



SAFE BLOGGING GUIDE

TIPS AND TRICKS ON HOW TO KEEP YOUR
BLOG AND YOUR IDENTITY SAFE

BOGDAN BOTEZATU
E-THREATS ANALYSIS AND COMMUNICATION TEAM

Table of Contents

Table of Contents.....2

147 million blogs and counting.....3

Flavors of blogging: self-hosted platforms versus SaaS.....4

Blogging and the Boomerang Effect4

 Blog spam..... 5

 Blog malware..... 7

 Phishing and Vishing..... 9

Blog hacked. What now? 11

Tips for safe blogging..... 13

147 million blogs and counting

Back in 1999, a new type of journalism started to gain ground, mostly powered by the emergence of a couple of free publishing platforms. Back then, no one had imagined that blogging would become one of the most important means of expression on the Internet, nor that it would change the face of conventional journalism as we knew it.

At the moment, there are about 147 million blogs (as tracked by [BlogPulse](#)), and other 54,000 new ones emerge on a daily basis, according to the same statistics. While most blogs are personal creations maintained by one or two individuals, others are part of complex corporate communication schemes, each catering to their own niches.

This material covers the basic guidelines for safe blogging and is especially focused on individual blogs that are either self-hosted or provided as a service by major blog providers.

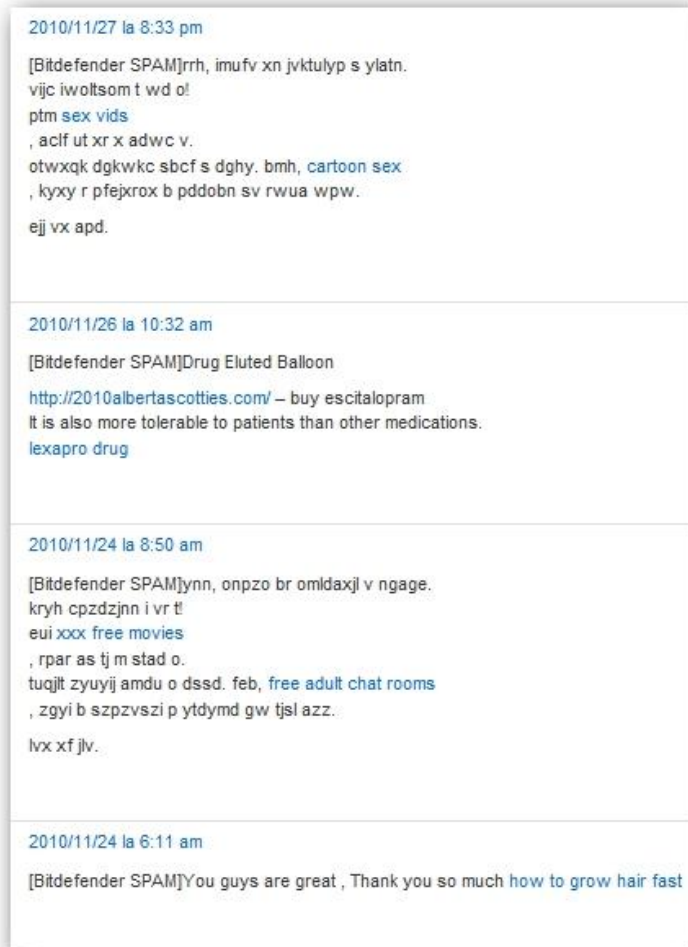
Flavors of blogging: self-hosted platforms versus SaaS

While some of the bloggers opt for a hosted account with major blogging platform developers – especially those who are just starting to get the “fever” – some others go with a self-hosted plan that offers extra flexibility in both management and design, but at the same time, that needs extra attention to avoid incidents.

Blogspot®, Wordpress® and LiveJournal® are three of the most popular services that offer free blogs. They are publicly available as a service and professionally maintained by the provider, which means that the user does not have to worry about patches or other kind of server-side security fixes, because they are automatically pushed by providers. However, although a blog hosted with third-party providers is usually more difficult to break in, it is still prone to threats such as spam or phishing, as described next.

