ZIGGY ZAPATA

Guitarist Entertainer
Entertainment Agent
Computer Consultant

Ziggy Zapata Enterprises
8 Barrington Drive, Dural NSW 2158
Mobile Phone: 0414 587 586
Email: ziggy@ziggy.com.au
Website: www.ziggy.com.au
Skype: ziggy-zap
ABN: 67 640 497 765

COMPUTER SECURITY

VIRUSES, WORMS AND TROJAN HORSES

The amazing growth of the Internet has spawned a proliferation of vandals who write and spread viruses and Trojan horse programs that can wreak havoc on personal computers. Many of these programs are not created just to cause trouble, but have far more sinister purposes, such as hijacking computers to be used in bot networks for denial of service attacks to extort money, or to surreptitiously turn computers into spam machines without the consent of their owners.

Many of these programs are spread by the running of unverified software downloaded from websites, but most come in email attachments and are activated when the attachments are opened. They can be in the form of EXE, COM and Visual Basic files, Microsoft macros and a variety of other formats. Facilities such as ActiveX can compromise computers when exploited by websites set up especially to take advantage of the gaping security holes that such add-ons create.

EMAILS

Reading emails themselves will not activate viruses, so the best policy to avoid problems is to be most suspicious of all email attachments and to never open any from sources that cannot be trusted implicitly. Installing a good antivirus program with regular virus signature updates is the first line of defence, but ultimately the best safeguard is to not open any attachments and thus risk virus or Trojan horse contamination. There is an excellent virus checker at Housecall that will scan a computer on-line using the latest virus signatures and the best part is that this service is totally free. AVG has a free installable antivirus program with free updates that is excellent.

SECURITY HOLES

Software such as Microsoft Windows, Outlook Express and Internet Explorer have a long history of security holes that allow hackers to penetrate computers connected to the Internet and even remotely install malicious programs. To see how insecure the average computer can be, visit the Gibson Research Corporation website and run the Shields Up utility. Most users will be shocked to find how many ways hackers can penetrate their computers with the greatest of ease. However there are many tools and tips on this site that will enable users to secure their computers, starting with such simple measures as resetting network bindings and controlling print and file sharing.

BEWARE OF FREE SOFTWARE

Many websites, especially pornography and hacker sites offer supposedly free software or content that can be obtained by downloading a small executable piece of software. This is a most dangerous practice, because in many cases this software will install back doors on computers that allow hackers to penetrate them with total transparency. Many websurfers have been shocked to find that their personal details and content on their computers have been accessed by hackers who have then used this information literally to steal their identities and then fraudulently make unauthorised transactions.

INSTANT MESSENGER AND VoIP THREATS

Since Instant Messenger and Voice over Internet Protocol (VoIP) technology have become very popular with programs such as Microsoft Messenger and Skype, scammers have found another avenue they can use to exploit Internet users. One common technique used is when a hacker contacts an unsuspecting user and asks to download a seemingly innocuous file to that user. This file will contain a virus or Trojan horse program that will compromise the user's computer and expose it to being taken over by the hacker as a spambot or having a keylogger surreptitiously installed so that the hacker can discover secret banking details and passwords of the user.

Files containing viruses are not dangerous until they are run, so if such files are downloaded, they should be scanned by an antivirus program with the latest virus signatures to determine if they are safe or not. If a virus is detected, then the sender should be immediately blocked from being able to make further contact. In any event, it is far better to refuse all offers of files from strangers in the first place.

FIREWALLS

One of the best security measures for any computer connected to the Internet is to install a firewall. There are many different firewalls, either using hardware devices or software based types. Probably the very best software firewall is ZoneAlarm, which has so far been found to be impregnable to literally everything thrown at it. Apart from the peace of mind that using such a good product can bring, the most amazing aspect is the cost. ZoneAlarm is totally free for personal use and is easily downloaded from the ZoneAlarm website. The importance of running a firewall cannot be overstated.

ROUTERS

One of the best security measures for Internet users is to use a router. Most modern routers have built-in DHCP servers that generate IP addresses for each computer on the network, thus totally masking any sign of their presence. Many modern routers also have built-in hardware firewalls with stateful packet inspection that will monitor every piece of data in and out of the system. As an added security measure against port scanning, stateful inspection firewalls close off ports until connection to the specific port is requested by the user's computer.

