passwords and other sensitive date by posing as a legitimate entity. Such emails will typically include a weblink that appears to be legitimate thus encouraging you to divulge your information.

## 9 Never open emails from unknown people.

If the sender of an email is not known to you, avoid opening such emails as it could pose a potential danger to your data.

## 10 Don’t click on links in emails from suspicious or unknown sender.

These mails attempt to relieve you of your passwords and other sensitive date by posing as a legitimate entity. Such emails will typically include a weblink that appears to be legitimate thus encouraging you to divulge your information.



## 11 Use a pop-up blocker.

Enabling the pop-up blocker on your browser prevents those annoying and sometimes malicious pop ups from hindering your work. Trojans and malware could disguise themselves as pop-ups and you could unwittingly click on them.

## 12 Be careful about using external hard drives and pen drives.

Do not connect unknown pendrives or hard drives to your computer without running a scan first. Keep pendrives you use from your home PC and office PC separate, so you do not cross contaminate. Buy pendrives only from reputed and legitimate companies as some unfamiliar manufacturers could manufacture these drives with malware preloaded on to them.

## 13 Run maintenance techniques.

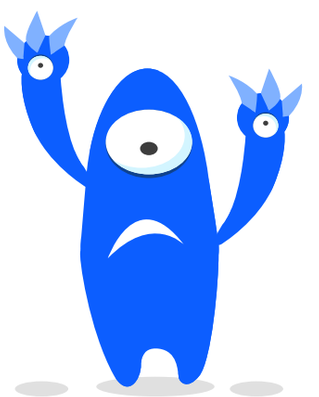
Defragment, remove cookies, delete unwanted files and software, back up your work, perform scan disk operations and basically do some digital housekeeping to keep your computer clean and resistant to vulnerabilities.

## 14 Use passwords for all added programs.

Password protecting executable files heightens security in case you're using a shared computer or even at the office.

## 15 Run all service packs.

Ensure you run every service pack for the OS, that the company releases. These ensure that all vulnerabilities are patched up and the software is resistant to attacks.

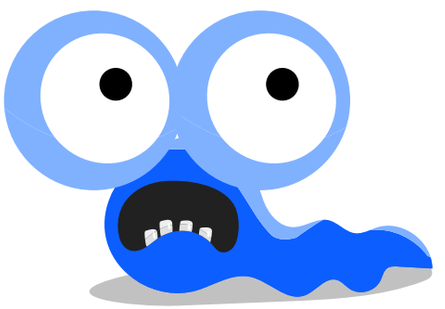


## 16 Scan your PC regularly.

Use the antivirus scan on your PC - free or paid - regularly. The more files you have, the longer the scan will take. Do not run the quick default scan, run the scan on each and every part of the hard drive/s.

## 17 Follow the PoLP.

This Principle of Least Privilege (POLP) is the concept that at any user, program, or process should get only the bare minimum privileges necessary to perform its function. If you have multiple users, ensure you carve out privileges for each one so you protect important transactions actions done by you.

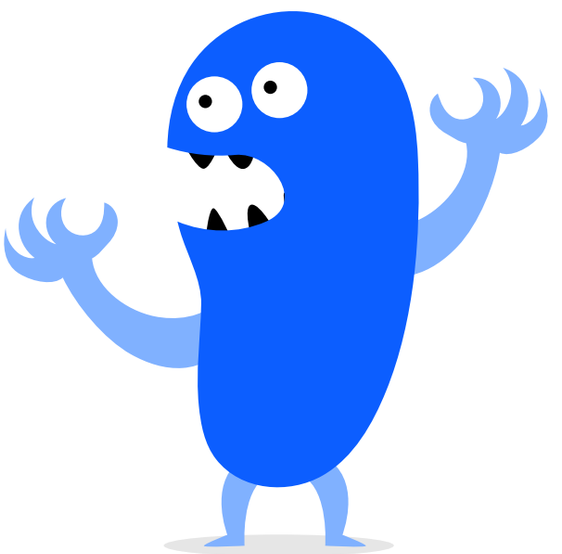


## 18 Don’t use illegal software.

Be sure you download software from legitimate sources. Do not use third party media to download. If the software has a price attached to it, you might as well pay for the software rather than downloading it for free from third party sites, that could potentially open a back door to your PC.

## 19 Choose an Operating System based on security and vulnerability.

Different versions of Operating Systems are more susceptible to hackers and viruses. Ensure you choose one that is recently updated and bulletproof.



