Chapter 15

Accounting on the Internet

After reading this chapter, you will:

1. *Understand* some of the basic concepts of the Internet, such as TCP/IP, URLs, and web page addresses.
2. *Appreciate* why electronic communication is useful to accountants.
3. *Know* why XBRL is important to financial reporting.
4. *Understand* electronic data interchange (EDI), and why it is important to AISs.
5. *Know* the differences between business-to-consumer and B2B e-commerce.
6. *Appreciate* the privacy and security issues associated with e-commerce.
7. *Know* why businesses use firewalls, proxy servers, and encryption techniques.
8. *Understand* digital signatures and digital time-stamping techniques.

"It is important to understand that e-commerce is simply a tool to conduct business efficiently, so you still need a sound business model. It doesn't really change what you do, but rather the way you do it."

Heather Douglas, ''E-Commerce and the Home Business''
NZ Business (June 2006), p. 63.

INTRODUCTION

Most accountants use the Internet for research, education, and email on a daily basis. Auditors regularly evaluate their client's internal controls to ensure complete, accurate, and authentic transmissions of transactions over the Internet. In fact, it's nearly impossible to imagine how accountants would accomplish their various job responsibilities without the many technologies that support today's businesses.

This chapter describes the Internet and some of its accounting uses in detail. The first section describes Internet components such as Internet addresses and software. This section also discusses some Internet concepts of special importance to accountants (i.e., intranets and extranets). We also discuss XBRL, a financial reporting language, in this section.

One of the most important uses of the Internet is for electronic commerce (e-commerce)—the topic of the next section of this chapter. Although the terms e-commerce and e-business are often used interchangeably, there *is* a difference. E-commerce involves buying and selling electronically, and can be between two businesses, between a for-profit company and a governmental entity, between a business and a customer, and other similar combinations. We use the term e-business to describe the electronic infrastructure that supports e-commerce. Here, we discuss such vital concepts as retail sales, e-payments, electronic data interchange (EDI), and virtual PBXs.

As more organizations conduct at least some business on the Internet, it is only natural that managers increasingly recognize the importance of Internet privacy and security. This includes protecting consumers' personal privacy, protecting proprietary data from hackers, and safeguarding information that businesses send to one another over the Internet. The final section of this chapter discusses these topics in detail.

THE INTERNET AND WORLD WIDE WEB

The **Internet** is a collection of local and wide-area networks that are now connected together via the Internet backbone—i.e., the main electronic connections of the system. Describing the Internet as an ''information superhighway'' makes sense because over 1 billion people from around the world now use it, just as a set of state, interstate, and international highways connect people physically. Almost all universities are connected to the Internet, as are most commercial information services, businesses, government agencies, and not-for-profit organizations. This section of the chapter discusses Internet basics, including Internet addresses and software, intranets and extranets, the World Wide Web, IDEA, groupware, electronic conferencing, and weblogs.

Internet Addresses and Software

To transmit data over the Internet, a computer uses an Internet address and a forwarding system that works much the same way as the post office system. On the Internet, the initial computer transmits a message to other computers along the Internet's backbone, which in turn relay the message from site to site until it reaches its final destination. If the message is large, Internet computers can divide it into smaller pieces called *data packets* and route each of them along different routes. The receiving computer then reassembles the packets into a complete message at the final destination.

An Internet address begins as a **domain address**, which is also called a **uniform resource locator (URL)**. This is a text address such as ''www.Name.com.uk.'' As suggested by this generic example, the lead item indicates the World Wide Web. The second entry designates the site name, and the third entry (''com'' for commercial user) is the organization code. Other organization codes are ''edu'' (education), ''gov'' (government), ''mil'' (military), ''net'' (network service organization), ''org'' (miscellaneous organization), and ''int'' (international treaty organization). Finally, a domain address can include a country code as well—for example, ''ca'' for Canada, ''uk'' for the United Kingdom, or ''nz'' for New Zealand.

For transmission purposes, Internet computers use tables of domain names that enable them to translate a text-based domain address such as www.Wikepedia.org into a numeric **Internet protocol (IP)** address such as 207.142.131.248. The elements in this address contain a geographic region (''207''), an organization number (''142''), a computer group (''131''), and a specific computer (''248''). The IP address enables Internet computers to deliver a specific message to a specific computer at a specific computer site—for example, send an email message to a friend at another university using the standard **Transmission Control Protocol (TCP)/Internet protocol**. IP addresses are useful to auditors because they help identify the sender, which is an important control in e-commerce applications.

Intranets and Extranets

Because Internet software is so convenient to use, many companies also create their own **intranets** for internal communications purposes. These computer networks use the same software as the Internet but are internal to the organization that created them. Thus, outsiders cannot access the information on intranet networks—a convenient security feature.

Companies, governmental entities, military organizations, and educational institutions are all finding many uses for intranets. These systems allow users to access and interact with a range of internal databases. Advanced search engine technology coupled with an intranet can deliver user-defined information when needed. For example, a purchasing agent can access a centralized listing of approved vendors using his or her web browser and a local area network.

Another valuable use of an intranet is for gathering and disseminating information to internal users. For example, employees can collaborate with each other by posting messages and data on the internal network, updating records, checking out job postings, completing forms to request office supplies, and entering travel expenses through their organization's intranet. Universities offer many of the same services to their employees, as well as a similar variety of services and educational opportunities to students.

Case-in-Point 15.1 Students at Baylor University's Hankamer School of Business have direct access to *The Wall Street Journal Online* through the university's intranet. Baylor

was one of the first academic institutions to implement intranet-based access to the journal through a recently launched Journal-in-Education service. Although students do not need to register, they still have access to all of the online journal's regular personalization features, including company and industry tracking, email alerts, portfolio and interactive tools, and special reports with interactive graphics.[1]

Extranets enable selected outside users to access corporate intranets. Users connect through the Internet itself via passwords or private data communications channels. The following is an example.

Case-in-Point 15.2 Chamberlain Group, Inc., distributes door operators, gate operators, and telephone entry systems. The firm's extranet helps the independent dealers who sell its products place orders, view invoices, obtain return authorizations, track warranty claims, and download manuals in PDF format. The company is particularly proud of its "resource center"—a separate portion of its website—which allows dealers to obtain advertising assistance, download high-resolution logos and pictures of products, and even TV and radio commercials.[2]

The World Wide Web and HTML

The multimedia portion of the Internet is commonly called the World Wide Web or just "the web." As you probably already know, you view these graphics using a web browser such as Microsoft's Internet Explorer. A typical entity on the web is a web page—i.e., a collection of text, graphics, and links to other web pages stored on Internet-connected computers.

HTML. Developers typically create web pages in an editing language such as **hypertext markup language (HTML—** see Figure 15-1a). Web designers store these instructions in one or more files and use the Internet to transfer these pages from a source computer to a recipient computer using a communications protocol such as **hypertext transfer protocol (HTTP)**. Your web browser then deciphers the editing language and displays the text, graphics, and other items of the web page on your screen (Figure 15-1b).

Because HTML is an editing language, many of its instructions are simply pairs of tags that instruct a web browser how to display the information bracketed by these tags. Thus, in Figure 15-1a, note that the entire file begins with an <html> tag and ends with a closing </html> tag. Similarly, the and tags bold and unbold text, and the and tags begin and end italicized text. Using Figure 15-1b, you can probably guess the purpose of anchor tags (beginning with <a>), ordered-list tags (beginning with <ol>), and list-item tags (beginning with <li>). Problem 15–18 is an exercise to help you understand HTML tags.

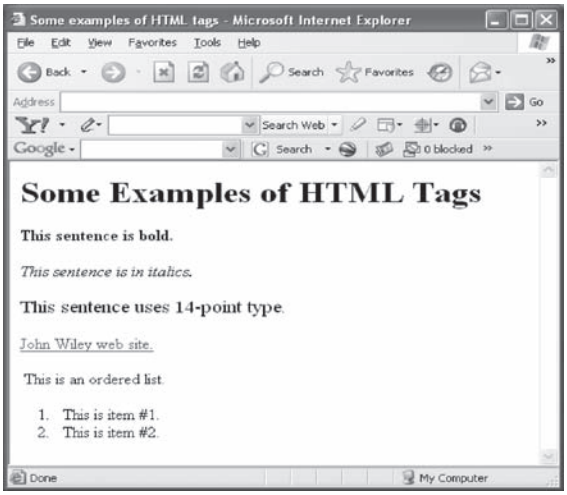
Groupware, Electronic Conferencing, and Blogs

Groupware allows users to send and receive email, collaborate on work tasks, make revisions to the same document, schedule appointments on each other's calendars, share files and databases, conduct electronic meetings, and develop custom applications.

