For example, ATMs require a bank card (something you possess) and a PIN (something you know). In contrast, passwords are associated with single-factor authentication used for networks, Web sites, and other situations in which the hardware for dealing with ID cards is not available.

PASSWORD HACKS

◗ **How serious is password theft?** To a hacker, obtaining the password for a specific user ID can be even more rewarding than a burglar figuring out the combination to a house safe. Once hackers get into a user account, a wealth of personal information can be at their fingertips. This information could be anything from juicy e-mail gossip to Social Security numbers, credit card numbers, bank account numbers, health data, and other private details. When someone gains unauthorized access to your personal data and uses it illegally, it is called **identity theft**. Victims of this increasingly common crime often don't realize what has happened until it's too late.

TERMINOLOGY NOTE

Hacker can refer to a skilled programmer or to a person who manipulates computers with malicious intent. The terms *black hat* and *cracker* are also used to refer to a malicious or criminal hacker.

Armed with your password and other personal data, a cybercriminal can rack up bills using your credit card, apply for a mortgage using your financial data, create fake accounts in your name, send embarrassing e-mail messages, or wreak havoc on your bank account. Once a thief breaks into an online account, he or she can also change your password and you will no longer be able to log in. Password theft is serious and pervasive, so it is important to understand how hackers get passwords and how you can protect yours.

◗ **How can hackers get my password?** Hackers employ a whole range of ways to steal passwords. Some primitive means include shoulder surfing, which is looking over your shoulder as you type in your password, and dumpster diving, which is going through your trash.

Password thieves can easily find your password if you write it down on a yellow sticky note hidden under your keyboard or in plain sight on top of your monitor. If a hacker doesn't have physical access to your work area but your computer is connected to a network, your password can be discovered by a hacker using a remote computer and software tools that systematically guess your password, intercept it, or trick you into revealing it.

A **dictionary attack** helps hackers guess your password by stepping through a dictionary containing thousands of the most commonly used passwords. Password dictionaries can be found on black hat sites and packaged with password-cracking software, such as John the Ripper. Unfortunately, dictionary attacks are often enough to break a password because many users choose passwords that are easy to remember and likely to be in the most commonly used list (Figure 1-42).

FIGURE 1-42

Some of the most commonly used passwords are included in the dictionaries packaged with password-cracking software. These passwords (listed in order of popularity) should not be used.

12345
abc123
password
computer
123456
tigger
1234
a1b2c3
qwerty
123
xxx
money
test
carmen
mickey
secret
summer
internet
service
canada
hello
ranger
shadow
baseball
donald
harley
hockey
letmein
maggie
mike
mustang
snoopy
buster
dragon
jordan
michael
michelle
mindy
patrick
123abc
andrew
bear
calvin
changeme
diamond
matthew
miller
ou812
tiger
trustno1
12345678
alex
apple
avalon
brandy
chelsea
coffee
dave
falcon
freedom
gandalf
golf
green
helpme
linda
magic
merlin
molson
newyork
soccer
thomas
wizard
Monday
asdfgh
bandit
batman
boris
dorothy
eeyore
fishing
football
george
happy
iloveyou
jennifer
jonathan
love
marina
master
missy
monday
monkey
natasha
ncc1701
newpass
pamela
pepper
piglet
poohbear
pookie
rabbit
rachel

The **brute force attack** also uses password-cracking software, but its range is much more extensive than the dictionary attack. Because it exhausts all possible combinations of letters to decrypt a password, a brute force attack can run for days to crack some passwords.

If hackers can't guess a password, they can use another technique called **sniffing**, which intercepts information sent out over computer networks. Sniffing software is used legitimately by network administrators to record network traffic for monitoring and maintenance purposes. The same software can also be used for illicit activities. If your user ID and password travel over a network as unencrypted text, they can easily fall into the hands of a password thief.

TRY IT!

How fast can you guess the password for this account?

Log in

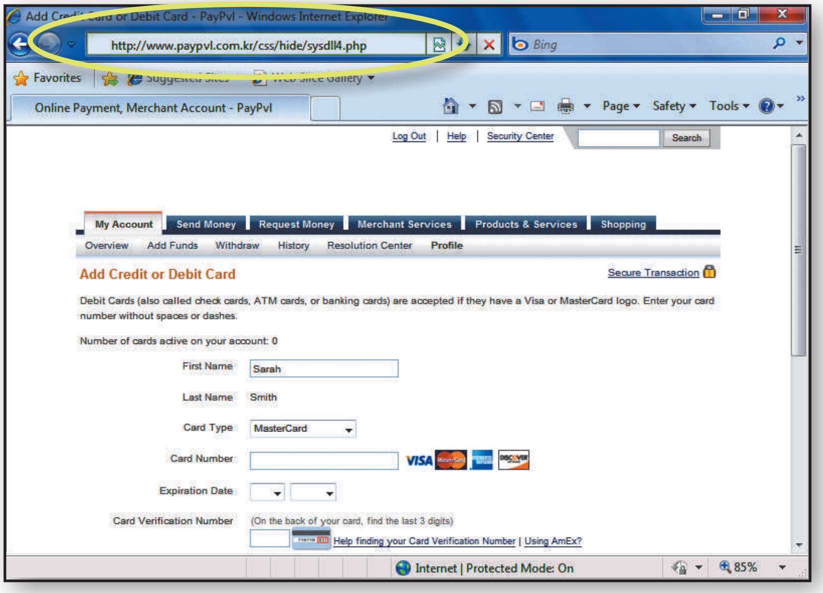
User name:

