

# Anytime Adviser—Identity Theft Coach

Welcome.

This interactive guide coaches you to safeguard your personal and financial records from fraud and identity theft.

## ***Introduction***

First, let's see how well you're currently protecting your identity.

On each page, select the phrase that best completes the sentence. Last year, an estimated 10 million Americans became victims of identity theft. On average, a victim spends \$500 and 30 hours resolving the problems.

How secure is your identity?

Select the phrase that best completes the sentence. Choose A, B, or C.

---

Q1 I review my monthly credit card statements to confirm they contain only purchases I initiated...

- A Never.
- B Couple of times a year.
- C Monthly.

Reviewing your statement is one of the best ways to detect fraudulent use. Learn more in the "Safe at Home" chapter.

---

Q2 When reading e-mail, I click on links to visit Web sites...

- A Usually.
- B Rarely.
- C Depends on who sent the message.

The chapter on "E-mailing Precautions" explains the dangers of visiting Web sites through links from official-looking messages.

---

Q3 Annually, I request a copy of my credit report to check for signs of identity theft...

- A Never.
- B From one credit bureau.
- C From all three credit bureaus (Equifax, Experian, and Trans Union).

Requesting annual reports from all three can help you identify misuses of your identity. The "Annual Credit Check" chapter explains what to look for when reviewing your credit reports.

---

Q4 My Social Security number (SSN) appears on my check, driver's license, or some other ID in my wallet.

- A True.
- B I don't know.
- C False.

Keeping your SSN off items you routinely carry in your wallet will also keep it out of the hands of pickpockets. The "Paying in Person" chapter has more tips.

---

Q5 When shopping online I make sure the site is secure before giving payment information...

- A Never.
- B Only when I shop at a new site.
- C Always.

The "Buying Online" chapter shows you how to ensure a site is secure and not a spoofed site.

---

If you answered "A" 1 or 2 times: Good. You're already looking for ways to protect your identity. Feel free to skip ahead to the chapters on the left that can help you most.

If you answered "A" 3, 4, or 5 times: Your current behaviors put your identity at risk. Be sure to view this entire guide for preventive steps you can easily take. Safeguarding account numbers, passwords, and identification numbers is the best way to prevent identity theft, which can range from fraudulent charges to the worst-case scenario where your identity is linked to a criminal's record.

## **Are you familiar with common methods of stealing identities?**

Which is not a common method of stealing your identity?

- Stealing your wallet or purse
- Dumpster diving
- Shoulder surfing
- Phishing
- Mind reading
- Mail theft or diversion

Common identity theft methods include:

- Stealing your wallet or purse
- Dumpster diving
- Shoulder surfing
- Phishing
- Mail theft or diversion

Mind reading is not a technique to steal your identity, but the rest are.

## **How do thieves use stolen identities?**

How thieves use stolen identities

- Make purchases on your credit card and have statements sent to a different address.
- Open new accounts.
- Drain your checking and savings accounts.
- Establish wireless service.
- Open car loans in your name.
- Give your name when arrested.

This quick guide coaches you to:

- Spot common methods of identity theft.
- Implement safeguards to prevent identity theft.
- Identify the signs of identity theft.
- Take action when you suspect identity theft.

## ***Safe at Home***

Let's take a look through a home to spot ways thieves might steal your personal and financial records.

Select the best description of the problem shown.

---

**Photo of outgoing mail tucked next to home mailbox.**

- A) Rain might get the envelope wet. (True, but try again to find how your personal information can be stolen.)
  - B) Anyone can take this envelope. (Yes. Anyone can take this envelope, which contains your credit card number, name, and address.)
  - C) Wind might blow the envelope away. (True, but try again to find the greater danger.)
- 

**Photo of someone getting mail out of a mailbox.**

- A) The kids brought in the mail, and dropped a piece outside. (While this can be a problem, there's a greater concern. Try again.)
  - B) The mail carrier was late today. (While this may be inconvenient, there's a greater concern. Try again.)
  - C) This mailbox is accessible to anyone. (Yes. Make sure your mailbox is secure. Consider a locked mailbox—some allow anyone to deliver, but only those with a key can remove.)
- 

**Photo of IRS refund check sticking out of an envelope.**

- A) Several people handle a refund check; whereas an electronic payment is secure.
- B) Thieves often rummage through mailboxes on the days checks typically arrive.
- C) Paper checks are more expensive to issue and process than electronic transactions.

