

# Frequently Asked Questions

- 1) What is MyLaptopGPS™?
- 2) Does it really work? Overseas? Globally? Outdoors? Indoors? Underwater?
- 3) How does it work?
- 4) Do these little SafeTags™ have satellite GPS chips in them or something?
- 5) Why doesn't MyLaptopGPS™ use regular satellites like my car GPS does?
- 6) Will a thief actually connect to the Internet?
- 7) What if the thief reformats the hard drive?
- 8) Does MyLaptopGPS™ work over wireless links (WiFi, etc.)?
- 9) What if the thief is on a private network (with gateway) or behind a firewall?
- 10) Can you really remove my data from my stolen laptop and get it back to me?
- 11) What documents or information can you recover?
- 12) Does my computer have to be powered on in order to get my data?
- 13) How do you go about getting the recovered files onto my new computer?
- 14) How secure is your data center?
- 15) Will a thief know that MyLaptopGPS™ is running?
- 16) Is MyLaptopGPS™ compatible with my firewall (including ZoneAlarm™)?
- 17) Is MyLaptopGPS™ compatible with my anti-virus software?
- 18) What is this "Microsoft .NET Framework™" thing?
- 19) Isn't it enough for me to simply password-protect my system login process?
- 20) Can you just crash my stolen computer so that the thief cannot use it?
- 21) Can you send a message from me to the thief?
- 22) What should I do the moment my laptop is stolen?
- 23) Can you recover my laptop hardware itself?
- 24) How do you physically apprehend the thief?
- 25) Do law enforcement agencies cooperate with you?
- 26) Does MyLaptopGPS™ run on MacOS™ (Apple)?
- 27) What are the system requirements?
- 28) What is a SafeTag™?
- 29) Do SafeTags™ really stop theft?
- 30) Won't a thief just remove the SafeTag™?
- 31) Can a thief use my information to steal my identity?
- 32) How do I get started using the system after I sign up?
- 33) Do I just stick on the SafeTag™ and I am done?

## 1) What is MyLaptopGPS™?

MyLaptopGPS™ is computer software built to **track your stolen computer**, worldwide, and **recover your data**, all right under the thief's nose via the Internet.

## 2) Does it really work? Overseas? Globally? Outdoors? Indoors? Underwater?

It certainly does. MyLaptopGPS™ really does **track stolen computers worldwide**, really does **remove the data** from them, and really does **return the data to the rightful owner**. That includes:

1. In the United States
2. Overseas
3. Indoors
4. Outdoors
5. **Worldwide**

and

6. Underwater? OK, probably not.

## 3) How does it work?

MyLaptopGPS™ uses a **proprietary** Internet homing technology and data transfer protocol to facilitate covert hardware tracking and data recovery.

1. Install MyLaptopGPS™ on your computer. The software runs covertly.
2. Rest easy.
3. When the computer is stolen, alert the SafeRecovery Team™ immediately via telephone or online. The SafeRecovery Team™ will flag your machine as stolen.
4. As soon as the thief connects to the Internet, **MyLaptopGPS™ locates your machine and removes all of your important files**, right under the thief's nose, and **returns those files to you** via fully-encrypted transfer to our secure data center.
5. MyLaptopGPS™ continues to track your machine whenever it is connected to the Internet. Information about the global physical location of your stolen machine is relayed to law enforcement of jurisdiction in order to facilitate a **surprise strike/raid on the thief's position** if possible, in which case your **actual computer itself is returned to you**.

#### 4) Do these little SafeTags™ have satellite GPS chips in them or something?

**ABSOLUTELY NOT.** SafeTags™ **DO NOT** have satellite-based GPS receivers/transmitters embedded in them. They have been **specifically designed NOT to use electronics.** The entire system **uses the Internet and NOT the GPS satellite network** deployed by the **US Department of Defense.** Please continue reading to find out **WHY.**

#### 5) Why doesn't MyLaptopGPS™ use regular satellites like my car GPS does?

SafeTags™ were specifically designed **NOT** to use satellite GPS technology. Instead, together with MyLaptopGPS™, they were **designed to overcome serious, crippling limitations** with the current satellite-based GPS infrastructure when it comes to **tracking stolen computers.**

### **TWO THINGS HAPPEN TO A STOLEN LAPTOP.**

1. It goes **INDOORS.** Thieves don't hang out in the public park with your laptop.
2. It connects to the **Internet.** Thieves don't steal your laptop in order to compose offline word processing documents and play Solitaire. Get the idea?

