Millions of Credit Cards Stolen from Online Site.” “Vast Online Credit Card Threat Revealed.” “FBI Warns of Credit Card Rings that Prowl Web.” It's no wonder many consumers are still leery of using credit cards to order merchandise online. But what’s ironic is that while all the attention is being paid to the risks consumers face from online credit card fraud, which are actually relatively minimal for the customer, it is usually the merchant who ends up the victim.

Neil Kugelman's company Goldspeed.com is a case in point. Goldspeed sells jewelry online, an ideal target for fraudsters because of the high value of goods. Neil has become an expert at detecting fraudulent orders, which in 2005 totaled about 30% of all orders. One red flag is an order that has a different shipping, billing, and customer address. Those orders get denied, as do orders that do not include the credit card's three-digit security code. But one recent order cost his company $8,384, despite taking all known protective measures! A customer named Vincenza Wells ordered an $1,199 Aqua Master men's diamond watch and four minutes later, ordered a $1,259 diamond ring. Kugelman thought something must be wrong. He checked to make sure the billing, shipping, and customer addresses were identical, and checked for the security code. That afternoon, the same customer ordered another $5,950 in jewelry. He then called the bank that issued the Visa credit card being used, to confirm the name, address, and phone number of the customer. Finally he checked the account balance to ensure the card was not maxed out. He asked the bank to verify all the information and it did. When everything checked out, he released the goods and shipped. Then, he lost the entire value of the order.
What Kugelman and the bank did not count on is that someone had stolen Vincenzo Well's identity, including address, social security, and other information when she responded to a telephone offer of free cable TV service a month earlier, and set up an entirely new account using her name. She gave all her personal information, including credit card number, to the caller. The caller ran up thousands of dollars in phony charges, including the Goldspeed jewelry. A Visa arbitration panel determined that Kugelman would have to eat the entire loss. Visa declines to comment on the case. Kugelman feels that with so much identity theft going on, it is nearly impossible for him and his staff to figure out which of the 50,000 orders they receive are fraudulent. One thing for sure; his company is facing a huge risk.

Credit card fraud costs Web merchants over $1.4 billion annually. Now, retail executives are uniting to fight credit card fraud online. The Internet Merchant Risk Council, a non-for-profit group of large retail industry member merchants, is working to help e-commerce companies set up a database to counter credit card fraud on the Web. They hope to block fraudulent sales and help to catch those who commit online fraud. The Federal Reserve has formed the Payments System Development Committee (PSDC) to address issues such as identify theft of consumer information.

In the "off-line" world, when a credit card is stolen and then used to purchase merchandise, if the merchant has followed proper procedures (such as obtaining a signature and checking it against the signature on the back of the card), the credit card issuer absorbs the cost.

Many of the security procedures that the credit card companies rely on are not applicable in an online environment. Internet credit card charges fall under the heading of CNP (cardholder not present) transactions. As a result, typically there is no tangible signature to check and hold as proof that a customer actually placed an order. Internet speed means that a high volume of purchases can be processed before the credit card company or consumer becomes aware that a card has been stolen. The global nature of the Internet is another consideration. Credit card companies can verify addresses of U.S. residents, but not those of international buyers. In some instances, such as digitally delivered products like downloads of software, there is no address—the product is "shipped" directly and immediately to the purchaser's computer.

As a result, credit card companies have shifted most of the risks associated with e-commerce credit card transactions to the merchant, even though the credit card company supposedly authorizes the transaction. So, although a card owner is only liable for the first $50 of unauthorized purchases, online merchants that are victims of credit card fraud are generally liable for everything they ship.