Trick question! All three are true. Your identity is better guarded when you establish direct deposit to your credit union account for regular payments and refunds.

---

**Photo of several months of statements from the same creditor in a pile of mail.**

- A) Looks like no one reads the mail here. (Try again to find the real danger here.)
- B) There may be a great offer in the bottom of this pile that is about to expire. (Try again to find the real danger here.)
- C) Months of statements have gone unread, meaning this person has no idea if her credit card is being misused. (Yes. Compare your statements with your

actual charge slips each month to detect misuse. Check more often if your credit union offers online access.)

---

**Photo of credit card offers and statements in the trash can.**

- A) "Dumpster-diving" thieves can steal your identity right out the trash. (Yes. Be sure to confetti (or cross-cut) shred all paper statements, utility bills, and especially preapproved credit applications. To opt out of most preapproved credit card offers, call 888-5OPT-OUT.)
  - B) Raccoons might get into this can and eat your financial records. (Try again. This doesn't impact your identity.)
  - C) Someone forgot to put the can at the curb this week. (Try again. This doesn't impact your identity.)
- 

**Photo of financial records and checkbook sitting on a desk next to a window.**

- A) Someone needs to get organized. (Look for a threat to your identity. Try again.)
  - B) In the event of a break-in, thieves would have any easy time finding your financial records. (Yes. Store records out of sight. These records are clearly visible from a window! Keep originals of official documents--car title, deed, birth certificate--in a safe deposit box.)
  - C) This person has too many accounts. (Look for a threat to your identity. Try again.)
- 

**Photo of an empty mailbox.**

- A) The mail carrier is late today. (While inconvenient, there's a real problem here. Try again.)
  - B) This mailbox isn't large enough to hold packages. (Try again. Look for a threat to your identity.)
  - C) This is the third day of no mail, and monthly statements usually arrive by now. (Yikes! Perhaps your mail has been stolen or a thief may be diverting your mail with a change of address. Contact the post office and the credit union.)
- 

Another way thieves gain personal information is by asking you in a phone solicitation.

Listen in while my friend poses as a good Samaritan.

**Caller**

**Pat**

Hello, is Patricia Johnson there?

This is Pat.

Good. I'm calling because I think we found your credit card. Can you give me your card number to verify?

I didn't realize I'd lost it. Can you tell me where you found it?

I don't think I should give that out until you've verified the number on the card. Can you read it to me off one of your statements?

Maybe I should check with the credit union.

Look, I've got to go.

Listen in while my friend poses as a salesman.

**Caller**

**Pat**

Hello, is Patricia Johnson there?

This is Pat.

Good. Pat, how are you doing tonight?

Fine thanks. Can I help you?

Actually, I'm calling with great news for you. As a special promotion, we're offering you and your family half price tickets to Waldo's Water World.

Wow, that's nice.

Great. You can use these tickets anytime. How many would you like?

Pat: I'm not sure. Can you send me the information?

You know, I'd like to. But this offer is good only today, and you save about \$15 a ticket.

Well, thanks for calling, but I'll have to take a pass. Good-bye.

Don't give personal information over the phone to strangers, and don't buy over the phone.

On phone solicitations:

- Don't authorize payment over the phone.
- Ask for the offer to be sent to you in mail.
- Check with Better Business Bureau and you state's attorney general to ensure this is a legitimate company.

