PUBLIC INTEREST ADVOCACY CENTRE
LE CENTRE POUR LA DEFENSE DE L'INTERET PUBLIC
ONE Nicholas Street, Suite 1204, Ottawa, Ontario, Canada K1N 7B7
Tel: (613) 562-4002. Fax: (613) 562-0007. e-mail: piac@piac.ca. http://www.piac.ca

PROTECTING YOURSELF AGAINST "DIALERS"

OVERVIEW

A "dialer" is a software application that is installed on your computer. This software generally is installed by a technology called "ActiveX". A dialer usually entices an Internet user with the prospect of free access to online content such as pornography, computer games or software piracy tools. Once installed on your computer, the dialer will deactivate your usual Internet connection and use your telephone connection to dial either an international or other long-distance number or a 1-900 or 1-976 billable number, incurring significant costs to you on your next phone bill.

Some dialers do notify the user of the connection cost, as required by law, but many are deceptive or misleading. In a worst-case scenario, the dialer establishes an Internet connection with a foreign server, at the user's expense, and saves the server's dial-up number as the user's default Internet connection, ensuring that the user continues to incur significant charges for each minute spent connected to the Internet. The victim will usually only become aware of such fraud upon receipt of her or his next telephone bill.

ARE YOU AT RISK?

If you own a Macintosh computer, your risk of contracting a dialer is significantly lower than those users running Windows. So far, dialer incidents involve Internet users with a PC running Windows. (This is not due to more effective security in the Macintosh operating system but rather is simply a reflection of the fact that the Windows operating system is currently market dominant. Thus, if dialer programs for Macintosh don't yet exist, this doesn't mean one isn't being written right now!)

If you are a high speed Internet subscriber (whether cable or DSL), you *may* be safe. This is because a "dialer" needs an analogue modem (the older dial-up modem technology) connected to a regular phone line, in order to dial a long distance number or billable phone number (e.g. 1-900 or 1-976 services). When you connect to the Internet via a high-speed digital subscriber line or cable connection, the dialer cannot use this connection. However, many computers are equipped with an internal dial-up (analogue) modem. Many high speed Internet users still keep this modem connected to a phone line even when connecting to the Internet via their high speed connection – either through neglect or in order to operate certain data services such as fax machines. If so, a dialer installed on your computer could activate and establish a telephone connection via this

modem, even if you are still connected on your high-speed Internet connection! This underlines the importance of disconnecting unused telephone (analog) modems.

Those who surf the Internet using Microsoft's Internet Explorer should be particularly vigilant, as most "dialers" use the ActiveX technology to install themselves on your computer. ActiveX is embedded in Microsoft's Internet Explorer.

HOW TO GET RID OF DIALERS

It is crucially important to remove any dialer programs on your computer as soon as possible. A number of free software applications publicly available on the Internet will purge your computer of unwanted dialers as well as of a number other problems such as 'spyware'. Two of the most reliable programs of this kind are Ad-Aware and Spybot.

Download a Free Version of Ad-Aware:
http://download.com.com/3000-2144-10045910.html?part=69274&subj=dlpage&tag=button

Download Spybot
http://www.safer-networking.org/index.php?page=download

Carefully read the instructions before using either of the above-mentioned programs and be sure that the automatic updating functions of each application are activated.

Online help is available for both of these applications:

Support for Ad-Aware
http://lavasoft.element5.com/support

Support for Spybot:
http://spybot.safer-networking.de/index.php?page=support

HOW TO STOP DIALERS – AN OUNCE OF PREVENTION . . .

Since most dialers install themselves by means of ActiveX technology, the deactivation of this technology in Internet Explorer will greatly reduce your exposure to risk. However, although ActiveX technology may allow malicious applications such as "dialers", it enables, and was written for, beneficial actions, (for example, see Symantec's website, which performs a virus scan by means of an ActiveX control. Visit: http://security2.norton.com).

However, as websites making legitimate use of this technology are, at present, relatively rare and since this technology is increasingly being used to deceive and defraud Internet users, we suggest that you deactivate ActiveX. A simple procedure for deactivating ActiveX is described below. However, remember that ActiveX is sometimes of great utility and even essential at times – the best example being the updating of the Microsoft Windows operating system via "Windows Update", also addressed below. Therefore it will sometimes be necessary to reactivate ActiveX on a temporary basis.

Another way of protecting yourself from "dialers" is to install a firewall. A firewall acts as a filter between your computer and the Internet, intercepting all suspect transmissions before they reach your computer, and only transmitting to those you authorize. Firewalls may be either hardware (such as a network router) or software. Be sure to read and understand what type of transmissions the firewall will block before using it.

ZoneAlarm is an excellent software firewall with a free trial version of its product.