Taking these few simple precautions will virtually eliminate intrusions and viruses:

- NEVER OPEN ANY EMAIL ATTACHMENTS BEFORE CHECKING THEM
- DO NOT DOWNLOAD FILES FROM STRANGERS IN INSTANT MESSENGER OR VOIP PROGRAMS
- DISABLE AUTOMATIC MACRO EXECUTION IN SOFTWARE SUCH AS MICROSOFT WORD
- CHECK UNUSUAL OR EXCESSIVE HARD DISK ACTIVITY WHEN ON-LINE
- REGULARLY SCAN FOR VIRUSES USING THE LATEST SIGNATURES
- SET NETWORK BINDINGS TO ENSURE THAT PORTS ARE NOT AVAILABLE TO HACKERS
- DISABLE FILE AND PRINT SHARING UNLESS ABSOLUTELY REQUIRED
- NEVER DOWNLOAD OR RUN SUSPECT SOFTWARE THAT COULD INSTALL A BACKDOOR
- BLOCK OR CONTROL THE USE OF ACTIVE-X AND OTHER ADD-ONS
- INSTALL A TOP-CLASS SOFTWARE FIREWALL SUCH AS ZONEALARM
- USE A MODERN ROUTER WITH A HARDWARE FIREWALL AND NETWORK ADDRESS TRANSLATION

MALWARE

Although usually not as damaging as viruses and worms, this class of intrusive and unannounced software called adware and spyware planted on the computers of unsuspecting users performs a number of invasive functions. Malware is usually installed surreptitiously while seemingly benign and usually free software such as screen savers, toolbars and other utilities are installed.

HOME PAGE HIJACK

Malware may hijack the browser's home page to make it always go to the advertiser's website and no matter how many times a user tries to revert to his usual home page, the malware will constantly forcibly change it back to the advertiser's site. It may force advertising pop-ups to appear frequently, becoming an absolute nuisance that can quickly render enjoyable websurfing into a very unpleasant nightmare.

For instance, CoolWebSearch is one of the most complex, sophisticated, and devious browser hijackers ever invented. The latest versions have grown increasingly aggressive and complicated and manual removal is virtually impossible. Complete re-installation of the entire operating system is often required, thus use of a reputable spyware remover with the latest updates is highly recommended.

SPYWARE AND KEYLOGGERS

Some malware is more discreet, transmitting the websurfing habits back to the operators so that they can survey the effectiveness of advertising. Even worse, it may even send personal or other details it gleans from a user, such as email addresses or a log of keystrokes so that the operators can target spam at the user or even raid the user's bank account.

There are effective remedies against malware. The main line of defence is to remember that very little is really free and that supposedly useful or amusing piece of software on the Internet may come with very high hidden costs.

To prevent malware infesting a computer, these measures should be taken:

- CHECK TOOLBARS, EMOTICONS AND OTHER SUPPOSEDLY FREE DOWNLOADS FOR MALWARE
- RUN SPYWARE CHECKERS FREQUENTLY WITH THE LATEST MALWARE SIGNATURES
- ALMOST NOTHING IS REALLY FREE ON THE INTERNET - THERE IS USUALLY A CATCH
- BE AWARE THAT MANY DOWNLOADS COME WITH A NASTY HIDDEN STING

COOKIES

Cookies are small text files that websites load onto computers to track activity or to facilitate navigating certain areas. For instance, most banks and internet finance institutions require their cookies to be on a user's computer to track transactions.

However, many websites plant cookies that are actually data miners that facilitate the transmission of the web surfing habits of users for targeted marketing and advertising purposes. Some cookies can actually even transmit personal data of users so that spam advertising can be sent to them.

The best way to deal with cookies is to disable their acceptance and only allow cookies to be loaded from known legitimate websites, such as banks, transaction sites such as eBay, PayPal and update sites for legitimate software. If a cookie needs to be accepted, permission can be issued on an individual basis, thus negating the open-ended acceptance of cookies from every site that wishes to plant one on a computer, enhancing security to a high degree.

HOW TO DISABLE COOKIES FOR HIGH SECURITY

- In Internet Explorer, click Tools and click Internet Options.
- When the dialogue box opens, click the Privacy tab on the top to open the Privacy section.
- Click the Advanced button and then check the Override Automatic Cookie Handling box.
- In both First Party Cookies and Third Party Cookies, select Block.
- Ensure that the Always allow session cookies box is unchecked.
- Click OK to set these parameters. Then click OK in the Internet Options dialogue box to close.

HOW TO ACCEPT INDIVIDUAL COOKIES WHILE RETAINING HIGH SECURITY

- In Internet Explorer, click Tools and click on Internet Options.
- When the dialogue box opens, click the Privacy tab on the top to open the Privacy section.
- Click on the Sites button and the Manage Sites dialogue box will open.
- Enter the URL of the site that needs to load a cookie, ie, microsoft.com, then click the Allow button.
- Add more website URLs as required.
- Click OK to set these parameters. Then click OK in the Internet Options dialogue box to close.
- If you need to unblock a URL, open this dialogue box and change its status from blocked to allowed.
- Another quick way to get to the cookie control is to click on the Privacy icon on the status bar if it is visible.
- It is wise to occasionally check the list of allowed cookies and delete any URLs that are not further required.