[1]Source: P. Li. "Baylor University offers business students intranet access to the Wall Street Journal Online," *College Planning & Management* (January 2004), p. 8.
[2]Source: no author. "The Chamberlain Group Updates its Extranet", *Security Distributing and Marketing* Vol. 37, No 10 (October 2007), pp. 26–27.

```
<html>
<title>Some examples of HTML tags</title>
<body lang=EN-US style='tab-interval:.5in'>
<h1>Some Examples of HTML Tags</h1>
<p><b>This sentence is bold.</b></p>
<p><i>This sentence is in italics.</i></p>
<p><span style=font-size:14.0pt>
This sentence uses 14-point type
</span>
</p>
<p><a href="http://www.wiley.com">John
  Wiley web site</a></p>
<p>This is an ordered list.</p>
<ol><li>This is item #1.</li>
<li>This is item #2.</li>
</body>
</html>
```

(a) HTML code



(b) What the code in part (a) displays

FIGURE 15-1 An example of HTML code and what that code displays in a web browser. Note the anchor tag <a>, which allows you to create a link to another web page—in this case, the Wiley website.

Examples of such software include Exchange (Microsoft), Groupwise (Novell), Lotus Notes (Lotus Development Corporation) and Outlook (Microsoft).

Instant messaging software enables remote users to communicate with each other in real time via the Internet. You are probably already familiar with such software if you use MSN Messenger, Yahoo Messenger, or Internet Relay Chat (IRC) to chat with distant friends. Many of these packages also support audio, video, and **electronic conferencing (**enabling several users to join a discussion instead of just two). Accounting applications include the ability to interview job applicants remotely, consult with clients about tax or audit problems, discuss projects from several remote sites, or plan corporate budgets.

Large consulting and accounting firms have access to a wealth of information within their organizations. Groupware is one of the technologies behind **knowledge management** that many professional service firms (such as accounting and consulting firms) use to distribute expertise within the organization (frequently on its intranet). This information includes descriptions of clients' best practices, research findings, links to business websites, and customized news. For example, an employee with a client issue can access the knowledge database to learn how others handled similar issues.

Weblogs or **blogs** are collaboration tools that allow users with web browsers and easy-to-use software to publish a personalized diary online. Blogging introduces a new way to create, share, and leverage knowledge in an organization, and therefore can be valuable to accountants. Enterprise blogs provide companies with easy-to-use tools to manage internal and external information, which in turn affects relationships with customers, partners, and investors, as well as internal decision-makers.

Case-in-Point 15.3 The U.S. Department of Defense's Naval Undersea Warfare Center (NUWC) in Newport, R.I., uses TeamPage enterprise blogging software to create a secure communications hub for a project to evaluate night-vision technology. The blog is part of a pilot project to speed up communications within the DOD's test and evaluation programs. NUWC will blog information about its tests of the night-vision technology so the information is available in real time to its partners (Ford Motor Co. and the U.S. Army's night-vision lab).[3]

[3]Source: Linda Rosencrance, ''Blogs Bubble into Business,'' *Computerworld* (January 26, 2004), p. 23–4.

XBRL: FINANCIAL REPORTING ON THE INTERNET

Although the Internet supports general financial reporting, exchanging financial information between trading partners often requires more detailed specifications. XML or **eXtensible Markup Language** is similar to HTML in that it also uses tags such as and to format data. But there are two important differences between HTML and XML. One is that XML tags are ''extensible,'' allowing users to define their own tags such as <SalesRevenue>. The other difference is that the XML tags actually describe the data rather than simply indicate how to display it. For example, if a business wants to report sales revenue of $1 million, it could use the XML tags: <SalesRevenue> $1,000,000 </SalesRevenue>. Now, this data item has meaning.

A problem with XML tags is a potential lack of consistency among users. For example, your company might use the XML tag <SalesRevenue> but another company might choose <Revenues>. Without standardized markers (tags), users cannot exchange financial information or extract data from XML files for comparison purposes. **XBRL** or **eXtensible Business Reporting Language** solves this problem by standardizing the tags that describe financial information in documents for both profit and not-for-profit organizations. In short, XBRL is a specialized subset of XML for reporting financial information. Figure 15-2 provides an example of XBRL code and what that code creates.

The XBRL International Consortium (discussed below) creates XBRL standards that anyone can use, license-free. In addition, many accounting software packages are now *XBRL-enabled*, meaning that they can insert appropriate XBRL tags automatically in user financial files.

XBRL Instance Documents and Taxonomies

XBRL documents are called **XBRL instance documents** because they are examples (''instances'') of a class of documents defined by a standard or specification. Figure 15-2 shows an example—a portion of an income statement in XBRL. In this example, note that

XBRL code:

```
<ifrs-gp:CashCashEquivalents contextRef=''Current_AsOf'' unitRef=''U-Euros''
      decimals=''0''>1000000</ifrs-gp: CashCashEquivalents>
<ifrs-gp:OtherAssetsCurrent contextRef=''Current_AsOf'' unitRef=''U-Euros''
      decimals=''0''>200000</ifrs-gp: OtherAssetsCurrent>
<ifrs-gp:AssetsCurrentTotal contextRef=''Current_AsOf'' unitRef=''U-Euros''
      decimals=''0''>1200000</ifrs-gp:AssetsCurrentTotal>
```

What the XBRL code displays in a web browser:

Current Assets:	
Cash and Cash Equivalents	1,000,000
Other Assets, Current	200,000
Current Assets, Total:	1,200,000

FIGURE 15-2 An example of XBRL code and what that code creates.

XBRL tags follow conventional HTML and XML coding rules that use a beginning tag such as <ifrsgp:OtherAssetsCurrent> and an ending tag such as </ifrsgp:OtherAssetsCurrent> to define a value. The number itself sits between these two tags. XBRL tags identify financial values uniquely. For example, the term ''CashCashEquivalents'' within a tag unambiguously defines ''cash and cash equivalents.'' Finally, you can use optional entries in each tag to identify currency units (e.g., ''Euros'') and the number of decimal places (e.g., ''0'').

To create an XBRL instance document, you need to know: (1) the standard tags that define such familiar items as net revenues and operating expenses, and (2) the rules that govern how to use these tags. XBRL Specification 2.1 currently defines the rules and syntax for XBRL taxonomies and XBRL documents. XBRL taxonomies define the tags that represent accounting and financial terms used in XBRL instance documents. With standard tags for each piece of common financial data, accounting software can create instance documents for income statements, balance sheets, and similar financial statements in a straightforward manner. Figure 15-3 lists a number of ways that XBRL affects accountants.

The Benefits of XBRL

The business potential of XBRL seems great. One obvious benefit is the ability to transmit financial information in a standard format. This facilitates communications between suppliers and their buyers, companies and their shippers, and retailers and their customers. The same standardization applies to financial filings. For example, the Securities and Exchange Commission (SEC) now requires XBRL-formatted financial statement reports, which businesses can also use to help complete loan applications.

Another important advantage of XBRL is that it defines data items uniquely. Consider, for example, how a spreadsheet stores financial information. The only way we know that a particular number *in* a spreadsheet is, say, ''net revenue'' is because we also see a label that identifies it as such. Move the number somewhere else in the spreadsheet and you also lose its meaning. In contrast, a ''net revenue'' figure remains ''net revenue'' no matter where it appears in XBRL instance documents as long as it remains within its tags.

XBRL's standardized tags also make searching for items in XBRL financial documents relatively easy. If you know the standard tag for an item of interest, you can unambiguously

- Due to corporate scandals, shareholders, analysts, and reporters are demanding more transparent reporting. XBRL allows readers to quickly access the information they need.
- XBRL permits the automatic and reliable exchange of financial information across all software formats and technologies, including the Internet.
- XBRL does not require a change to existing accounting standards of corporate disclosure policies.
- XBRL improves access to financial information because data is in a digital, reusable form.
- XBRL eliminates the need to reenter financial data for different users, which reduces risks associated with data entry and lowers the cost to prepare and distribute financial statements.
- XBRL improves investor and analyst access to information.
- XBRL allows accountants to more quickly and easily consolidate and scrutinize internal data for use in financial reports.
- XBRL allows CEOs and CFOs to deliver more transparent information to investors and analysts, and allows a vehicle for control within the firm.

Source: Charles Hoffman and Carolyn Strand, *XBRL Essentials* (New York: AICPA), 2001; and www.xbrl.org

FIGURE 15-3 How does XBRL affect accountants?

find and extract the number in question from those documents. One repository of such financial information is the Security and Exchange Commission's new **interactive data and electronic applications (IDEA)**, which the agency unveiled in August of 2008 and now contains XBRL data for over 10,000 companies—a particularly important source of financial information and a particularly important reason why standardized reporting is useful.

In business environments, the term *semantic meaning* refers to the fact that the financial data are related to one another through such formulas as ''Assets = Liabilities + Equity.'' An additional advantage of XBRL is its ability to express such relationships in formulas, thereby making the data self-checking. This is important because organizations often need to transmit financial data to others, and XBRL provides a means of internal control.

Case-in-Point 15.4 The Federal Deposit Insurance Corporation (FDIC) insures banks and similar financial institutions throughout the United States. The FDIC exchanges financial information with member institutions all the time, and uses a set of 1,800 rules to validate such data. The FDIC was an early adopter of XBRL in part because this language has the ability to perform data-validation tasks automatically.[4]

Companies using XBRL-enabled software can save their financial information in standard XBRL format, thus avoiding the errors that may come from reentering data multiple times from multiple sources. Companies can then directly upload their business information in this format onto their websites. This is important because a recent study by Forrester Research estimated the cost of re-keying information at $402 billion per year.[5]

Another advantage is that XBRL permits the automatic and reliable exchange of financial information across all software platforms and technologies, including the Internet. Thus, anyone interested in comparing the cash and cash equivalents of several companies can search for the data and export it to a spreadsheet for analysis purposes.