The percentage of Internet transactions that are charged back to the online merchant is much higher than for traditional retailers—from 3%–10% for online retailers compared to one-half of 1% for traditional retailers, according to industry estimates. The merchants lose more than just the cost of the goods. They lose the cost of shipping goods, the administrative cost of dealing with the problem transactions, and so-called "charge back" fees that banks demand to offset their own administrative costs. Then there are the orders that online merchants reject in their determination to prevent fraud. No one knows the size of these unfilled orders.
So how can an online merchant protect itself? Some refuse to process purchases from overseas customers because numerous studies have found that overseas criminals account for up to one-third of all online fraud within the United States today. Others no longer take credit card orders online, or they rely on PayPal for small purchases. Many insist that the billing address on the credit card and the shipping address match—perhaps the most common check. Others ask for the security code on the back of the card. Criminals with stolen cards hardly ever ship the goods to the legitimate card holder, and often the criminals do not have a physical card, only a digital card number, usually without the security code. According to the Merchant Fraud Squad, a nonprofit group based in New York, about half of all online merchants now require users to type in the three-digit security code that is printed on the back of credit cards. These codes are effective in preventing fraud in those cases where the card number—and not the card itself—is stolen. Larger companies have developed their own sophisticated software to track both stolen cards and customers who have attempted fraud in the past. Small merchants can purchase anti-fraud software from a variety of firms, or take advantage of services such as Yahoo’s OrderProcessor, which stops suspicious orders and requires manual authorization by the merchant.

The ultimate solution to merchant credit card fraud lies with Visa, MasterCard, and their issuing banks assuming a larger share of the risk and liability. Visa says its online e-commerce business is growing at 50% a year, and that e-commerce now accounts for 5% of its sales volume, but 10% of its fraud. Visa’s solution: a program called Verified by Visa in which customers are vetted by Visa and issued a security code. Customers then can use this security code at online retailers, who are guaranteed payment. If a fraud occurs, Visa pays the merchant. Visa has shared the program code with MasterCard International, which now markets a program called SecureCode. MasterCard’s SecureCode runs on your Web site and interacts with both the customer and their card issuer. When your customer is checking out, a simple pop-up box appears asking them to enter a private code that has been registered with their bank. Their bank then validates that code and provides you with a means of achieving a fully guaranteed transaction.

To encourage online merchants to participate, Visa and MasterCard are promising to shift the liability for fraud to the card-issuing banks. Unfortunately, so far, most online merchants are not taking advantage of these programs.

**Sources:**
- "A Summary of the Roundtable Discussion on the Risk and Security Involving Retail Payments over the Internet," The Federal Reserve Board, September 21, 2005;
'EVIL TWINS' AND 'PHARMING': KEEPING UP WITH THE HACKERS

Phishing is passé. Very 2005. The latest hacking inventions are “evil twins” and “pharming.” Both make effective use of social engineering techniques and the plain gullibility of people. But these new techniques also play on built-in vulnerabilities on the Internet. You have to run fast to keep up with the hackers online. Remember: They do this for a living.

Phishing attacks are now widely recognized. The bait is sent via e-mail to an unsuspecting user, asking for account verification or other personal information. If the user clicks on the link, he or she will be taken to a site that looks like their bank or another Web site, and asked to enter login, password, and other information. Phishing requires the user to be deceived by the e-mail and the site.

Pharming takes the process one step further. Here the user does not have to do anything out of the ordinary. Hackers instead capture a domain name, such as Amazon.com, and when users enter the URL into their browser, they are directed to a site that looks just like Amazon, but in fact is a spoof (fraudulent copy) of the real Amazon.com site. Once there, the user is asked to enter login and password or financial information, which is then stolen by the hackers and either sold or used to steal funds from the user’s financial accounts. Many believe pharming is more dangerous than phishing because millions of users can be re-directed to phony sites without taking any unusual action, or responding to any e-mail (which often has obvious misspellings or looks odd and can be detected by the informed user).

How can hackers do this? It’s all about the domain name system and DNS servers. Every time you enter a domain name into your browser, the request is sent to a nearby DNS server that resolves the English-like domain name into a numeric IP address (review Chapter 3). These DNS servers are located all over the Web, starting with one on your own local area network, right on up to the country’s root DNS servers. Generally, local DNS servers resolve most names. The problem is that DNS server software can be targeted by hackers so that users receive the wrong IP address.

For instance, in January 2003, someone changed the DNS address of Panix.com, a New York ISP. The IP address was changed to a company in Australia, requests to reach Panix.com were re-directed to a site in the United Kingdom, and e-mail was directed to a site in Canada. In March 2005, the SANS Institute uncovered a single cache-poisoning attack that re-directed 1,300 brands, including ABC, American Express, Citi, and Verizon Wireless. In April 2005, Hushmail’s main name server’s IP address was changed to that of a hacker graffiti site.