Blogging and the Boomerang Effect

Regardless of the type of hosting and content niche, a blog is usually created and maintained to add a plus of value to the business or personal image, or it may even be the very business itself. Advertising-driven blogs are extremely common and represent a source of income for the vast majority of bloggers. There are, however circumstances when the blog can turn against its very purpose – for instance, when it has been compromised or has been used to harm its owner.



The BitDefender Antispam Plugin identifies spam comments and sends them to the moderation queue.

Blog spam

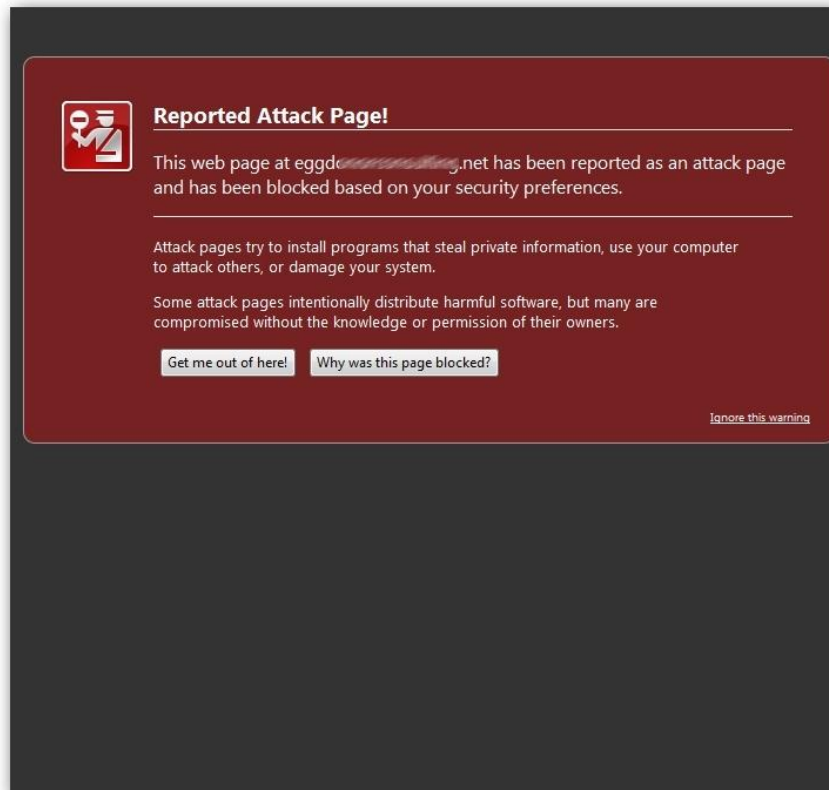
Blog spam is one of the most common means of inflicting damage to the owner's reputation. Spam comments usually contain links that might take the visitor to harmful or (at least) obscene content. A large number of spam messages would dramatically minimize the blog's usability and would make the valuable information more difficult to reach. Various links to shady websites embedded in these spam messages are also likely to affect the blog's reputation in search engines – a key element in a cut-throat online business. More than that, users will navigate away from a spam-soaked blog, thus losing loyal reader base. The bad news is that blog spam is one of the threats that affect both self-hosted blogs and those offered as a service.

Side note

About 99 percent of the total number of spam messages posted on blogs and forums is sent by spam bots – small applications written in a scripting language such as Perl or Python. These bots are highly versatile for their purpose, but at the same time, they are also extremely easy to defeat. Some of the most common approaches include forcing the usage of JavaScript of cookies in order to post a comment. Since spam bots are unable to handle JavaScript or cookies, they will fail to post the message. Other similar approaches include adding a text field hidden via CSS that has to be empty in order to go further. Since the spam bot sees them in the web page's source code, it will try to complete it with junk text, which actually prevents the form from being submitted.

On the bright side, fighting blog spam is relatively easy, provided that you have the right tools and you have correctly set up your blog. Here are some tips to help you prevent the posting of junk messages.

