CHAPTER 1

Motive

Have you ever seen a bank robbery? Before the Web, the chance that you would have seen an actual bank robbery was quite small. Today, though, if you have e-mail, it is almost certain that you have been targeted by bank robbers.

By the last count, I receive more than 2,500 criminal e-mails a day. These criminals want my money; they want your money. How are we going to stop them?

The first step toward finding an answer is to understand how the crimes work. Knowing how Internet crimes work will do little to reduce the number of victims: it will only take a little longer for the criminals to find them. It is, however, the best way to make sure *you* do not become the victim.

Internet crime is real. It's organized. Internet criminals have stolen hundreds of millions of dollars and caused billions of dollars' worth of damage. The number of attacks and their sophistication is on the rise, and this trend is expected to continue for the next several years.

In the early years of the Web, Internet crime was mostly the actions of teenage vandals looking for a way to pass time. Attempting to make money from hacking was considered too risky, too likely to attract the attention of the authorities. Today it's all about the money.

One consequence of this change is that Internet crime has become much easier to predict. Only the most obsessive vandal would attempt the same crime in the same way, again and again for long enough for investigators to build a profile. The professional criminal does not become bored so easily and will keep doing what he is doing until the act no longer makes money or he is caught.

The Internet criminal changes his tactics frequently. The techniques that Internet criminals used to perform bank fraud three years ago simply do not work today. The techniques they are using today are not likely to be as profitable or as safe in three years' time. But the goal of the professional Internet criminal remains the same—to take money from other people—and so do the three basic strategies that he uses to achieve this goal: extortion, impersonation, and persuasion.

- **Extortion**—Criminals have operated extortion rackets for millennia. The Internet is a major engine of the global economy. Many companies cannot carry out their business when their Web site is down. A criminal who can make a site unreachable may find businesses willing to pay for protection.
- **Impersonation**—The money that the criminals are after is mostly stored in banks. Taking the money from the bank directly is far beyond the capabilities of most Internet criminals. Instead, they attack the system at its weakest link: the customer. The customer has access to his bank account through the Web. All the attacker needs to do is to cause the customer to divulge his account name and password.
- **Persuasion**—The most pervasive type of Internet crime is the confidence trick. The larger the pool of potential victims that the attacker can reach, the less credible the story needs to be. The Internet allows a criminal to reach an audience of more than a billion.

Internet crime is a mile wide and an inch deep. What appears at first glance to be something new invariably turns out to be a new way to perform an old scam.

The Tools of the Trade

The tools of the Internet criminal are chosen for effectiveness rather than sophistication. The Internet allows the criminal to contact a vast audience of potential victims, to communicate in ways that are difficult to trace, and to collaborate with other criminals. Criminals have always done such things but on a smaller scale. The Internet gives the criminal enterprise global reach and the whole world to hide in.

The Internet also gives the criminal a new capability: the ability to spy on the activities of people who are not in their immediate vicinity by taking control of their computer.

Of Bots and Botnets

Traditional criminals use stolen cars as getaway vehicles. Cyber criminals cover their tracks using stolen machines but do one better—the real owner continues to pay for gas.

Many Internet users believe that they are not at risk from Internet crime because they have nothing of value on their computer. But the computer itself has a value to the Internet criminal. The thief can steal the use of the machine without taking the physical machine, but the owner continues to provide the necessary space, power, and network connectivity.

In hacker jargon, there are many names for a machine that has been taken over. News reports often use the terms **bot** or **zombie**; within the field, the term **owned machine** is sometimes used.

Control of one bot gives the criminal a getaway vehicle. Running an Internet crime from your own house using the network connection you (or your parents) pay for is risky. Channeling communications through a bot allows the Internet criminal to lay a false trail.

The sophisticated criminal hides his activities through a constantly changing series of machines carefully chosen so that the trail passes through as many jurisdictions as possible.

Bots are also used to perform the crime itself. A bot can be used to attack other machines, to send spam, and to create other bots, forming a **botnet**. The more bots an Internet criminal controls, the more crime he can perform. Most worrying of all, perhaps, a bot can spy on the owner of the machine and watch as he logs in to his online bank or enters his credit card number.

Some years ago, taking over (**cracking**) machines was a bespoke industry. The attacker would select a machine and work on ways to break into it until something worked or he decided to give up and move to another target. Today it is easy to obtain hacking tools that probe thousands of machines at a time.

Botnet management has become a commodity, a low-skill, low-return Internet crime. Skilled professional criminals often prefer to "rent" the use of bots. A bot is priced on the black

market according to the utility to the criminal: the speed of the Internet connection, the speed of the processor, and whether the network management is likely to shut it down quickly.