Opt out of many telemarketing calls at [www.donotcall.gov](http://www.donotcall.gov) or 800-382-1222.

## ***E-mailing Precautions***

An even more popular way for thieves to gain your personal information is over the Internet.

In minutes, a thief can purchase millions of e-mail addresses for less than \$10; send phony "urgent" messages (called "phishing") that lead to a "spoofed" Web site—then try to scare you into revealing private information.

Spoofing = Copying the look of a legitimate Web site for fraudulent use.

Phishing = Phony e-mails using spoofed/fake Web sites that try to fool you into revealing personal financial data.

New scams are detected daily. See current phishing scams at [www.antiphishing.org](http://www.antiphishing.org).

Consider these Internet precautions:

- Protect the data stored on your computer with current virus software.
- Install firewall software through your operating system (included in Windows XP).
- Read mail only from senders you know.
- Do not open attachments. (If it's from a friend, verify first.)

Now, let's look at actual phishing e-mail messages.

### **Typically, they use a generic greeting.**

This is a phishing message. Notice the message is addressed to "Microsoft Customer"—not to you specifically. This same message may have gone to millions.

### **Does the message refer to an "urgent problem"?**

This phishing message is trying to rattle you into immediately giving away personal information. In this case, you could contact Yahoo directly to verify this message.

### **Check the Web addresses for any links.**

Check the URL, which is the Uniform Resource Locator or Web site address. Roll over any links or submit buttons, and the URL will appear at the bottom of your browser window.

This message goes to a spoofed/fake site. Notice the long, suspicious URL. A spoofed site may look just like a legitimate site and attempts to trick you into giving out personal data.

Do not give out over the Internet:

- Social Security number (SSN)
- Account numbers
- Passwords
- Mother's maiden name
- Birth date
- PIN

With this information, a thief could open new accounts using your identity.

### **Beware of pop-ups, which often don't reveal the address line.**

A clever phishing message linked to the legitimate Citibank site, but also opened a pop-up that is spoofed. Notice the address line is hidden in the pop-up, so you don't see the spoofed URL. Your best clue is that no legitimate company would ask you for personal information on a site that wasn't secure.

### **Does this site look secure?**

This is a spoofed site. There is an "S" after HTTP to indicate it's secure, but you're actually looking at a fake URL in a text box, covering the real one. Look closer, and you can see how the text box slightly overlaps the bottom of the address window.

Does this site look secure to you? Notice the closed padlock. This is a spoofed site. There is a closed padlock symbol, but it appears in the page, not the browser. This is not a secure site.

Here is a real site. Notice the closed padlock in the lower right corner of the browser window. Double click on the padlock, and you'll see a certificate, authenticating the Web site.

If you receive a phishing e-mail:

- Do not follow the link.
- Do not reply.
- If you have an account with this company, contact it directly.
- Forward the message to the Federal Trade Commission (FTC) at [spam@uce.gov](mailto:spam@uce.gov).
- Consider installing a spam blocker, free from [www.antiphishing.org](http://www.antiphishing.org).

## ***Buying Online***

Buying online can be efficient, fun, and safe—if you exercise caution before giving out your credit card number and expiration date.

How careful are you when buying online? Try this quiz. We'll keep score.

For each question, select one answer.

---

Q1 The safest companies to buy from online are...

- A) Only U.S. companies. (Actually, internationally based companies can be completely safe, as long as it's a company you know.)
  - B) Companies I know. (Yes. Buying from companies you know is your best bet, even if it isn't offering the lowest price.)
  - C) All companies. (No. Buy from companies you know. Many sites offering too-good-to-be-true prices are just that.)
- 

Q2 For online purchases, pay...

