



### 10 Check Your Credit Report

Credit reports contain information about you such as a listing of your accounts and your bill paying history. If an ID thief has opened up an account in your name, it will turn up on your credit report.

Order a free credit report once a year from each credit bureau to check for accuracy and possible fraud. You can order free credit reports online at [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling 1-877-322-8228.

#### The Westchester County Department of Consumer Protection

112 East Post Road, 4th Floor  
White Plains, New York 10601

(914) 995-2155  
FAX (914) 995-3115

8:30 a.m. to 5 p.m.  
Monday through Friday

Visit our website:  
[www.westchestergov.com/consumer](http://www.westchestergov.com/consumer)

Westchester gov.com  
Robert P. Astorino, Westchester County Executive  
County Board of Legislators

# Worried about identity theft?

## Top ten ways to avoid it.



DEPARTMENT OF CONSUMER PROTECTION



Identity theft occurs when someone steals personal information such as your social security or credit card number, and uses the information to obtain credit, merchandise or services in your name.

You probably won't know that you're a victim of identity theft until you get billed for something you didn't order or your credit card statement lists purchases that you didn't make.

Identity theft can happen to anyone. Indeed, the Federal Trade Commission reports that ID theft affects up to 10 million Americans each year.

Unfortunately, you can't completely eliminate the possibility that your identity will be stolen. However, you can make it a lot harder for the ID thieves. Here are ten ways to safeguard your personal information and reduce the risk of identity theft.

Robert P. Astorino  
County Executive



### 1 Watch for "Shoulder Surfers"

When using your credit card or debit card in public, or filling out a form that calls for personal information, look out for people standing close by. If you're not careful, someone can easily look over your shoulder to obtain - - and, with the advent of cell phone cameras, photograph - - your card number, PIN number or other personal information. Shield the keyboard or paperwork to prevent others from seeing your entries.

### 2 Shred Sensitive Documents

ID thieves known as dumpster divers often rummage through the trash looking for documents that contain personal identifying information, such as bank statements, credit card bills and receipts, pre-approved credit card solicitations, and tax returns.

Therefore, it's important that you shred all papers containing personal information before you throw them away. This simple action makes it impossible for ID thieves to read your personal data.

As a public service, the county has purchased a paper-shredder truck to help residents destroy unwanted papers and documents that contain personal identifying information. The Mobile Shredder is available at all Household Recycling and Electronic Waste Days, and makes additional appearances throughout the county.

### 3 Keep Sensitive Documents Out of Sight in Your Home and Office

A visitor or contractor who enters your home or office - - or even a roommate - - can put you at risk of identity theft by swiping documents that contain personal identifying information.

Do not leave sensitive documents such as check-books and bank statements in plain view. Keep them in a secure place. Don't make it easy for someone to have access to your personal information.

# MOBILE Shredder



## 4 Safeguard Your Mail

Thieves know to look for mailboxes with the red flag up - - it their cue to steal outgoing mail. That's why outgoing bills and other correspondence that contain personal information should be mailed at the post office or in a blue postal collection box, not using an unlocked mailbox at the end of your driveway. Otherwise, it's easy for someone to steal your mail - - and your identity.

Your incoming mail - - such as bank statements, credit card bills and pre-approved credit card solicitations - - can also be a treasure trove of personal information about you. Collect your mail promptly each day. If you'll be away, ask someone you trust to collect your mail or have the mail held at the post office.

## 5 Only Write Four Digits Of Your Account Number on Checks

Your outbound checks can be a source of information for identity thieves if you write your entire credit card, mortgage or loan account number on the "Memo" line of the check. That's because a check is handled by dozens of people during the check cashing process. These include employees of the credit card company, the bank and the vendor.

Although you are routinely asked to write your entire account number on the "Memo" line of the check, you don't have to comply. Instead, just write the last four digits of your account number. It's enough to link your payment with your account (especially if you include the stub portion of the bill with your payment), but you won't have given your entire account number to everybody who handles your check during the cashing process.

Similarly, when paying your taxes, you should never write your entire social security number on the "Memo" line of the check. Again, just write the last four digits.

## 6 Shop Safely Online

Shopping online is a convenient way to avoid crowds and save gas. But to protect your personal information from identity thieves, make sure that the website you are using is secure.

Many websites scramble sensitive information, such as your credit card number, so that it can be read only by the merchant you are dealing with and your credit card issuer. Look for the picture of an unbroken key or closed lock in your browser window. Also, make sure that the web address on the page that asks for your credit card information begins with "https" instead of "http."

## 7 Don't Get Phished

Phishing is an email scam that lures personal information from unsuspecting victims. Someone will send you an unsolicited email falsely claiming to be from a bank, credit card company or other legitimate business. The email states that there's a problem with your account and directs you to contact the company immediately by clicking on a link that takes you to the company's website. The email may even claim to be from a governmental agency such as the Internal Revenue Service, and state that you're entitled to a refund.

If you click on the link in the email you are directed to a bogus, look-alike website - - not the real thing.

Once you've reached the website, you are prompted to input personal information such as your social security number, credit number or password - - supposedly to confirm your identity. However, if you provide the information that is requested, you've just handed it to the identity thief.

To avoid being phished, don't reply to emails that ask for personal or financial information, and don't click on links in the message. Instead, if you need to reach an organization that you do business with,

call the number on your statement or the back of your credit card. If you wish to contact the company via the Internet, type the company's web address into the browser box.

## 8 Beware of Vishing (or voice phishing)

Vishing is a scam that attempts to trick people into supplying sensitive personal information via the telephone.

Here's how it works: You're contacted by phone. The caller says he or she is from the security department of your credit card issuer and claims that your account has been compromised or needs updating or verification. The caller already has personal information about you, including your credit card number. That creates a false sense of security. Then the caller says "we need to verify that you are in possession of your card," and asks for the three or four digit security code on the back of the card. Armed with that additional piece of information, the con artist can now process charges against your account - - even with vendors which require the security code.

Vishing uses Voice over Internet Protocol (VoIP) technology that makes Internet phone calls cheap, anonymous and difficult to trace. Additionally, VoIP allows for Caller ID "spoofing," which makes it appear that the call is actually coming from the consumer's financial institution. However, the call could be generated from anywhere in the world.

If you receive an unsolicited call from someone who claims to work for the security department of your bank or credit card company, hang up immediately if the caller asks you for personal information. Financial institutions don't request identifying information over the telephone, as they already have that information on file. Call your bank or credit card company using the telephone number on the back of the card or on your billing statement and report the incident.

To verify that a call about your account is legitimate, ask the caller to provide his or her name and department. Then call back using the number listed on the back or your credit card or on your billing statement.

Don't automatically trust the authenticity of a call based on Caller ID. Con artists can make it appear that the call is coming from your financial institution.

## 9 Secure Your Wireless Router

Many people use a wireless router so they can access the Internet from anywhere in their home. However, wireless (or Wi-Fi) networks are more vulnerable to security problems than wired forms of networking. Anyone within range can theoretically tap into your network and steal confidential data.

While there are security features built into wireless networking products, most manufacturers turn them off by default because it makes the networks easier to set up. This effort to make wireless networking more user-friendly has rendered most equipment completely insecure from the moment it comes out of the box.

There are a number of steps you can take to secure your wireless network. One of the easiest ways to guard a network from attack is to set up a personal firewall. You can also protect your network by changing your default SSID (network name), disabling SSID broadcasting, scrambling or encrypting your data, and blocking casual intruders by restricting network access to devices with an authorized Media Access Control (MAC) address. For more information see [www.westchestergov.com/consumer](http://www.westchestergov.com/consumer).