An attacker can gain control of a machine in much the same way that an army can capture a walled city: by direct assault or by subterfuge.

A direct assault requires the attacker to find an exploitable vulnerability in the defenses of the machine. Computers have no common sense; they just follow instructions. If a program is written properly, the only instructions that the computer will execute are the ones the programmer writes. If a program has a specific type of programming error, the computer might end up executing instructions that an attacker supplies.

A direct assault is unlikely to compromise a "securely" configured machine with every nonessential service turned off and every security fix installed. With a billion users and a billion-plus machines, there will never be a shortage of vulnerable targets.

Every machine that is connected to a network and has some form of processing capacity is a potential point of compromise: every router, every wireless gateway, every cable modem, every printer.

The vandals competed to crack the machine in the most ingenious ways they could. The professional Internet criminal is only interested in results and accordingly attacks the system at its weakest link: the user. Why bother working out how to bypass the computer defenses when the user can run any program you want? All you need to do is to persuade him to run it.

A program that has a hidden malicious purpose is called a **Trojan** after the Trojan horse of Greek legend. Mistaking the horse for a parting gift, the Trojans wheeled it into their city and left it unguarded while they went off for a feast. During the celebrations, the soldiers hidden inside the horse quietly slipped out and opened the city gates to let the waiting Greek army through.

Computer Trojans work in the same way. The user thinks that he is doing something harmless while the Trojan takes over his machine.

Five years ago, a Trojan attack could be neatly classified as a **virus**, **worm**, or **spyware**. But the changing tactics of the criminals have rendered the distinction obsolete. The terms **malware** and even **crimeware** have been introduced in an attempt to keep pace.

A true computer "virus" spreads from one infected machine to another as a biological virus does. Today the analogy is obsolete. Instead of waiting for their creations to spread gradually from one machine to another, the criminals pump out Trojan-bearing e-mails from a botnet.

Equally obsolete are the tools based on the assumption that the criminals will continue to respect these distinctions.

By the time the "virus" has been detected and analyzed, and "antivirus" signatures have been distributed, the attack will already have reached tens or hundreds of millions of machines, and the attacker will be busy creating his next attack.

When spyware first began to appear as a significant concern for computer owners, it was mostly ignored by the suppliers of "antivirus" software. It took a new group of vendors offering antispyware solutions for the antivirus vendors to realize that their customers expected to be protected from all forms of harm regardless of cause.

Spam

In the words of FTC Commissioner Orin Swindle,[1] "Spam is killing the killer application of the Internet." But spam is no longer merely a nuisance that threatens to make e-mail unusable; spam is one of the primary vehicles for Internet crime. Virtually every Internet crime involves spam at some point, and most spam is sent to further a criminal end.

Spam frauds range from simple consumer frauds such as peddling quack medicines and bogus get-rich quick schemes to sophisticated confidence tricks. The vast majority of spam products are fake, stolen, or nonexistent. Spam is cheap, difficult to track, and provides access to a billion potential victims.

Stopping spam is widely considered to be an intractable technical problem. That's true: The cause of spam is social, not technical. Spam can, however, be controlled and to a large extent "solved" by a social solution, and technical measures can be designed to support that social solution.

There is no "technical solution" for graffiti either. The problem of graffiti has existed for thousands of years, as the remains of Pompeii attest. But as New York City Transit Police Chief William J. Bratton demonstrated, control of graffiti is entirely practical given the necessary determination and resources. Bratton's "policy" of erasing the work of vandals within 24 hours of its being created coupled with a zero-tolerance policy toward fare-dodging and other types of vandalism had a noticeable effect. Technical measures such as graffiti-resistant paint are not by themselves a solution, but the right technical measures can make a social solution possible or more effective.

The problem of spam is caused by the lack of accountability in the e-mail system. The social solution to the spam problem is to establish accountability. How this is done is the topic of later chapters.

Like graffiti, the problem of spam was largely ignored as a nuisance until people decided that the problem mattered. Users who complained that their electronic Inbox was full of junk were told not to worry about such a trivial matter; just don't respond to it.

The catalyst for the New York subway graffiti crackdown was the "broken windows" theory[2] that tolerance of minor crimes creates an environment perceived to be permissive of crime that leads to major crimes.

Whether the broken windows theory is true and whether the zero-tolerance policy is the main cause of the reduction in crime is open to debate. Social change almost never has a single cause. If we wait for absolute certainty before we act, we can be certain of only one thing: Our actions will come too late.

Internet Crime Markets

The term **organized crime** suggests a single group of criminals organized in much the same way as a business. Al Capone and his fellow bootleggers organized their criminal enterprises using the principles of modern business management then being developed by Alfred Sloan and others. Professional Internet criminals continue the tradition, applying the organizational principles of the "virtual corporation" long before the legitimate businesses of the day have fully realized them. A free-market approach is

pursued in which individual criminals or groups of criminals specialize in particular tasks, selling their services to others or buying services that they need.