Download the Free Trial Version of ZoneAlarm:
http://www.zonelabs.com/store/content/company/products/zap/trial/zap4x_trial.jsp?lid=pdb_zaptrial

Carefully read the instructions before using the product.

Online assistance for this product is available on Zone Labs' website.

Support for ZoneAlarm:
http://www.zonelabs.com/store/content/support/support.jsp?lid=nav_ss

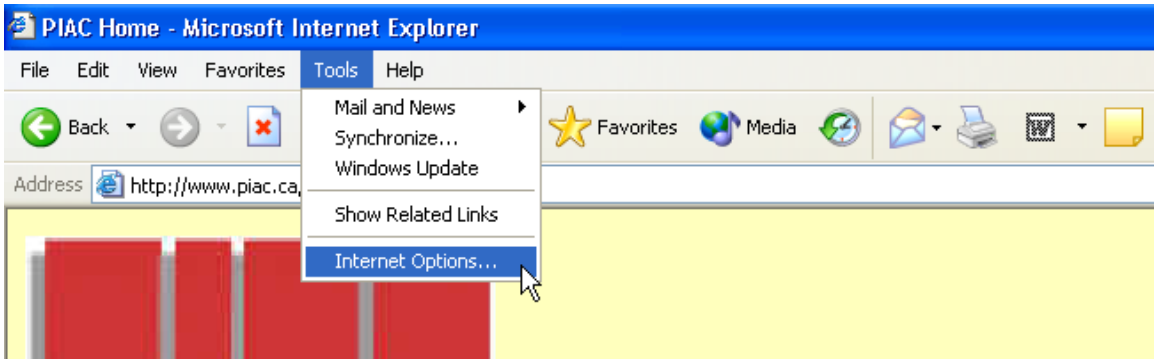
Vigilance is the key to effective protection from dialers, spyware, viruses and other problems. Dialer programs in particular take advantage of the ignorance or inattention of an Internet user to install themselves on his or her computer. They are also deceptive. Sometimes software dialog boxes authorizing the downloading of dialers are disguised as something else, like a link to a contest or even a fake image of a dialog close button. Regular Internet users know that a single mouse-click on a website can sometimes provoke a cascading avalanche of "pop-up" windows, with links to pornographic websites or simply advertising various wares or services. These windows can confuse the user and possibly induce him or her to make a misplaced mouse-click signifying consent to downloading and installing a "dialer". Be careful and teach your children about such dangers. Keeping your computer located in open area that allows for adult supervision of your children's Internet activities will also increase your protection.

DEACTIVATING ActiveX

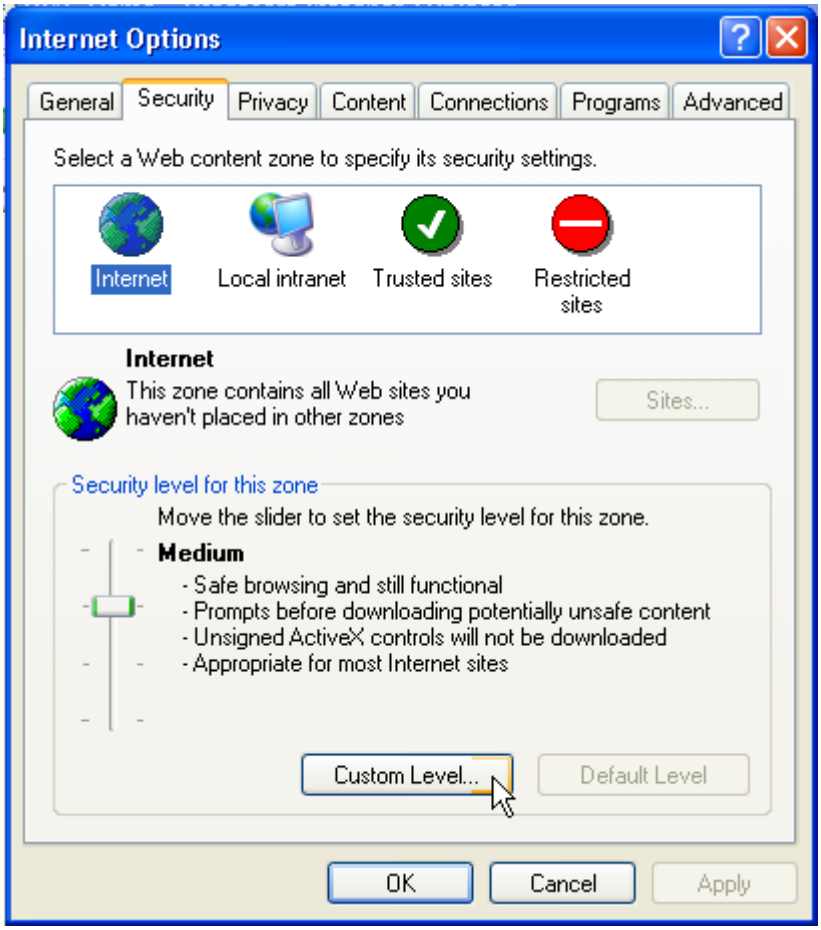
As noted above, deactivating ActiveX is one way to reduce your risk from dialer programs. The appropriate deactivation procedure varies depending on which version of Internet Explorer version you are using. The procedure described below applies to the latest version of Internet Explorer (Internet Explorer 6) and we discourage the use of older versions of this program. New security weaknesses, which can be exploited by malicious individuals, are continuously being discovered and corrected by Microsoft personnel – but their attention is focused on updating the security of the latest version. It is therefore essential to update all of your Microsoft applications and operating system with the latest security patches from Microsoft. However, this is of critical importance with Microsoft Internet Explorer. Free Microsoft security updates may be downloaded to your computer by visiting Microsoft Windows Update webpage:
http://windowsupdate.microsoft.com