### **But satellite-based GPS FAILS COMPLETELY:**

1. **Satellite-based GPS units DO NOT WORK INDOORS.**

There are some assistant technologies, such as A-GPS, that attempt to overcome this major limitation by relaying GPS information to receiver units. Those technologies work well for operations such as certain GPS download operations. But for tracking stolen computers, the ability to **reliably communicate** with the necessary GPS satellite infrastructure is simply **not present in GPS devices when inside buildings** (especially dense structures and away from windows). **But MyLaptopGPS™ works INDOORS!**

2. **Satellite-based GPS units DO NOT TRANSFER YOUR DATA.**

Have you ever had your computer stolen? **If you have, then you know perfectly well that your stolen hardware is the LEAST of your concerns.** Your **data** is worth up to **300 times more** than your hardware. In fact, in many cases the data is literally priceless. Plus, your computer contains all sorts of information about you: email, bank and credit card information, passwords, private documents, names and addresses (and email addresses) of friends and family, etc. **Is this the kind of information you want in the hands of a criminal?** Satellite-based GPS offers absolutely no ability to transfer user data. Satellite-based GPS is for transferring geographic coordinates. And that is

what it does. You CANNOT upload and download arbitrary data using the DoD satellite GPS network as if it were some kind of Internet. **YOUR DATA IS WHAT MATTERS.** **MyLaptopGPS™ recovers your data and destroys it from the hands of the thief.**

**3. Satellite-based GPS units require considerable electrical power.**

This limitation is improving rapidly in the GPS industry. Nevertheless, if you own a handheld satellite-based GPS unit then you know that you'll need a good supply of batteries with you if you plan to use it much.

**4. Satellite-based GPS units do not work like your favorite Hollywood movie.**

In your favorite movie or TV show, the hero probably plants some sort of amazing homing beacon on the crooks car, under his lapel, in his briefcase, or some other creative spot. The hero then follows in his car at a safe distance, waiting to save the day. **Real life is not Hollywood.** Even if your laptop is stolen by a thief who simply wants to sit in a public, outdoor place and enjoy the weather with it (good luck), law enforcement does not drive around with an amazing little radar screen in the cruiser, which will take them within 1 foot of your laptop so they can tackle this person sitting there on the park bench. **At least not in America.** Law enforcement needs probable cause, reasonable suspicion, and it helps when they have a nice street address where your laptop is located, to obtain a search warrant. Guess what? **MyLaptopGPS™ provides precisely that. Welcome to Hollywood.**

**5. Satellite-based GPS units are very expensive.**

Thankfully this too is improving in industry, as you would expect. Nevertheless, satellite-based GPS units are pricey. **MyLaptopGPS™ and SafeTags™ work far better...for a fraction of the price!**

**Most people prefer not to pay huge prices for technology that does them no good. These folks choose MyLaptopGPS™ instead. Wise choice.**

## **6) Will a thief actually connect to the Internet?**

Answer: Do birds fly? Generally the thief will connect within a day. In almost every town across America, he can connect while sitting at any intersection or anywhere else, thanks to almost ubiquitous WiFi coverage. (Obviously most thieves are smart enough to wait for cover). Your stolen laptop makes a nice tool for the thief to use for online theft, gambling (especially if he now has YOUR credit card information), piracy, and other assorted "entertainment" for himself. If the thief doesn't connect, his buyer will. Rarely will your machine stay offline.