Stolen credit card numbers are traded in numerous criminal venues that are exchanged in chat rooms or offered for sale on bulletin boards. In some cases, the sellers even have Web sites offering their product. Figure 1-1 shows a Web site offering stolen credit cards (referred to as **dumps**) priced according to the card issuer, the region the card was issued, the credit limit, and so on.

Figure 1-1 *Online trading site for stolen credit card numbers, or dumps*

Criminals with technical expertise sell information and tools to the less expert criminals who do the actual dirty work. Like traditional arms merchants, these experts occupy a gray area of dubious legality. Some of the tools they sell might have legitimate purposes as well as criminal ones. A security scanner, for example, is used to detect the vulnerabilities in a system, but this can be done by a legitimate "white hat" hacker to identify a system needing attention or by a criminal "black hat" hacker looking for a vulnerability to exploit.

To make the situation even more murky; there is more than anecdotal evidence to suggest that some play both sides of the fence. The Internet security world is like a John le Carré spy novel; it is difficult to know the good guys from the bad.

Fortunately, the system works both ways: The bad guys cannot know which of their associates might turn out to be a police plant. This has allowed law enforcement to deal effectively with certain Internet crimes, such as attempts to establish online pedophile rings. A pedophile can never be sure whether the other person in the Internet chat room is really the 12-year-old child he thinks or an undercover police officer.

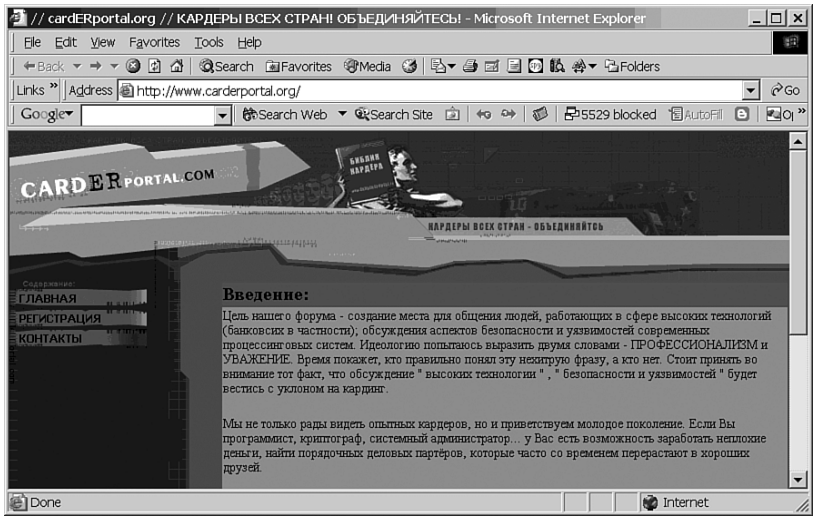

Figure 1-2 *Russian site offering advice on carding crime*

Figure 1-2 shows a Russian Web site (since closed) that provided online forums for various forms of Internet crime, including **carding**—the use of stolen credit cards. The banner on the site logo reads, "Carders of all lands unite." The picture is of Lenin, but the quotation is adapted from Karl Marx's closing lines to the Communist manifesto. The choice is somewhat unfortunate from the carders' perspective because the original quotation continues, "You have nothing to lose but your chains." Anyone who wants to avoid chains would be better advised to steer clear of carding rings, as the U.S. Secret Service and Department of Justice demonstrated in **Operation Firewall**, a multinational investigation of the **Shadowcrew** carding organization, which resulted in 28 arrests, including seven in foreign countries. The Shadowcrew Web site was taken over by the U.S.

Secret Service, who used it to send a message to the carding rings (see Figure 1-3).

Figure 1-3 *The Shadowcrew Web site after Operation Firewall*

The Internet allows criminals to communicate secretly and anonymously with others of their kind. Payment for services rendered might be made by wire transfer or courier service envelopes stuffed with up to $20,000 in used bills or through more anonymous means such as a gift card bought with cash or an anonymous Internet currency such as e-Gold.

Although it would take an entire book to describe every detail and development of every Internet crime, most are variations of the same basic schemes, which in turn are adaptations of much older schemes. The crime is old; only the context is new.

The existence of Internet crime markets is probably the single most important factor behind the recent explosion in Internet crime. Making money from stolen credit cards is a complex undertaking requiring a lot of different skills and knowledge. To perform every step in the process himself, a criminal must be a computer operating systems expert, a computer networking expert, a confidence trickster, a money launderer, and a handler of stolen property (**fence**).

