201106 SWCP Portal

Had to happen sooner or later

Phishing for Apples

By Jay Nelson, Editor

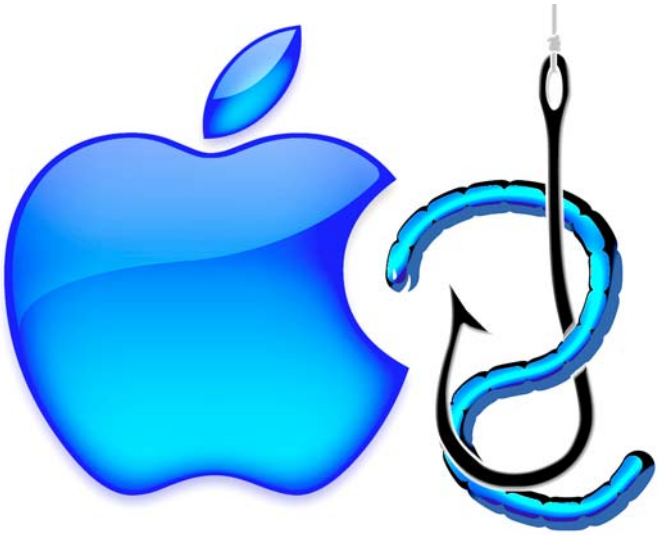
Macintosh users long enjoyed peace of mind and freedom from the malware threats which plague Windows. That simple, happy time is now sadly over. A new threat has emerged that directly targets Apple users. As of this writing, there's very much an arms race going on. The company just came out with an automatic security update, but the malware creators found a way around it within eight hours.

The signs are clear: Mac users must adopt safe surfing practices, if you haven't already. In this case so far, the new viruses are aimed at the **Safari** browser, which has an auto-install feature that **Firefox** and **Chrome** lacks. Disabling that, as described below, should make you much safer. But really, this is a case where the only thing you need to fear is fear itself. Caution and common sense are your best defenses.

Macs are better protected from viruses than Windows computers because malware can't get a toehold as easily without the user's permission. In any event, most viruses these days do *not* come from infected email but rather from deceptive webpages containing traps. This one uses a "fake virus" technique to scare you into buying and installing the virus for them.

How it works

This "**scareware**" attack starts with an official-looking pop-up or Web ad suddenly appearing to attempt to frighten you into downloading the virus by claiming the program, called something like **MacDefender**, **MacProtector**, or **MacSecurity**, has detected a threat on your machine. It offers to scan it for free.



The site then leads you to buy "antivirus software". Whatever you do, do ***not*** click "`OK`." Rather than protect your machine, MacDefender will infect it.

While pretending to scan, the virus downloads. You'll then be told your computer is infected and the software must be registered to remove the infection, which requires your credit card number. Of course, this only enables the criminals to steal money directly from your account.

This threat is actually a triple whammy: (1) you're suckered into paying for something you don't need, (2) you just gave your credit card to a criminal, and (3) the "antivirus" software is actually a virus.

Once installed, the MacDefender program can do all kinds of nasty things: stealing passwords; disabling firewall and antivirus programs, and nagging you with repeated obnoxious pop-ups to buy a fake upgrade. Therefore it's much better and simpler all around to avoid infection in the first place.

Staying safe

The easiest way to keep from being infected is really quite simple: **Don't Panic!**

Here's how to keep from falling for these scams:

- **Safari** users: Change your browser settings to prevent your computer from automatically installing downloaded programs. In Safari, go to `Preferences > General` and uncheck "**`Open safe files after downloading`**." Without auto-install active, you have to download the program and unzip the file yourself. **Think before you click.**
- If a window or strange warning pops up alerting you of infection, don't fall for the bait no matter how legitimate or Apple-looking it is. Do *not* click on any button - even "**`Cancel`**" - on *any* pop-up.

Continued on back

Southwest Cyberport
5021 Indian School NE, Suite 600, Albuquerque, NM 87110-8910 USA
swcp.com | help@swcp.com
505-232-7992
New Mexico's Leading Local Full-Service Internet Provider Since 1994

Continued from front

Click the red dot in the corner of the pane instead to kill it.