- A) By check or credit card. (No. Using a credit card gives you protection in the event of a dispute. A third party intermediary also may offer protection. With cash and checks, you're on your own.)
  - B) By check or intermediary, such as PayPal (No. Using a credit card gives you protection in the event of a dispute. A third party intermediary also may offer protection. With cash and checks, you're on your own.)
  - C) By credit card or intermediary, such as PayPal (Yes. Using a credit card gives you protection in the event of a dispute. A third party intermediary also may offer protection. With cash and checks, you're on your own.)
- 

Q3 You find a unique item online, but you've never bought from this company. What can you do to minimize risk?

- A) Check out the company with the Better Business Bureau. (Yes. Visit [www.bbb.org](http://www.bbb.org) for an online reliability report on any company.)
  - B) Call the company, and grill them for details on the item. (No. You'd learn more by visiting [www.bbb.org](http://www.bbb.org) for an online reliability report on any company.)
  - C) You can't. Skip it. (No. If you really want the item, visit [www.bbb.org](http://www.bbb.org) for an online reliability report on any company.)
- 

Q4 What should you check before giving payment information?

- A) Make sure you're not over budget. (No. To protect your identity, ensure the site is secure, with an "S" in the URL after "HTTP" and a closed padlock in the bottom right of your browser.)
- B) Check for a padlock on the payment page. (No. A padlock on the page is just a piece of art. Check for a closed padlock in the bottom right of your browser and an "S" in the URL after "HTTP.")

- C) Ensure the site is secure. (Yes! To protect your identity, ensure the site is secure, with an "S" in the URL after "HTTP" and a closed padlock in the bottom right of your browser.)
- 

Q5 How can you ensure the padlock symbol is a true sign of a secure page?

- A) If it's a closed padlock, it's secure. (No. It's best to double click on the padlock to view the certificate. It should be registered to the same company from which you're buying.)
- B) Double click it to view the certificate. (Yes. The certificate should be registered to the same company from which you're buying.)
- C) Call the company to verify. (This is no guarantee. Double click on the padlock to view the certificate. It should be registered to the same company from which you're buying.)
- 

Q6 You're an eBay user, and get a message to reauthenticate your credit card data on this page. What do you do?

- A) This is a spoofed site, not an eBay page. Forward the message to the FTC at [spam@uce.gov](mailto:spam@uce.gov).
- B) This site is not secure (no "S" after "HTTP"). Do not give information.
- C) Do not follow a link to give private information. Contact eBay directly at [www.eBay.com](http://www.eBay.com).

Trick question. All answers are correct. This is an unsecured spoofed site; not an eBay site.

---

How did you do?

Remember to shop with companies you know, and ensure the site is secure before you give payment information.

## ***Paying in Person***

When you step out your door, you're probably carrying a lot of private information with you. Here are some steps to protect it.

**Protect your identification and credit cards from pickpockets.** Button the pocket with your wallet; zip shut your purse.

**Limit the number of I.D. and credit cards you carry.** If they are stolen, you'll have fewer to replace.

**Ensure your Social Security number does not appear on any of your I.D. cards.** If your Social Security number is used as your driver's license number or appears on other I.D. card, ask the issuer for a new card with a different account number.

If your Social Security number is printed on your checks/share drafts, contact your credit union to reorder checks without it. Also consider removing your driver's license number.

**Keep your birth certificate and Social Security card in a safe deposit box.** Carry these items with you only on days you specifically need them.

How much information should you give a merchant when you pay by check? Our shopper, Francesca, is paying for a pair of shoes by check. The sales clerk asks to see her driver's license and a major credit card. What should she do?

- A) Turn over her license and a credit card.
  - B) Offer her phone number instead.
  - C) Show her license and credit card, but request the clerk not write this information on the check.
  - D) Leave—this is private information, and the clerk has no business asking.
- 
- A) Turn over her license and a credit card--Possibly, but Francesca should ensure the clerk stays in her sight and doesn't write this information on her check. If the clerk insists, Francesca might decide to shop elsewhere.
  - B) Offer her phone number instead--She can offer, but the clerk is just trying to confirm Francesca's identity. It's okay to show a license and credit card, but don't allow the clerk to write this information on the check.
  - C) Show her license and credit card, but request the clerk not write this information on the check--Yes. The clerk is just trying to confirm Francesca's identity, but there is no need to write this information on the check.
  - D) Leave—this is private information, and the clerk has no business asking-- Francesca need not leave. The clerk is just trying to confirm Francesca's identity, but there is no need to write this information on the check.