Finally, it is important to note that XBRL does not constrain companies to a particular *format* for their financial reports. To the contrary, the language is flexible, and therefore intentionally constructed to support financial reporting by companies in different industries or from different countries. The hope is that both the extensible capabilities of the language as well as this flexibility are great enough to meet business and governmental needs at all levels. Problem 15–20 invites you to explore the benefits of XBRL in further detail.

XBRL also has several disadvantages. Perhaps the most important is the fact that a common reporting language requires its users to learn, and conform to, the standards of that language. Another problem is that evolving XBRL standards require users to learn new rules for changing specifications.

The Current Status of XBRL

The **XBRL International Consortium** has about 450 members and is in charge of developing XBRL standards. Many U.S. accounting firms are members of this consortium, as is the American Institute of Certified Public Accountants and parallel accounting organizations around the world. The specifications for version 2.1 of XBRL were issued in July of 2008. The website at www.xbrl.org provides additional information on both current and proposed standards.

[4]Source: http://www.ubmatrix.com/Documents/XBRLComparedToXML-2005-07-06%20(4).pdf.
[5]Source: http://accounting.smartpros.com/x37643.xml; ''How XBRL Is Transforming Financial Reporting''.

As you might imagine, developing Internet standards for financial reporting is a massive undertaking. The language specifications require classification systems for different countries, different reporting segments (e.g., different industries), and even different organizational standards such as U.S. generally accepted accounting standards (GAAP). For example, oil and gas companies require specialized tags to identify reserve balances, casinos require specialized tags to identify allowances for unclaimed gambling chips, and so forth. Then too, the language requires standard tags for formulas (e.g., a Price/Earnings ratio) and different functions. For this reason, XBRL is best viewed as a dynamic language still in development.

Most accounting software vendors now support XBRL in one or more of their software packages, and the world-wide adoption of XBRL is moving along quickly. For example, in Germany, it's universal—XBRL is already built into a software package used by 80% of the accountants in that country. The XBRL International consortium publishes a progress report three times a year, available on its website, to offer the most current information about XBRL.

ELECTRONIC COMMERCE

The term **electronic commerce** refers to conducting business with computers and data communications. Often, e-commerce is done over the Internet, but businesses can also conduct e-commerce over proprietary data transmission lines. Recent surveys estimate the total annual revenues for e-commerce in the United States exceeds $1 trillion, and the FBI estimates that the banking industry transfers over $1 trillion *each week* by electronic means. Some general categories of electronic commerce are (1) retail sales, (2) e-payments and e-wallets, and (3) electronic data interchange, each of which we examine briefly in the paragraphs that follow.

Retail Sales

The World Wide Web offers businesses the opportunity to create virtual stores (''shopping cart applications'') for selling merchandise directly to customers. At the retail level, it is clear that such websites are really automated AISs that allow customers to create their own order forms, shipping forms, and payment documents. Testimony to the success of such retail e-commerce abounds. The number of online shoppers has increased steadily over the past decade. More than 90% of the U.S. population is now connected to the Internet, many of whom now purchase items over the Internet on a regular basis. For example, consumers now reserve most of their domestic airline tickets, rental cars, and hotel rooms over the Internet. Figure 15-4 lists some of the advantages of virtual stores. Note how many of these advantages relate directly to AISs.

Internet retail sales also introduce special issues. One problem is that customers usually cannot determine whether a retail website is legitimate. Similarly, consumers must usually rely on emails to voice their complaints (rather than speaking to someone in person) and returns are sometimes problematic. A third problem is that online stores frequently rely on suppliers rather than their own shelves for merchandise to satisfy orders, creating the potential for stock-out and backorder problems. Finally, a growing e-commerce problem is **click fraud**, in which dishonest managers inflate the number of clicks viewers make on an advertisement on a web page, and therefore bill the linked company for more referrals than actually occurred.

1. Web pages are much cheaper to create than creating and mailing catalogs.
2. Distribution is global.
3. Sales can occur around the clock.
4. Customers can search for specific products or services electronically, either within a particular website or as a ''hit'' from another site.
5. A business can easily outsource its web business to others, enabling it to focus on core processes.
6. The websites themselves can use automated tools to verify customer credit cards.
7. Businesses can send emails to confirm orders or advise customers about shipping dates.
8. Businesses can update product descriptions, sales prices, and information on merchandise availability immediately.
9. Customers create their own sales orders online.
10. Customers can track their own orders, freeing business personnel for other tasks.
11. The sales and customer-relations personnel required for virtual stores is minimal, thus reducing labor costs per dollar of sales.

FIGURE 15-4 Some advantages of virtual stores on the Internet.

Internet retail sales also provide retailers with a wealth of data *about* their customers, raising issues about privacy. For example, you might be concerned about the fact that your web purchase also means that a retailer now has (1) your email address, which it can use to send additional, annoying emails or sell to others, (2) your credit card information, which it may or may not protect as well as you would like, and (3) sensitive information about your purchase patterns—for example, prescription drugs. A later section of this chapter addresses these privacy and security issues in greater detail.

E-Payments and E-Wallets

Most customers pay for the merchandise they order over the Internet with a credit card, requiring vendors to use third-party affiliates to authenticate user credit-card numbers. This is a problem because such credit card verification systems only indicate that a card is valid, not that the online customer is authorized to use it. A related problem with online payments is that although online customers might not mind giving their credit card numbers to trusted merchants, they may not wish to share the number with unfamiliar businesses or unknown sellers on mass auction sites.

Some merchants and auction sites solve these problems with **electronic payments (e-payments)**, which proponents claim is a faster, easier, and safer way for both customers and sellers to handle online transactions. The e-payment service acts as a trusted intermediary because it collects a payment from a buyer and pays that amount to the seller.

Case-in-Point 15.5 Consumers who buy products on E-bay or other online auction sites may be familiar with Paypal (www.paypal.com), an e-payment system that operates via the Internet. Customers who want to bid for items in online auctions, but who don't wish to share their credit card number with unknown sellers, may open an account with Paypal. Account-holders can deposit cash in their Paypal account using credit cards, debit cards, or bank checks. When consumers purchase items, Paypal acts as an intermediary bank, withdrawing money from the purchaser's account and depositing similar funds into the seller's account (or sending a check).[6]

[6]To learn more about PayPal, log onto its website at www.paypal.com and click on ''How PayPal works.''

Businesses are not the only entities that can enjoy the convenience of e-payments. The U.S. government has its own system to conduct financial transactions online:

Case-in-Point 15.6 Pay.gov (Figure 15-5) enables businesses and individuals to make payments to the U.S. government electronically. Developed by the U.S. Treasury Department's Financial Management Services (FMS), Pay.gov is a central location through which businesses and individuals can make payments, submit forms, and send bills to federal agencies. This portal provides authentication services for secure transactions. FMS expects Pay.gov to handle approximately 80 million transactions worth over $125 billion a year, reduce paperwork, and save agencies over 5% in processing costs.[7]

Another Internet payment option is an **e-wallet**. E-wallets are software applications that store a consumer's personal information, including credit card numbers, email addresses, and shipping addresses. Shoppers pay for online purchases by providing their e-wallet account numbers to online vendors that also subscribe to the system.

An advantage of an e-wallet is that you can use it whenever you visit subscriber websites. These systems spare you the trouble of entering your personal information each time you make an online purchase. Also, because your e-wallet information is usually stored on your own hard drive, you control it. This maintains your email privacy as well. E-wallets may be as important for retailers as they are for consumers because many consumers cancel e-commerce transactions before they complete them, often because of frustration with online forms.

Case-in-Point 15.7 *AOL Wallet* is America Online's e-wallet application. The system enables users to store up to ten credit card numbers and 50 shipping addresses in a single account. AOL partners with a number of online retail merchants such as Macy's and Eddie Bauer, and shoppers can use AOL Wallet at any of them. When you visit an affiliated retailer,

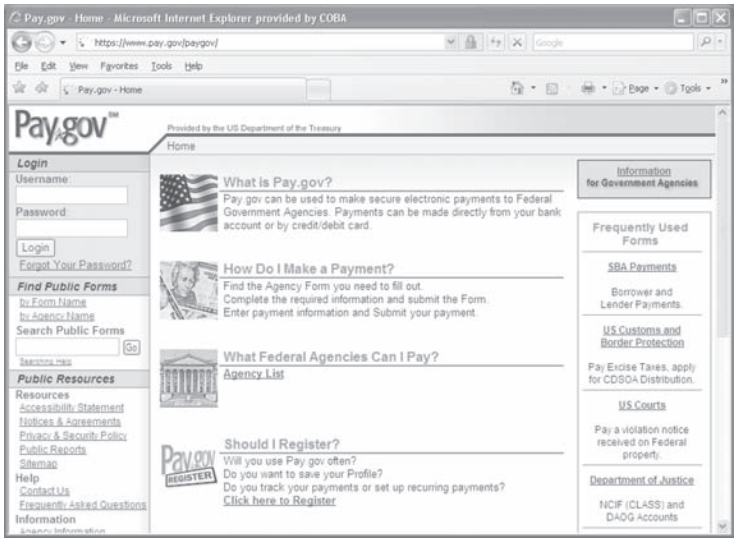


FIGURE 15-5 The home page for Pay.gov—an e-payment system supported by the U.S. government.