These security updates should be run before you deactivate ActiveX as they may require the technology for proper installation. Once you have deactivated ActiveX (see below) you must remember to temporarily reactivate ActiveX to update your Windows security. **How to deactivate ActiveX in Internet Explorer 6.** We suggest that you either take note of the following procedure or print this page in case you desire, at a later time, to reactivate ActiveX when necessary to properly access a website making legitimate use of this technology.

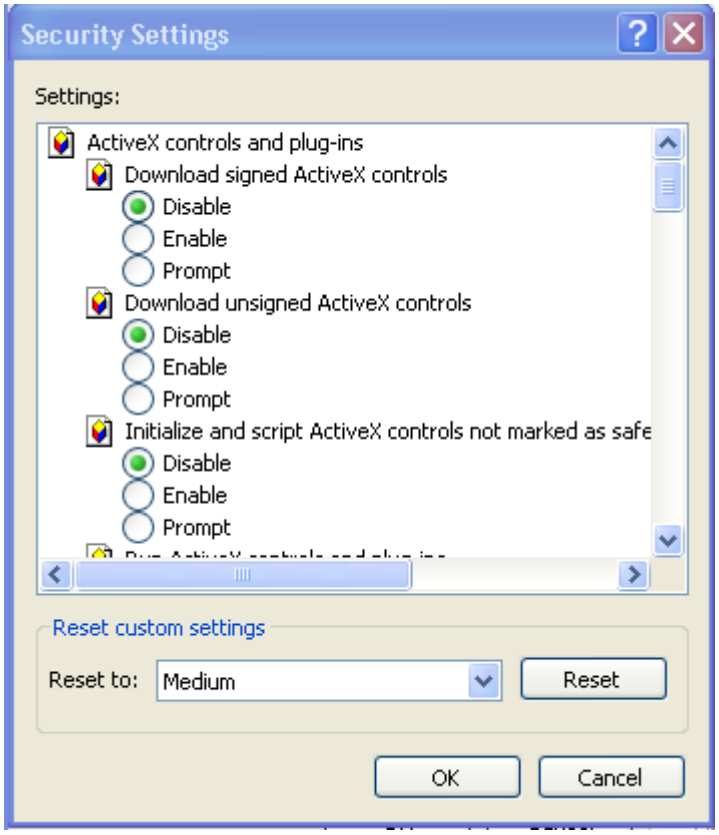
1. Start Internet Explorer
2. In the Tools menu found in your menu bar, click on “Internet Options. . .”



3. Click on the “security” tab
4. Under the “Security” tab, click “Custom Level”



5. Scroll down until you reach the ActiveX control parameters
6. Select the deactivation option in each of the 5 settings for ActiveX



7. Confirm your modifications by clicking on OK
8. Click on OK in the underlying "Internet Options. . ." window

To reactivate ActiveX controls at a later date, simply follow the above-mentioned steps until you find yourself at the "Custom Level" options. From there, click the "Activate" option for each of the ActiveX settings. When reactivating ActiveX, it is important to select the security level you desire. The "medium" security level is perhaps the most functional. However, remember that with that security level, you may be vulnerable to the results of a misplaced mouse-click or a moment of inadvertence.

An alternative to deactivating your ActiveX technology is to stop using Internet Explorer altogether and replace your browser software with one that is not initially configured to use ActiveX, for example, Mozilla or Netscape. Although these browsers do not come equipped with ActiveX, appropriate "plugins" may be installed to add ActiveX support. However, once ActiveX support is installed in any program, including these browsers, the same warnings as above apply and you should take the same security precautions.

