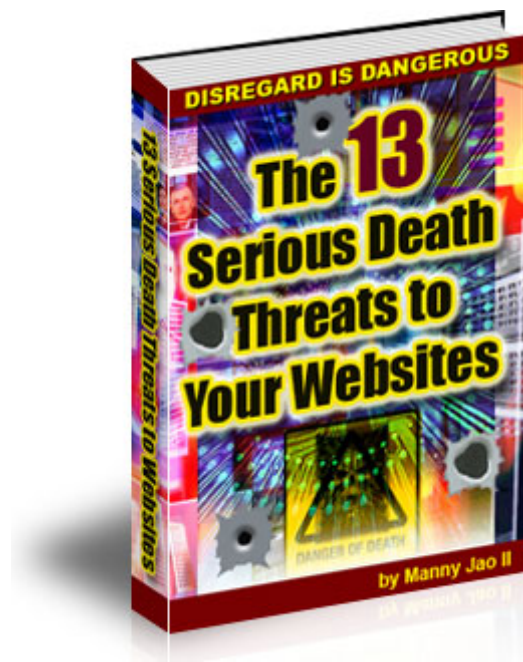# " THE **13** SERIOUS DEATH THREATS TO YOUR WEBSITES "

A SPECIAL WEBMASTER EBOOK

WEBSITE SECURITY AND MANAGEMENT SERIES

By Manny Jao II

RIGHTS AND DISCLAIMERS

This special Ebook is distributed and accepted by you with the understanding that the publisher is not engaged in rendering legal, accounting, technical or other professional advice.

If legal advice or other expert assistance is required, the services of a competent professional person or entity should be sought or consulted.

By mere possession, you now have **Master Resell, Redistribution and Giveaway Rights** to this special Ebook.

This Ebook can be given away for free or sold commercially to others **at any price** (suggested retail price of $29) you like to charge for it. You are allowed to include it as a product in membership sites or as a bonus to other information product packages.

However, with all these rights, you agree that you cannot and will not claim ownership of this ebook report. You have **NO Private Resell Rights** to this Ebook. This exclusive ebook report is originally published online and offline by **Manny Jao II** and **CPSiteSaver.com**.

If you like this Ebook and want to distribute it with your name and website link on it, we can re-brand this Ebook for you free of charge. See **"Announcements"** on the last page for more info on how to rebrand this Ebook.

Table of Contents

Overview and Introduction

In today's world that's driven by technology, more and more people and companies as well, are riding on the **fast-moving world of the digital revolution platform we call the internet.**

More often than not, these people or companies only knew how to build their websites and show it off to their visitors, customers, members, subscribers, friends and acquaintances without regard to the serious threats their creations are facing amidst the unstable network of computers and servers connected to the internet.

Like many industries of the IT world, these savvy **Webmasters are not fully aware of the dangers** that their websites face everyday as they rely heavily on their webhosts and new technology to protect their websites.

The reason they don't care that much is simple…

Most Webmasters are not appreciative of the fact that **there are real threats** that can seriously affect their online existence now more than ever. They normally build, deploy and conquer but don't believe (or tend not to believe) the real dangers of losing their websites in a snap (like the dreaded harddisk failure on their very own PC or Mac).

This comprehensive Ebook will show you at least **thirteen (13)** of the most serious threats (that's why we call them **"Death Threats"**) to your website existence and what you can do to avoid their destructive impact when they strike you and your web sites (can be anytime from now).

Some of these death threats you can avoid. Other threats are really beyond you, your webserver and even your webhost. And statistics shows that **94.6% of active websites** have been affected by or suffered one or more of these **"death threats"** in their online existence.

There are several ways to ensure that your websites will not be affected by these online plagues and disasters. This special report will show you how to avoid or prevent many of these threats, how to stop some of them and how to prepare for those that you cannot control.

So sit back, relax and enjoy a worthwhile read of the **13 most dreaded Death Threats** to your websites. Find out why we say **Disregard is Dangerous** to you as well as your websites.

1. SERVER TIMEOUTS / DOWNTIMES

Symptoms include:

Inability to access your website; server timeouts occasionally; webpages not responding; page cannot be displayed errors; page not found errors and similar problems.

This is one of the most common problems in the webhosting industry.