## 7) What if the thief reformats the hard drive?

There's an old saying: "In theory, there is no difference between theory and practice. In practice, there is." This is true here. In theory, every thief who steals a laptop will reformat the hard drive before continuing on with his business. But MyLaptopGPS™ customers tend to care more about **practice** (what happens in the real world) than theory. And in the real world, most laptop thieves are not college-educated, white collar, computer-savvy engineers who have nothing to live for and want to make a buck. Instead, they tend to be interested in various other illicit activities. While it is true that *sometimes* thieves do reformat stolen machine's hard drives, what matters most are the numbers. And the numbers indicate that a reformat is unlikely.

Surviving hard drive reformatting makes a wonderful marketing point. But at MyLaptopGPS™, we're much more interested in developing features, and providing service, that truly serves real-world customers. Therefore, we consider this feature to be an extremely low priority.

A hard drive reformat does indeed stop the MyLaptopGPS™ system from functioning.

This question also gives good opportunity to list our helpful Top Five list.

### **Top Five Reasons Why Hard Drive Reformat Survival is a Waste of Resources**

- 1) In theory, most thieves reformat the hard drive. In practice, they do not. In this industry, practice is worth more than theory.
- 2) In order to survive a reformat, code must be burned into the BIOS of the machine. That generally requires that you buy a new computer that has a supported BIOS already installed with the code, unless yours happens to be supported already.
- 3) If a thief reformats the hard drive, most MyLaptopGPS™ clients would like to pat him on the back and buy him a coffee, because he's done our work for us. That is, if data protection is the goal, there's no better protection than a thief reformatting the hard drive for us. Be our guest!
- 4) A thief cannot reformat what he does not possess. The real-world performance resume of MyLaptopGPS™ boasts a 00.4% theft rate, which is 31 times less than the average. If a thief does not possess your machine, he cannot reformat it. We stop theft before it happens.
- 5) The MyLaptopGPS™ system is guaranteed to work. In fact, it's 300% guaranteed to work in 6 mere days. If a thief beats the 00.4% real-world MyLaptopGPS™ theft rate, AND reformats your hard drive (two enormous assumptions), you'll get 3 times your money back. That's a 200% profit on your investment. See [www.MyLaptopGPS.com/guarantee.php](http://www.MyLaptopGPS.com/guarantee.php)

**8) Does MyLaptopGPS™ work over wireless links (WiFi, etc.)?**

Absolutely. The system works over ANY Internet connection. **If your computer connects to the Internet in any fashion, MyLaptopGPS™ goes to work.**

**9) What if the thief is on a private network (with gateway) or behind a firewall?**

**No problem.** MyLaptopGPS™ is not defeated by “NAT” gateways and firewalls. The SafeRecovery Team™ not only knows the outside “public” Internet location of your stolen computer, but also knows the internal location. This is handy when the thief joins a large campus network or other private system.

**10) Can you really remove my data from my stolen laptop and get it back to me?**

Yes, we really can. As soon as your computer is connected to the Internet in any way, MyLaptopGPS™ goes to work.

**11) What documents or information can you recover?**

We can access generally any portion of your computer's hard drive (“file system”) that is accessible to Windows. That means, generally, we can recover just about anything you want.

**12) Does my computer have to be powered on in order to get my data?**

Yes.

**13) How do you go about getting the recovered files onto my new computer?**

Your recovered files are transferred, using bank-grade 128-bit SSL data encryption, into our secure data center. From there, you can download your files online or, in some cases, we can

email them to you (large files are not suitable for email).

## 14) How secure is your data center?

Answer: Ever heard of Fort Knox? Wide open, as far as we're concerned. But seriously, our data center boasts the kind of security that most companies know only by watching their favorite spy movies. Here are some highlights about our data center:

### **Security:**

Strictly monitored access using keycard protocols, biometric scanning protocols and continuous interior and exterior surveillance.

- Access limited to data center personnel only, without exception.
- All data center employees undergo thorough background security checks before being employed.

### **Precision Environment:**

Our data center's HVAC (Heating Ventilation Air Conditioning) systems are N+1 redundant, ensuring that a duplicate system can immediately come online in the event of an HVAC system failure.