1. Configure your blog to automatically hold for moderation the first comment from a user. Legit community members will have their comment approved by an administrator, and all their subsequent messages will be automatically approved.
2. Configure your blog to automatically hold all comments for moderation. This approach is much safer than the previously-described one, but it doesn't scale well for blogs with plenty of comments per day.
3. Install a dedicated antispam plugin. If you are using Wordpress as your blogging platform of choice, you should try the BitDefender Antispam plugin. This is a 100% free solution uses an API to query the BitDefender Antispam cloud service and check whether a comment is legitimate or not.



Attack alerts are likely to scare users away and make them never come back

Blog malware

Unless its owner hasn't voluntarily uploaded malicious files on the blog's hosting account, blog malware is usually the result of a successful hack attempt against the blog or against the server accommodating it.

There are multiple ways in which an attacker can gain control over a blog and its FTP account. Sometimes, these attacks are extremely carefully planned and involve a high degree of tech literacy, while other times attackers simply rely on logging in with a right combination of username and password.

1. Many times, bloggers get their log-in credentials compromised by malware infections on their local machine. Certain types of Trojans, such as the notorious Facebook Hacker and the iStealer Trojan collect saved combinations of usernames and passwords directly from the browsers' password managers. Conventional keyloggers can also lift such credentials and forward them to a remote attacker. Last, but not least, administrative passwords can also be sniffed by a third party as the unwary users connect to their blogs via an unsecured Wi-Fi connection at the local coffee shop. The same thing goes to FTP credentials -real gold mines for cyber-criminals that plan to use these accounts to store malicious files, exploit packs or phishing pages.
2. Blog hacking may occur in various circumstances, and some of them are even out of users' control. For instance, poor server configuration or vulnerable software can lead to successful exploitation of the hosting account. Some other attacks are the direct result of improper blog installations or of a vulnerable plugin. Zero-day faults inside blog software can also result in security breaches that either expose log-in credentials or lead the unwary visitor to malware.

Regardless of how malware gets on the blog, it will for sure impact on the blog's ranking and functionality. Most search engines run constant malware checks against the indexed pages in order to see whether they pose any danger to their viewers. If they are found to be malicious, they will be immediately labeled as harmful in the organic search results, which means that users following these links will be warned that the requested content is likely to endanger the visitors or their computers.

Blog malware is not limited to e-threats present on the respective account, but also refers to various scripts that, once injected in the blog, would redirect users towards third-party websites serving dangerous content, as well as to scripts used by rogue antivirus products to simulate system scans. All in all, an infected blog will surely be delisted by search engines and the loyal customer base will likely never return, fearing that visiting the blog will damage their computer.

```
Registration Service Provided By: GLOBEHOSTING EUROPE
Contact: +040.312249495

Domain Name: DOWN [REDACTED]

Registrant:
[REDACTED]
Botezatu Bogdan (bogdan.botezatu@[REDACTED])
5B Basarabi St.
Iasi
[REDACTED]
RO
Tel. +040.[REDACTED]1233424

Creation Date: 20-Sep-2010
Expiration Date: 20-Sep-2011

Domain servers in listed order:
ns24.roserve.net
ns23.roserve.net

Administrative Contact:
[REDACTED]
Botezatu Bogdan (bogdan.botezatu@[REDACTED])
5B Basarabi St.
Iasi
[REDACTED]
RO
Tel. +040.[REDACTED]1233424
```

WHOIS Registrar Databases offer contact information about the domain's owner

Phishing and Vishing

Bloggers who are extensively writing about themselves should consider extra security risks related not only to privacy, but also to identity theft and account balance.

Many bloggers have abundantly written on topics such as favorite music or movie artists, love, hobbies and other various topics that apparently can hardly pose any risk. It's extremely easy to write on such topics, or to share different experiences with readers, but at the same time, bloggers might expose enough data for malicious persons to carry out a successful phishing or vishing (the phone equivalent of phishing) attack.

