

Avoiding Traps

Security experts and law-enforcement officials offer this advice on protecting your personal information from criminals.

- Don't respond to phone or email messages that are unsolicited or from unknown senders. Likewise, don't open or forward attachments from unknown sources.
- If a message appears to be from a financial institution, contact your financial institution directly using a phone number you obtain independently from a bank statement or phone book.
- Install firewalls and up-to-date antivirus software. Also install updates, when available, to your computer's operating system, Web browsers and third-party applications, such as RealPlayer.
- Check that a Web site connection is secure before sending information to financial institutions or retailers. Check the browser for an "s" in the prefix before a Web address so that it reads "https." Look for the padlock icon, which many browsers display to indicate encryption is in place so that information you send is less likely to be intercepted in transit.
- If you believe your computer is compromised, reset your password immediately. Change user names and passwords for any sensitive Web sites that are visited on that computer, such as banking and credit cards sites.