- All air is circulated and filtered every 90 seconds to remove dust and contaminants.
- An advanced fire suppression system designed to stop fires from spreading in the unlikely event one should occur.
- All cables are securely tied down with cable racks suspended from ceilings providing dual routes for all cables.

### **Conditioned Power:**

In the unlikely event of a total utility power outage, the data center's power systems are designed to run uninterrupted with all servers being fed conditioned UPS (Uninterruptible Power Supply) power.

- The UPS power subsystem is N+1 redundant, with instantaneous failover if primary UPS fails.
- For extended utility power outages, routinely tested, on-site diesel generators can run indefinitely.

### **Core Routing Equipment:**

Our data center uses only fully redundant, enterprise-class routing equipment.

- All routing equipment is housed in a secured core routing room fed by its own redundant power supply.
- Fiber carriers enter facilities as disparate access points to guard against service failure.

### **Network Technicians:**

Our data center employs only certified networking and security teams that are thoroughly

experienced in managing and monitoring enterprise level networks.

- Certified Network Technicians are trained to the highest industry standards to ensure our guaranteed 100% infrastructure.

## **15) Will a thief know that MyLaptopGPS™ is running?**

No. MyLaptopGPS™ is designed to run covertly on your computer.

## **16) Is MyLaptopGPS™ compatible with my firewall (including ZoneAlarm™)?**

Yes. In general, MyLaptopGPS™ works with any OS-based firewall, such as the varieties used with Windows™. As explained earlier, network firewalls themselves (on network borders) are not a problem. If you have a firewall running your computer itself, you will need to make sure that when you install MyLaptopGPS™ you “allow” it to access the network. Most firewalls will prompt you the first time a new application tries to gain access, asking if you want to allow the application. Once you have allowed it, it is permanently allowed (see your firewall manufacturer's documentation if necessary).

## **17) Is MyLaptopGPS™ compatible with my anti-virus software?**

Yes, in general. The same notes apply here as in the above question regarding firewalls.

## **18) What is this “Microsoft .NET Framework™” thing?**

This is software installed automatically by Windows™ if you do not already have it. The Microsoft .NET Framework™ version 2.0 is required to run MyLaptopGPS™ and it provides certain functions and services to the system. If you do not already have the Microsoft .NET Framework™ 2.0 installed on your computer, such as for another application you may use that requires it, then Windows™ will pause the MyLaptopGPS™ installation process and, after prompting you and receiving your confirmation, will download and install the framework.

## 19) Isn't it enough for me to simply password-protect my system login process?

**NO**, for two major reasons.

1. There are some easy ways to bypass the regular system login password infrastructure.

While it is true that most thieves are, shall we say, not the brightest bulb in the bunch, it is also true that bypassing the password prompt (or at least creating an alternate user account on your PC) is a fairly trivial exercise.

2. What about your **DATA**?

Remember, your data is your life. MyLaptopGPS™ **recovers your data and destroys it in the hands of a thief.**

## 20) Can you just crash my stolen computer so that the thief cannot use it?

We can delete critical system files and make life generally hard on the thief. And if you ask us to, we will. But, remember that the longer the thief stays connected to the Internet with your computer, blissfully tapping along without suspecting he's being beaten, the longer the SafeRecovery Team™ can be recovering files that you need (if you think of more), and the longer they can work with law enforcement to actually bust the thief himself.

## 21) Can you send a message from me to the thief?

Yes, we actually can. **You can give the thief a piece of your mind.** But we do not recommend that you do this. Once again, the longer the thief stays connected to the Internet with your computer, blissfully tapping along without suspecting he's being beaten, the longer the SafeRecovery Team™ can be recovering files that you need (if you think of more), and the longer they can work with law enforcement to actually bust the thief himself. You don't want to tip him off that "something's up."

## 22) What should I do the moment my laptop is stolen?

Contact us immediately at (800) 963-1137 or go online to [www.MyLaptopGPS.com](http://www.MyLaptopGPS.com) to flag your machine as stolen. In addition, we highly recommend that you change as many of your passwords as you possibly can (bank websites, email, subscriptions, etc.). If you have credit card information on your computer, go ahead and consider it a stolen credit card—call your

bank and have them cancel it and issue you a new one.

