How to Check Your Security Software, Settings, and Status

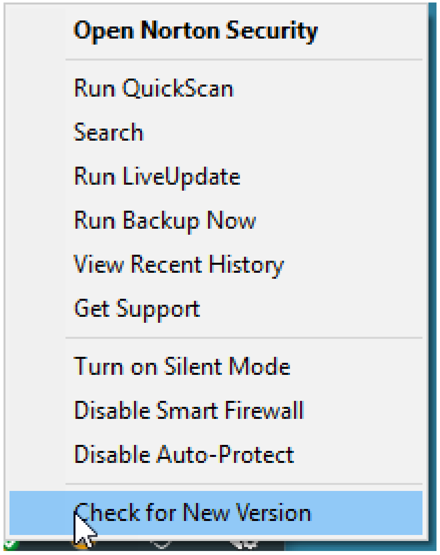
ByNeil J. Rubenking | December 5, 2018 | PC Magazine

Sure, you've installed antivirus, a VPN and other security software on your PC, phones, and tablets, but is it all working, or have you already been hacked? We've got 10 tips to help you perform your own security checkup.

How long ago did you install your antivirus or security suite? How many times have you looked at it since then? Security products are generally designed for users who plan to set them and forget them, but occasionally you should remember, and check on them.

Here are 10 simple steps you can take to make sure you get the most out of your security systems.

1. Keep Your Antivirus Up to Date



Modern antivirus utilities use behavior-based detection systems, so they can stop malware they've never seen before. However, most still also use malware signatures, a kind of digital fingerprint, to pick off the easy, known threats. Open your antivirus. Do you see a message about needing to update the databases? Even if you don't, rummage around to find the command that runs an on-demand check for updates. It couldn't hurt!

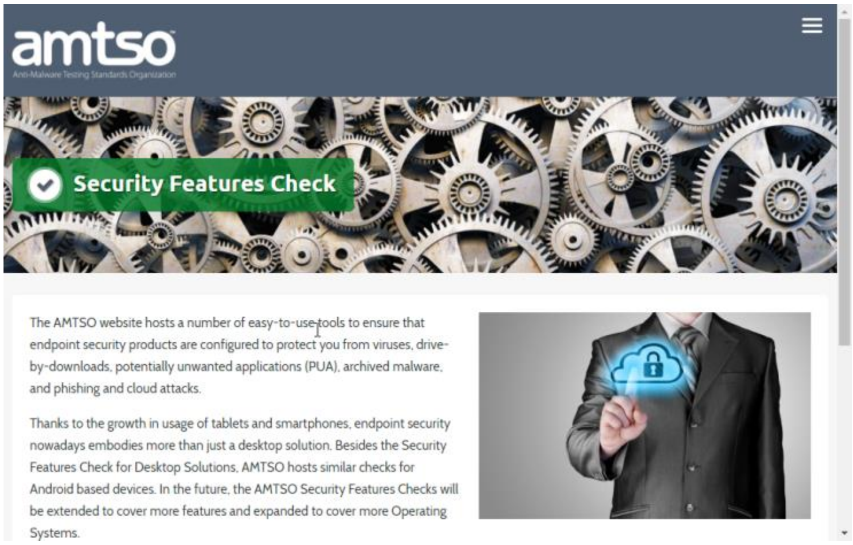
Also check whether an update is available for the product itself. In fact, check all your security products for updates. Typically, you'll find an option to check for updates in the File or Help menu, or in the menu that appears when you right-click the products icon in the notification area. It's possible that in doing this you'll discover that the subscription expired; renew right away!

2. Use the Best Security Software

Look at each of your security products and consider how you came to choose it. Did you see an ad on TV? Did a friend suggest it? Did it come with the computer?

To make sure you've got the best, visit pcmag.com and peruse our review of the product. If we found flaws in the product's protection, or just didn't rate it highly, check out our Editors' Choice products for the category. You may want to jump ship.

3. Put Your Antivirus to the Test



The AMTSO website hosts a number of easy-to-use tools to ensure that endpoint security products are configured to protect you from viruses, drive-by-downloads, potentially unwanted applications (PUA), archived malware, and phishing and cloud attacks.