INTERNET DIALLERS AND CREDIT CARDS

Many Internet users have been severely shocked to receive their monthly telephone bills with thousands of dollars in overseas calls appearing on them, calls that they were convinced they did not make. Some users have actually been bankrupted by their inability to pay these debts, but wondered how this could have happened to them. The explanation is very simple.

There are a number of ways operators earn revenue from the Internet. Most reputable and well established companies selling goods and services ask for credit card details and it is generally quite safe to provide this information. Some Internet based businesses, predominantly pornography websites, charge for access and demand credit card details for payment of membership fees. Some of them operate legitimately, but others use very devious methods to part unsuspecting or gullible users from their money.

UNAUTHORISED DEBITS

One common method pornography sites employ is to offer low resolution free pictures and video clips to entice users to other areas of their websites, often called protected archives, where they can then be charged for obtaining better quality content. To obtain passwords or further access, users are asked to provide credit card and personal identification details supposedly only to verify age, often with exhortations and guarantees that no charges will ever be made to those cards. In most cases the exact opposite occurs, as users suddenly find amounts debited to their credit cards every week or month, with virtually no means of obtaining refunds.

The forms users are asked to fill in are often thinly disguised authorisations allowing charges to be made to their credit cards and cancelling such authorisations is usually very difficult, if not impossible. Often the only way to stop such continued billing is to actually cancel the credit cards, with the resultant inconvenience that this entails. However these pitfalls are easy to avoid, because as long as users refrain from providing credit card and personal information voluntarily, they cannot be legally billed. Of course if credit card numbers are somehow obtained illegally and the credit cards are used without authorisation, action can be taken to obtain refunds from the credit card providers.

DIALLERS

Due to many users now being reluctant to provide credit card information on the Internet, many porn and hacker websites have instituted a far more devious method of extracting money from unsuspecting users, the main one being the surreptitious deployment of Internet diallers. Their operation is very insidious. Users are invited to download a small piece of software to enable them to view and copy supposedly free pictures, video clips or pirated computer programs. As soon as this software is executed, it literally hijacks their modems and without indicating that anything out of the ordinary is occurring, it dials other numbers, often to third world countries such as Botswana or Nigeria, with huge per-minute overseas call rates. Even worse, these numbers are generally the premium call type that charge exorbitant fees, often around $12 to 15 per minute.

From that point, the call costs quickly accumulate as long as users stay on-line, as they still believe that they are merely connected to their local ISPs. The porn websites receive a portion of these high charges as their revenue and the users receive massive telephone bills. However as the diallers were voluntarily downloaded and run and the calls were initiated from the actual telephones of these hapless victims, they bear full responsibility for paying the bills and there is generally no recourse to obtaining refunds from the websites that employ these diallers.

Anybody who accesses the Internet should be running a good firewall as a matter of course and good practice. Apart from browsers and email client software, very few programs need to access the Internet. If a surreptitious dialler tries to access the Internet, a firewall will indicate this and the dialler can be blocked immediately.

A good measure against diallers is to block access to international phone numbers with a password or PIN. All telecommunications providers offer this service. Then if a dialler attempts to access overseas numbers, it will be stopped dead in its tracks, however legitimate calls can be made overseas by the subscriber just using the password. However, this is not always a complete remedy, as some diallers are programmed to ring a local number and divert a user's international access to another telecommunications provider and thus get access to an international line. For instance a Telstra subscriber can be caught by a dialler program that accesses another service provider such as Optus or APPT for instance, thus negating the international calling block that was put on the Telstra service.

Another good security measure is to block calls to premium services that can charge massive amounts of money per minute, such as the 1902 prefix numbers. Most of the premium services are a total waste of time and money, such as bogus clairvoyants and astrology services. The safest and simplest way to increase telephone line security is to use ADSL or cable broadband and eliminate all dialup services entirely. If a dialup modem is installed and not actually required for faxing, it should be removed or disabled.

These simple precautions should be taken to protect against such scams:

- NEVER DOWNLOAD OR EXECUTE PROGRAMS REQUIRED TO ACCESS CONTENT ON WEBSITES
- NEVER SUBMIT ON-LINE FORMS WITHOUT READING AND UNDERSTANDING THE FINE PRINT
- NEVER GIVE CREDIT CARD OR PERSONAL INFORMATION EXCEPT TO VERY REPUTABLE COMPANIES
- IMMEDIATELY DISCONNECT FROM THE INTERNET AT ANY SUSPICIOUS MODEM ACTIVITY
- ALWAYS USE A FIREWALL AND ONLY ENABLE TRUSTED PROGRAMS TO ACCESS THE INTERNET
- ENABLE INTERNATIONAL DIALLING ACCESS ONLY BY PASSWORD
- BLOCK ACCESS TO PREMIUM SERVICES NUMBERS
- CHANGE TO BROADBAND INTERNET AND ELIMINATE THE RISK ENTIRELY
- REMOVE OR DISABLE DIALUP MODEMS IF THEY ARE NOT REQUIRED