[7]Source: Nicholas Morehead. "Treasury Antes up E-Payments," (April 3, 2004) at www.fcw.com/articles.

the software enters your name, address, phone, credit card number, and other relevant information automatically in the payment form.[8]

Business-to-Business E-Commerce

Although there has been tremendous growth in retail e-commerce, it is dwarfed by **business-to-business (or B2B) e-commerce**—i.e., businesses buying and selling goods and services to each other over the Internet. Buying goods online shortens the time from purchase to delivery and also allows businesses to shop from vendors all over the world. Like retail consumers, corporate purchasing agents using B2B e-commerce tools can select items from online catalogs, confirm purchases, track shipments, and pay bills electronically. E-commerce software can also expedite internal paperwork by first sending purchase orders to the appropriate managers for approvals and then forwarding them to the vendor, thus reducing the costs of processing purchase requisitions.

Case-in-Point 15.8 BASF is one of the world's largest chemical, plastics, and energy companies, with sales of $81.8 billion in 2008 and 94,000 employees on five continents. Company managers credit much of its recent 75% growth in revenues to its new e-commerce initiatives. Says Herbert Fisch, head of global e-commerce, "In addition to order management, e-commerce provides our customers with information and service tools. Customers benefit from greater transparency and we gain valuable time to better serve them."[9]

Further back the supply chain, the Internet affects accounting activities just as strongly. Another feature of B2B e-commerce is the wider availability of real-time data that allows managers to view up-to-the-minute information. Take, for instance, a distributor whose business customers in turn sell products to end users. With current data about its customers' retail sales, the supplier could quickly increase or decrease its operations as required. Similar online information can determine the location of specific trucks (using GPS systems), check the estimated arrival date of incoming cargo ships, or determine the current status of finished products, parts inventories, or even working assembly lines.

Even vendors of inexpensive accounting software now include an e-commerce interface with their products. An example is Peachtree software's Peachlink feature, which provides users with tools to create and use a shopping-cart website and accept Internet orders.

Although the Internet has streamlined procurement and inventory tracking operations, it has been slow to impact accounts payable or accounts receivable. In part, this is because companies like to hold their money as long as possible. However, delayed bill payment works *against* these same businesses who want to *collect* on their own accounts receivable. Software from such companies as Time Capital allows vendors and customers to view purchase and shipping documents so that they can resolve discrepancies quickly and cut checks or make electronic payments as needed.

Electronic Data Interchange and Virtual PBXs

Two further uses of Internet technology are electronic data interchange and virtual PBXs. We examine each of them in the following paragraphs.

---

[8]Source: www.AOL.com.

[9]Source: Elaine Burridge. "E-commerce Revenues Boost Achieved by BASF" *European Chemical News* Vol. 83, No. 2174 (December 5, 2005), p. 14.

Electronic Data Interchange (EDI). Literally thousands of companies use **Electronic Data Interchange (EDI)** to electronically exchange billions of dollars every year as well as many business documents. EDI means transmitting information over high-speed data communications channels. Examples of EDI business documents include requests for quotes (RFQs), purchase orders, bills of lading, freight bills, sales invoices, customs documents, payment remittance forms, and credit memos. Thus, EDI automates the exchange of business information and permits organizations to conduct many forms of commerce electronically.

Case-in-Point 15.9 Pressured by budget cuts, British libraries are turning to RFID and EDI technologies to reduce costs instead of closing libraries. Staffordshire library is an example, which uses EDI for vendor quotes, catalogue services, acknowledgements, and invoicing to help it streamline its acquisition processes. As a result, the stock manager reports that vendor replies to requests have improved, new stock arrives more quickly, and staffing costs have been reduced by 42%. She estimates that EDI saves the library over $155,000 per year.[10]

Government agencies also depend heavily on EDI. One example is the U.S. Customs Service:

Case-in-Point 15.10 Before EDI, imported goods could wait on docks for weeks while officials processed the paperwork. But information about some imports can be sent weeks before the merchandise itself arrives. The U.S. Customs Service now uses EDI to process almost 95% of all customs declarations. This usage has lowered error rates from 17% before EDI, to about 1.7% now. This improvement translates into annual savings of $500 million in processing costs, and about 10% in productivity gains.[11]

One potential advantage of EDI compared to Internet e-commerce is that many business documents are simply faxed over telephone lines, avoiding computers completely. Another advantage is that many EDI documents include hand-written signatures, providing assurance of their authenticity. A third advantage is that EDI includes the exchange of graphic and photographic documents—media that *can* be scanned and captured electronically, but at additional time or cost.

Virtual PBXs. The acronym PBX stands for ''private branch exchange''—the phone system that most businesses use in their offices. The primary motivator is cost—these systems enable a business to lease a smaller number of external lines from telephone service providers than if each office had its own outside line. Because modern PBXs are computer-based, additional benefits include the use of passwords for system access, the ability to classify long-distance phone charges by handset or by password account, and the availability of answering-machine services, call-forwarding, call recording, caller ID, and internal call conferencing.

Virtual PBXs are Internet-based PBX systems that enable organizations to outsource their PBX services. Most of these systems use **VoIP (**voice over Internet protocol) to transmit digitized versions of voice-grade messages over the Internet. In addition to such common advantages of outsourcing as lower costs, greater reliability, and perhaps enhanced capabilities, virtual PBXs become invaluable in emergencies or disasters. At such times, for

[10]Source: Hannah Davies, ''The Electronic Chain to Cost Cutting'' *Bookseller* (February 2009), pp. 6–7.
[11]Source: Theodore Prince. ''EDI Outlook: Good Technology, Problematic Results'' *Journal of Transportation Law, Logistics, and Policy* Vol. 71, No. 4 (Summer 2004), pp. 440–446.

example, a virtual PBX can reroute toll-free calls to alternate landlines or cell phones, as well as redirect ''internal calls'' from one employee to another. Thus, managers can work at home but still use their ''office phone'' as conveniently as ever.

PRIVACY AND SECURITY ON THE INTERNET

The most important advantage of the Internet and World Wide Web—*accessibility*—is also its greatest weakness—*vulnerability*. This means that someone who *poses* as an authorized user may be able to access any email, web page, or computer file that an authorized user can access through the Internet. This section of the chapter discusses Internet privacy and security in detail.

Privacy and Identity Theft

Do organizational managers have the right to view the emails of their employees? Do businesses have the right to use the personal information collected from their online retail customers? These are some of the privacy issues first discussed in Chapter 10. Both state governments and such groups as the Electronic Frontier Foundation and the Online Privacy Alliance continue to work on legislation to protect the privacy of data transmitted over the Internet.

Of particular concern is **identity theft**, in which someone uses another person's personal data in some way that involves fraud or deception (usually for economic benefit).[12] The most current statistics released by the FBI indicate that almost 10 million Americans were identity-theft victims and experienced losses totaling $52.6 billion.[13] The most common complaint related to identity theft is credit card fraud. The Department of Justice prosecutes ID theft violations under the **Identity Theft and Assumption Deterrence Act (ITADA) of 1998**. The punishment can be a prison term of 15 years, a fine, and forfeiture of any personal property used to commit the crime.

Although companies need strong preventive controls to help protect customer information, individuals should also exercise reasonable caution in protecting personal information. Unscrupulous individuals, posing as a company or bank employee, might call or send email messages to solicit personal information. Use your professional skepticism. If you are uncertain about the authenticity of the request, ask the person to send the request in writing on company letterhead. If you question the authenticity of a particular website, do more research on the company before purchasing goods or services through it—especially if you must give your credit card number. Figure 15-6 outlines some additional steps that you can take to better protect your personal information—almost all of them accounting-related.

Security

Security policies and procedures safeguard an organization's electronic resources and limit their access to authorized users. As noted in Chapter 1, **information security** has been the number one technology in each of the last five years in the AICPA's survey of the ''Top 10 Technologies'' expected to have a powerful influence over business.

[12]Source: www.usdoj.gov/criminal/fraud/idtheft.html.
[13]Source: http://www.identitytheftsecurity.com/stats.shtml.

1. Only give personal information such as Social Security numbers and dates of birth to those absolutely needing it.
2. Mail checks, credit applications, and similar materials directly in locked outgoing mail boxes, not in front-yard mail boxes with red, ''steal me'' flags on their sides.
3. Do not leave purses, wallets, or similar carrying cases unattended—for example, in unlocked gym lockers.
4. When asked by a legitimate business person such as a bank teller for your personal information, write it down for them—do not recite it verbally.
5. Be wary of unsolicited calls from individuals claiming to be bank representatives, credit-card issuers, or others, especially if they ask for personal information. A similar rule applies to emails from unknown agents.
6. Do not ''lend'' personal information to others—for example, a password.
7. Do not simply toss sensitive information in trash cans where others can retrieve it. Shred or burn it first.
8. Be wary of relatives in financial difficulties. Sadly, family members who are well known by the victims account for a high percentage of identity theft.
9. *Phishing* describes a website that appears to be from a well-known company, but that gathers personal data for illegal purposes. Don't fall for them.
10. *Key-logging software* is software that captures your keystrokes—usually for illicit purposes. Use security software to guard against it.

