# Do You Use a Mac? Safeguard It Against “MacDefender” Malware by Understanding the Scam and Getting the Fix!

Apple announced last night that it would be sending an update to its OS X operating system that would protect users from and **remove** a program called “MacDefender” (alias “MacProtector” or “MacSecurity”) that had been finding its way onto some consumer’s machines. The program is a piece of malicious software (or “Malware“), that is ultimately designed to get you to send your credit card number to a company to sell you a program to “fix” the problem.

## Here’s how MacDefender works:

- You are browsing Google Images and when you click on an image, you are redirected to a fake “security alert” webpage.
- The security alert webpage informs you that you have been infected with a virus, and recommends you download a free program – MacDefender – to solve the issue.
- MacDefender pops up on your computer as an offering. If you click OK, you’ve just invited the malware onto your system.
- Here’s where it gets malicious. The installed malware begins to make your system appear as if it has become infected with a virus.
- The program regularly opens up new browser windows to pornographic websites. Needless to say, this is very embarrassing, as well as making computer very hard to use.
- At this point you are probably thinking “well, I just

installed a new anti-virus program", and you try to run the MacDefender program. Now it gets really nasty.

Screenshot of MacDefender

- When you runs "MacDefender" your fears are confirmed – the program does find a nasty virus – but you have another problem.
- The software is "unregistered" aka "unpaid for" so the software can only detect the malware, but not delete it. The only way to delete it is to "register" the program by sending your credit card number to pay for the software. Of course, once the Bad Guys have your credit card info, I doubt they'll stop at registering your software.

Although people had been reporting problems with the malware for a few weeks now, Apple only publicly acknowledged the problem today, and according to some reports, had been instructing support representatives to not acknowledge the problem.

Of course, Windows users have been having to deal with trojan horse programs like MacDefender for years. Traditionally Macs haven't been the target of malware, as the vast majority of the problem was with Windows machines, but why that is is a matter of opinion. Mac users say that they don't get malware because the OS X operating system has fewer security holes, and is harder to attack. Windows users generally counter that since Apple machines take up so little market share, there's no economic incentive for malware writers – who are only after money – to focus on Apple users.

So the fact that Apple had to respond to the threat with an update to its OS X, and acknowledge that malware is a problem

for their system is both a good and a bad sign for Apple. Bad in that they now have to support users against malware, and provide security updates to its OS, but good in that Mac-specific malware is definitely a sign of the platform's growing popularity.

As the Naked Security blog said in a post today "Dear Apple: Welcome to team anti-malware".