Causes and Effects:

Sometimes, web servers don't perform as they should due mainly to overcrowding or overselling these servers. Others freeze up because the server hardware can't handle the load anymore without an upgrade. As a result, the processes are too much to bear for the poor servers and they end up not responding. Normally, it occurs on shared server/hosting environment. Shared hosting means you are not the only one customer in that server and/or have no control over it.

It basically happens when the major server components (like the CPU, memory and hard disks) fail, freeze or malfunction because it can't cope up with large simultaneous tasks it processes at the same time.

When too many domains are hosted on the server (overselling) and many are abusing the server resources at the same time, the core of the server system fails.

As the server stops operating, your websites and all the other sites on that server will not be displayed to your visitors. On and off... Up and down... This can happen several times in a day without you even noticing it at some point yet it can ruin your website's reputation.

Server downtimes normally result to partial loss of websites and databases. It could also mean lost opportunities and business to the webmasters.

Up to 99.9% Uptime Guarantee ONLY!

These downtimes are anticipated and expected by most webhosts that's why you'll notice that most of them give you less than 100% uptime guarantee to make sure that their customers will not blame them later. This is also setting up expectations with their customers that their service is not error-free.

Solutions/Preventive Measures

- Go for those hosts with assured backup capability.
- Check your hosts reputation on webhosting forums like WebhostingTalk.com
- Stay away from those known webhosts that oversell their servers.
- Ask your host how they are handling downtimes even before you sign up with them.
- Clarify with your host what their uptime guarantee means and how will you be informed or alerted in cases of scheduled downtimes. Uptime Guarantee explained here.
- Stay away from super cheap hosting offers to which the old adage applies, "what you pay is what you get".
- Backup your websites and databases on your local computer and try to save them on offline like on flash disks, CDs and DVDs.

2. SERVER CRASH PROBLEMS

Problems include:

Long downtimes - depending on how fast your host can or will replace faulty server parts. Uncertainty of when your websites will be back online.

Causes and Effects:

Server Crash is a sudden, usually drastic hardware failure. Others call it server breakdown or server meltdown. It only means that the server stops working due to one or more problematic hardware components and thus become offline.

When it comes to technology, hardware components are the most troublesome and the most risky part of a computer or server. Compared to software issues (which you can reinstall in case of problems), hardware problems normally gives us longer downtimes and headaches.

The issue commonly lies on how fast these hardware parts can be repaired or replaced in case of unexpected breakdowns. Imagine when the server you are hosted on suffered a CPU breakdown, memory conflicts and the most common of them all – hard drive crashes.

Aren't you scared when your own computer's hardware crashes? I bet you are that's why we believe that hardware failure is one of the worst form of hosting server problems.

Server crashes not only take time to replace parts, it also exposes you to risk of data loss – your website and databases if you have any like in the case of harddisk crashes or memory failures. And you know you're doomed to longer waiting time when the server part that failed is obsolete or is in limited stock in the marketplace.

Crashed hard drive is the most common culprit in the loss of most of our websites in the past. This devastating event cannot be predicted even by our webhosts. It's a tough luck to guess which server parts will fail first so better be ready for any impending disaster.

The bottom line is hardware breakdowns do happen with any webhosts. It will hit us the hardest if we don't expect them at all. Its a real threat to your website so better be prepared for it anytime since this is one of those threats that we, as webmasters, cannot do something about.

Solutions/Preventive Measures

- Go for those hosts with assured backup capability.
- Verify with your hosts how you they manage server hardware breakdowns and if they have standby/spare computer parts in case of emergency.
- Know where your hosts manage their servers. It's better if they own their datacenter or if they are located in reliable datacenter so the server parts are readily available.
- You may want to know also how fast they can switch from one server to another if there are extreme problems on the server you are hosted on.
- Backup your websites and databases on your local computer and try to save them on offline like on flash disks, CDs and DVDs.

3. SERVER SOFTWARE PROBLEMS

Problems include:

Erratic website performance. Error pages all over the place. Scripts won't run or perform as before. Problems persist until your host aligns the server settings to your site or vice versa.

Causes and Effects:

This happens when server softwares are updated either manually or automatically on schedule. Patch application to the server softwares can also affect website performance if not cautiously done. Server hardening (against hackers and abusers) can be a culprit as well.

I remember some time back when CPanel was auto-updated on our server and rendered many of our sites dead and not working.

Since it automatically upgrades or updates the softwares, sometimes your host will not know about this until you notice it or if your visitors alerted you of the problem.