FIGURE 15-6 Steps that you can take to safeguard your personal data from identity theft.

Case-in-Point 15.11 Richard Farina of AirTight Networks was traveling on an American Airlines flight in October of 2008 that supported Internet access for its passengers. As an experiment, he used some of his company's intrusion protection software and found that he could view all his fellow passenger's Internet activities due to the airline's poor security.[14]

Of special importance to AISs is **access security**—e.g., restricting access to bona fide users. *Access authentication* requires individuals to prove they are who they say they are. The three types of authentication are based on: (1) what you *have*, (2) what you *know*, and (3) who you *are*. What you *have* may be a plastic card that provides you physical access to information or a restricted area. Examples are your ATM card, debit card, or employee card that gives you access to certain premises. What you *know* refers to unique information you possess, such as a password or your mother's maiden name. You can authenticate *who you are* with a unique physical characteristic such as your fingerprint or the pattern of the retina in your eye. As you might guess, using security that forces a user to prove who they are is the highest level of authentication. Some security systems require a combination of authentication techniques—for example, using both your debit card and your password to withdraw cash from an ATM.

Spam and Phishing

A current Internet problem is the increasing amount of **spam**—those annoying, unsolicited email messages that clog your email inbox. However, spam is more than a simple bother—it is distracting, often illegal, and increasingly costly to organizations. AOL and Microsoft, two of the biggest Internet service providers, estimate that they each block over 2 billion spam emails per day.

[14]Source: Taylor Buley. ''Phishing at Gate B22'' *Forbes* Vol. 182, No. 12 (December 8, 2008), pp. 52–52.

Although about 35% of spam messages are harmless advertising, a greater percentage contains pornographic solicitations, attempts to steal identities, or fictitious stories asking recipients for money. Clicking on the ''unsubscribe button'' in such messages usually accomplishes the exact opposite effect because it tells the sender that you are a legitimate user who actually reads such emails. Spammers sell lists of such prized, active email accounts to one another, furthering the problem.

Case-in-Point 15.12 The Radicati Group has 21 Exchange email servers, of which five handle nothing but junk mail. The company estimates that it spends almost half a million dollars annually on such server capacity to process spam transmissions.[15]

Although some spam email contains legitimate sales offers, many more are bogus. In such cases, the spammers advertise products at ''too-good-to-believe prices,'' take credit-card orders, collect the money, and then quickly fold up shop before consumers realize they've been victimized.

Case-in-Point 15.13 At the time this book was written, New Zealand brothers Shane and Lance Atkinson were in federal court as a result of a suit filed by the Federal Trade Commission (FTC) for "deceptive and fraudulent practices." The FTC claim is that, in less than nine months in 2007, the team used a botnet-driven spam network to defraud victims of more than $7 million.[16]

As we described in Chapter 10, **phishing** websites trick users into providing such personal information as Social Security numbers, debit-card PIN numbers, or similar personal information—for example, for ''routine security purposes'' or even ''because we believe your account has been compromised.'' Phishing activity is growing. For 2007, the Gartner research group estimated that 3.6 million Americans were victims of phishing—a 40% increase over the previous year—and that total losses were more than $3.2 billion. According to a banking group in the United Kingdom, the comparable growth figure is 180%. These statistics are especially relevant to accounting information systems because most phishers want personal information that in turn provides access to financial resources. In 2007, for example, the Anti-Phishing Working Group found that over 90% of the targeted companies were financial service companies.

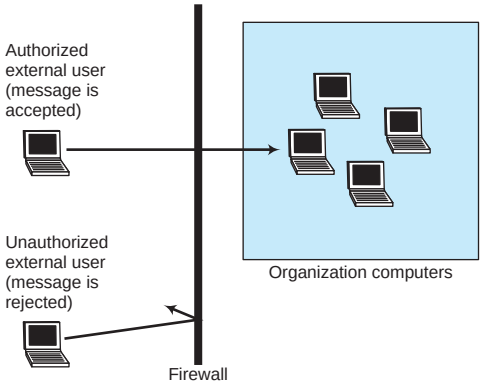
Firewalls, Intrusion Detection Systems, Value-Added Networks, and Proxy Servers

To gain access to a company's files, a computer hacker must first obtain access to that company's computers. The firewalls, intrusion detection systems, and proxy servers discussed here protect against unwarranted intrusions from external parties.

Firewalls. A **firewall** (Figure 15-7a) guards against unauthorized access to sensitive file information from external Internet users. On networked systems, firewalls are often stand-alone devices with built-in, protective software (Figure 15-7b). On mainframe or host systems, firewalls are usually software.

The two primary methods of firewall protection are *by inclusion* or *by exclusion*. When firewalls protect internal systems by *inclusion*, the software examines packets of

[15]Source: no author, ''Spam Wars Cost'' *Controller's Report* Vol. 2004, No. 9 (September 2004), p. 15.
[16]Source: http://www.scmagazineus.com/SC-World-Congress-Anatomy-of-a-spam-business/article/122708/.



(a) Firewalls accept messages from bona fide users but reject messages from unauthorized users.

(b) This hardware-based firewall from Sonicwall can support an unlimited number of users and 8 gigabytes of traffic per second.

FIGURE 15-7 A firewall acts as a barrier between unauthorized external users and organizational (internal) computers and files.

incoming messages and limits entry to authorized (''included'') users. To do this, the software maintains an **access control list (ACL)** of bona fide IP addresses that network administrators create for this purpose. If the software does not recognize the IP address of an external user, it refuses that user access to the files he or she requested. When firewalls protect internal systems by *exclusion*, the software compares the incoming packet IP address to a list of known threat addresses, rejecting messages from these sources but accepting all others.

Firewalls are useful Internet security controls but (like most security features) are not foolproof. One problem is that they cannot protect against **denial-of-service attacks**, which overwhelm system resources with a volume of service requests. Another problem is **spoofing** (i.e., masquerading as an authorized user with a recognizable IP address). A similar, but less obvious, problem is the ability of a determined hacker to alter the contents of the access control list itself—a security breach that is especially difficult to overcome. A final problem is that most firewalls can only protect against external attacks, not internal (authorized) users bent on mischief.

Intrusion Detection Systems. Whereas firewalls simply reject unauthorized users from access, **intrusion detection systems (IDSs)** create records of such events. *Passive IDSs* create logs of potential intrusions and alert network administrators to them either via console messages, alarms, or beepers. *Reactive IDSs* have the ability to detect potential intrusions dynamically (e.g., by examining traffic flows), log off potentially malicious users, and even reprogram a firewall to block further messages from the suspected source.

Perhaps the most important advantage of an IDS is its ability to both prevent unauthorized access to sensitive information and to alert system administrators to potential

violations. This may also increase the perceived risk of discovery, dissuading would-be hackers. IDSs may also be able to detect preambles to attacks, forestalling their effectiveness. Finally, an IDS is an important tool for *documenting* an attack, thereby generating invaluable information to both network administrators and investigators.

Value-Added Networks. Message-routing is important to accountants because the security of a data transmission partially rests on the security of all the intermediate computers along a given communications pathway. Thus, the greater the distance between the sending station and the destination computer, the more intermediary routing computers there are and the more vulnerable a message becomes to interception and abuse. This is one reason why businesses often prefer to create their own (proprietary) networks to transmit data electronically.

Value-Added Networks (VANs) are private, point-to-point communication channels that large organizations create for themselves—usually for security reasons (Figure 15-8). When it first implements a VAN, the business assigns each user a unique account code that simultaneously identifies the external entity and authenticates the organization's subsequent electronic transactions.

There are at least three ways to create VANs. One way is to start with a blank slate and create everything from scratch—an approach first used by the military and later by Wal-Mart. A second way is to lease secure, dedicated transmission lines from conventional long-distance carriers such as AT&T—the approach used by IGT's Megabucks system (see Chapter 2).

A third alternative is to create a **virtual private network (VPN)** on the Internet. As the name suggests, a VPN mimics a VAN in many of its security features, but enjoys the benefit of transmitting messages cheaply over existing Internet connections. A VPN creates secure data transmissions by (1) using ''tunneling'' security protocols embedded in the message frames sent to, and received by, the organization, (2) encrypting all transmitted data, and (3) authenticating the remote computer, and perhaps also the individual sender as well, before permitting further data transmissions. Most AIS VANs use this approach.