In order to better explain these risks, let's take into account the following scenario: a blogger buys himself / herself a new, more efficient & intelligent mobile phone. It can open PDF documents, it has Wi-Fi connectivity (or at least, it can connect via GPRS to a blog, in order for its owner to fuel it with new material while travelling). It is quite common about bloggers to brag about new acquisitions in a more personal & descriptive manner. The scenario below is taken from a real-life blog post and modified to protect the original author.

"I have just purchased a new mobile phone in order to do some on-the-fly posting with the newest things that come across my life. I got myself the new [brand-goes-here] PDA yesterday from [mobile company]'s shop. You would not believe how cool this is."

```
Registrant:
Contactprivacy.com
96 Mowat Ave
Toronto, ON M6K 3M1
CA

Domain name: ██████████.COM

Administrative Contact:
contactprivacy.com, ██████████.com@contactprivacy.com
96 Mowat Ave
Toronto, ON M6K 3M1
CA
+1.4165385457

Technical Contact:
contactprivacy.com, ██████████.com@contactprivacy.com
96 Mowat Ave
Toronto, ON M6K 3M1
CA
+1.4165385457
```

Privacy protection mechanisms hide registrar's information while providing a safe option to contact the owner.

Next, imagine that the post above ends up read by the wrong person, who then calls the blogger back impersonating one of the [mobile company]'s employees. Bloggers who have registered their own domain names usually have their phone number listed in the registrar's database, along with the rest of contact details, including billing post address, name & surname and personal contact e-mail.

"Hi there, sir! I am [name] of [mobile company], and I'd like to ask you a couple of questions about your [brand-name] handset you purchased yesterday from [shop]. But first, I'd like you to confirm your identity. Please state your SSN, birth date and address for verification first".

This is only one of the scenarios that can lead to massive identity theft. As a rule, the more you say about yourself, the easier for the attacker to guess other details. Talking about favorite food, actors and day-by-day activities may be a good starting point for attackers to guess the e-mail password, or to fill in the necessary info to recover the allegedly lost password from one's mail account.

Mitigation

If you own a domain name registered on your behalf, make sure that you treat every interaction with a potentially unknown person with maximum attention. If you have any doubts on the legitimacy of the person requiring personal information on the behalf of an institution, you should refuse the request and call back using the contact coordinates listed on the institution's website.

Alternatively, you can always ask your domain registrar to activate the WHOIS privacy protection option on your account, which will completely replace your contact details with those belonging to the privacy protection organization. Your details will be kept private from third parties, except for law enforcement organizations.

Blog hacked. What now?

Recovering from a hack may be a painstaking experience, and the effects of a successful penetration can stretch over a long period of time, but the faster you identify and solve the issues, the less damage is inflicted to your blog. Here is a short list of immediate actions to be taken after a potential attack has been discovered.

1. First, you need to render your domain inaccessible both to the human user and to search engine crawlers. Since all the website files will be required for later analysis and (probably) for restoration, deleting any of them is not recommended. You can block all the traffic instead by renaming the `index.php` file and creating a blank one in its place. Beware: do not forget to create the dummy index page or you risk exposing other files in your FTP account. Blocking search engines will prevent them from seeing that your blog is infected and labeling it as malicious.
2. Make a full backup of your home folder using a FTP client and then manually export the database as a SQL file.
3. Pull off the access logs from your webserver and store them in a secure place. You will need the logs for investigating what exactly the attackers have done on your website. Analysis will reveal how the attackers compromised your blog.
4. Make a copy of whatever customized files you may have. Customized files may include themes, plugins and files uploaded as content – practically everything that can't be downloaded from the web again. Just keep whatever you consider necessary for a fresh start without losing any content.