Another good example of software problem is the update of famous and open source softwares like PHP and MYSQL. Many updates from these scripts have affected installed scripts written on previous versions.

Software issues pose a big threat to any website. You must be assured as a customer that such changes or updates will be communicated well to you are customers.

And on your part, you must be ready to respond to these changes as well if your host is not reliable enough to support your needs.

Solutions/Preventive Measures

- Go for those hosts with assured backup capability and facility in place.
- Verify with your hosts how if any updates on the server will be communicated to you as a customer.
- Know who manages your host's servers. It's better if they are manned by their own technical staff or if they are located in reliable datacenter where experts can immediately troubleshoot the problem.
- Sometimes server hardening limits certain features which you need for your website so be sure you know about this before even hosting on that "tightened server".
- Have a programmer or server admin on hot standby to fix your site in case of problems. You can try finding quick fixers from sites like scriptlance.com or elance.com.
- Backup your websites and databases on your local computer and try to save them on offline like on flash disks, CDs and DVDs.

4. DATACENTER DISASTERS AND PROBLEMS

Problems include:

Long or intermittent downtimes. Unsure of what will happen to your website and its content. Uncertainty of when the sites will be back online. Backups maybe compromised as well.

Causes and Effects:

If you think your datacenter is the best, think again. Datacenters are huge facilities where webhosting servers are maintained and located. These are normally secured facilities and only authorized personnel can access the site. Most of them are built to withstand the toughest tests.

But sometimes, even the unexpected can happen to the most secure place in the world (imagine when Murphy's Law is at work). When disasters are not expected to happen, things just go wrong from bad to worse. And sadly, you and I can't do anything about it.

I encountered one of these when my host (they resell servers) told me that my dedicated server is one of those "fried up" by faulty electrical problems that started a fire in the datacenter we are collocated with.

At first, I can't believe it really happened. I even argued with my host pointing out that this is impossible to happen since I am thinking that he is just using this as an excuse for long downtimes. But when I verified that it was in the news on the internet, it shocked me to know how vulnerable those hosting servers and my websites are in cases like this.

I have heard and read many other stories of datacenter disasters like leaking pipes that affected server racks, faulty technical workmanship, major network component breakdowns (e.g routers and switches), unavailability of spare parts and equipment and many others.

No matter how great or how well-built these datacenters are, anything can happen from good to worse. So what more if your host is running a few servers at a small home office? Then the risks are even higher.

Solutions/Preventive Measures

- Go for those hosts with assured backup capability and facility in place.
- Normally, webhosts brag about their datacenters on their websites. So verify where your server is hosted and review first the datacenter's reputation and built.
- Take a tour of the facility if you can offline or online. If not, then ask your host of the Datacenter location (exact mailing or business address) so you know in the news if there is something going on in that place (like bad weather) at certain points in time.
- If you can ask for and review your host's and its Datacenter's Business Continuity Programs (BCP) or at least their Disaster Recovery Program (DRP), then it will be good for comfort. At least you know there is a plan such as this in place.
- Choose to backup your websites and databases on your local computer and try to save them on offline media like on flash disks, CDs or DVDs.

5. SERVER MOVEMENTS AND TRANSFERS

Problems include:

Long downtimes on erratic website transfer and restore. Incomplete data transfers. Missing files and configuration data. Error pages abound. Page cannot be displayed errors.

Causes and Effects:

I have read a lot of horror stories related to this death threat.

Sometimes, we need to move to a new server because our webhosts need to. Even if you own a dedicated server like me, chances are you will transfer if a new and better server arrives. It also happens at times that you have no choice but to move because of problems, opportunities and convenience.

Reasons include if the server may have outgrown its capacity or has been acting problematic (intermittent downtimes) or a cheaper server is found.

Take the case when you are on a shared server with a very low uptime rate because of some customers abusing the server resources. You have no choice but to move or your sites will be affected more.

Another reason is if you, the customer, request your websites to be moved to another server for some other compelling reasons like getting away from a blacklisted IP address on SPAM Real-time Black Listing (RBL) sites which affects your emails.

When hosts move from one server to another, you normally have no choice but to wait and watch for it to happen. You wait until all websites and databases have been transferred from the old to the new machine while crossing your fingers that your website data will be restored very well.

If you know how to do it, you know it's a very tedious process. And you will be happy if you will not encounter any problems. But if something happens along the way, what will you do?