Proxy Servers. Given the large amount of information now available on the web, some organizations seek to limit the number of sites that employees can access—for example, to ensure that employees do not use web-access privileges for frivolous or counterproductive purposes. A **proxy server** is a network server and related software that creates a transparent gateway to and from the Internet and controls web access. In a

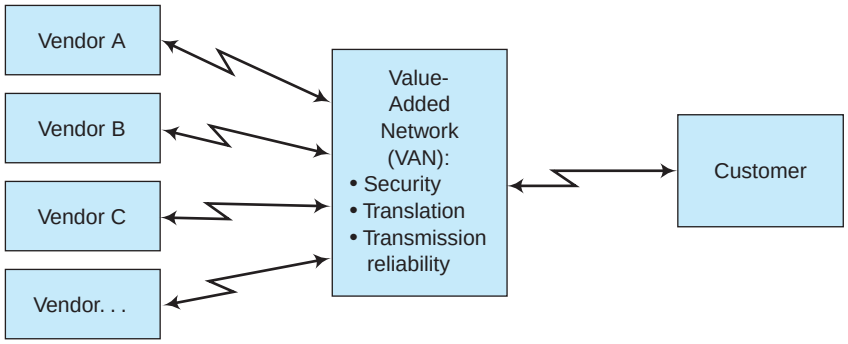


FIGURE 15-8 A VAN-based EDI system.

typical application, users log onto their familiar file server as before. But when they attempt to access a web page, the initial network server contacts the proxy server to perform the requested task.

One advantage of using a proxy server is the ability to funnel all incoming and outgoing Internet requests through a single server. This can make web access more efficient because the proxy server is specifically designed to handle requests for Internet information. A second advantage is the proxy server's ability to examine all incoming requests for information and test them for authenticity (i.e., the ability to act as a firewall). A third advantage is that a proxy server can limit employee Internet access to approved websites (i.e., to only those IP addresses contained in an access control list). This enables an organization to deny employees access to gambling, pornographic, or game-playing websites that are unlikely to have any productive benefits.

A fourth advantage is the ability to limit the information that is stored on the proxy server to information that the company can afford to lose. If this server fails or is compromised by hackers, the organization is only marginally inconvenienced because its main servers remain functional. To recover, the company can simply restart the system and reinitialize the server with backup data.

Netscape Communications estimates that between 30–60% of Internet requests are redundant. A final advantage of proxy servers is the ability to store ("cache") frequently-accessed web pages on its hard drive—for example, the web pages of preferred vendors. This enables the server to respond quickly to user requests for information because the web-page data are available locally. This feature also enables managers to obtain some idea of what information employees need most and perhaps take steps to provide it internally (rather than through web sources).

Data Encryption

To safeguard transmitted data, businesses often use **data encryption** techniques that transform plaintext messages into unintelligible cyphertext ones. The receiving station then decodes the encrypted messages back into plaintext for use. There are many encryption techniques and standards. The simple method shown in Figure 15-9 uses a *cyclic substitution* of the alphabet with a displacement value of "5" to transform the letters of a plaintext message into alternate letters of the alphabet. To decode the message, the recipient's computer performs the encryption process in reverse, decrypting the coded

Encryption Scheme:

Letters of the alphabet:	A	B	C	D	E	F	G	H	I	J	. . .
Numerical equivalent:	1	2	3	4	5	6	7	8	9	10	. . .
Plus displacement key:	5	5	5	5	5	5	5	5	5	5	
New values:	6	7	8	9	10	11	12	13	14	15	
Letters to use in code:	F	G	H	I	J	K	L	M	N	O	. . .

Example:

Plaintext message:	HI, ABE!
Cyphertext message:	MN, FGJI

FIGURE 15-9 A simple data encryption method.

message back into readable text. To make things more secure, the sender can use a different displacement value for each coded message.

The method that computers use to transform plaintext into cyphertext is called the **encryption key**. This is typically a mathematical function that depends on a large prime number. The **data encryption standard (DES)** system used by the U.S. government to encode documents employs such a system. DES uses a number with 56 binary digits to encode information, a value equal to approximately 72 quadrillion. Thus, to crack the code, a hacker must guess which of 72 quadrillion values was used to encrypt the message.

The data encryption method illustrated in Figure 15-9 uses a single cryptographic key that is shared by the two communicating parties and is called **secret key cryptography**. This system derives its name from the fact that its users must keep the key secret and not share the key with other parties. The most common encryption methods today use **public key encryption**, a technique that requires each party to use a pair of public/private encryption keys. Two examples are SSL (Secure Socket Layer) and S-HTTP (Secure Hypertext Transport Protocol).

To employ public key encryption, the sending party uses a public key to encode the message and the receiving party uses a second, private key to decode it. A major advantage of public key encryption is that the same public key cannot both encode and decode a message. Data transmissions using public key encryption are likely to be secure because the transmitted message itself is scrambled and because neither party knows the other's key. This is the main reason why most web applications use public key encryption systems.

Digital Signatures and Digital Time Stamping

Many businesses want proof that the accounting documents they transmit or receive over the Internet are authentic. Examples include purchase orders, bids for contracts, and acceptance letters. To authenticate such documents, a company can transmit a complete document in plaintext, and then also include a portion of that same message or some other standard text in an encrypted format—that is, can include a **digital signature**.

In 1994, the National Institute of Standards and Technology adopted Federal Information Processing Standard 186—the **digital signature standard (DSS)**. The presence of the digital signature authenticates a document. The reasoning is straightforward: if a recipient's private key decodes a message, then an authentic sender must have created the message. Thus, some experts consider digital signatures even more secure than written signatures (which can be forged). Further, if the sender includes a complete message in both plaintext and cyphertext, the encrypted message provides assurance that no one has altered the readable copy. If someone has altered the plaintext, the two copies will not match.

Another authentication technique is a **digital certificate**—an authenticating document issued by an independent third party called a **certificate authority** (e.g., Thawte or VeriSign). The certificates themselves are signed documents with sender names and public key information. Certificates are generally encoded, possibly in a certificate standard such as the X.509 certificate format. Customers can also use digital certificates to assure themselves that a website is real.

Case-in-Point 15.14 In the future, each U.S. citizen may have a taxpayer's digital certificate within a smart card. Citizens could use the smart card for all their transactions with the federal government. The government program responsible for developing this card is called Access Certificates for Electronics Services project, or ACES. Although ACES is meant to ensure secure communications, privacy advocates are afraid that maybe the cards are *too* smart. This is because they contain *all* your personal information in one place. ACES does

include safeguards to ensure that the data on the cards can't be used in the private sector and are available only to a federal or authorized agency. But those concerned with privacy worry that the existence of the card will lead to unintended uses.

Many important business documents are time sensitive. Examples include bidding documents that must be submitted by a deadline, deposit slips that must be presented to banks before the close of business, buy orders for stock purchases that depend on the date and time of issue, and legal documents that must be filed in a timely fashion. Then, too, most businesses also want to know when customers ordered particular purchases, when they paid particular bills, or when specific employees entered or modified data items in important databases. Finally, a good way to protect intellectual property such as computer software is to clearly establish the date and time it was first created or distributed.

What these items have in common is the need for a time stamp that unambiguously indicates the date and time of transmission, filing, or data entry. PGP Digital Time Stamping Service and Verisign are two of several **digital time-stamping services (DTSSs)** that attach digital time stamps to documents either for a small fee or for free. In a typical application, the user sends the document to the service's email address along with the Internet address of the final recipient. When the service receives the document, it performs its time-stamping task and then forwards the document as required.

Digital time stamping performs the same task electronically that official seals and other time stamps perform manually: authenticate the date, time, and perhaps place of a business transaction. This can be important over the Internet. Although most documents are transmitted almost instantaneously, time delays can occur when file servers temporarily falter or power failures disrupt wide area networks. DTSSs enable businesses to overcome these problems.

AIS AT WORK
The Benefits of Online Accounting Outsourcing

The advantages of outsourcing such accounting functions as payroll processing or tax preparation are well known, but outsourcing additional accounting tasks to online providers is a different matter. Can an external or offshore provider perform general ledger or deprecation computations as well? A growing number of businesses say ''yes!''

The most common reason organizations outsource a given business process is ''reduced cost,'' and this applies to accounting outsourcing as well. Additional benefits include faster turnaround, improved quality, enhanced access to expertise, reduced variability in accounting costs caused by peak processing volumes, and reduced capital expenditures (e.g., in computers and software). Experts note that online outsourcing enables the clients to reduce in-house labor costs, pay only for the services they need, and focus on their core businesses.

Perhaps the most commonly-cited objection to outsourcing is a loss of control. In a recent survey of over 800 businesses by Accenture, however, over 85% of the respondents said that outsourcing actually gave them more control—especially in the ability to plan. In addition, over 55% thought that accounting outsourcing enabled them to implement strategic changes faster and at more controlled rates. But the biggest benefit of outsourcing may be the increased business for those accounting companies providing these services—yet one more opportunity made possible by the Internet.

Source: ''Why Outsourcing is a Good Idea for You'' *Articlesbase*, www.articlesbase.com/outsourcing-articles/why-outsourcing-accounting-is-a-good-idea-for-you-591876.html.