Thanks to the growth in usage of tablets and smartphones, endpoint security nowadays embodies more than just a desktop solution. Besides the Security Features Check for Desktop Solutions, AMTSO hosts similar checks for Android based devices. In the future, the AMTSO Security Features Checks will be extended to cover more features and expanded to cover more Operating Systems.

How do you even know your antivirus is working? If it doesn't pop up to say, "malware quarantined," does that mean there's no malware? Or that it's not working? Here's how you can test your protection without risk.

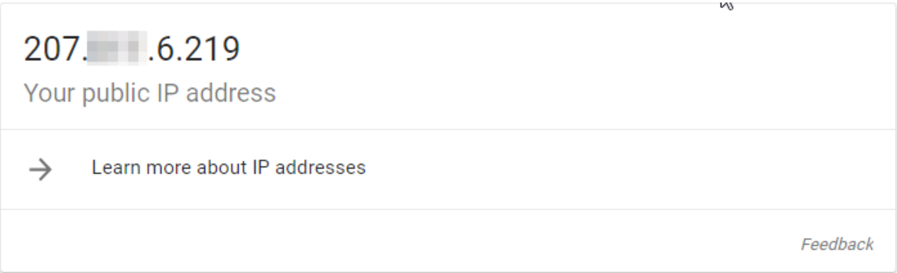
Start by visiting the Security Features Check on the website of the AMTSO (Anti-Malware Testing Standards Organization) (www.amtso.org/security-features-check/).

Now run the various tests, which check several aspects of malware protection, as well as protection against phishing websites. Do note that this only works if your antivirus supports the AMTSO test pages. You'll find a list of supporting companies at the bottom of each test page.

4. Verify Your VPN

A VPN, or virtual private network, protects your internet traffic by routing it through an encrypted connection. Nobody can view your data, not even the owner of the network. And the sites you connect with see the IP address of the VPN server, not your own, thereby protecting your privacy. But how do you know it's working?

Here's how to check if your VPN is leaking. Turn off the VPN and search "what is my ip" in Google to see your actual IP address. Now engage the VPN and check again. You should see a different IP address. You can also use a geolocation website to verify the location of that IP address, to make sure it matches the location stated by the VPN.



207.[redacted].6.219

Your public IP address

5. Check Your Mobile Devices

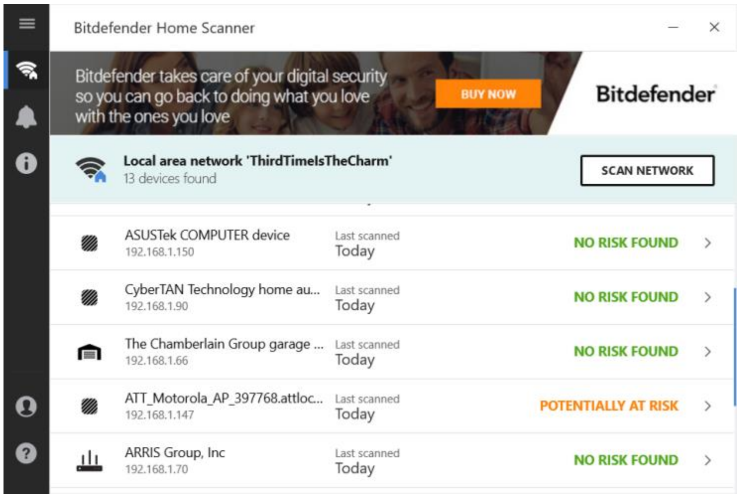
Apple has made iOS pretty airtight, but Android devices aren't nearly as secure. There are millions of malicious programs specifically aimed at wreaking havoc on Android devices. If you don't have a security program on your Android, you're taking a risk. And the typical Android security tool offers both malware protection and antitheft features.

It's possible you already have Android protection available as part of your desktop security suite. Many modern suites cover multiple platforms. Check out our roundup of the suites that offer the best Android protection (www.pcmag.com/article/358984/the-best-android-antivirus-apps)

6. Scan the Internet of Things

Your computers and mobile devices aren't the only things communicating over your home network. Chances are good you have many other devices on that network, things like game consoles, video doorbells, garage-door openers, and whatnot. The problem is, you can't install security software on these devices, so you can't be sure they're secure.