Mickey@gmail.com

Password:

An even more sophisticated approach to password theft is **phishing**, in which a hacker poses as a legitimate representative of an official organization such as your ISP, your bank, or an online payment service in order to persuade you to disclose highly confidential information. Mostly through e-mail or instant messaging, a fake customer representative or administrator asks you to visit a Web page to confirm billing information or verify your account by providing your password, credit card number, or Social Security number.

If you examine phishing messages more closely, you might realize that the Web sites referred to are fake. However, seasoned hackers try to make the URLs look as close as possible to the official Web sites they claim to represent (Figure 1-43).



Add Credit or Debit Card

Debit Cards (also called check cards, ATM cards, or banking cards) are accepted if they have a Visa or MasterCard logo. Enter your card number without spaces or dashes.

Number of cards active on your account: 0

First Name: Sarah

Last Name: Smith

Card Type: MasterCard

Card Number:

Expiration Date:

Card Verification Number: (On the back of your card, find the last 3 digits)

Help finding your Card Verification Number | Using AmEx?

FIGURE 1-43

A fake Web site can look very similar to the real thing, but this fraudulent site originates in Korea. Do you notice that the URL is www.paypvl.com.kr instead of the legitimate *www.paypal.com*? You should avoid clicking links in e-mail messages that attempt to get you to confirm or renew account data.

As users became better at identifying phishing messages, password thieves resorted to the use of keyloggers. Short for *keystroke logging*, a **keylogger** is software that secretly records a user's keystrokes and sends the information to a hacker. A keylogger is a form of malicious code called a Trojan horse, or Trojan. Trojans are computer programs that seem to perform one function while actually doing something else. They can be embedded in e-mail attachments, software downloads, and even files. Trojans are discussed in more detail in the security section of the Software chapter.

SECURE PASSWORDS

How do I create a secure password? With password theft becoming more and more widespread, security experts recommend using a strong, secure password for financial transactions such as those that involve PayPal, iTunes, or bank accounts. A strong, secure password is one that is easy to remember but difficult to crack. Figure 1-44 offers guidelines for selecting secure passwords and avoiding ones that are easily crackable.

FIGURE 1-44

Tips for Creating Secure Passwords

⬆

- Use passwords that are at least eight characters in length. The longer the password, the tougher it is to crack.
- Use a combination of letters, numbers, and special characters such as $, #, if permitted.
- Use uppercase and lowercase letters if the hosting computer is case sensitive.
- Use a passphrase based on several words or the first letters of a verse from a favorite poem or song. For example, the words from the nursery rhyme “Jack and Jill went up the hill” can be converted to jjwuth. You can then insert special characters and numbers, and add some uppercase letters to create a password that still makes sense to you personally, such as J&J w^th!ll. This type of password appears random to anyone else but you.

⬇

- Do not use a password based on public information such as your phone number, Social Security number, driver’s license number, or birthday. Hackers can easily find this information, and other personal facts such as names of your spouse, children, or pets.
- Avoid passwords that contain your entire user ID or part of it. A user ID of bjeffe coupled with a password of bjeffe123 is an easy target for password thieves.
- Steer clear of words that can be found in the dictionary, including foreign words. Dictionary attacks can utilize foreign language dictionaries. Even common words spelled backwards, such as drowssap instead of password, are not tricky enough to fool password-cracking software.

How do I protect my password? Once you have selected a strong password, you must take steps to keep it safe. Do not share your password with anyone. Avoid writing down a password. If possible, memorize it. If you must write down a password, do not leave it in an obvious place such as under your keyboard or mouse pad. Recording passwords in an unencrypted file stored on your computer is risky, too, especially if you have more than one password. A hacker who gains access to that file can use the passwords to access all your accounts.

If you think one of your passwords has been compromised, change it immediately. Even if you have no evidence of password tampering, security experts recommend that you change passwords periodically, say every six months. When you change your passwords, do not just make a slight variation to your current one. For example, do not change just4Me1 to just4Me2. You should not reuse your old passwords either, so it’s best to keep a password history list.

TRY IT!

Which password for Dave Meyers is most secure?

○ DaveBMeyers

○ Dave12345

○ Gilgamesh

○ Ih2gtg8pw

○ HomeGilgamesh