## 20 Your Mac needs antivirus too.

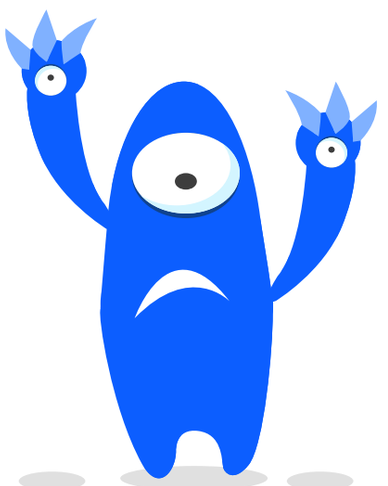
If you're using a Mac, to be on the safer side, download an antivirus from a trusted company, since it doesn't come installed with built-in antivirus.

## 21 Remove or disable Java.

If you don't use Java, it's simply sitting on your PC waiting to be exploited.

## 22 Use heavy-duty security.

If possible use a business-class antivirus protection. The reason being, these products are more frequently updated and provide better protection.



## 23 Investing in real time spyware protection is always a good idea.

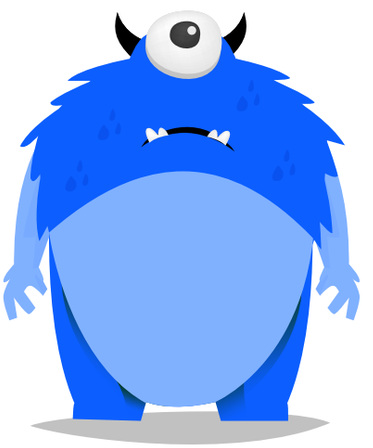
Paid protection is better since it constantly runs in the background and protects your PC in real time. Most free products detect spyware only after the computer is infected.

## 24 Scan and scan again.

Run scans on your computer before you go online every day.

## 25 Updating is key.

Running a scan is not enough. Update your antivirus and spyware protection every day and habituate yourself to run updates after your scans.



## 26 Disable Auto launch.

Ensure you disable auto-launch/run features in your Operating System. Disabling programs that auto run at Windows startup prevents vulnerable programs from running automatically.

## 27 Hardware over software.

A hardware-based firewall is much better than a software-based firewall and is one you should invest in. A hardware firewall is deemed more secure, is capable of protecting more computers and by running on its own processing power does not affect your computer's performance.

## 28 Update your browser.

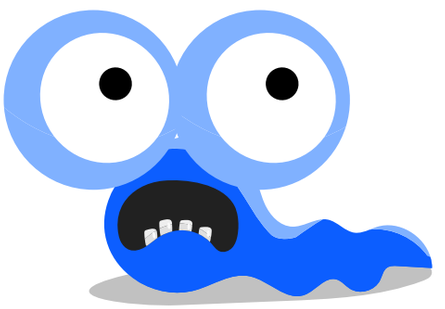
Like your Operating System and antivirus, your browser too needs to be up-to-date to remain secure. Regularly go to your browser's settings and make sure it updates and is set to block distrustful sites.

## 29 Encrypt your files.

If your PC is stolen, don't let the thieves get their hands on your data. Put your sensitive files in an encrypted folder.

## 30 Avoid using open Wi-fi.

Using an open Wi-fi makes it easy for malicious elements to eat into your connection and download illegal files. You must protect your Wi-fi with an encrypted password and refresh your gear every couple of years.



## 31 Use strong routers.

Use the newer crop of routers since some older ones have vulnerabilities that are almost never patched. The newer routers have features that allow you to provide your guests with isolated wireless access.

## 32 Do not upload sensitive data to the cloud.

As a rule of thumb, if the data is sensitive and too personal, keep it off the cloud.

## 33 Avoid linking accounts.

Don’t be lazy. If you want to comment on an article on a particular site and are prompted and tempted to sign in with Twitter or Facebook, do not do that. Accessing one account with the information from another, allows services to acquire a lot of personal information.

## 34 Control access.

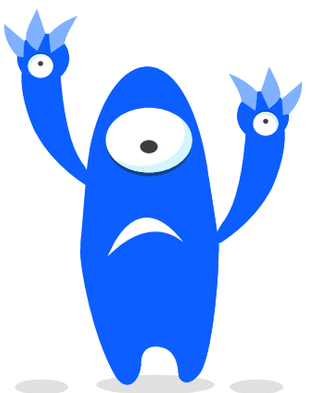
Turn on the User Account Control (UAC) option in your computer to ensure that any changes made in your system will require administrator-level-permission that can come only from you.