The crime markets allow the criminal who has only one skill to make money, and the would-be criminal with no skill to quickly learn one. It is not in a criminal's interests to teach his own special expertise; it reduces the value. But teaching another criminal's expertise lowers the cost.

The Crimes

Money is the motive: Internet criminals change their tactics frequently and their strategy rarely. Their goal is constant.

Phishing

At one time, spam was used to advertise products. It is possible that some spammers of the old school still exist, and they actually intend to make good on their offer to sell penis potions, fake Viagra, ink-jet cartridges, or whatever. Or the spammer might just take note of your credit card number and billing address and sell it to another group of criminals who will run up as many charges on your account as they can before the credit card company blocks it.

Stealing credit card numbers or other personal information—in hacker lingo **phishing**—was the first form of professional Internet crime to gain widespread notice. The complacent belief that professional Internet crime was a myth propagated by Internet security companies quickly evaporated as people's Inboxes started to fill up with fake e-mails from banks they had never heard of telling them that their account details had been compromised.

The gangs are after any type of personal information they can use to obtain money: usernames and passwords for financial sites such as online banks, stock brokers, payment schemes, and so on. In some cases, the gangs are attempting to perform **identity theft**—applying for credit using the identity and credit history of someone else.

Phishing attacks are not unprecedented. Almost as soon as credit cards appeared, so did ways of stealing card numbers. Each card has the account number clearly printed on the front of the card to be seen by every shop assistant, waiter, and hotel clerk who accepts the card for a purchase. Fraudulent mail

order companies are also set up. These usually operate legitimately for some time until they suddenly saturate their advertising channels with an offer that is too good to be true. The perpetrators charge the cards, take the money, and run.

Some phishing e-mails are easy to spot, but many are not. The criminals impersonate anyone they think people might give their credit card number to: banks, merchants, charities, and even politicians. An attack in 2004 sent e-mail that appeared to come from a presidential campaign. In 2005, many phishing attacks solicited money on behalf of charities to support victims of the Asian tsunami and the Katrina hurricane within hours of the event.

Phishing e-mails use a wide range of techniques to fool the victim. Obscure Web browser features are used to conceal the address bar showing the user which site is being visited. In some attacks, the user is directed to the real Web site of the brand being impersonated, and the phishing attack page appears separately in a pop-up window.

Click Here for the Egress

You are in a crowd listening to a carnival barker describing the attractions you are about to watch. He warns the audience to make sure they know where their wallet is, as pickpockets have been operating. The pickpockets watch as hands instinctively reach out to wallets: now they know who might be nervous about carrying a large amount of cash and where they keep it. The barker gets his cut later.

Security problems lead to the call to "raise public awareness." But merely raising awareness of a problem without telling people *how* to protect themselves is counterproductive.

Phishing attacks frequently use concern for security against their victims. Attack messages often contain detailed instructions describing how users should protect themselves against phishing spam, which would clearly identify the message as a fake. The phrase "Protect your security: Verify your account" has become a criminal cliché.

A legitimate e-mail was sent out providing Australians with ten tips to prevent identity theft. Within hours, criminals were sending out the same e-mail with tip ten changed to "Click here to verify your account."

User education is useful only when the advice can be acted on. Telling people "Beware" does no good. Telling people what to beware of is better. Telling people what to do is best.

Unfortunately as you will see later in this book, the state of Internet security is so poor that we cannot provide the concise and understandable safety instructions today that as we would wish. In 2004, the U.S. Federal Trade Commission began an online safety campaign with the advice Stop—Look—Ask. "Look" would be good advice if consumers could be expected to look at a typical Internet e-mail and determine if it were genuine. As of 2007, this is a difficult task that an expert might be unable to answer with confidence.

We must work to change the Internet infrastructure so that any user can tell if an e-mail is genuinely from a trusted source, without the need for any special expertise. Until that is achieved, the best user education we can give is to tell users about the scams the criminals are using to try to steal their money and to tell them to stop, think and ask (see Figure 1-4).

Fact: there is no reason to ever give your credit card number to anyone unless you are making a purchase and certainly no set of circumstances that would lead to your bank forgetting your username and password.

A good procedure to follow whenever receiving any unexpected offer is to **stop, think** and **ask:**

Stop
The old Quaker advice of counting to ten works well in most situations. Even in the Internet age there are few situations that genuinely require immediate action and none that require an immediate response to someone you have never heard from before.

Think
Are the claims made plausible? A bank that has a security problem will contact you by paper mail. The chances of winning a lottery are slim, the chances of winning a lottery you never entered are zero. Before buying anything from an Internet merchant ask if they can be trusted.

