Tool: ID Protect
ID Protect protects a domain owner’s contact information from becoming public. The WHOIS database contains a domain owner’s address, phone number, and other private information. ID Protect’s dynamic e-mail system constantly changes the e-mail address visible in the WHOIS database, so any spammer that harvests the address will get an invalid address. A user’s private information is held in confidentiality and protected by the Domain Privacy Protection Service. The Domain Privacy Protection Service secures and maintains the user’s real e-mail address on file so he or she receives important information regarding his or her domain.
A domain name with ID Protect can shield a user from the following:
- Domain-related spam
- Identity theft
- Data mining
- Name hijackers

U.S. Laws against E-Mail Crime: CAN-SPAM Act
The CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003) does the following:
- Establishes requirements for individuals and organizations that send commercial e-mail
- Details the penalties for violating the law
- Gives consumers the right to request that spammers stop contacting them
The law pertains to e-mail whose primary purpose is advertising or promoting a commercial product or service, including content on a Web site.
The following are the main provisions of this act:
- Header information must be accurate. The sender and recipient e-mail addresses must be correct.
- Subject lines must not be misleading. The subject of the message must relate to the content of the message.
- E-mail recipients must be given a way to opt out of receiving further messages. This method must be spelled out in each e-mail message.
- Any commercial e-mail must identify itself as an advertisement or solicitation. It must also include the individual or organization’s physical address.
The following are the penalties for violating the provisions of this act:
- Each violation is subject to fines of up to $11,000. Commercial e-mail is also subject to laws banning false or misleading advertising.
- Commercial e-mailers who also do the following are subject to additional fines:
  - Harvest e-mail addresses from Web sites that have posted a notice prohibiting the transfer of e-mail addresses
  - Generate e-mail addresses using a dictionary attack
  - Use automated methods to register for multiple e-mail accounts to send commercial e-mail
  - Relay e-mails through a computer or network without permission
The law allows the Department of Justice to seek criminal penalties for commercial e-mailers who do the following:
- Use someone else’s computer without authorization and send commercial e-mail from it
- Use a computer to relay or retransmit multiple commercial e-mail messages in an attempt to mislead recipients about the origin of the message
- Falsify header information in multiple e-mail messages and send those messages
- Register for multiple e-mail accounts or domain names using false identification information