The Best Ways to Protect Your Devices From Hackers

No comments

Hackers are criminals who gain unauthorized access to a network and devices, usually with the intent to steal sensitive data, such as financial information or company secrets. In this article you learn how to protect your computers by using firewalls and antivirus software and by following best practices for computer use.

Computer Hackers

An online hacker breaks into an internet-connected device, such as a computer, tablet, or smartphone, to steal, change, or delete information. The purpose of hackers is usually to break into devices for negative reasons, just as other thieves have malicious intent. (One exception, however, is white hat hackers, who companies hire to find security holes in their devices.) Hackers can sometimes access your devices by installing malware (software used for malicious purposes) that you might not even realize exists. These thieves might access your most precious data before you're aware of a break-in.

Various types of hacking

There is a wide range of motives for hackers, ranging from financial gain to political goals. Knowing these intentions can help you anticipate attacks that may negatively affect your business.

1 - Vandalism: Hackers have a separate subculture, so some may want to vandalize certain websites to show off to their peers. According to Malwarebytes, this motivation occurs fairly frequently. don't overlook it.

2- Crimes related to money: We've all heard the classic story of someone checking their credit card statement and seeing transactions they didn't make. To create these false transactions, computer hackers often steal your credit card number, checking account information, or other financial data.

3- Corporate espionage: Hacking has only made espionage more accessible to the general public since espionage existed long before the internet era. Since so much of the world is connected to the internet, one company could hack into other companies' devices to acquire information about them and use it to gain an unfair competitive edge.

4- Hacktivism: An example of hacktivism is the alteration or destruction of websites for political reasons. Cyberterrorists may want to do this.

The best way to protect your computer from hackers

While computer hackers persist, most businesses use the internet for tracking their finances, ordering and maintaining inventory, conducting marketing and PR campaigns, connecting with customers, engaging in social media, and performing other crucial tasks. The number of massive computer breaches continues to rise, even at big corporations with robust security measures. In addition to large businesses, small businesses are often targeted, especially because they underestimate the risk of cybercrime and can't afford expensive cybersecurity solutions. You can protect your devices and safeguard your sensitive data using these tips:

1- Make sure your network is secure

You should set a secure, encrypted password on your router when setting up your network. This will allow intruders to not intrude on your network and mess with your settings.

2- Anti-spyware packages should be installed

Generally, spyware is a type of software that secretly collects and monitors personal or organizational data. It is designed to make it hard to detect and difficult to remove, and it tends to deliver unwanted ads and search results that lead you to specific (often malicious) websites. It is common for spyware to record every keystroke and gain access to financial information and passwords. Antivirus packages, such as those from Webroot, McAfee, and Norton, often include anti-spyware for this threat. By scanning and blocking all incoming information, anti-spyware packages provide real-time protection.

3- Make sure your OS, apps, and browser are up-to-date

Make sure you always install the latest updates to your operating system. Many updates include security fixes that prevent hackers from accessing and exploiting your data. The same applies to apps. Browsers are becoming increasingly sophisticated, especially in security and privacy. In addition to installing all-new updates, review your browser's security settings. Using your browser can prevent websites from tracking your movements, increasing your online privacy. Or, you can use these private web browsers.

4- Protect your computer with a firewall

Firewalls are software designed to block unauthorized access to your business network and notify you if an intrusion is attempted. Windows and macOS have built-in firewalls intended to create a barrier between your information and the outside world.

Be sure the firewall is activated before you go online. Depending on your broadband router, which has a built-in firewall that protects your network, you can purchase a hardware firewall from companies like Cisco, Sophos, or Fortinet. An additional firewall for business networking can be purchased if your business is more prominent.

5- Make a backup of your computer

You should back up your hard drive immediately if your business doesn't already do so. Backing up your information is critical in case hackers succeed in getting in and destroying your data. If you experience a data breach or loss, always make sure you can rebuild as soon as possible. Mac OS (Time Machine) and Windows (File History) have built-in backup utilities. External backup hard drives can also provide enough space for these utilities to function.

6- Use virtualization

Not everyone needs to take this route, but if you visit sketchy websites, expect to be bombarded with spyware and viruses. While the best way to avoid browser-derived intrusions is to steer clear of unsafe sites, virtualization allows you to run your browser in a virtual environment, like Parallels or VMware Fusion, that sidesteps your operating system

to keep it safer.

7- Secure your network

Routers don't usually come with the highest security settings enabled. When setting up your network, log in to the router, and set a password using a secure, encrypted setup. This prevents intruders from infiltrating your network and messing with your settings.

8- Use encryption

Even if cybercriminals gain access to your network and files, encryption can prevent them from accessing any of that information. You can encrypt your Windows or macOS hard drive with BitLocker (Windows) or FileVault (Mac), encrypt any USB flash drive that contains sensitive information, and use a VPN to encrypt web traffic. Only shop at encrypted websites; you can spot them immediately by the "HTTPS" in the address bar, accompanied by a closed-padlock icon.

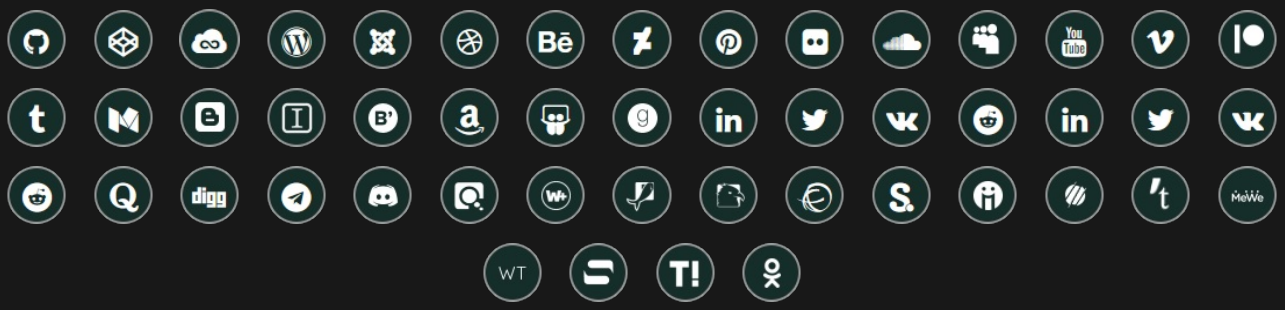
Conclusion

In this article, you learned about the ways of protecting your devices from hackers. These methods vary from using anti-viruses and firewalls to keeping the programs up to date, securing your network, virtualization, and encryption. Combining security tools and best practices can protect your computers and your network from unauthorized access.

Join Arashtad Community

Follow Arashtad on Social Media

We provide variety of content, products, services, tools, tutorials, etc. Each social profile according to its features and purpose can cover only one or few parts of our updates. We can not upload our videos on SoundCloud or provide our eBooks on Youtube. So, for not missing any high quality original content that we provide on various social networks, make sure you follow us on as many social networks as you're active in. You can find out Arashtad's profiles on different social media services.



Get Even Closer!

Did you know that only one universal Arashtad account makes you able to log into all Arashtad network at once? Creating an Arashtad account is free. Why not to try it? Also, we have regular updates on our newsletter and feed entries. Use all these benefitial free features to get more involved with the community and enjoy the many products, services, tools, tutorials, etc. that we provide frequently.

SIGN UP | NEWSLETTER | RSS FEED