Ask
Fraudsters often tell their target not to talk to anyone else. They know that a target who talks to a second person is more than twice as likely to become suspicious. Simply trying to explain a scheme to a second person is usually enough to raise suspicions.

Figure 1-4 *Advice for Internet users: stop, think, and ask.*

User education can help protect against visible danger. Impersonating a merchant, a lottery, or a famous brand is a threat that users can guard themselves against. User education

cannot protect when the danger is hidden. A **Trojan keylogger**, a spy in the machine that watches as users log on to their online bank, is a challenge for even the most expert user.

Even this scam is not unique to the Internet. At one time, a gang would set up a fake ATM that would steal the card details of anyone trying to use it. More recently, the criminals have discovered that it is much easier to just attach some additional equipment to an existing ATM.

The problem of Trojan phishing has led some banks to introduce new authentication schemes that use the mouse for input rather than the keyboard. But some phishing gangs have already found ways to bypass this technique.

Stolen credentials are used as currency. A perpetrator needing information might offer five fulls for the first person to supply it. A **full** is a credit card number with the full name and billing address of the card holder. The value of a stolen card number on the black market varies according to the amount of supporting information available. There is little demand for raw card numbers, which are worth only pennies. Most valuable are COB (change of billing) card numbers, with an account username and password that allow the billing address of the card to be changed.

Conversion to Cash

Criminals are not really interested in credit card numbers; they want the money. We have already seen that criminal markets allow phishing criminals to sell stolen credit card numbers. They are only worth money to the buyer if he has a means of turning them into cash. This process is known in criminal circles as **carding**.

When the phishing epidemic began, it was possible for a perpetrator to use his stolen information to create fake ATM cards with PIN numbers that could easily be turned into cash. Today, carding is a much more difficult and risky crime. The crime markets are awash with stolen card numbers, and the prices paid for stolen cards reflect this.

A typical carding scheme was described in the hacker magazine *Phrack*.[3] The perpetrator used the stolen card number to buy goods from a mail order outlet. After the goods were

shipped, he would ask the shipper to change the delivery address to a location where he could safely collect them.

This scheme worked (for a time) by exploiting a loophole in the credit card security controls. The merchants would only ship the goods to the billing address on the card, but it was possible to reroute the package after shipping.

Turning card numbers into cash is the most time-consuming and risky aspect of credit card fraud, as many who have attempted to use the *Phrack* carding scheme have discovered. One of the factors that has until recently kept the problem of phishing in check is that supply of stolen card numbers has far exceeded demand. The sudden increase in phishing attacks, therefore, indicates that the fraud rings have discovered ways to turn large numbers of stolen credentials into cash.

Some carding gangs make fake credit cards that are resold to petty criminals. One of the pieces of evidence that points to an Eastern European origin for many of the carding frauds is that many of the fake cards end up being used in German department stores by Eastern European youths.

Making fake cards works, but counterfeiting physical objects is an approach from the age of atoms, not bits and is thus difficult to scale. Each recruit who is brought into the organization represents a risk. As soon as the organization grows beyond a certain size, the risk of detection becomes a certainty. In the real world, there is no honor among thieves, and the chance that a low-ranking member of an organization will be willing to trade information in return for a lighter sentence is good.

Recruitment is a major problem for any organization that has to operate clandestinely. When I was at Oxford, some of my fellow students complained that they were disappointed that nobody had ever asked them to join the Secret Service. But the recruitment problems of the British intelligence services are surely minor compared to those of James Bond's adversaries. Where, for example, do you go to find sufficient hired help to carve out the inside of a volcano without anyone noticing? How does a criminal mastermind go about recruiting dispensable henchmen?

Recruiting through the Internet scales much better. The advertisements do not need to reveal the true nature of the

enterprise. The recruit thinks that he is a shipping facilitator, but to the carding ring, he is a dispensable mule.

The carding ring buys goods with the stolen credit card numbers, giving the home of the mule as the delivery address. The mule then calls an international shipping company that offers expedited delivery and sets up a pickup. These companies specialize in shipping goods door to door in a hurry. In most cases, the package is delivered within 36 hours, 48 at the outside. These services are not inexpensive, but the carding rings don't mind; they can pay using a stolen card.

This scheme is called **package reshipping,** and it is a form of receiving stolen goods. There is absolutely no legitimate business of this type. The mule is dispensable and replaceable. The carding rings know that it is a matter of *when* rather than *if* the mule is caught.

The fraud control systems of the credit card companies are designed to quickly identify the possible use of a stolen card. The carding rings use the mule to bypass these fraud control mechanisms long enough for the goods to be shipped overseas.