Careful planning is needed when moving sites to avoid the dreaded downtimes. Sometimes, when you are in a hurry, you just can't do much about it. But without planning, it simply won't work out the way you want it to be. So you have to be prepared for whatever scenario you will be into.

Solutions/Preventive Measures

- Go for those hosts with assured backup capability and facility in place.
- Plan carefully up to the exact time and date of the movement so everyone, even your visitors, is aware of the situation.
- Stop your site operations for a while and backup all your data in your local computer. Download your backup files twice for added security.
- If your host triggered the movement, coordinate with your host accordingly. Be sure you know the exact date and time the movement will occur so you can backup your websites accordingly.
- Choose to backup your websites and databases on your local computer and try to save them on offline media like on flash disks, CDs or DVDs.

6. VIRUSES, WORMS AND OTHER EXPLOITS

Problems include:

Intermittent or long downtimes or erratic website performance. Lost data is also possible leading to website collapse.

Causes and Effects:

It tends to happen when scripts are being run in a server-side language or passwords are not encrypted or the data is not protected against exploitation by some happy-go-lucky fellow.

If a hacker finds a security flaw in a script they may try to exploit it. They do this by either running some code to trick the script into revealing passwords or by intercepting an authorized member/visitor who submits the information over the internet.

With this exploitation, hackers can implant viruses, bots and malicious scripts that run in the background for their benefit. Typical of these are spam scripts.

More often than not, exploits came from illegally purchased scripts (either cracked, nullified or warez). Once the unsuspecting webmaster installs any of these illegal scripts, the crackers and nullifiers will know how to get around the server and access it.

Server performance takes its toll when viruses and renegade scripts run wildly in the background and sometimes even on the forefront. This slows down performance on an overwhelmed server resulting to long downtimes or data loss.

It also compromises the whole Datacenter where your server is located and the owners may even shutdown the server so that it will not affect other customers on their network.

Solutions/Preventive Measures

- Go for those hosts with assured backup capability and facility in place.
- Ask your host to harden your server against malicious intrusions and breach of security.
- Do not install illegal softwares and/or scripts to your websites even if you got them cheap or free. It always best and legal to pay for softwares or scripts that you want to use on your website.
- Update your scripts whenever there is an applicable update that fixes security issues especially those categorized as open source.
- Check your website logs from time to time and report any unusual logins or processes in the system. You may also find unusual files in one of your web directory. If this happens, report to your host immediately.
- Choose to backup your websites and databases on your local computer and try to save them on offline media like on flash disks, CDs or DVDs.

7. SERVER HACKING PROBLEMS

Problems include:

Intermittent or long downtimes or erratic website performance. Lost website files and databases are also possible leading to website collapse and demise.

Causes and Effects:

If someone breaks into a hosting server, they could do things such as changing big company websites into worthless bunch of pages. The hacker can edit website contents, delete files, damage databases or steal information. They can shut down or wipe out the whole server before the webmasters or server administrators can even react.

If the hacker is really malicious, it will benefit him more if the company is selling a product online by collecting visitors' credit card numbers and other details which he can keep for himself for later use.

Another form of hacking often perpetrated by fame-hungry programmers is commonly known as "website defacements". This happens when an intruder compromises a website or a webserver and changes the data/content on webpages or publishes one of his own.

Defacement is often done to mock the owner of the website and to make fun of the system administrator for failing to maintain server security. These hackers take pride in what they can do as can be seen on the wordings they placed on the defaced websites. You are lucky if site files are intact.

Hacking can also be caused by revengeful people that you don't even know you offended online. If someone is angry at you, they can pay some geeks to hack your sites and you cannot do something about it. If you happen to offend a real hacker, you're in bigger trouble as they can do harm to you at anytime.

Most hackers are eventually caught but if a hosting server is not secured properly, more and more websites will be compromised without the owners knowing it. Many webhosts now implement anti-hacking tools and softwares on their web servers and even employ people for 24/7 monitoring of the servers to thwart these attacks. But still, some clever guys will manage to sneak in these barriers and create chaos on the server.

Solutions/Preventive Measures

- Go for those hosts with assured backup capability and facility in place.
- Ask your host to harden your/their server against malicious intrusions and breach of security.
- Be sure to change your passwords from time to time. Do not share your website login details to others and if you really need to, change it immediately as soon as you can.
- Be careful not to offend other people online and offline. You'll never know what they can do to you and your websites.
- Choose to backup your websites and databases on your local computer and try to save them on offline media like on flash disks, CDs or DVDs.