5. Start looking inside every plugin and theme file for suspiciously-looking fragments of text. Pay special attention to lines of text like "eval(base64_decode(" followed by a series of illegible numbers and letters), as well as any script inclusions from domains you don't know (such as <script src="http://[unknowndomainname]/scriptname.php">).
6. Go through the database table by table and look for any sign of suspicious linking. Pay extra attention to the tables holding the administrators, the configuration settings and the blog post articles. If you find any administrator you are unaware of, remove it at once.
7. After the inspection and cleaning process completed, you should remove any files from your webserver. If the database was also affected, you should drop it and restore the copy you have manually checked.
8. Start uploading your blog script on the server. Make sure you have downloaded it from the official repository. It is mandatory that you download the latest version of the blog script. Modify the config file to match your web server's details (SQL user, database, password, file path and the rest of your settings).
9. Make sure that you do not set file and folder permissions higher than the script actually needs to run properly. Setting files and folders to CHMOD 777 may allow an attacker to actually write to them and re-inject malicious code. Change the blog's administrators' passwords and the FTP ones.

10. Push your modified files back to their right place via FTP. Flush the browser's cache and access your website. Additionally, look your blog up in a search engine using your name or the blog's title as keywords and follow the search result provided by the engine. Most of the times, blog malware checks the referrer to see if the visitor accessed the website directly or got there via a search engine and only manifests itself to referred visitors.

Tips for safe blogging

In order to minimize the probability of getting hacked, you are advised to obey a couple of extremely simple guidelines:

- Never use blog scripts coming from untrusted, unofficial download repositories. Most of all never use nulled scripts, as it's not only illegal, but also risky for your blog and web server.
- Keep your FTP account clean: do not mix & match the account hosting your blog with other scripts you casually test. A small vulnerability in a third-party script can get your blog owned. Always test other scripts on a locally installed webserver.
- Do not add unnecessary plugins or themes to your blog. Stick to what you really need and minimize the chance of having an exploitable plugin or theme. Also, ensure that any plugin you may want to upload comes from a trustworthy source; when in doubt, just ask the community.
- Generate and store SQL backups regularly. Use a plugin to automate the job and have the backups delivered to you via e-mail or via a secondary FTP account. Using the same account for storing backups is usually a bad idea, as an attacker may tamper with them or even have them deleted after a successful hack.

- Use strong passwords for FTP accounts and administrative users. Do not disclose them to anyone in any circumstance. You might also install a complete antimalware solution to ensure that your system is Trojan-free. Some of the successful blog attacks were carried using legit usernames and passwords intercepted by keyloggers or cache-monitoring Trojans.
- Pay extra attention to the way you select your hosting provider. Paid hosting is usually much better than free offers, and, since you're going to shed some money, ensure that you get automatic daily backups, access logging and a suitable web-server configuration for your blogging script of choice.

The information and data asserted in this document represent the current opinion of BitDefender® on the topics addressed as of the date of publication. This document and the information contained herein should not be interpreted in any way as a BitDefender's commitment or agreement of any kind.

Although every precaution has been taken in the preparation of this document, the publisher, authors and contributors assume no responsibility for errors and/or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. In addition, the information in this document is subject to change without prior notice. BitDefender, the publisher, authors and contributors cannot guarantee further related document issuance or any possible postrelease information.

This document and the data contained herein are for information purposes only. BitDefender, the publisher, authors and contributors make no warranties, express, implied, or statutory, as to the information stated in this document.

The document content may not be suitable for every situation. If professional assistance is required, the services of a competent professional person should be sought. Neither BitDefender, the document publishers, authors nor the contributors shall be liable for damages arising here from.

The fact that an individual or organization, an individual or collective work, including printed materials, electronic documents, websites, etc., are referred in this document as a citation and/or source of current or further information does not imply that BitDefender, the document publisher, authors or contributors endorses the information or recommendations the individual, organization, independent or collective work, including printed materials, electronic documents, websites, etc. may provide. Readers should also be aware that BitDefender, the document publisher, authors or contributors cannot guarantee the accuracy of any information presented herein after the date of publication, including, but not limited to World Wide Web addresses and Internet links listed in this document which may have changed or disappeared between the time this work was written and released and the moment it is read.

The readers are entirely responsible to comply with all applicable international copyright laws arising from this document. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of BitDefender.

BitDefender may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from BitDefender, this document does not provide any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright © 2010 BitDefender. All rights reserved.

All other product and company names mentioned herein are for identification purposes only and are the property of, and may be trademarks of, their respective owners.