SUMMARY

- The Internet is a collection of local, wide-area, and international networks that accountants can use for communication, research, and business purposes. Most accountants also use the World Wide Web—the multimedia portion of the Internet—for similar purposes.
- Intranets are private networks that businesses create for such internal purposes as distributing email. Extranets are similar to intranets, except that they allow external parties to access internal network files and databases.
- Groupware is software that supports email on business networks, plus allows users to share computer files, schedule appointments, video conference, and develop custom applications.
- To exchange financial information on the Internet, businesses can use XBRL—a form of XML that provides a common format for financial data and allows searches of the data and extractions for comparison purposes. The XBRL International Consortium develops XBRL standards.
- Electronic commerce includes retail sales on the Internet, electronic data interchange (EDI), and business-to-business (B2B) applications. In addition to credit and debit cards, consumers use e-payment and e-wallet systems to pay for Internet purchases.
- For security reasons, some businesses prefer to use expensive, but private, value-added networks (VANs) rather than the Internet to support e-commerce applications.
- Authentication requires users to prove they are who they say they are—for example, with something they have (a plastic card), something they know (a password), or something they are (a retina scan). Privacy concerns also include the need to protect users' private information and the growing threat of identity theft.
- Internet privacy and security concerns include hacking, identity theft, spam, and phishing, all of which impact AISs. These concerns prompt many businesses to use firewalls, intrusion detection systems, proxy servers, data encryption techniques, digital signatures, and digital time stamping to achieve control objectives.

KEY TERMS YOU SHOULD KNOW

access control list
access security
certificate authority
click fraud
data encryption
data encryption standard (DES)
digital certificate
digital signature
digital signature standard (DSS)
digital time stamping service (DTSS)
domain address
e-commerce
electronic conferencing
Electronic Data Interchange (EDI)
electronic payments (e-payments)
electronic procurement
encryption key
e-wallet
Extensible Business Reporting Language (XBRL)
Extensible Markup Language (XML)
extranets
firewall
groupware
hyperlinks
hypertext markup language (HTML)
hypertext transfer protocol (HTTP)
IDEA
identify theft
Identity Theft and Assumption Deterrence Act (ITADA) of 1998
information security
instant messaging
Internet protocol (IP)
intranets

intrusion detection system (IDS)
knowledge sharing
phishing
proxy server
public key encryption
secret key cryptography
spam
spoofing
TCP/IP
uniform resource locator (URL)
value-added network (VAN)
virtual PBX
virtual private network (VPN)
Voice over Internet protocol (VoIP)
XBRL instance documents
XBRL International consortium

TEST YOURSELF

Q15-1. Which of the following is most likely to contain only numbers?
a. Domain address **b**. URL address **c**. IP address **d**. Postal address

Q15-2. Which of the following enables users to view data with a web browser?
a. Intranet **b**. Extranet **c**. Internet **d**. All of these

Q15-3. All of the following are protocols for transmitting data over the Internet except:
a. IP
b. HTTP
c. XML
d. All of these are protocols

Q15-4. All of the following are markup languages (that use edit tags) except:
a. HTML **b**. XOR **c**. XML **d**. XBRL

Q15-5. Which of these is *not* an acronym?
a. HTML **b**. Blog **c**. PBX **d**. Firewall

Q15-6. Which of the following is true?
a. XBRL is a subset of XML
b. XML is a subset of TCP
c. PBX is a subset of HTML
d. None of these is true

Q15-7. A document file containing XBRL tags is a(n):
a. Extranet document
b. Intranet document
c. Instance document
d. URL

Q15-8. Which of these identifies a private, point-to-point network?
a. EDI **b**. DES **c**. IP **d**. VAN

Q15-9. Which of these statements is correct?
a. A VPN is a type of VAN
b. DES stands for ''data entry system''
c. An IDS is the same as a firewall
d. All of these statements are correct

Q15-10. Spoofing means:
a. Kidding someone about their firewall
b. Simulating a disaster to test the effectiveness of a disaster recovery system
c. Posing as an authentic user to gain access to a computer system
d. Encrypting data for security purposes

DISCUSSION QUESTIONS

15-1. What are intranets? What are extranets? Why are intranets and extranets important to accountants?

15-2. What are blogs? How are they used? Who is using them?

15-3. What is hypertext markup language? How does it differ from XML and XBRL? (Note: for a more comprehensive description of the differences, you may want to search the Internet.)

15-4. What is the relationship between XBRL and IDEA?

15-5. Describe some important uses of electronic commerce and explain why it is important to accountants.

15-6. What are electronic payments? How are they different from credit card payments?

15-7. What is electronic data interchange? Why do companies use EDI?

15-8. Most retail-sales websites require customers to use their credit cards to make purchases online. How comfortable are you in providing your credit card number in such applications? Why do you feel this way?

15-9. What is click fraud? Who benefits and who loses when click fraud occurs?

15-10. What is spamming? How is spam related to accounting information systems? Should all spamming be illegal? Why or why not?

15-11. What are Internet firewalls and proxy servers? How are they created? How do businesses use them for Internet security?

15-12. What is data encryption? What techniques are used for data encryption?

15-13. Describe and contrast the three types of authentication. Can you think of a business situation where someone would need to use a combination of all three levels to gain access to information?

15-14. What are digital signatures? Why do businesses use them? How can businesses use a digital certificate for Internet security?

15-15. Analysts claim that businesses can increase sales on the Internet, but not profits. What evidence does this chapter provide to support or refute this claim? Discuss.

PROBLEMS

15-16. The Internet uses many acronyms. Within the context of the present chapter, what words were used to form each of the following?

a. EC	b. EDI	c. email	d. HTTP	e. IDS	f. ITADA
g. IP address	h. blog	i. URL	j. VANs	k. VPN	l. WWW
m. XBRL	n. XML	o. IDEA			

15-17. In Discussion Question 15-1 above, you discussed intranets and extranets, and identified the importance of each to accountants. Now, assume that you are a partner in a medium-sized, local CPA firm. Your firm has 4 partners, 10 staff accountants, 1 research assistant, and an administrative assistant. Your firm is considered a technology leader in the local area and you consider this a competitive advantage for your firm. At the weekly staff meeting next Friday you want to discuss the topic of developing an intranet for the firm. To be sure everyone is prepared to discuss this topic, you want to develop a ''talking paper,'' which is a one page summary of salient points that you want to be sure you cover in your presentation to everyone. Assume you are the research assistant and the partner asks you to prepare this one-page discussion aid.

15-18. Create an HTML document of your own, using the example in Figure 15-1 to guide you. Put the name of this assignment in the <h1> tag for the heading. Put your name in bold. Include at least one hyperlink to a favorite web page using the anchor <a> tag. Finally, include an ordered list in your web page with at least three items—for example, a list of your favorite books, favorite restaurants, or the courses you're taking this semester. You will find it easiest to work in Notepad for this problem, but you can also use a word processor—as long as you save your document as ''text.'' Also, be sure to add the extension ''html'' to the end of your file name. View your completed document in your web browser—for example, by selecting File/Open in Microsoft Internet Explorer—and screen capture your work.

15-19. At the time this book was written, the U.S. Securities and Exchange Commission still supported Edgar—a depository of corporate accounting filings. Log onto Edgar at www.sec.gov/edgar.shtml, click on ''Search for Company Filings,'' click on ''Company or Fund Name,'' and finally, select two companies in the same industry (either your instructor's choice or your choice) so that you can compare various financial data. Note that you can select either ''text'' or ''html'' formats. Compare these formats to Figure 15-1. Are they similar? Looking at either image, can you download the financial information into a spreadsheet? Can you easily do financial comparisons such as ratio analysis? What do you have to do if you want to make financial comparisons?

15-20. Visit the XBRL home page at www.XBRL.org, and read the section entitled ''What is XBRL.'' Then, do each of the following:

a. Select the option ''Latest News'' from the home page, which lists several articles that describe recent developments. Choose one of these and write a one-page summary of your findings.

b. Select ''Benefits Across Business'' at www.xbrl.org/BenefitsAcrossBusiness/. This site contains a set of articles describing the various benefits of XBRL to different types of businesses. Select one article from this list and write a one-page summary of it.

15-21. Write a one-page paper on each of the following topics as they relate to XBRL:

a. What is the history of XBRL? What professional accounting organization helped in the early stages of this concept?

b. What is an XBRL specification and what is the latest version? When was it released? By whom?

c. How could XBRL help a company engage in ''continuous reporting?'' Find a website or an e-journal (an article) that discusses XBRL and continuous reporting. What are the main points of the article?

d. Find at least two other companies (other than Microsoft) that are publishing their financial statements on the Internet using XBRL. What business are they in (what industry)?

15-22. Examine the data encryption technique illustrated in Figure 15-9. Use a displacement value of ''8'' to encrypt the following message:

''Those who ignore history are forced to repeat it.''

15-23. The message below was encrypted using the technique illustrated in Figure 15-9 (using a displacement key other than 5). Using trial and error, decode it:

OZ OY TUZ CNGZ CK JUTZ QTUC ZNGZ NAXZY AY
OZ OY CNGZ CK JU QTUC ZNGZ PAYZ GOTZ YU

15-24. A number of accounting journals now post back issues, or even publish their entire journals, online. Access the *Journal of Accountancy* website at www.aicpa.org (or another website selected by your instructor). Select an article that pertains to a topic in this chapter and write a one-page report on it. Be careful to correctly cite any information that you use from this article!

15-25. The following stated policies pertain to the e-commerce website for Small Computers, Inc., a (fictitious) personal and handheld computer manufacturer and seller.

Privacy Statement

- We will only use information collected on this web for legitimate business purposes. We do not give away or rent any information to third parties.
- We will only contact you for legitimate business purposes, possibly from time to time, as needed. Please be 100% assured that we hold all transactions between you and our company in the strictest confidence.

