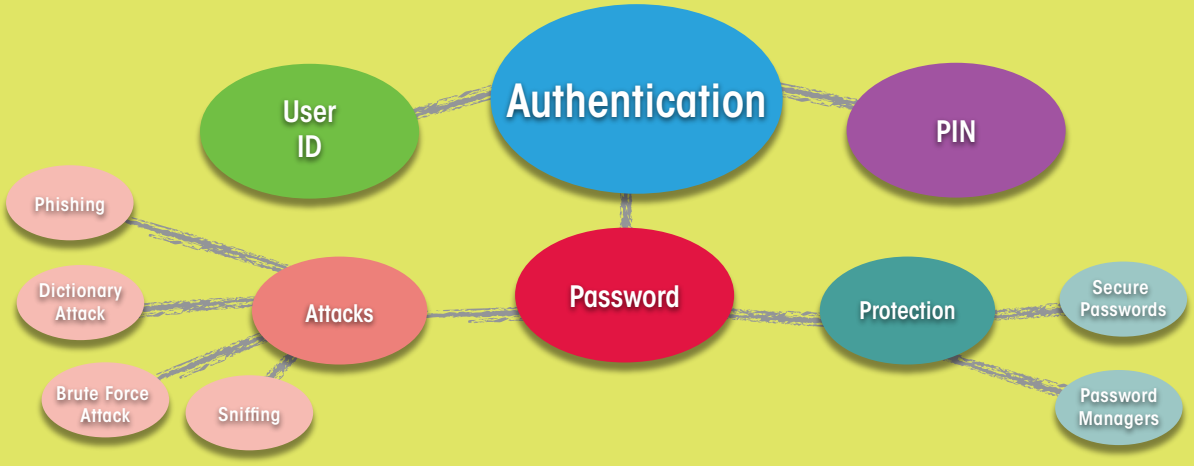

Password Security

SECTION E

USER IDS, passwords, and personal identification numbers (PINs) are a fact of everyday life in the information age. They are required for activities such as using ATMs and debit cards, logging in to Windows, accessing wireless networks, making an iTunes purchase, instant messaging, reading e-mail, and file sharing. Many Web sites encourage you to sign up for membership by choosing a user ID and password. Section E provides information about selecting secure passwords and managing the mountain of passwords you collect and tend to forget.

AUTHENTICATION PROTOCOLS

What is an authentication protocol? Security experts use the term **authentication protocol** to refer to any method that confirms a person's identity using something the person knows, something the person possesses, or something the person is. For example, a person might know a password or PIN. A person might possess an ATM card or a credit card. A person can also be identified by **biometrics**, such as a fingerprint, facial features (photo), or a retinal pattern (Figure 1-40).

Authentication protocols that use more than one means of identification are more secure than others. Two-factor authentication, which verifies identity using two independent elements of confirmation such as an ATM card and a PIN, is more secure than single-factor authentication, such as a password. Computer-related security is primarily based on passwords associated with user IDs. The level of protection offered by single-factor authentication depends on good password selection and management on the part of users.

What is a user ID? A **user ID** is a series of characters—letters and possibly numbers or special symbols—that becomes a person's unique identifier, similar to a Social Security number. It is also referred to as a user name, login, screen name, online nickname, or handle. User IDs are public. Because they are not secret, they do not offer any level of security.

The rules for creating a user ID are not consistent throughout all applications, so it is important to read instructions carefully before finalizing your user ID. For example, spaces might not be allowed in a user ID. Hence, the underline in brunhilde_jefferson is used instead of a space. There might be a length limitation, so Ms. Jefferson might have to choose a short user ID, such as bjeffe. It is becoming common to use your e-mail address as a user ID; it is unique and easy to remember.

FIGURE 1-40

Biometric authentication protocols include retinal scans that identify unique patterns of blood vessels in the eye.

TRY IT!

When you use a debit card, you have to enter your PIN. This is an example of:

- ❍ single-factor authentication
- ❍ single user ID
- ❍ two-factor authentication
- ❍ password security

Some computers that host password-protected resources don't differentiate between uppercase and lowercase letters, and would consider the user IDs B_Jefferson and b_jefferson to be the same. Other computers are **case sensitive** and differentiate between uppercase and lowercase. On such computers, if Ms. Jefferson selected Brun_Jeff as her user ID, she would not be able to gain access by typing brun_jeff.

What is a password? A **password** is a series of characters that verifies a user ID and guarantees that you are the person you claim to be. Although you might be assigned a password, more commonly you are asked to provide your own. In some situations, you might be given a temporary password and then be asked to change it as soon as you successfully log in for the first time. Passwords and user IDs are created on a registration or enrollment screen similar to the one in Figure 1-41.

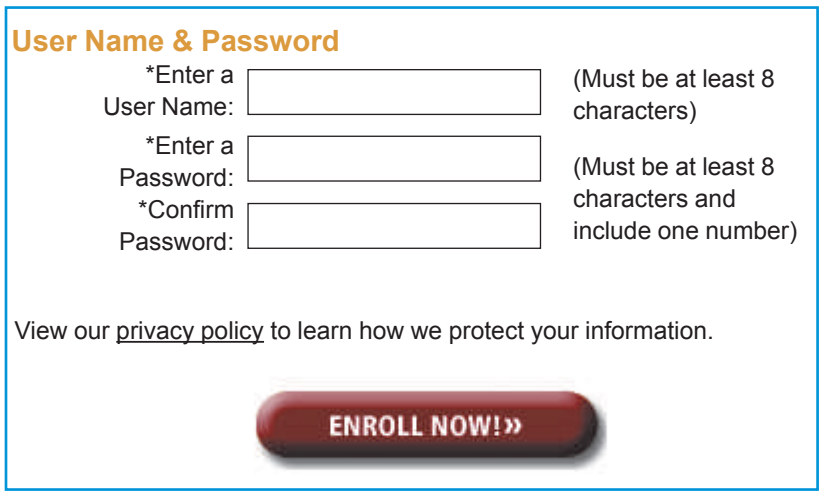

FIGURE 1-41

When you create an account, you are usually required to enter a user ID and password. Then you are required to confirm the password to make sure you typed it correctly.

What if I forget my password? Login screens for many applications provide a "forgot my password" link. Clicking this link checks your identity using your answer to a personal question. If your identity checks out, your password is e-mailed to you. A personal question provides an alternative authentication protocol to ensure that you are not a hacker pretending to be a legitimate user who has lost a password.

Personal questions and answers are usually set up at the same time you create an account. After selecting a password, you are required to choose a question that you must answer before your forgotten password is e-mailed to you. This question might be something like: *What is your mother's maiden name?*, *What is your favorite color?*, or *Where were you born?* You should be careful about the question you choose because public information like your mother's maiden name or the town of your birth can be researched by any hacker.

What is the difference between a password and a PIN? Both passwords and PINs are classified as *something-the-user-knows* authentication methods. In practice, PINs tend to be a short sequence of numbers that can be entered using a numeric keypad, whereas passwords tend to be longer sequences of letters, numbers, and special characters that require a full qwerty keyboard for entry. PINs are commonly used with two-factor authentication protocols, whereas passwords are used in conjunction with single-factor authentication protocols.

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