The carding schemes sometimes involve Internet auctions. The mules are told that a distribution company needs domestic agents for its product because the auction company "will not let them in its system." The mules are told that the distributor is being unfairly excluded; they either don't think to ask why or don't care.

The Last Mile

Communications companies used to talk about the problem of the "last mile." Deploying a new network for long-distance telephone or data communications is relatively easy. The cost of this infrastructure can be shared among thousands or hundreds of thousands of customers at the same time. The biggest expense is cabling the last mile to the customer, where the costs are not so widely shared.

Internet criminals face a similar problem. It is relatively easy for them to endlessly shuffle funds between bank accounts using the Web. Their problem is how to convert their stolen funds into cash without being caught in the process.

A common approach is to recruit **money movers**. These perform essentially the same function as the package-reshipping mules but transfer money rather than forwarding parcels of stolen goods.

Employment advertisements for this type of scheme offer positions with impressive titles such as finance manager, financial consultant, and finance director but turn out to have only one actual requirement: The recruit has to have his own bank account. The real name for these positions, of course, is **money launderer**.

The money mover is instructed to open an account with one or more of the Internet payment services that facilitate anonymous payments. There are (or rather were) several schemes of this type offering an Internet currency backed by either a hard currency such as the U.S. dollar or in some cases a precious metal such as gold, platinum, or silver. The commissions charged by the operators of these services are typically in the range of five percent per transaction, a rate that would generally be considered prohibitive for a legitimate transaction.

It is hard to understand why any legitimate customer would want to invest money in a "bank" that does not reveal its owners, its directors, or even its place of business; is neither licensed nor insured as a bank; and makes no financial reports.

Pump and Dump

One way to cash out that is rapidly gaining favor requires no direct financial route between the accounts of the victim and the accounts of the perpetrator.

In a traditional **pump and dump** scheme, the perpetrator touts a penny stock with false promises of a sure-fire rapid increase in price (the pump). If the stock chosen has a small trade volume, a small increase in demand can cause the price to escalate rapidly. When the price has risen sufficiently, the perpetrator sells all his stock, leaving the investors with worthless stock they will soon find they are unable to sell (the dump).

Pump and dump scams have circulated through spam for several years. In some cases, the e-mails are designed to fool the reader into thinking that he has been inadvertently sent a hot tip by mistake. In others, the spam is carefully crafted to appear to have been sent by a well-known investor information service. But such pitches still rely on the ability to convince people to

buy, and the perpetrator has to time his exit from the position carefully; if he waits too long, someone else might unload his position, leaving *him* with a pile of worthless stock.

The solution that some criminals have found to this difficulty is to remove the element of choice on the part of the victim. The criminals gain access to the victim's accounts using a phishing attack and place orders for the junk stock on their behalf.

Premium Service Fraud

Premium rate telephone services allow a service provider to charge people calling their telephone number. Services on offer range from erotic conversation to phone sex. High prices are charged; a single call can cost $5 a minute or more.

From a security perspective, everything that *can* be wrong *is* wrong.

Telephone subscribers have no reliable way of knowing if a telephone number is a premium rate service or not. There is no way to know what rate is to be charged and no way to know if the advertised services will be provided. The result is fraud.

In theory, subscribers can opt to have premium rate numbers blocked, but they are expected to know to ask for it. In practice, they can have access to 900 numbers blocked, which is not the same thing.

A premium rate service is typically set up through a service bureau whose function is similar to that of a book publisher in that it performs the necessary technical functions to provide the service, collects money from the telephone companies, and pays royalties to the service provider less their own (substantial) fees.

In the early 1990s, many bureaus were not particularly diligent in checking the credentials of companies applying to establish an account. Complaints from fraudulently charged customers were a problem for the telephone company or the service provider. Both preferred to consider any problems to be the customer's fault.

The telephone companies understood that fraud was likely. To control risk to themselves, they adopted a rule that payments would only be made to service providers after the telephone subscribers had had the opportunity to review their bills and make a complaint. Dishonest service providers would not be paid.

Paying the service providers late was good for the telephone companies, but a cash-flow problem for the service providers waiting to be paid. Some service bureaus stepped in to solve this cash flow problem by offering to **factor** an account—that is, to pay the service provider as the payments were earned (less a fee).

Factoring solved the cash flow problem for the legitimate service providers but eliminated the only fraud control. The telephone companies did not much care, as they were making big profits from the service, and the only security problem they recognized was the risk of the company being unable to recover money that they had already paid out. This risk had been accepted by the service bureaus factoring the account. The risk to the customer and the potential for criminal profit were ignored.

Con artists quickly developed ruses to trick the unwary into calling the premium rate number unintentionally. Some hackers took a more direct approach and took over the private exchange systems of businesses so that they could make calls to their own premium rate lines.

