Town of Dublin
P.O. Box 277 Dublin, NH 03444
Phone: (603) 563-88544

Identity Theft

Dublin Police Department
1122 Main St / PO Box 283
Dublin, New Hamsphire 03444

Phone: (603)-563-8411 Fax (603)-563-5401

Identity Theft

Seven million Americans were victims last year of ID theft.~ The fastest-growing financial crime, it involves the fraudulent use of someone else's identity to get credit or merchandise.~ Follow these steps if you have become a victim and also consider the second set of tips to protect yourself from becoming a victim.

~

Report the crime.~ Filing a report with your local police and keeping a copy yourself will make it easier to prove your case to creditors and merchants and may help you build a lawsuit if you have to sue to recover losses or clear your name later. In some states, you may have to report the incident in the jurisdiction where the fraud occurred, such as the location of the store where the theft charges merchandise to your account, even if that is not where you live.

~

File a complaint.~ The Federal Trade commission (877-ID-THEFT; TDD, 202-326-2502) investigates interstate and Internet fraud.~ Download a copy of an ID theft affidavit from the FTC's Web site at www.consumer.gov/idtheft to help you notify merchants, financial institutions and credit bureaus.~ For fraud involving stolen mail, also file a complaint with postal officials at www.usps.com/postalinspectors/idthft_ncpw.htm

~

Alert credit-report report agencies.~ Use the FTC ID-theft affidavit mentioned above to help you do this.~ Call TransUnion, 800-680-7289; Experian, 888-EXPERIAN; and Equifax, 800-525-6285, to get addresses and instructions.~ Ask to have your account flagged with a fraud alert, which asks merchants not to grant new credit without your explicit approval.~ Keep copies of all your correspondence.

~

Notify banks, creditors and utilities.~ Close accounts that have been used by thieves.~ Choose new passwords and PINs for all your accounts and don't use your mother's maiden name as a password.~ Notify merchants that issued credit or accepted bad checks in your name; use your police report or FTC affidavit as backup.

~

Order your credit report each year.~ Get credit reports from all three credit bureaus, and study them closely.~ Some victims say that it took years to clear their credit files and that new credit was sometimes granted in their names without their permission even after fraud alerts were placed on their accounts.

~

Seek other help.~ For other information, check out the nonprofit Identity Theft Resource Center at www.idtheftcenter.org and the Privacy Rights Clearinghouse at www.privacyrights.org.~
~
~
Follow these tips to reduce your chances of becoming a victim.
~
Check financial statements promptly.~ Always review your monthly banking, brokerage, and credit card statements for accuracy.~ Report problems immediately.
~
Watch your credit.~ Order copies of your credit report every year from each of the three major credit reporting agencies and report errors promptly and in writing. ~They are:~
~
Equifax, 800-685-1111, P. O. Box 105851, Atlanta, GA 30348
TransUnion, 800-888-4213, P.O. Box 1000, Chester, PA 19022
Experian, 888-397-3742, P.O. Box 2002, Allen, TX 75013
~
Be stingy with information.~ Never disclose your Social Security number, birth date, or mother's maiden name unless you initiated the transaction.~ On paper documents, don't include such data unless required to do so on an official application for employment, financing, or insurance.~ Never put such information on personal Web pages or publicly posted resumes or directories.~
~
Just say no.~ Consider opting out of information-sharing at your financial institutions.~ (Check your company's financial privacy notice, which is mailed annually and usually posted on company Web sites, to find out how.)~ Also opt out of pre-approved credit offers by calling the Credit Reporting Industry Pre-Screening Opt-Out Number at 888-567-8688.
~
Travel light.~ Don't carry ID that contains sensitive data like your Social Security number unless absolutely necessary.
~
Lock it up.~ Safeguard your driver's license and other government ID at all times.~ Lock desks, cabinets, and safes containing such information in your office and home.
~
Shred and destroy.~ Before throwing out files containing Social Security numbers, account numbers, and birth dates, shred them with a cross cut shredder.~ Destroy CD's or floppy disks containing sensitive data by shredding, cutting ore breaking them.~ Use hard drive shredding software or remove and destroy your hard drive before discarding a computer.~ Just deleting files isn't enough.
~
Guard mail.~ Consider using a locked mailbox or slot to receive mail at home.~ Deposit mail in postal mailboxes or in the post office to discourage mail theft.
~
Keep your eye on the prize.~ Try not to let waiters, sales clerks, or gas-station attendants disappear from view with your credit or debit card, to avoid "skimming."~

Crooks can use a handheld card reader to copy the information from your car's magnetic strip.
~
Beware of strange ATMs.~ Avoid using private or strange-looking automated teller machines, because they may be rigged to skim data off your card's magnetic strip.~ Six or seven character PINs are harder to crack than shorter ones, but you may not be able to use them at machines abroad.
~
No surfing allowed.~ Watch out for "shoulder surfers" when using pay phones or public Internet access; use your free hand to shield the keypad.~ Don't use cordless phones to conduct sensitive financial or medical business, because eavesdroppers on other phones and those using eavesdropping equipment may be able to overhear your conversations.
~
Build a wall.~ Install firewalls and virus detection software on your home computers to discourage hackers.
~
Log off.~ Quit your browser and log off after using public Internet-access computers in libraries, Internet cafes, and the like.~ Don't pay bills, bank, or conduct other financial transactions on public computers.~ If you have a high-speed Internet connection at home, unplug the computer's cable or phone line when you are not using it to discourage hackers.
~
Deal only with reputable Web sites.~ Check privacy and security policies of Web sites before making purchases, trading stocks, or banking online.~ A professional-looking Web site is no guarantee of security.~ Don't respond to unsolicited e-mail requests for personal information.
~
Get complicated.~~ Consider password-protecting all your bank and brokerage accounts.~ Create passwords at least eight characters long.
~
Check your workplace.~ Ask how your employer safeguards employee records.~ Request that Social Security numbers not be used as employee numbers.
~