## 23) Can you recover my laptop hardware itself?

Yes, we can. Much here depends on the circumstances of the theft itself, and timing. The SafeRecovery Team™ works with law enforcement in the area where your computer is located (where the thief is) to zero in on a bust. If law enforcement personnel are successful in the raid, then your machine is on its way back to you.

## 24) How do you physically apprehend the thief?

The SafeRecovery Team™ coordinates with law enforcement of jurisdiction in the location where your stolen laptop has been pinpointed, to provide necessary information to obtain a search warrant, and law enforcement personnel do the dirty work of apprehending the thief.

## 25) Do law enforcement agencies cooperate with you?

Yes, in general. One nice thing about MyLaptopGPS™ is that even though our SafeRecovery Team™ is working on your behalf to coordinate law enforcement for the apprehension of the thief and recovery of **your** hardware, experienced law enforcement agencies know that when they bust the thief they are very likely to find a **whole cache of other stolen goods**, not to mention all sorts of other illegal behavior. Thus the MyLaptopGPS™ system may lead to the solution of a good number of open theft cases.

## 26) Does MyLaptopGPS™ run on MacOS™ (Apple)?

No, not currently.

## 27) What are the system requirements?

**Supported Operating Systems:** Windows 2000 Service Pack 3; Windows 98; Windows 98 Second Edition; Windows ME; Windows Server 2003; Windows XP Service Pack 2; Windows Vista

**Memory:** Minimum 128 MB recommended

**Available Disk Space:** 280 MB

## 28) What is a SafeTag™?

A SafeTag™ is a permanent property label that affixes to your laptop or desktop computer. The SafeTag™ bears a globally-unique “SafeTag number” emblazoned front-and-center, along with contact information for our SafeRecovery Team™ (both phone and web). When you register your SafeTag™ online, which you must do as soon as you receive it, we have a way to trace the property back to you in the event of a police raid or a found item.

**But most importantly**, the SafeTag™ serves as an extremely bold and visible warning to potential thieves: **THIS PROPERTY IS MARKED AND POLICE TRACKABLE.**

## 29) Do SafeTags™ really stop theft?

**Yes, they certainly do.** Have you noticed that home security system companies insist that you place stickers in your windows and a sign in your yard? Have you ever asked why? It is not to advertise, though that is a fringe benefit for the home security company. They affix such warnings to your real estate property because they know full well that **the sign stops crime.** Thieves casing a potential hit, particularly laptops and other such items, have a very brief and very important window of opportunity, which is usually only 20 seconds long, or so. In that period of time, a **bold warning** to the thief that the property is not the average, wide open, unprotected, ripe-for-the-taking property, is very effective in causing the thief to simply **move on to an easier target.** Your property just isn't worth the added risk to him.

## 30) Won't a thief just remove the SafeTag™?

**NO**, because:

1. **SafeTags™ are permanent.**

SafeTags™ feature a 3M 300LSE adhesive that is used in industry as a **functional replacement for welding.** What does this mean? It means if you follow the instructions for applying the SafeTag™, it won't be coming off, at least not without likely damaging the stolen property itself (not appealing for the thief).

2. **A thief cannot remove what he does not possess.**

Remember the 20 seconds that the thief has to determine whether or not to “hit” (steal) your machine? **Thieves quite simply do not steal SafeTagged items.** It just does not happen much. **The SafeTag™ stops theft BEFORE it happens.**

**31) Can a thief use my information to steal my identity?**

Most definitely. That's why you need that information returned to you and then destroyed.

**32) How do I get started using the system after I sign up?**

The system comes with instructions—be sure to follow them. In general, you must **REGISTER** your SafeTag™ (or SafeTags™) online in your account, apply them to your machines, and **INSTALL** MyLaptopGPS™ software on each machine.

**33) Do I just stick on the SafeTag™ and I am done?**

**NO.** Please follow the instructions that come with the system.

