

Security Tips / Best Practices

(for use with ALL editions of PDshop)

PageDown Technology, LLC / Copyright 2003-2009 All Rights Reserved.



Last Updated: 11/21/2008
For Use with: all editions of PDshop (and PDshopPro)

Table of Contents

Table of Contents	2
Best Practices	3
1. Periodically check that your database is properly protected against unauthorized access.	3
2. Rename your "admin" and "data" directories to help protect against unauthorized access.....	3
3. Change your passwords often, and do not use the same username/password combinations more than once.....	3
4. Make sure your web host/server admin has properly protected your web server.....	3
5. Download and Install the latest revision of PDshop periodically.	3
6. Enable all 'Recommended Security Settings' in PAdmin.	4
7. Download and Install PDScan.....	4
Terms & Conditions	5

1. Periodically check that your database is properly protected against unauthorized access.

If you installed PDshop with the default Microsoft Access database, make sure it is impossible for someone (other than you) to download/access your database file. Your database directory should be configured with special permissions (a.k.a. Security) in such a way that PDshop & PDAAdmin can read/write to the database, but no one else can see or download it. We recommend that your database be kept in a special directory that is only accessible by FTP. Consult with your web host or server administrator for their procedures and suggestions for securing database directories.

IMPORTANT: We strongly recommend that you rename your database file. You should use a unique name that only you would know. For example, do not leave your database with a name like "pdshoppro.mdb". You will need to update your setup.asp (or web.config) file accordingly.

2. Rename your "admin" and "data" directories to help protect against unauthorized access.

Since these directory names are common knowledge, as an added level of security we suggest that you rename these directories to something only you would know. You will need to update your setup.asp (or web.config) file accordingly.

3. Change your passwords often, and do not use the same username/password combinations more than once.

Change your password at regular intervals and make sure your PDAAdmin username/password is not the same as your FTP, hosting account, or server control panel logins. This can be devastating if your password is ever found or discovered thru some of the various hacking techniques.

4. Make sure your web host/server admin has properly protected your web server.

A web server with poor firewall protection, or insufficient settings, or an "unpatched" operating system, can make your website vulnerable to many internet threats, including unauthorized access, malicious attacks, and virus infection.

5. Download and Install the latest revision of PDshop periodically.

Our developers are always improving how PDshop works, for this reason revisions to each edition of PDshop are released from time to time. These revisions/updates are full versions that often contain improvements, bug fixes, critical security updates, and even new features. To download the latest revision, login to your account and click 'Your Downloads'. See the Upgrading & Installation Guides for help with installation or upgrading procedures. If you need assistance with installing these revisions/updates, contact PageDown Technology.

NOTE: If you are using a customized version of PDshop or made your own script changes, consult with your web developer or PageDown Technology before installing any revisions.

6. Enable all 'Recommended Security Settings' in PAdmin.

Since you may be hosting PDshop on a public or shared web server, as a general precaution, we do not recommend storing sensitive credit card information in your PDshop database. If you are processing credit cards, you should do so thru one of the payment gateways that PDshop supports. When processing thru the supported payment gateways, PDshop does not need to store any credit card information; it is securely passed to the payment gateway's own system for processing. Storing credit card data on your own web site can put your customer's information at higher risk. See PAdmin 'Help' for more information on these settings.

7. Download and Install PDScan

NOTE: All PDshop editions downloaded after 11/15/2006 include PDScan built-in!

Installation IS REQUIRED if PDshop was installed or downloaded before 11/15/2006!

PDScan is a free security add-on for our older, classic "ASP" Editions, of PDshop. This add-on is not required for any ASP.NET (.NET) based Editions of PDshop. The .Net Editions have a similar security tool already built in.

PDScan is a simple HTTP request scanner that can easily be "included" into any edition of PDshop. The purpose of this Add-On is to provide an extra layer of security & protection. PDScan filters all incoming http requests, such as URLs & Querystrings, Forms, and Cookies. If it detects malicious or erroneous data in an http request, the request will be rejected; it may be able to protect your website from future or unknown internet threats and exploits. If you have customized your copy of PDshop, you can still install PDScan by simply "including" it into your setup.asp file. See the PDScan Installation guide at <http://www.pagedowntech.com/install> or contact PageDown Technology for assistance.

Special Notes:

If your copy of PDshop was installed by a 3rd party, or by PageDown Technology, you need to contact the person or company who handled your installation, or you can order the "Installation Service" from PageDown Technology. To order our Installation Service, please login to your account. Click "My Account" from anywhere on the PageDown Technology website.

Terms & Conditions

This guide is intended for licensed users of PDshop only.

See the Terms & Conditions for PDshop on the PageDown Technology website, see <http://www.pagedowntech.com/terms>.

Additional Support and Information about this product can be found on PageDown Technology's website, <http://www.pagedowntech.com>.

Copyright Notice:

All Text and Images contained on this document is the property of PageDown Technology, LLC (pagedowntech.com) and cannot be reproduced, copied, or used without our written permission.

PageDown Technology, LLC / Copyright 2003-2009 All Rights Reserved