Evil twins are yet another new scam. An evil twin is a wireless access point (hot spot) that masquerades as a legitimate site but in fact is designed to fool people into entering financial and other information. It turns out to be fairly easy for hackers to set up a phony wireless access point by positioning their laptop close to the legitimate access point to discover the frequency and name, and then moving closer to unsuspecting users in, say, an airport. The users’ wireless card will default to the strongest signal—in this case, the phony site’s signal. Once fooled, the user will be asked to enter information that can later be used by the hackers for financial gain. In April 2005, at a technical conference in London, fraudsters set up a Wi-Fi network masquerading as the

(continued)
conference's legitimate network, and then later, as networks from BT Group PLS and T-Mobile. A conference in Las Vegas produced several evil twin networks pretending to be either T-Mobile (a legitimate wireless network provider) and a Hilton Hotel network.

There are some potential solutions to both pharmling and evil twins. The solutions rely on both the user and the Web site server using digital certificates to authenticate Web sites. In the case of evil twins, the user needs to use only Web sites with secure Web pages that begin with "https" rather than the standard "http." The user's browser will automatically check the digital certificate of such sites and alert the user if the certificate presented does not match. In the case of pharmling, the use of digital certificates could easily prevent the spoofers. But generally, most users shy away from using digital certificates because they do not understand them. Therefore, pharmling and evil twins are likely to continue to plague the Web for at least some time to come.


**DENIAL OF SERVICE (DOS) AND DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS**

In a Denial of Service (DoS) attack, hackers flood a Web site with useless traffic to inundate and overwhelm the network. Increasingly, DoS attacks involve the use of bot networks built from hundreds of compromised client computers. According to Symantec, the number of DoS attacks per day grew from 119 during the last six months of 2004 to 927 during the first six months of 2005, an increase of 679% (Symantec, 2005). DoS attacks typically cause a Web site to shut down, making it impossible for users to access the site. For busy e-commerce sites, these attacks are costly; while the site is shut down, customers cannot make purchases. And the longer a site is shut down, the more damage is done to a site's reputation. Although such attacks do not destroy information or access restricted areas of the server, they can destroy a firm's online business. Often, DoS attacks are accompanied by attempts at blackmailing site owners to pay tens or hundreds of thousands of dollars to the hackers in return for removing the DoS attack.

One type of DoS attack, called a smurf, brings a network down by sending out a request to many broadcast addresses—an address that can communicate with up to 255 host computers—to verify that the address is working. (This is called a Ping request, for Packet Internet Groper, discussed in Chapter 3.) When the 255 hosts on each broadcast address reply to the verification request, the hacker spoofs the IP address, listing a particular company's server as the supposed reply address. Soon the victim company's server is quickly inundated with thousands of Ping responses that tie it up.

A distributed Denial of Service (DDoS) attack uses numerous computers to attack the target network from numerous launch points. For instance, on February 1, 2004, hackers launched one of the largest DDoS attacks in history against the SQ
ADVANCES IN QUANTUM CRYPTOGRAPHY MAY LEAD TO THE UNBREAKABLE KEY

Today's digital encryption techniques rely on algorithms that mathematically transform a text message into an undecipherable cipher text. There are several problems with this method. As computers become more and more powerful, the duration of the protection becomes shorter and shorter. While it might take a contemporary PC over a year to decipher a message, in a couple of years, ordinary PCs could decipher that same message in a few months or even days because of their greater speed. The potential development of so-called "quantum computers," which are orders of magnitude more powerful than today's fastest computers, would mean most of today's "secure" information would be easily and quickly deciphered. With mathematically based encryption, in order to extend the period of security, it will be necessary to keep extending the size of the encryption key. As keys get longer, they produce much longer messages and the entire Internet slows down. The keys become so cumbersome that they are used to encrypt only the most sensitive information. What's needed is an encryption system that would be immune to any increases in computing power likely to occur ever: the everlasting unbreakable key. This has seemed an impossible task until recently.