When paying in person, it's up to you to decide how much identification to show. A merchant can ask for additional identification to confirm your identity. If you're uncomfortable with this, explain you don't give out that information. If the merchant persists, pay with cash, use a debit card, or shop elsewhere.

## ***Warning Signs***

What happens when thieves steal your identity?

When thieves steal your identity, they can...

- Run up charges on your account.
- Open new accounts in your name.
- Take out loans.
- Give your name in an arrest.

Watch for these signs that someone has stolen your identity:

- Fraudulent charges on your credit card statement.
- Credit card or bank statements don't arrive.
- Bills arrive for goods or services you didn't request.
- Suspicious inquiries on your credit report.
- Phone calls from creditors.
- Suddenly denied credit.

## ***Annual Credit Check***

If someone is applying for credit in your name and you haven't noticed any warning signs, you're likely to catch this by annually reviewing your credit report from all three credit bureaus.

Why all three bureaus? Few lenders report to all three bureaus. You get the full story when you order all three reports. You can contact any one bureau to order all three reports.

Beginning in 2005, the federal Fair Credit Reporting Act requires all three credit bureaus to provide you a free credit report, at your request, every 12 months.

Working together, the bureaus have established a single, secure web site and phone number to meet this requirement. Do not contact the bureaus directly. Instead contact **[www.annualcreditreport.com](http://www.annualcreditreport.com)** (877-322-8228). Note: You will be asked to provide your Social Security number.

### **What types of information appear on a credit report?**

Test your skills.

Is this on a credit report?

YES

- Credit history
- Bankruptcy records
- Credit inquiries

- Previous addresses
- Loan records

NO

- Criminal record
- Medical history
- Checking accounts
- Savings accounts
- Race

When you receive your credit reports, check all information for accuracy, especially personal and current accounts information.

Take a close look at the list of credit history inquiries. This section is often divided in two. One is requests initiated by you (to get a loan, a credit card, or insurance). Look for suspicious entries, such as credit cards or loans issued for which you did not apply. The other type of inquiry is requests initiated by others (to offer you a preapproved loan or credit card, most often). These promotional inquiries do not affect your credit.

If you find an error in one of your accounts (such as late payment) write the credit bureau to begin an investigation—you can do this online. The dispute process can take up to 30 days.

If you find a fraudulent account, call the bureau and ask for fraud victim assistance.

Remember to request your credit history each year. If you're looking for convenience, ask your credit union about service plans that automatically monitor your credit.

## ***Report Suspicions***

If you suspect your identity is being misused, take action.

### **Five Steps to Reclaim Your Identity**

**Step 1:** If suspicious, place a fraud alert on your file with all three credit bureaus:

- Experian, 888-397-3742
- Equifax, 800-525-6285
- TransUnion, 800-680-7289

**Step 2:** Close all accounts that were affected.

It may help to write down all the facts regarding the situation in an I.D. Theft Affidavit and file it with all affected creditors.

Download the FTC's I.D. Theft Affidavit (PDF) from <http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf>

**Step 3:** File a police report and keep a copy. An over-worked police department may indicate that this won't do much good, but insist on it.

**Step 4:** File a complaint with the FTC. Your complaint can help law enforcement officials track down identity thieves and stop them. Call 877-438-4338 to file a complaint with the FTC.

**Step 5:** Alert your credit union and all your unaffected creditors. A fraudulent charge may have been reported to them, causing a change in your rates.

To learn more about recovering your identity, download the I.D. Theft kit prepared by the Federal Trade Commission.

Thank you for taking this I.D. Theft course.