

---

# Descargar libros victoriaparaprim erogradodeprimaria

The pass-code was used only a handful of times, not unusual in any application. A program was designed to mimic the user logging in, and stealing the password from memory. It's a method that, he said, thieves use across industries. In the case of Mr. Waterfield, he said, it was so successful that he had to buy a new card. "It's such a big business, it's taken over peoples' lives," he said. For those who shop on the internet, it has become impossible for companies to get a truly unique card number for any particular transaction, or to verify online that a particular card belongs to a company. The numbers, at least for consumers, are growing randomly, or are their own cryptographically scrambled secrets. But they can be easily guessed by hackers who scan a vast database of numbers, or a million credit cards at a time, searching for matches. And so the age-old security practice of writing down a password, hiding it in a drawer or on a key chain, and using it only when needed, is falling out of favor in a world of insecure devices, software programs, websites and banks. "It's really a matter of security companies trying to increase their security by automatically trying to guess your password before you type it in," said Michael Harris, chief executive of NICE Systems, a company that provides security products. "It makes it much easier for sophisticated hackers." The more passwords that can be easily guessed, he said, the easier it is for hackers to break in to Internet and computer systems. Last year, Fidelity National Financial, the insurance company, found that hackers had guessed 95 percent of its corporate passwords. The company hired a new chief information security officer and increased the size of the job from about 40 people to 200. The ability to outsmart computer security systems is known as the password "crack," a reference to the number of combinations a pass-code can be broken into. The problem for merchants and customers is that it is usually harder to keep a password secret than to remember it. In the case of Mr. Waterfield, the name of his credit card,



