# 4 Types of Security Tools that Everyone Should be Using

Devolutions

## DATA BREACHES ARE ON THE RISE

We all know that data breaches are on the rise. Which means that most people are increasing their cyber security IQ, right? Unfortunately, that's not the case! According to a survey by Pew Research Center, the majority of people are still unclear about some critically important cyber security topics, terms and concepts.

To help bridge this knowledge gap, **here is an overview of four security tools that everyone should be using:**

## 1. FIREWALLS

A firewall is the **first (of many) layers of defense against malware, viruses and other threats**. It scrutinizes and filters both incoming and outgoing data. Users can also customize rules and policies based on their needs. For example, it's often necessary to create exceptions that allow certain apps to pass through the firewall so that they don't constantly trigger false alarms.

## 2. ANTIVIRUS SOFTWARE

Signature-based antivirus software scans files (from any source) to make sure that there aren't any hidden threats. And if it finds something shady or scary, it can often remove or quarantine the affected file. While **antivirus software certainly isn't bulletproof** — especially when it comes to zero-day threats (i.e. vulnerabilities that hackers have found before software vendors have a chance to patch them and/or users have a chance to install updates) — **it's still a critical piece of the cyber security puzzle**. There are many options to choose from that range in price from free to hundreds of dollars a year.

## 3. ANTI-SPYWARE SOFTWARE

As the term implies, **spyware secretly snoops on victims to see where they go online and, even more so, what they type** — such as usernames and passwords, and any other confidential or personal data. That's where anti-spyware software fights back by (ideally) detecting and removing threats such as key loggers, password recorders, and so on.

## 4. PASSWORD MANAGEMENT SOFTWARE

Good password management software not only **saves a great deal of time, but it strengthens security and prevents major mistakes**, such as saving passwords in web browsers. If you're looking for something to fit your needs and budget, here is a review of some popular options.

Of course, you can also use Remote Desktop Manager to securely store all of your passwords on a centralized platform, along with all of your remote connection data and other sensitive information (credit card numbers, etc.). If you're new to RDM, please request a trial to see if it's the right solution for you.

## Your Turn...

What security tools do you use to stay safe and avoid getting attacked by cyber criminals? Please share your advice and experiences with the community by commenting below.