In November 2002, scientists at Northwestern University reported that they had developed a high-speed quantum cryptography method that allowed them to send encrypted data over a fiber-optic line at 250 Mbps, more than 1,000 times faster than what was achievable with existing quantum technology.

The research team, led by Northwestern professors Prem Kumar and Horace Yuen, used standard lasers and existing optical technology to transmit a large bundle of photons, the particles that make up light. The Northwestern technique uses a form of "secret key" or symmetric key cryptography, in which the two people communicating with each other use the same secret key. The Northwestern technique uses the granularity of light, known as quantum noise, which is revealed only through the secret key's pattern. One method the team used to change the light's granularity was randomly polarizing the light. To an eavesdropper who does not have the key, the data is indecipherable because the lifted message emits too much fuzz. However, the recipient, who has the secret key, can get the pattern and can receive the signal with much less disturbance. This allows him to decipher the message.

The first money transfer encrypted by quantum keys was performed between two Austrian financial institutions in April 2004. However, sending a secure quantum-encrypted message from one computer to another is child's play compared to creating a network of computers capable of sharing such encrypted information. In June 2004, a group of scientists at Harvard and private research firm BBN set up the first computer network in which communication is secured with quantum cryptography. The project is funded by the Pentagon's Defense Advanced Research Projects Agency.

The network, known as Quantum Net (Qnet) currently consists of six servers, but ultimately could be attached to the Internet. The data in Qnet flows through ordinary fiber-optic cables over a distance of about 10 kilometers, from BBN to Harvard University. The data is encrypted using keys determined by the exchange of a series of single, polarized photons. Software-controlled
optical switches made of lithium niobate crystals steer the photons down the correct optical fiber.

Quantum cryptography works as a method of securing communication by taking advantage of the quirks of photons. An attempt to intercept the photons disturbs their quantum state and alerts users that someone has tampered with the communication. But even quantum cryptography does not provide 100% security. Although quantum keys are theoretically impossible to intercept without detection, in reality, there are several potential ways they can be observed. For instance, lasers may produce more than one photon, and an eavesdropper could potentially siphon off the extra photons and decrypt the key. Nevertheless, quantum cryptography is considered to be more secure than current Internet cryptography.

The first commercial applications of quantum cryptography are now just beginning to appear. In June 2005, a French company, id Quantique, began offering an encryption solution based on quantum cryptography. This service is aimed at businesses and government agencies with a need for flawless data confidentiality.


messages exchanged. However, once the merchant receives the encrypted credit card order information, that information is typically stored in unencrypted format on the merchant’s servers.

While the SSL protocol provides secure transactions between merchant and consumer, it only guarantees server-side authentication. Client authentication is optional.

In addition, SSL cannot provide irrefutability—consumers can order goods and then claim the transaction never occurred. Other protocols for protecting financial transactions such as SET (Secure Electronic Transaction Protocol) have emerged that require all parties to a transaction to use digital certificates. SET is discussed further in Chapter 6.

**Secure Hypertext Transfer Protocol (S-HTTP)**

A competing method is called Secure Hypertext Transfer Protocol (S-HTTP). S-HTTP is a secure message-oriented communications protocol designed to use in conjunction with HTTP. It is designed to coexist with HTTP and to be easily integrated with HTTP applications. Whereas SSL is designed to establish a secure connection between two computers, S-HTTP is designed to send individual messages securely. Not all browsers and not all Web sites support S-HTTP. You know you are dealing with a supporting site when the URL starts with "SHTTP." The use of this as part of an anchor tag indicates that the target server S-HTTP capable. Using S-HTTP, any message may be signed, authenticated, encrypted, or any combination of these. Basically, S-HTTP attempts to make HTTP more secure.
How do you find out if your Web site or corporate system is vulnerable? There are typically two accepted ways to understand your security vulnerabilities: perform a security audit led by your own internal security officials, or hire an outside, independent team of hackers and ask them to attempt to break into your system. The problem with having your own security officials perform a security audit is that they often cannot see the vulnerabilities of systems they have built themselves. Hence the concept of hiring "tiger teams" of computer experts to attack systems arose. Tiger teams originated in the 1970s with the U.S. Air Force, which used special teams of experts to test security vulnerability at bases. The idea spread throughout the government and, in 1973, the Department of Defense documented the use of tiger teams to assess computer security. By the 1980s and into the 1990s, the use of tiger teams had spread into the corporate arena, with companies hiring elite squads of consultants to break into their computer networks by any means necessary. Today, the phrase "tiger teams" has been largely replaced by the much more up-scale, professional, and clinical term "penetration specialist." There are even professional associations of penetration specialists such as the Institute for Security and Open Methodologies (ISECOM) and the Open Information Systems Security Group (OISSG), both of which have established methodologies for penetration testing. And the federal government's National Institute of Standards and Technology (NIST) describes penetration testing in Special Publication 800-42, Guideline on Network Security Testing.