8. DOS or DDOS ATTACK

Problems include:

Long downtimes or erratic website performance. Lost data is highly probable as the server may totally crash leading to website collapse and demise.

Causes and Effects:

A Distributed Denial-Of-Service attack (DDOS attack) happens in an attempt to make a computer or web server resource unavailable to its intended users.   This is the cause of many lost opportunities for website owners and online businesses.

Typically the targets are high-profile web servers where the attack is aiming to cause harm on the hosted web pages to be unavailable on the Internet. It is considered an internet crime by the Internet Architecture Board (IAB).
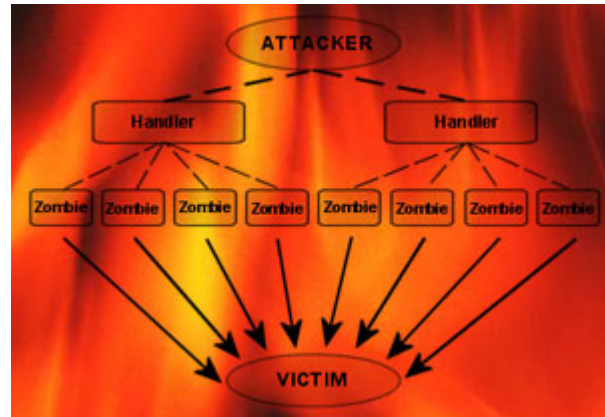
There are two (2) general forms of DOS attacks:

1. To force the victim server(s) to reboot, reset and/or consume its resources such that it can no longer provide its intended service.
2. To block the communication media between the intended users and the victim server(s) in such that they can no longer communicate adequately.

Not all web server outages and downtimes, even those resulting from malicious activities, are denial-of-service attacks. Sometimes, DOS attack is just part and parcel of the cause of a server downtime. But at worse, the victim web server may become a host to a DOS attack and/or a part of a larger attack to bombard other sets of servers or network somewhere. The effect is the same.

Illegitimate use of resources may also result in denial of service. For example, an intruder may use one's anonymous FTP area as a place to store illegal copies of commercial software, consuming disk space and generating massive network traffic that will alert the Datacenter owners to shut that server down. Another example is mail bombing by using the server's mail server to send tons of emails directed to another server rendering that target server useless.

Solutions/Preventive Measures

- Go for those hosts with assured backup capability and facility in place.
- Ask your host to harden your/their server against malicious intrusions and security breaches to avoid DOS and DDOS attacks.
- Be sure to change your passwords from time to time. Do not share your website login details to others and if you really need to, change it immediately as soon as you can.
- Be careful not to offend other people online and offline. This can cause a DOS attack. You'll never know what they can do to you and your websites.
- Choose to backup your websites and databases on your local computer and try to save them on offline media like on flash disks, CDs or DVDs.

9. WEBHOST TROUBLES, DISPUTES AND PROBLEMS

Problems include:

Site suspensions and/or deletions. Inability to access website or domain. Uncertainty of the fate of the website and domain.

Causes and Effects:

Sometimes, the web host and the webmaster disagree on something or issues which results to misunderstandings, debates, quarrel or disputes.

A typical example is the violation of the host's Terms of Service, Acceptable Usage Policies and/or Legal Terms. When this happen, the host can shut down the site or in extreme cases terminate the account to oblivion. This is another scary death threat.

Take the case of a webmaster whose site has been reported as sending spam emails to a visitor who just forgot he/she signed up for the webmaster's newsletter.   When someone reports this to the webhost and/or through some spam complaint sites, the unsuspecting webmaster will be likely hit with a site suspension. Before he/she knows it, his/her website is down and offline. The chaos begins.

Another typical contention is about payment of the hosting service. Most host will shut down the delinquent webmaster site without warning as stated in their Terms of Service.   But sometimes, payment system automation (in the case of credit cards) will never verify that there maybe problems with the credit card company and not the webmaster's account per se. This will result to unnecessary arguments and quarrels.

The problem for the webmaster is greater if he/she does not have control on the domain being hosted. This means that the host is the one managing the domain for the webmaster and therefore can control where and when the site will be hosted. For the webmasters, its better to lose the website but never the domain. If this happens, the poor webmaster is left with nothing.