- Do not visit untrusted sites; especially those preying on a hot or unlikely news topic.
- Only install programs from reputable sources and supply your administrative password only when you intentionally install software from them.
- If you get a pop-up or email telling you to get some antivirus software that you are unfamiliar with, check it out before reacting. You can email *help@swcp.com* and ask if we know about it. Or a quick Google inquiry could be a great help.
- Be very careful of following links that come in email. **Twitter** and **Facebook** phishes have been very popular recently. They usually say something like, "You have unread notifications on Facebook", and provide a link to a page that looks identical to the real Facebook login page, but is a trap to steal your password. If you think the message might be legitimate, do not click the link in the email. Instead, type "*facebook.com*" into your browser to go to the site directly.
- **Finally, no reputable company will *ever* ask for your password or account details in email.**

First aid

Like all malware, MacDefender resists removal. You can't get rid of it simply by hauling it to the Trash. It is difficult to close, and even if dumped will relaunch itself whenever you turn your Mac back on. The malware will then do obnoxious things to encourage you to pay, like opening up constant prompts and unwanted sites in your browser. Special steps must be taken to ensure that it is completely removed.

Fortunately, MacDefender is much easier to eliminate than many nasty Windows viruses out there. So if you discover that your computer is infected, don't panic then, either. First take steps to protect your credit card account and then deal with your machine.

To remove MacDefender or other rogue software:

1. Launch the **`Activity Monitor`** by going to your **`Applications`** folder, then the **`Utilities`** folder. You can also use **`Shift+Command+U`** from the desktop.
2. Look in the list of active processes for those names that match MacDefender, MacProtector, and MacSecurity names, but realize that it might be some new variant that could have a similar but not identical name.
3. Highlight the process to select it and then click the "**`Quit Process`**" button. If a pop-up appears asking if you are sure, click the "**`Force Quit`**" button on the left.
4. Next, go back to the **`Applications`** folder, and find your rogue antivirus program. Move the program to the **`Trash`**, and then empty the Trash.

   Note: it's safe to enter your system password if prompted when emptying the Trash.
5. Now click the **`Apple Menu`** from the upper left of the desktop taskbar and go to **`System Preferences > System > Accounts`**, and click "**`Login Items`**". This will open a window with a list of programs that automatically start up when your computer does.
6. Find the name of the malware program in the list, click on it and then click the "**`Minus`**" button at the bottom of the window to remove the program from startup. This will prevent the rogue program from reinstalling itself the next time you reboot your computer.

Remember you can always call SWCP Technical Support. We'll help walk you through clearing out the malware over the phone, or you can schedule for us to do it for you in our office. Call for **505-232-7992** for more information.

Good antivirus software for Macs is commercially available, like **Intego**, or **ClamX AV**, which is free. Though not inherently much more secure than their rivals, Macs themselves are still very safe. They probably will continue to be as their more robust nature and small market share make Macs harder and less profitable to attack. Less than a dozen malware programs aim at Apple products, compared to the uncounted thousands that target Microsoft.

But no user can afford to be entirely naïve online any more. Taking a few precautions, not freaking out, and knowing that **SWCP's Tech Support** is there to help, you should surf confidently and safely, whatever system you use.

The Drums of Cyberwar Beat Ever Louder

Large, sophisticated attacks by hackers against major corporations and governments continue to keep the threat level steadily rising. Sony's popular **PlayStation** network and their movie site, for instance, were lately seriously compromised by the **LulzSec** hacker group, who posted the details of over a million users online, bragging of the exploit. They claimed it was to get Sony to increase security, but it may cost the entertainment giant over $1 billion.

Meanwhile, aerospace defense contractor **Lockheed-Martin** and **Google** have both reported serious assaults, probably from state-sponsored hackers. Also, **Chinese** hackers were said to be able to read Gmail and Hotmail of hundreds officials and activists for months, although the Chinese vehemently deny these and all other accusations.

In response, the **US** and **UK** have both announced plans to develop cyberweapons programs. Moreover, the Pentagon has announced that cyberattacks could lead to actual physical military responses. The cyberwarriors are arming up.

- Telegraph, Guardian, Wired