Premium service fraud reached a completely new level as large numbers of computers were connected to the Internet through modems connecting to the telephone system. The first attack of this type to gain public attention was the Beavis and Butthead incident in 1997. This involved a program whose advertised purpose was to view movies. Two versions of the viewing program were distributed. The version of the program that most victims admitted to having used included cartoons of the MTV cartoon characters Beavis and Butthead. The other version catered to an interest in gynecology. The Beavis and Butthead viewer was a Trojan that reconfigured the victim's machine to silently dial a telephone number in Moldova.

The Moldovan telephone company, like many serving smaller countries at the time, was acting as a premium rate service bureau, splitting the inbound international calling charge with the content providers. Premium rate call blocking had no effect because it only blocked premium rate calls to a 900 premium rate number.

An Accountability Failure

It is easy to get lost in the technical details. The real failure is social, not technical. There were plenty of companies and governments that might have chosen to act. The reason they did not is a failure of accountability. Everyone who could have stopped the fraud pointed the finger back at someone else, leaving the consumer to bear the loss.

The central theory of this book is that the principle cause of Internet crime is the lack of accountability in the Internet architecture, and the solution to Internet crime is to establish an accountability infrastructure for the Internet. Accountability means taking responsibility when our online actions might result in harm to others. Accountability means deterring crime with the prospect of consequences. Accountability means accepting responsibility to protect others from harm.

Wherever possible, the tools chosen to establish this infrastructure are technical rather than governmental. This choice is pragmatic, not ideological. The legislative process rarely works well when forced to move at a rapid pace. Legislative action should be the last resort, not the first. Technologists made the Internet an attractive medium for Internet crime, and technologists must take the lead in making the Internet an unattractive medium for crime.

Premium rate fraud illustrates an important exception. Regulation or the threat of regulation is sometimes necessary to align responsibility with the ability to act. The problem of premium rate fraud was created by the telephone companies, not the consumer. It is the telephone companies that must act.

In the case of international premium rate frauds, the carriers can plausibly claim that regulation prevents them from acting. Payment for international connection charges is an international treaty obligation, and carriers are obliged to pay for charges their customers incur.

There are, however, measures the telephone companies can take, including covering the cost of this fraud with a surcharge on all calls to any country that facilitates it and in extreme cases refusing to carry any calls to that country. In 2004, the telephone regulator in Ireland became the first to take action: blocking calls to 13 countries linked to this type of fraud.[4]

A middle ground would be for regulators to require deployment of a mechanism that would only block automatically dialed numbers. When a person attempted to dial, he would hear a message that told him that because of repeated failure to control frauds, it was necessary to screen calls to that country. The caller would then be asked to repeat a word or phrase to demonstrate that the call was intended. The user experience would be suboptimal, particularly because of language issues. But this would be all the more encouragement for complacent (or complicit) governments to take this crime seriously.

Extortion

Protection rackets have long been a favorite of organized crime. The extortionists approach the owner of a business and suggest that they need "protection" in case trouble occurs. The unspoken threat is that, unless payment is made, the extortionists will create the trouble themselves.

Peter Cook, owner of The Establishment, a London comedy club, once recalled being threatened in this way by the Kray twins, a pair of notorious criminals then waging a campaign of terror in the East end of London. Fortunately, Cook was a quick thinker and replied, "Oh I don't think it's very likely that there will be any trouble, and in any case, there is a police station next door." Cook did not see them in his club again and later named them as gangsters in the satirical magazine *Private Eye*.

Online protection rackets follow the same basic scheme, but the "trouble" in this case is bringing down the victim's Web site and the perpetrators calling themselves "security consultants."

This type of attack is known as a **denial of service** (DoS) attack. Instead of stealing information or using the machine itself, the attacker denies the legitimate owner the use of his system.

New virus releases were at one time frequently followed by DoS attacks against well-known targets. An army of captured machines will send a stream of nonsense packets to the targeted service in hopes of overwhelming it. This is known as a **distributed denial of service** (DDoS) attack.

DoS attacks are relatively easy to perform and difficult to prevent. It is unlikely that attackers expect to successfully extort money from the high-profile targets that result in newspaper

headlines. But these attacks still serve a practical criminal purpose: demonstration of a protection ring's ability to take out any system it chooses at a time of its choosing.

DoS attacks often target online betting sites before a major sports event likely to attract many wagers. The online gambling industry is somewhat controversial in the U.S., where it competes for revenues with state monopolies and has been made illegal in most states. As a result, the industry has moved offshore to a number of Caribbean havens where specialist ISPs cater to their needs.

Like many industries that operate at the fringe of legality, the online gambling industry is considered easy prey by organized crime. It is quite likely that, in addition to outright extortion attacks, some attacks are intended to keep a competitor off the net before a lucrative football game or boxing match.