Solutions/Preventive Measures

- Go for those hosts with assured backup capability and facility in place.
- Always get hold of your domain and be in control. If it comes free with your hosting service, ask the host to deduct the cost of the domain from the initial fee and register the domain yourself.
- Be sure you attend to Spam complaints promptly.   Also check from time to time if your site or the server IP is listed on some spam blacklisting. Sites like DNSStuff.com helps.
- Be sure that your credit card information is up to date and you don't have problems with your credit card company. Ask your host for some alternative payment system in case your current option fails.
- Choose to backup your websites and databases on your local computer and try to save them on offline media like on flash disks, CDs or DVDs.

10. WEBHOST DECEPTIONS AND FRAUDS

Problems include:

Long downtimes. Inability to access website or domain. Uncertainty of the fate of the websites and domains.

Causes and Effects:

This typically happens to bargain-hunting and risk-taking webmasters.

Once in a while, webmasters like you and me will stumble on an ad that gives us almost the whole server space at $1 a pop. I maybe exaggerating here but I am sure you know these tempting offers. As they say, "you always get what you pay for" and oftentimes, it's true.

There are cases wherein a webmaster saw a very cheap website hosting service offer and decided to move their sites to this new host. Unfortunately, the gullible hoster doesn't know that his webhost is a 13-year old wiz kid who got hold of his father's credit card and bought a reseller account somewhere. Scary eh?

What about a bunch of artistic geeks who can create stunning websites that really look professional but can neither support the technical and emotional needs of their clients? They too can scare the hell out of me and you if we know that they can't fix even our email problems much more if there are problems with their server.

And there are those mom and pop webhosting shops that lure more webmasters because of the sheer size of their offer like those gazillion of web space and bandwidth in their Starter Plans. Because you like what you'll get, you will pay for one year and after 3 months, their server is gone and so are your websites.

I haven't even mentioned those professional fly-by-night hosts that hop around. They come and go as soon as their tactic is revealed or when they got enough money from their poor customers. Once you're hooked in their bait of deceit, your online presence is doomed.

Solutions/Preventive Measures

- Go for hosts with a good reputation on the internet. You can get info from people by interacting in webhosting rating sites like FindMyHosting.com and WebhostingTalk.com
- Don't fall prey to cheap offerings. If you have to for financial reasons, always take time to verify that the company behind it is reputable and honest.
- Before you sign up with a webhost, try to get hold of them on the phone. If you can't get them on the phone, at least chat with them. Doing this pre-purchase talk will give you more or less on the capabilities of your hosts.
- Always trace the location of your hosts. Know how long they are operating in business and what websites they are currently hosting.
- Choose to backup your websites and databases on your local computer and try to save them on offline media like on flash disks, CDs or DVDs.

11. FORCE MAJEURE - ACTS OF GOD

Problems include:

Server and/or internet shutdown due to natural calamities. Inability to access website or domain. Uncertainty of the fate of the websites and domains.

Causes and Effects:

Force Majeure is the happening of a disastrous event brought about by acts of nature or as they say, acts of God.

Natural calamities such as typhoons, hurricanes, tidal waves, earthquakes, flooding, volcano eruptions and other similar forces of nature are real threats to your web hosts. It may also include wars and acts of terrorisms.
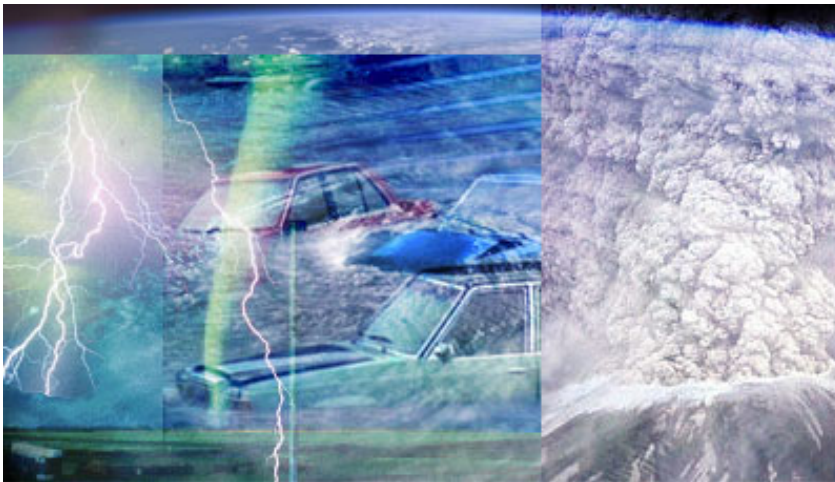
As you know, nature's fury has not been controlled by any man. We can't even predict accurately yet when and where it will strike. No structure created by man can ever be considered safe no matter how architecturally sound and technologically advanced this structure is.

