

# How STOPzilla Works

When it comes to online fraud, the odds are clearly against you: Spyware, Phishing, Pharming, identity theft... all of these things can interfere with your surfing, at the very least. More than likely, they will monitor your Web use, allow others to capture information you enter via your keyboards (passwords, logins, account numbers, etc.), disable your security settings and waste your time with unwanted advertising.

## **True Real-Time™ Spyware Protection:**

Many anti-Spyware and anti-Phishing products hope to capitalize on users' fears and a poorly understood problem. The worst of these products will install their own Spyware on your computer. Some extract Malware (malicious software) applications, only to enable them to return when you boot up again.

STOPzilla's pioneering approach is to target Malware. During the past five years, STOPzilla has grown and kept pace with the proliferation and increasing complexity and sophistication of Malware. STOPzilla's Research staff, assisted by its Singularity Spider, combs the Web to find Malware and then creates "target definitions" for each new piece of Malware found. Essentially, target definitions are actions the software takes to detect and block Malware before it does damage to a user's system, rather than removing it after the fact. The target definitions are included in the next update of the product so that no other subscriber will ever need to worry about this particular parasite. STOPzilla is updated as often as daily to ensure that it kills even the newest varieties of Spyware.

In addition, when a subscriber reports some new Malware, trained Customer Support technicians perform a diagnostic scan of his/her computer, which is then forwarded to the iS3 Research Department. There, the new Malware is observed and targeted.

As a result, iS3 has amassed one of the world's largest databases of Malware. For each Malware file in our database, our researchers have created a target definition.

With most anti-Spyware products, the user must download the latest updates manually in order to get the latest definitions. With STOPzilla, from the moment a subscriber boots up and for as long as the computer remains on, STOPzilla is protecting that machine with absolutely no user interaction required. The product will update automatically, at least once every 24 hours. Users can opt to be notified or not, whenever an update takes place. With STOPzilla's straightforward, intuitive user interface, even the novice can benefit from advanced technology.

Many other anti-Spyware products claim to operate in “real-time”, but these products only scan the user’s system periodically, at pre-configured intervals. Such scanning uses a lot of bandwidth, thereby compromising performance. This is not a technologically sophisticated approach to malicious programs that can perform their tasks and destroy themselves in milliseconds.

After initial installation, STOPzilla does not rely solely on scanning to detect Spyware. STOPzilla’s True Real-Time® protection automatically detects, blocks and quarantines all types of online threats including: malicious BHOs, Keyloggers, Backdoor Trojans, Browser Hijackers, Web Dialers and Messenger Service Ads, without interrupting your surfing in any way.

### **Blocking Phishing Attacks**

STOPzilla’s advanced Phishing protection uses multiple technologies to detect known and potential Phishing sites. The addresses (URLs) of the latest known Phishing sites are downloaded from multiple databases as often as every ten minutes, and included in the STOPzilla updates.

In addition, STOPzilla researchers use heuristics—analysis of content and behavior—to determine the likelihood that a particular site is unsafe. Its unique Anti-Phishing Scoring Engine subjects the Web content in the user’s browser to a set of sequential evaluations intended to identify fraudulent Web sites. When the score reaches the threshold level, STOPzilla displays a Phishing Alert indicating that the site is a potential phishing site.

### **STOPzilla has the Service Advantage**

STOPzilla is the only product of its kind that offers free, unlimited toll-free technical support and customer service from iS3’s U.S. based Call Center.

For Internet Service Providers and many other vendors, anti-Spyware products are not their primary lines of business, thus they offer limited support. Anti-Spyware is what iS3 does; it’s all we do and we do it the best.

Combined into one easy-to-use product, STOPzilla, these features represent a true paradigm shift in anti-Spyware technology.