REPORT

Why Today's Connected Consumer Needs Security Beyond Free PC Antivirus

The last few years have seen a real shift in how consumers use technology. They now rely on an increased number of devices, applications, and online services to manage and store their highly personal information.

But at the same time, digital threats are on the rise. Malware and phishing continue to escalate, along with targeted attacks on mobile devices and networks.

All of this means that the days of simply securing your computer and feeling protected are in the rear-view mirror. Today's consumers need an umbrella of connected security tools to protect their digital lives.

US Households have:

11

connected devices on average

7

of which have smart screens

7

the average number of hours a day on the internet

Tech Use & Current Threats

To really understand the new landscape let's start by looking at the numbers. U.S. households are now estimated to have an average of 11 connected devices, including 7 smart screens like tablets and smartphones. Users report spending nearly 7 hours a day[1] on the internet, and 48% of this time is spent on their mobile devices.

This is significant because mobile threats are one of the fastest growing areas of risk. McAfee recorded around 800,000 new mobile malware samples in the fourth quarter of 2019 alone, bringing total detected mobile threats to over 35 million. Given that the average U.S. consumer checks their mobile device 96 times[2] a day, mobile security is more important than ever.

Now let's consider networking and online services. Around 40%[3] of consumers consider connecting to open Wi-Fi networks and entering PINs and passwords risky, and for good reason. Open Wi-Fi networks offer cybercriminals a great opportunity to steal information as it flows over the network.

That's why helping users securely connect to the internet and sensitive accounts, such as online banking and social media, is essential as they move from offices and schools, to home, and places in between.

And no matter how or where consumers connect, cybercriminals and scammers lie in wait. Risky websites and links, malicious ads, and phishing emails and texts continue to propagate and evolve, changing their tactics to fit the moment. It's no wonder then that less than 10% of consumers[4] report feeling "very safe" on the internet. In fact, a majority (60%) of consumers are worried about the safety of their data, and specifically about their financial data.

Concerns over the safety of financial and personal information are certainly warranted, given that companies are increasingly being targeted for the wealth of consumer data they hold. In 2019 alone, data breaches in the U.S. reached 1,473[5] with over 164.68 million sensitive records exposed.

With all of these potential security risks—over networks, via devices, and with the safety of data and passwords—consumers need more than just piecemeal solutions. If security tools are not integrated, consumers may think they are protected in areas where in fact they aren't, or they may give up on some tools because they are scattered and hard to manage.

Security Options: Free Vs. Paid

All of this data shows that to truly protect consumers a security solution must be comprehensive; it has to cover not only their computers and devices, but also their connections and online behaviors. This is where free and basic, built-in antivirus applications such as Microsoft Defender fall short.

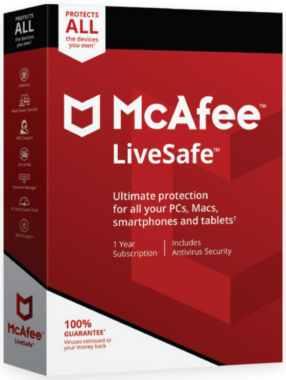
Free products often lack the continuous innovation, and world-class threat research that is needed to keep up with the evolving threat landscape.

Let's Take a Look at Some of the Limitations of Free

Most free security applications are for use on one device, and have limited security capabilities. In addition, they often impose limits on which browser or email program the user can choose, as well as carry in-app advertising, and offer little to no customer support. For more comprehensive security, consumers usually have to pay to upgrade.

Free products also often lack the continuous innovation, and world-class threat research that is needed to keep up with the evolving threat landscape. But most importantly, these tools simply don't offer the level of protection that modern tech users need. Security should be an umbrella that covers not just the devices consumers use, but how they connect, where they go online, and how they manage and store their information.

For robust security we need solutions like those offered in McAfee® LiveSafe™.