The most vulnerable in cases like this is your host or where your host is keeping their servers. Big hosting companies typically have their own datacenters while those small and medium hosting companies rent a space or servers on public datacenters. This renting of space is also known as collocation.

When these datacenters (owned or rented) are hit by Force Majeure events, you will never know what will happen with your websites as well. This is something even your host cannot control to which both of you should be ready to face anytime it happens.

Solutions/Preventive Measures

- Go for those hosts with assured backup capability and facility in place.
- Always get hold of your domain and be in control. If it comes free with your hosting service, ask the host to deduct the cost of the domain from the initial fee and register the domain yourself.
- Be sure you know the location of the server you are hosting. That way, you can keep abreast on what's happening in that particular place through news and updates.
- Always be prepared with a migration plan in case you need to transfer to a new host because of these events. A standby host on another location is recommended.
- Choose to backup your websites and databases on your local computer and try to save them on offline media like on flash disks, CDs or DVDs.

12. PROBLEMS DUE TO ACTS OF MAN

Problems include:

Inability to access website or domain. Medium to long downtimes. Uncertainty of the fate of the websites and domains. Erratic website performance. Error pages everywhere.

Causes and Effects:

Inexperience, unreliability and accidents play a big role here.

Imagine if your host has folded his business down for no reason and leave you with nothing but a dead website. Imagine if there are labor disputes or strikes in the datacenter or in your hosting company premises.

Imagine if you don't know that your host has sold his/her business to someone else and the new owner does not recognize you as a customer and has deleted your account in the process.

Imagine if someone in your host's technical team went crazy or became a disgruntled employee and wipe out all data on web servers where you are hosted as a form of revenge.

Imagine if some crazy webmaster working on the same server your sites are hosted suddenly became the object of a DOS attack or a hacking incident that affected your sites as well.

Imagine a newbie webmaster on the same server you are in tinkers with his websites and accidentally clicked on something or uploaded something that should have not been done in the first place and because of it the server went down and rendered useless.

Imagine when your hired programmer accidentally wrecks your website while working on a script you want developed or fixed.

Any or all of the above can happen to you and me. There is no question about it. The question now is "Are you ready for the consequences just in case?".

Solutions/Preventive Measures

- Never underestimate the power of accidents and intentional disasters.
- Always get hold of your domain and be in control. If it comes free with your hosting service, ask the host to deduct the cost of the domain from the initial fee and register the domain yourself.
- Always be prepared with a migration plan in case you need to transfer to a new host because of these events. A standby host on another location is recommended.
- Choose to backup your websites and databases on your local computer and try to save them on offline media like on flash disks, CDs or DVDs.

13. YOUR OWN ERRORS OR OMMISSIONS

Problems include:

Problematic server access. Short downtimes. Probably long downtimes due to needed fix and redevelopment of the sites.

Causes and Effects:

Again, inexperience and accidents play a big role here. This normally happens to a newbie webmaster.

More often than not, newbie webmasters explore their hosting account and to some extent tries to click here and there in order to see what's working and what's not. In short, exploration and experimentation often results to unwanted scenarios like lost websites and databases.

There are cases when webmasters are working on a certain portions of the site where mistakes can happen such as:

- Deletion of important files (like config scripts, includes or templates)
- Deletion or failure to delete directories or folders (like config.php, update.php, install.php)
- Accidental edits of files and directories
- Deletion or erroneous edit of MySQL databases
- Conflicting script installation

There are cases also that a webmaster can't wait for someone to help, tries to fix a problem he doesn't really know how to fix and ends up creating a bigger mess out of it. This has happened to me many times because of my guts to mess up with my websites and scripts.

Accidents do happen and often times we are not ready for it. But if you as a webmaster are prepared for the consequences of your actions, then these mishaps will not affect you or your websites at all.