## 35 Two is not better than one.

Running two antivirus is not recommended. Though it does logically seem like a good idea to have “double protection “, it could crash your computer.

## 36 Scan all removable media before use.

Remember, your computer having an antivirus does not mean that it cannot get infected by a virus or other malicious software.



## 37 Scan email attachments.

This goes for even emails that come from trusted sources. Scan the attachments before you download them, since scammers are constantly finding new ways to infect systems. Vigilance is never for naught.

## 38 A private wireless connection is a must.

If you access the internet via a wireless connection, you must set up a secure account so that strangers can't ride the network and log on to your account and access saved passwords or ISP information.

## 39 Never save email or password settings.

Online transaction sites, social-media sites and ecommerce sites let users save their passwords and log-in information for ease of use. Saving this information leaves your account vulnerable to access by others.

## 40 Clear your browser's cache.

It is recommended that you erase your browser's cache after an online transaction. This is to get rid of stored information like bank account numbers and passwords, that may be extra sensitive.

## 41 Scrub and discard.

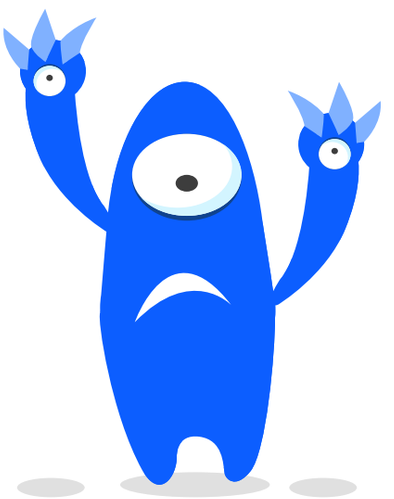
You should scrub your computer of all settings and memory before donating it, giving it away or simply discarding it. Wipe it clean, reformat it or destroy the hard drive.

## 42 HTTPS is key.

The "s" at the end of "https" indicates that the connection is secure and encrypted. You must look for this “s” when banking, shopping online or even simply browsing.

## 43 When using a public Wi-fi surf via VPN.

Apart from getting a new IP address so you can bypass geo-restrictions, surfing via VPN will help you browse the Internet more securely as connecting through a VPN, allows encryption of all data packages which protects your personal information from being monitored and exploited.



## 44 Use BitLocker Encryption.

While using a strong password to log into your Windows PC can help to protect it from regular users, someone who knows Command Prompt could very easily reset your password. Enabling BitLocker will encrypt and protect your data.

## 45 Log out of your bank account.

It doesn't matter how secure the connection is. Always log out of your bank account after transactions. Do not leave the page open or even simply close the window. Log out.

## 46 Ramp up VoIP security.

VoIP calls are vulnerable to identity theft and surveillance groups. Neglecting security on this front is not advisable.

## 47 Protect your cellphone.

Your mobile devices, that can access the internet and Bluetooth, need protection and security too. Use facial recognition, unique pattern or fingerprint identification to protect your smart devices.

## 48 Password-protect your cell phone.

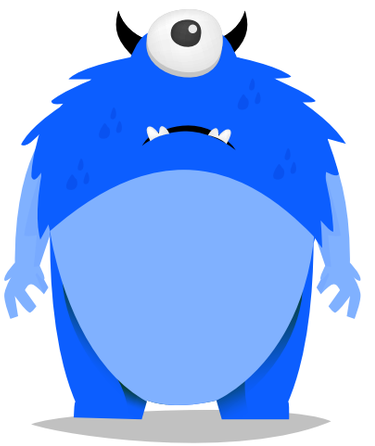
If you back up your data from your cellphone onto your PC, install passwords for your contacts list and other folders or files on your cell phone in the off chance that it is stolen or lost.

## 49 Don’t store card details on shopping sites.

Storing your credit/debit card details on ecommerce sites is not advisable. Take the few seconds it takes to feed in the card number and CVV number every time you need to make a purchase.

## 50 Enable two-step verification.

If this service is on offer, use it. You can never be too safe and erring on the side of caution is prudent. Gmail, Apple, Dropbox and Facebook offer this service, so take it!



Antivirus
REVIEWS

www.antivirusreviews.com