Worldwide, firms spent over $18 billion in 2005 on information technology security services and an unknown percentage of that went to "white hat" hackers (supposedly the good guys) to act as penetration specialists by trying to break into corporate systems. Big consulting firms such as Ernst & Young and PricewaterhouseCoopers pull together groups of penetration specialists on behalf of their clients. And companies such as IBM Research form their own investigative teams, using white hat hackers as contractors. In some cases, corporations considering partnerships with smaller firms require that they consent to an attack by the firm's penetration specialists, a failing grade results in the partnership going further.

Some clients have been surprised at the lengths to which these teams will go to break into secure networks, including dumpster diving for scraps of computer paper, stealing ID badges, and crawling through ceiling tiles to access computer rooms. Mark Seiden is one specialist who was given an assignment from a bank to see if he could find out the two most valuable pieces of information in the bank: the names of firms and individuals in pending merger deals and the financial details of the plans. Within a week Seiden produced both of these deep dark secrets plus keys to the bank's International offices, fire plans for each office, and a suitcase stuffed with backup tapes that would allow a bad hacker to steal much of the bank's customer information.

One thing most companies will not do is hire unknown grey or black hats for penetration specialist assignments. Although some claim to have "gone straight" and work only under contract, security consulting firms are wary of them, afraid that in breaking into a client facility, these grey or black hats may try to profit from the assignment.
Some penetration specialists are so dedicated to improving the operations of computer networks everywhere that they run their own drills, testing major sites and then publicly reporting on weaknesses they discover. One such famous specialist is Johnny Long, whose Web site, johnny.ihackstuff.com publishes some of the Internet’s more famous vulnerabilities, including really dumb logins and passwords. Perhaps his most famous contribution has been to catalog the ways in which Google can be used by hackers to discover logins, passwords, and identify the structure of a target Web site. For instance, searching on "nasa.site" will reveal a list of NASA’s servers. However, as specialists publish weaknesses they discover in Web sites, they potentially create more problems than they solve, and can quite easily move over into the black hat and grey hat camps of hackers who encourage hacking rather than discourage it. For instance, Long’s work with Google has spurred thousands of hackers to use the power of modern search engines to discover flaws in business Web sites.


THE ROLE OF LAWS AND PUBLIC POLICY

The public policy environment today is very different from the early days of e-commerce. The net result is that the Internet is no longer an ungoverned, unsupervised, self-controlled technology juggernaut. Just as with financial markets in the last 20 years, there is a growing awareness that e-commerce markets work only when a powerful institutional set of laws and enforcement mechanisms are in place. These laws help ensure orderly, rational, and fair markets. This growing public policy environment is becoming just as global as e-commerce itself. Despite some spectacular internationally based attacks on U.S. e-commerce sites, the sources and persons involved in major harmful attacks have almost always been uncovered and, where possible, prosecuted.

Voluntary and private efforts have played a very large role in identifying criminal hackers and assisting law enforcement. Since 1995, as e-commerce has grown in significance, national and local law enforcement activities have expanded greatly. New laws have been passed that grant local and national authorities new tools and mechanisms for identifying, tracing, and prosecuting cybercriminals. Table 5.3 lists the most significant federal e-commerce security legislation.

Following passage of the National Information Infrastructure Protection Act of 1996, which makes DoS attacks and virus distribution federal crimes, the FBI and the Department of Justice established the National Infrastructure Protection Center (NIPC). Now subsumed within the National Cyber Security Division of the Department of Homeland Security, this organization’s sole mission is to identify and (continued)