PROTECTS ALL the devices you own
McAfee
LiveSafe™
Ultimate protection for all your PCs, Macs, smartphones and tablets
1 Year Subscription
Includes Antivirus Security
100% GUARANTEE Viruses removed or your money back

McAfee® LiveSafe™
Robust security software with a comprehensive, yet holistic approach to protection.

McAfee's Comprehensive, Yet Holistic Approach

Hardware—Computers, tablets, smartphones, and connected devices are all safeguarded from malware and spyware, with cloud-based threat protection that uses both machine learning and behavioral algorithms to detect new threats. This means that the software's detection capabilities are constantly being updated and enhanced, without compromising the performance of users' devices.

After all, performance is important to users of all stripes, from stay-at-home workers to gamers, who can't afford to give up the speed and efficiency of their devices. That's why McAfee is proud to be among the leaders (top 3) in real-world performance impact testing, beating out both major competitors and free providers alike in delivering minimal resource consumption on Windows PCs.

Networking—To connect safely, consumers at a minimum need security software that includes a firewall. This monitors traffic coming in and out of the network, and prevents unauthorized access. While Windows Defender includes a firewall, advanced users may benefit from the additional customization offered by a third-party provider, like McAfee LiveSafe.

For broader protection when using public Wi-Fi or traveling, McAfee LiveSafe also includes a virtual private network (VPN). Personal VPNs allow users to make a secure connection over the internet, so their data and transactions remain safe.

Web Surfing—When users are searching online they can face a minefield of malicious ads or copycat websites, designed to download malware or steal their private information. This is why McAfee LiveSafe includes McAfee® WebAdvisor, that warns users of risky websites, links, and files, with the flexibility of running on different browsers.

Mobile Protection— Given that consumers are spending nearly half of their online time via their mobile devices, we believe it's crucial to extend protection to all the devices that they use. After all, cybercriminals are fully aware that we live in a mobile world. They have stepped

up mobile attacks in recent years, with phishing via text, and malicious apps that download malware, or run silently in the background, zapping the device of memory and speed.

McAfee provides free support options to make managing consumer technology easier, including an extensive online knowledge base, and chat/phone options which are often available 24/7.

Spam & Phishing—A recent study found that 94% of malware[6] is delivered via email. This makes spam and phishing protection across email platforms essential. In addition to an antispam tool, McAfee LiveSafe also includes identity theft protection for customers in the U.S., in case a user's personal information is compromised.

Password Security—With nearly one-third of data breaches involving stolen credentials[7], users need an easy way to create and store complicated and unique passwords for their high-value accounts. This way, even if one of their passwords is stolen in a data breach it cannot be used to access other accounts. That's why McAfee LiveSafe includes a password manager that syncs across all of the user's devices, since storing passwords on a PC alone doesn't address how consumers toggle-between devices.

Customer Support—When you are protecting against so many different threats on such a wide variety of devices users will naturally have questions and issues that need to be addressed by their security provider. McAfee LiveSafe comes with free options to make managing consumer technology easier, including an extensive online knowledge base, and chat/phone options which are often available 24/7.

Conclusion

Today's consumers move seamlessly between devices and digital services, all while encountering different areas of risk. This is why security cannot be siloed on one computer or device. It needs to touch on all of the aspect of the tech user's digital life, moving from devices to connections, and to data. After all, cybercriminals already understand all of these digital touch points, and will find and attack the weakest links.

While free security tools offer some level of protection, there are far too many holes where modern threats can slip in.

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place.

www.mcafee.com

1. GLOBALWEBINDEX (Q2 & Q3 2018).
2. https://www.prnewswire.com/news-releases/americans-check-their-phones-96-times-a-day-300962643.html
3. STATISTA GLOBAL CONSUMER SURVEY 2019
4. STATISTA GLOBAL CONSUMER SURVEY 2019
5. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
6. 2019 Verizon Data Breach Investigations Report (DBIR)
7. 2019 Verizon Data Breach Investigations Report (DBIR

McAfee™

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com