Or can you? There's a growing category of free home security scanners, programs like Avira Home Guard, that do two useful things. First, they let you know exactly what devices are on your network. You may be surprised at the length of the list. Second, they check for security problems with those devices.



Bitdefender Home Scanner
Bitdefender takes care of your digital security so you can go back to doing what you love with the ones you love
BUY NOW
Bitdefender
SCAN NETWORK

Local area network 'ThirdTimeIsTheCharm'
13 devices found

ASUSTek COMPUTER device 192.168.1.150	Last scanned Today	NO RISK FOUND
CyberTAN Technology home au... 192.168.1.90	Last scanned Today	NO RISK FOUND
The Chamberlain Group garage ... 192.168.1.66	Last scanned Today	NO RISK FOUND
ATT_Motorola_AP_397768.attloc... 192.168.1.147	Last scanned Today	POTENTIALLY AT RISK
ARRIS Group, Inc 192.168.1.70	Last scanned Today	NO RISK FOUND

Bitdefender Home Scanner goes one step beyond simply reporting on possible vulnerabilities. It pops up a notification when a new device joins the network, and offers to scan it. It's also a heads-up; do you know who just joined?

7. Analyze Your Passwords

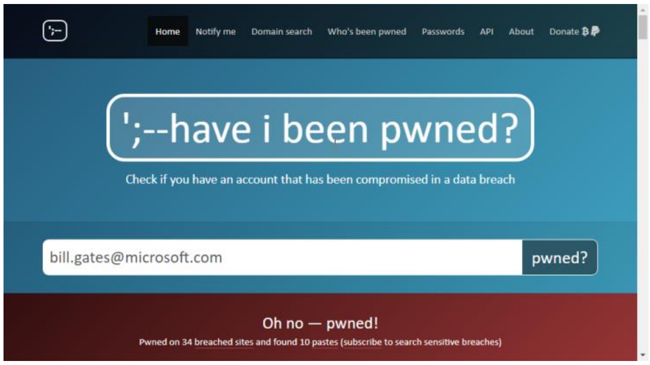
You're using a password manager, right? That's good! But is it saving a bunch of weak, duplicate passwords for you? Getting all your passwords into the system is only the first step.

Most password managers include a report on password strength. The best ones give you a list that you can sort by strength. If you come up with a raft of weak and duplicate passwords, start fixing them. Do the worst five, or however many you have time for. Fix some more tomorrow. Keep at it until the password manager gives you a gold star.

8. Have You Been Pwned?

Data breaches happen every week, and personal information leaks into the Dark Web. Yours may be exposed, but how would you know?

Fortunately, the handy website Have I Been Pwned can help. Just enter your email to find out whether that information turned up in a known breach, or in a data dump on a site like Pastebin. If you get the "Oh no—pwned!" message, change your account password immediately.



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

bill.gates@microsoft.com

Oh no — pwned!

Pwned on 34 breached sites and found 10 pastes (subscribe to search sensitive breaches)

9. Review Your Social Media Security

It goes without saying that your social media accounts (except for Twitter) should be set to private, so only your friends can see your posts. But have you checked to make sure yours are configured for best security? Log in, navigate to settings, and review anything related to security or privacy. On Facebook, for example, you want only Friends seeing your posts, and only Friends of Friends allowed to send new friend requests. And you don't want search engines linking to your profile.

Facebook also lets you review all the devices that are logged in to your account. Review the list, and if any of them look fishy, log out remotely.

You may not realize it, but even if your own settings are tight, friends and apps can leak your data. On Facebook, you can close that leak by disabling the sharing API. And you can download and view data saved by Facebook and Google.

10. Check Your Credit

How would you feel if you opened your credit card bill and found a charge for a ski vacation that you didn't take? Yeah, that would be bad. But you can get ahead of the game by proactively checking your credit.

We like Credit Karma, a free website and mobile app that keeps an eye on your credit scores. Yes, you can get your credit reports from each of the three big agencies once a year at no charge, but Credit Karma works directly with TransUnion and Equifax to check your scores as often as once per week. It also automates getting the full yearly reports on a regular basis. If you see a new account you didn't open, or a precipitous change in your score, you can straighten things out before the thief goes skiing.