Security Recommendations for ProductCart-powered stores

We encourage you to use the following security precautions to minimize the chance of unauthorized access to your ProductCart Control Panel and store database.

1. **Rename the "pcadmin" folder (ProductCart v2.1 and above).** Once you have activated ProductCart, you can change the name of the folder that contains all the files that are used for your store's administration area (the Control Panel). By default, this folder is named "pcadmin". By renaming the folder to something that is hard to guess, you will make it virtually impossible for hackers to find the location of your Control Panel. This increases the level of security for your store as it prevents hackers to locate the Control Panel login page and run attacks against it. To rename the "pcadmin" folder, follow these steps:

    a. Activate ProductCart v2.1
    b. Locate the file "secureadminfolder.asp" in the "includes" directory and download it to your local system using your favorite FTP program.
    c. Open the file with Notepad or an HTML editor and change the name "pcadmin" to any other name that you would like to use (only use alphanumeric characters in the name). Save the edited file and reupload it to your server via FTP.
    d. Change the name of the "pcadmin" folder to the new folder name that you have just entered in the "secureadminfolder.asp" file.
    e. You are done. To log into the Control Panel, remember to edit the URL to reflect the new folder name.

2. **Change the name of your MS Access database, and of the folder that contains it**. This does not apply to ProductCart stores that use a SQL database. The MS Access database that powers your ProductCart store is named "eipc.mdb" and is stored by default in the folder "productcart/database". You can rename both the database file and the folder it to anything you like, as long as you preserve the *.mdb extension for the database file. Just remember to edit the DSN or DSN-less database connection string accordingly (you will be able to test it on the next page).

3. **Password-protect your MS Access database**. This does not apply to ProductCart stores that use a SQL database. To password protect your store database you need to download it to your computer via FTP, open it using Microsoft Access, which is part of Microsoft Office Professional, and then select "Security/Set Database Password" from the "Tools" menu. When you open the database, make sure to do so using the "Open Exclusive" option from the "Open" drop-down selection menu.

    If you password protect your MS Access database, edit your database connection string to include the password.

    For example, if you are using a DSN connection:

    "DSN=productcart"

    becomes...

    "DSN=productcart;PWD=yourPassword"

    If you are using a DSN-less connection:

    "DRIVER={Microsoft Access Driver (*.mdb)};DBQ=c:\database.mdb"

    becomes...

    "DRIVER={Microsoft Access Driver (*.mdb)};DBQ=c:\database.mdb;PWD=password"

4. **Regularly change your Control Panel password**. You can do so from within the Control Panel, under "General Settings/Change Password". We recommend that you change your Control Panel password every month or two, and whenever someone that had access to it no longer works for your company.

5. **Backup your store**. Regularly backup your store to ensure quick and effortless recovery in case your store needs to be restored for any reason (e.g. hardware failures, unauthorized access, change of Web server, change of Web hosting company, etc.). This task should be performed on a weekly basis, more often for busy stores. You should back up the following store data.

    a. Your store database (if you are using MS SQL, enquire with your Web hosting company to find out how often they back it up for you)
    b. The "includes" folder, which contains a variety of store settings (include in backup when you have edited any of the store settings)
    c. Any ProductCart files that you have modified to better meet your needs (include in backup any file that was recently edited)

6. **Disable directory browsing**. When directory browsing is disabled, Web site visitors cannot view a tree of the folders that exist within the Web site. Contact your Web hosting company to ensure that they have disabled directory browsing.

7. **Remove or rename cmd.exe**. If you are hosting your store on your own dedicated Web server, then this security tip can help you further reduce the chances of unauthorized access to the Web server. The objective of a hacker attack is often to gain full control of the victim's computer. Hackers often do so by accessing a program called cmd.exe, which allows you to execute commands on the system. We recommend that you rename, move, or restrict access to cmd.exe. Renaming it or limiting its use to members of the administrator group removes this vulnerability. This is not a generally needed file for a Web server and if it doesn't exist then it is impossible for an attacker to gain access to it.

8. **Edit the Print Settings in Internet Explorer**. If you print out order invoices from the Control Panel and send them to your customers, note that Internet Explorer by default prints the complete URL to the page at the bottom of the document. You can easily change this setting in Internet Explorer by selecting File > Page Setup and removing the characters that appear in the Footer field.