Solutions/Preventive Measures

- Never underestimate the power of accidents and unintentional disasters.
- If you are working on your website directly, always get a backup of the files you are editing or deleting prior to any actions you have to make.
- Before you do anything big or do a significant change in your website, make it a habit to backup your files first.
- Do test new webpages, files and scripts on a test folder before publishing them online.
- Never forget to do as suggested by experts. For example, if you bought a script and it says after install, it's important that you delete the install.php or update.php file, then do it. Don't forget about it or it's a problem later.
- Choose to backup your websites and databases on your local computer and try to save them on offline media like on flash disks, CDs or DVDs.

Conclusion

These **13 Serious Death Threats** to your websites should not be ignored. In fact, if you are a true-blue Webmaster, you know these dangers are for real and only need to be reminded of the disastrous effects from time to time.

If you care enough about your online presence, you will take time to secure what you have now and be prepared to implement a disaster recovery plan in case of problems.

As always, communication is vital in your relations with your webhosting company. You should try to contact your host as soon as you are noticing problems with your websites.

And remember, your webhost should be treated as your partner in business. As such, you should choose your webhost wisely. Look for a host with proper communication channels like a hotline number in case of emergency or a live chat facility. This will greatly help in times of need.

Now that you are aware of these death threats to your website, it's time for you to implement it. You have to make a choice to protect your online presence today.

The time to secure your websites is now. Not tomorrow. Never procrastinate. Protect your self today while you can.

To your online success,

Manny Jao II
Owner – CPSiteSaver CPanel Website & MySQL Backup Software

Think about it...

"Procrastination is, hands down, our favorite form of self-sabotage." - Alyce P. Cornyn-Selby

"Procrastination is the grave in which opportunity is buried." - Unknown

"Procrastination is suicide on the installment plan." - Unknown

"If you only do what you know you can do - you never do very much." - Tom Krause

"Trust yourself. You know more than you think you do." - Benjamin Spock

SPECIAL ANNOUNCEMENTS

"ATTENTION CLICKBANK AFFILIATES, WEBHOSTS, WEBHOSTING RESELLERS & of course, The WEBMASTERS"

Own a rebranded version of this special Ebook for free.   **Yes, it's FREE!** We will create one customized PDF file for you with your name on it for your distribution.

Why distribute this report? Here are 5 Good Reasons WHY…

- **Because it does not only benefit you, it benefits your audience**, customers, visitors, subscribers, colleagues, readers and friends as well. Distributing this report will help many people realize the value you are placing on your connections with them.

- **Because if you are a webhost or a webhosting reseller,** your customers would love to know that you care for them online. You will let them know how much you are concerned for their websites by giving this valuable Webmaster Ebook. Not only you will solve the usual problems on loss of websites in case of disasters, you will also minimize the burden from your end of the responsibility for your customer websites. Now they know what to do.

- **Because this Ebook can add value to your business**. Give this Ebook as a bonus or a package to your hosting offers and differentiate yourself from the pack. Offer it as a freebie or bundle it with other ebooks and/or packages and win more subscribers to your ezines. Hosting security is a general concern so use it to add value to almost any area of your online business.

- **Because this can be a source of promotion for your websites**. Ebooks like these are known to have viral effects as they are distributed. So with your customized website links as one of our partners, your business will be known to as many people as your ebook can reach.

- **Because you can make money from it as well.** If you decide to become one of our resellers (which we think you should consider), we can insert your affiliate link in the rebranded version so that if someone purchase from that link, you can make money as well at Clickbank.

To request for your customized and rebranded ebook, simply send us an email request to **rebranding@cpsitesaver.com** with the subject   **"Re: ReBranding Rights to 13 Death Threats Ebook"**

Please include the following details:

Your Full Name:
Full Address:
Name of Your Company (if any):
Your Website URL:
Your CPSiteSaver Affiliate link: (You need to register on our website here)
A brief explanation of what you do or what your company can do or sells. (We may include some notes about you, as our partner, in your customized version).

Once done, we will email you a customized version of the Ebook with your name and links on it. Please allow us up to 5 working days to send your customized version. We promise to get back to you as soon as possible. If you are in a hurry, please specify so in your email as to where you will use this Ebook so we can assess its prioritization.

If you like this Ebook or have comments on it, please send us an email to **admin@cpsitesaver.com**.
We would love to hear from you. Thank you.

Manny Jao II
Developer and Owner – CPSiteSaver Cpanel Website & MySQL Databases Backup Software

Visit our Website to know more how to protect and secure your CPanel Websites and MySQL databases.