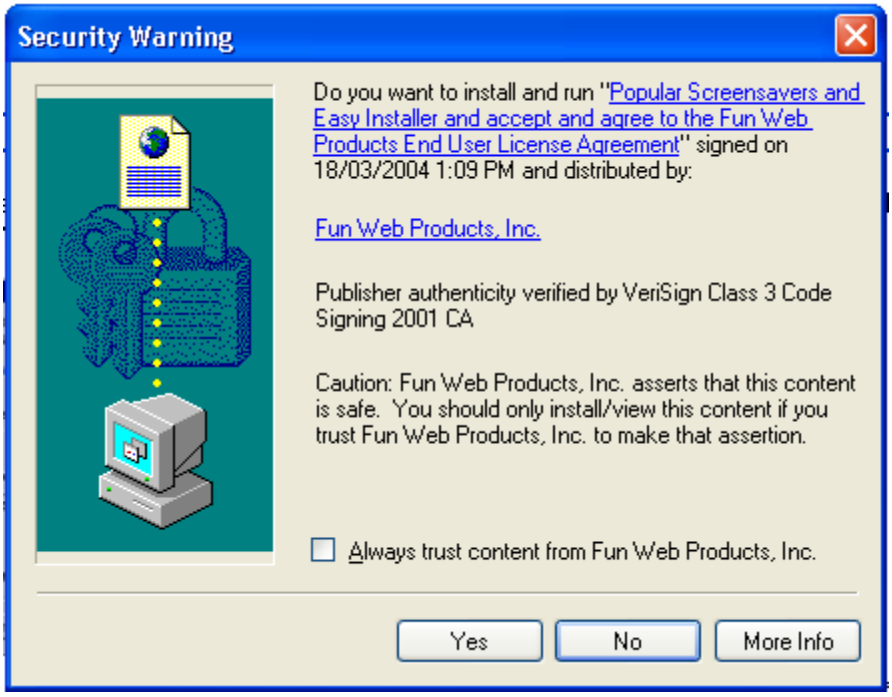
LEXICON

ActiveX
ActiveX is a Microsoft technology that permits the linking of Internet applications and desktop applications. ActiveX applications function only with Microsoft's Internet Explorer, or with other browsers via a plug-in. The use of ActiveX on websites is,

therefore, not required, but is adds the functionality of many applications to web surfing. Considering the possible effects ActiveX may have on your computer system (ActiveX applications can access most if not all files on your personal computer), it is strongly recommended that you be prudent and remain vigilant regarding use of ActiveX technology.

There are two types of ActiveX controls (code): signed and unsigned. Unsigned ActiveX code has not been certified and therefore should never be trusted. Signed ActiveX applications have been certified but may nonetheless contain corrupted code. Users should only accept those signed ActiveX controls which originate from a trustworthy website and only when you initiate the communication. To ensure this, Internet Explorer should be configured to prompt you for your authorization each time a website wishes to use a signed ActiveX control.

Many "dialers" self-install by means of ActiveX technology. The following is a screen shot example of an ActiveX control dialog box originating from a website (the example is not a dialer), prompting for authorization to install and activate itself. If for whatever reason, you have doubts about a particular ActiveX control, you should always click on the NO (do not install or allow the control to run) button.



Firewall

A firewall is a device (it may be either hardware or software) that controls the transfer of information within a computer network. Typically, firewalls are used to enhance a computer's or a network's secure access to another network (which may be the Internet – often described as a network of networks.) Firewall hardware is simply a 'box' (such as a router) placed between your local network and all other networks and which authorizes or refuses particular transfers by recourse to predetermined security configurations.

Firewall software is a program that is installed on your own computer to perform the same function as the hardware versions. Software versions offer the advantage of customizing security configurations based on the type of application transferring the data. However, software versions have the disadvantage of relying on configuration choices the Internet user, who may not always be well versed in security matters.

Crack
Refers to small downloadable programs that break or "crack" the security code of various applications. Cracks are used, for example, to permit a trial run of various programs and to deactivate them at the end of the trial period. Cracks may, however, be used by pirates to allow them to use "shareware" beyond the intended period of free use.

Spyware
Spyware are programs that transmit information identifying a computer's user over the Internet without the Internet user being made aware of the data transfer.

Spyware is not installed on your computer as a stand-alone software application. Rather, they are made up of a number of small components that the user can usually deactivate during installation. In most cases, end-user license agreements (EULAs) describe their privacy implications in a couple of well-buried lines in a long document. However, most users do not take the time to read these licensing contracts exhaustively and are often unaware of the presence of spyware on their computer system.

A variant of spyware is adware. Adware is similar to spyware though it either does not transmit your personal information or is configured so as to indicate that the entity that is collecting the information will not sell or otherwise share this collected information. Adware is generally used to collect non-identifying information of your computer activities.

Adware is also often a by-product of spyware as both such applications operate so as to track your computer activity. This is done to permit the delivery, generally in the form of "pop-ups", of advertisements purportedly tailored to your "interests".