



## Privacy, Security & Virus Information

### Internet Crimes – Reporting To Authorities

Protecting yourself against Internet crime and identity theft is critically important to a successful Internet experience. It is very important to keep your firewall and Web browser up-to-date. However, it is also important to report Internet crimes to the proper authorities in order to prevent identity theft and computer hacking from spiralling out of control. There are several different Internet crime prevention programs already in place – take the time to contact them if you have become a victim of online theft.

If you become a victim – or know of someone who has become a victim – of online theft, report the incident immediately. In the event of a suspected pedophilia or online stalking complaint, reporting a suspected crime can launch a police or government investigation.

By reporting organized software piracy, improper marketing to children, or general identity theft, your reporting can lead to the reporting of statistics used to enact important legislation. Reporting of crimes also helps raise awareness in your neighbourhood and community, and also allows officials to take action to keep the event from happening again.

If you become the victim of a virus, spyware, hacking, phishing scams, spam, or consumer fraud, the authorities in charge of investigating these crimes may use your information as part of their investigation. As a result of law officials' investigations, the identity of hackers and thieves becomes much easier. This will help prevent new scams and spot new fraud trends. These reports can also be used in court if you decide to take legal action against the violators of your computer's security.

### Preventing Your Computer From Becoming a Target

Hacking, viruses, spyware, phishing scams, and spam can lead to identity theft and other serious crimes. It's easy to help stop criminals before they even start. Here are several suggestions on how deal with online theft if you become a target.

- **If you notice that your computer has become hacked or infected by a virus**, disconnect from the Internet immediately. Install updated anti-virus software and update your firewall if necessary. McAfee has several solutions to help protect your computer – consider using them.
- **If you become the victim of online crime**, report the incident immediately to your Internet Service Provider (ISP). Be sure to file a complaint with the FBI's Internet Crime Complaint Center.
- **If spyware appears on your computer**, report the incident via the FTC's Consumer Complaint Form. Once again, McAfee has a software solution that will enable you to prevent and get rid of spyware from your computer.
- **If you believe that you have become the victim of 'phishing' e-mails**, and your personal information may be in jeopardy, forward the information to [spam@uce.edu](mailto:spam@uce.edu). If you have been scammed by a 'phishing' scheme, report the FTC and take more precaution against personal identity theft.



Web Security and Maintenance Services

## McAfee Security



- **McAfee offers the program McAfee SpamKiller** that will help you defend your computer against aggressive spammers. This software will also protect you from 'phishing' scams and other security threats.

### Sexual Exploitation of Children

Always be aware of what your child is doing in cyberspace. Parental involvement and due diligence are critical factors in preventing child sexual exploitation online. Make sure you are aware of the potential threats to your child while they are online. Children can use.