Disclosure of Business Practices, Shipping, and Billing

- We will ship all items at the earliest possible date.
- We will not require you to accept items that you did not order.
- We will accept any returns from you of damaged or defective merchandise.
- In the event that we should accidentally bill you more than once for the same item, we will immediately issue you a refund.

Evaluate these stated policies in terms of how well they promote customer trust and confidence in Small Computers, Inc.'s electronic business operations.

CASE ANALYSES

15-26. Hammaker Manufacturing IV (XBRL-Enabled Software)

Recall, from Chapter 8, the Hammaker Manufacturing Company (HMC) is located in Burke, Virginia, and manufactures specialty parts for Corvettes. The company implemented a new AIS with the help of a consulting firm. At the time, Hammaker was especially interested in collecting data about inventories. Then, HMC decided to accept the consulting firm's recommendation to reengineer some processes in the production departments, rather than outsource these processes. Generally speaking, the BPR project is considered a success, based on the results that have been achieved—increased profits and more satisfied customers. To Denise's credit, she kept the employees informed throughout the study phase so that they understood the need for change. As a result of employee involvement, many useful changes were made and no employees were terminated.

Now, with increased profits and a very optimistic view of future growth, Hammaker meets with Denise and Lloyd to discuss the advantages and disadvantages of a new, more powerful AIS. Lloyd's area of expertise is implementing ERPs, and he is eager to inform HMC about the advantages of selecting an XBRL-enabled software solution for the firm.

Requirements:

1. What does it mean when software is ''XBRL-enabled''?
2. Identify at least five advantages that Lloyd might discuss with Dick and Denise regarding an XBRL-enabled software solution. Identify any disadvantages that might also be relevant for HMC.
3. Assume that you are Lloyd's research assistant. Draft a memo for Lloyd to give to HMC that explains how XBRL works. Remember to keep in mind your audience. This should be an executive-level piece of correspondence.

4. Now, as the research assistant, develop a PowerPoint presentation for Lloyd to give to Dick and Denise explaining exactly what sorts of benefits they could realize with an XBRL-enabled software solution. Be creative, and use diagrams and examples where appropriate.

15-27. DeGraaf Office Supplies (Business Websites and Security)

DeGraaf Office Supplies is a national retailer of office supplies, equipment, and furnishings. The company opened its first store in 1932, in Columbus, Ohio. Currently, DeGraaf has 300 stores nationwide. Owner-managers purchase and run franchised stores. Kim DeGraaf, the founder's daughter, currently is President and CEO of the corporation.

Sales revenues grew steadily during the past decade, but 2009 sales were quite disappointing, down 8% from 2008. The company's stock price has also taken a big hit during the past few months. Kim resisted developing an Internet presence for the company, and it appears now that this was a mistake. Online sales of office supplies are growing rapidly, particularly in the business-to-business sector as business organizations are finding it faster and more efficient to enter their office supply orders electronically. The following is a conversation between Kim and Peter Brewer, Vice President of Marketing.

Peter: ''Kim, I warned you that we were going to see sales decline if we didn't hurry up and get on the Internet. The established brick-and-mortar businesses in many industries are suffering.''

Kim: ''You were right, Peter. I think I've been overly concerned about security and privacy issues. I also didn't really believe that online sales in our industry would take off the way they have. I hope we're not too late, because I want to move ahead immediately in developing a website. I know other companies have a jump start but hopefully our brand name recognition and reputation for quality will help us. I have contracted with a consulting firm to start the website development and am going to give a press release this afternoon about our plans. Fortunately, our current enterprise software has electronic commerce features and the consultants tell me that our Internet site should be ready for business in about six months. I need you to have your staff prepare an analysis of our competitor websites. I would also like as much information as possible related to providing retail and business customers with security and privacy over online transactions with us.''

Peter: ''This is great news! I will get my staff busy at once providing you and the consulting team with the information they need. There will be a lot of decisions to make. I've studied all the office supply websites and they are organized in a variety of ways. For instance, some sites provide customers with the option to select a type of product such as ballpoint pens and then show the vendor options in that category, while other sites are organized around the vendors. This type of site allows customers to select a vendor name, such as PaperMate, and then lists all the product offerings from that vendor. Hopefully, the consultants have a lot of experience with business websites and they can help us with many of these issues.''

Requirements:

1. Visit the websites of two office supply stores on the Internet. Develop a set of four to five criteria for evaluating their website.
2. Evaluate DeGraaf's chances for catching up to competitors in the online marketplace.
3. Discuss the privacy and security concerns for companies doing business electronically. Make recommendations to DeGraaf Office Supplies for addressing these concerns.

15-28. Barra Concrete (XOR Encryption)

Barra Concrete specializes in creating driveways and curbs for the residential market. Its accounting software uses exclusive OR (XOR) operations to convert the individual bits of a plaintext message into cyphertext. The rules are as follows:

	Exclusive OR rules			
	Rule 1	Rule 2	Rule 3	Rule 4
Plaintext bit	0	0	1	1
Bit in key	0	1	0	1
Cypertext result	0	1	1	0

In other words, exactly one of the bits must be a ''1'' and the other a ''0'' for the result of an exclusive OR operation to be a ''1.'' To illustrate, suppose that the bits representing a single plaintext character were 1010 0101 and the secret key used just the four bits 1110. Here are the results of the XOR operation, using this key:

Plaintext bits	1010	0101
Key (repeated)	1110	1110
Cypher text result	0100	1011

The encrypted bits are the cypher text, or 0100 1011 as shown. These (encrypted) bits are what the software would transmit to the recipient.

Requirements:

1. Decrypting the cipher text created by an XOR operation is easy—just use the same XOR operation on the encrypted bits! Demonstrate this for the example above.
2. Suppose the secret key were longer—the eight bits 1100 0011. Using this key and an exclusive OR, what is the cipher text for the plaintext message ''Go, team'' if the bit configuration for these letters is as shown below. (Hint: the final answer consists of seven sets of data, each containing eight bits.)

Message	G	O	,	T	E	A	M
Binary	0100 0111	0100 1111	0010 1100	0101 0100	0100 0101	0100 0001	0100 1101

REFERENCES AND RECOMMENDED READINGS

Bannan, Karen J. ''Detecting, Defeating Click Fraud,'' *B to B* Vol. 92, No. 2 (January 15, 2007), pp. 15–19.

Brandt, Andrew. ''The 10 Biggest Security Risks You Don't Know About,'' *PC World* Vol. 24, No. 8 (August 2006), pp. 76–88.

Burnett, Royce D., Mark Friedman, & Murthy Uday. ''Financial Reports: Why you Need XBRL,'' *Journal of Corporate Accounting and Finance* Vol. 17, No. 5 (July/August 2006), pp. 33–40.

Cranor, Lorrie Faith. ''Can Phishing be Foiled?'' *Scientific American* Vol. 229, No. 6 (December 2008), pp. 104–110.

Douglas, Heather. ''E-Commerce and the Home Business,'' *NZ Business* Vol. 20, No. 5 (June 2006), p. 63.

Farwell, Stephanie M. ''An Introduction to XBRL through the Use of Research and Technical Assignments'' *Journal of Information Systems* Vol. 20, No. 1 (Spring 2006), pp. 161–185.

Glover, Hannah. ''Next XBRL Frontier: Fund Disclosures,'' *Money Management Executive* Vol. 14, No. 19 (June 2006), pp. 1–34.

Hannon, Neal J. ''XBRL Alliances: Shall We Dance?'' *Strategic Finance* Vol. 87, No. 12 (June 2006), pp. 6–8.

Hucklesby, Mark. ''The Latest on XBRL,'' *Chartered Accountants Journal* Vol. 85, No. 4 (May 2006), pp. 46–47.

IASC Foundation XBRL Team. ''Fundamentals of XBRL,'' International Committee Standards Foundation website: www.iasb.org/xbrl/about_xbrl/fundamentals_xbrl.html (2006).

Kersnar, Scott. ''Will 2006 be Record Year for Online Identity Theft?'' *Mortgage Servicing News* Vol. 10, No. 7 (August 2006), p. 22

Kirchheimer, Sid. ''Scams Unmasked!'' *AARP Magazine* (May/June 2006), pp. 78–82.

Levey, Richard H. ''Security Leads Global IT Priorities,'' *Direct* Vol. 18, No. 7 (June 15, 2006), p. 5.

McMillan, Paul. ''E-Commerce Activity Doubles in the Last Year,'' *Money Marketing* (no volume or issue numbers) (July 6, 2006), p. 16.

Rosencrance, Linda. ''Blogs Bubble into Business,'' *Computerworld* (January 26, 2004), p. 23–4.

Samwel, Emad. ''E-commerce: Does Anyone Care?'' *Journal of Commerce* Vol. 7, No. 28 (July 10, 2006), p. 34.

Walper, George & Catherine McBreen. ''Identity Thieves Target the Affluent,'' *On Wall Street* Vol. 18, No. 10 (October 2008), pp. 66–70.

White, Skip. *The Accountants Guide to XBRL* (Delaware: SkipWhite.Com, 2006).

ANSWERS TO TEST YOURSELF

1. **c** 2. **d** 3. **c** 4. **b** 5. **d** 6. **a** 7. **c** 8. **d** 9. **a** 10. **c**