Loss of profits is not as effective as physical violence when it comes to persuading the target not to contact law enforcement. In the UK, betting is a legal and respectable business. When a number of UK bookmakers were threatened by a protection ring, they called the police. A payment was made in a sting operation that led to several members of the ring being arrested as they tried to pick up the money from banks in Latvia.[5]

Advance Fee Fraud

Next to phishing, the most visible Internet fraud is advance fee fraud. Early versions of this fraud often originated from Nigeria, and the Internet version is often referred to as the **Nigerian letter** or **419 fraud**, after the section of the Nigerian criminal code that deals with it. In this version of the scam, the perpetrator claims to be an official or businessperson who needs your help to move a large sum of money out of his country.

As the Nigerian letter version of the scam became a cliché, the fraud rings behind the scam developed endless variations on the same basic scheme. The e-mail may purport to come from practically any country, and the reasons cited for needing to move the money include payment of a ransom, diverting money from dormant bank account, or to prevent seizure of an inheritance. Another common tactic is to tell the recipient that he has won a lottery.

The sum of money is almost always large, usually $25 million or more, and your cut is never less than 10 percent. Some report that if you negotiate, you can increase this to 15 percent.

In a week, I get approximately 200 solicitations of this type purporting to come from Nigeria alone. At an average of $30 million per e-mail, that makes $300 billion a year, about twice Nigeria's total Gross Domestic Product.

In an **advance fee fraud**, the perpetrator offers the potential victim (the **mark**) an opportunity to make a lot of money if he pays some money in advance. When the mark replies to the offer, there will be some "problem" that will invariably require some money to be advanced for an "unexpected" cost: some paperwork to clear, an official to be bribed, and so on. The amounts start small but increase gradually so that each time the victim finds it easier to trust the con men and throw good money after bad rather than accept that their earlier investment is lost.

It is easy to see these schemes as outright frauds when you are alert to the danger and have your full wits about you. But many senior citizens do not, and many prefer not to report the crime in case people start thinking they might be senile.

The money does not always come from the mark. Olsman Mueller & James, a small law firm in Michigan, first found out that it had been a victim of advance fee fraud when a $36,000 settlement check to a client bounced. When the firm checked with the bank, it discovered that the client suspense accounts had been drained—more than $2.1 million in all. Ann Marie Poet, a 60-year-old grandmother who had been with the firm for nine years, was charged with 13 counts of wire fraud.

The charges alleged a Dr. Mbuso Nelson, who claimed to be an official with the Ministry of Mining in Pretoria, South Africa, had contacted Poet in January of that year promising a $4.5 million fee for helping Nelson transfer $18 million from South Africa to a bank account in the United States. Poet then "borrowed" from the firm to pay "expenses" that kept turning up, wiring amounts ranging from $9,400 to $360,000 to pay for fees such as "ecological damages," "currency fluctuation marginal difference" and a "drug, terrorists, and money laundering clearance certificate." Like many embezzlers before her, Poet soon discovered that, once started, she had little option but to

keep going and hope that the confidence tricksters were telling the truth.

This fraud is a modern twist on what was known in the 1930s as the **Spanish prisoner** con when it appeared during the Spanish civil war, but the scheme is even older and has been used in various guises since at least the Middle Ages when the story went that a rich knight on crusade had been kidnapped, needed to be ransomed, and would reward any lord handsomely for assistance.

Reliable estimates of the scope of 419 fraud are hard to come by. The thousands of complaints made to the police are likely to be only a fraction of the total, because most victims are unlikely to report that they were conned while engaging in a criminal conspiracy. The Michigan case is not an isolated one:

- A couple in Minnesota lost $2,600 after they wired the money to pay "taxes" on a fake lottery win paid with a forged cashier's check.[6]
- Melbourne financial planner Kerry Francis was jailed for 4½ years for transferring more than $700,000 from clients into a Nigerian letter scam.[7]
- Cuttle and Isaacs, a New Zealand livestock broker, went bankrupt owing farmers $4 million after two directors of the firm embezzled from the firm to participate in a section 419 fraud.[8]

In February 2003, the Nigerian Consul to the Czech Republic, Mr. Michael Lekara Wayi, was shot dead by a 72-year-old pensioner swindled of his life savings in a 419 scheme. The U.S. Secret Service reports that a U.S. citizen was murdered in Nigeria in 1995 while he visited Nigeria in connection with an advance fee fraud and that many more people have gone missing.[9]

Although the fraud is not unique to Nigeria, the vast majority of the advance fee frauds being operated through the Internet come from Nigeria, where the fraud accounts for a significant proportion of the country's income. The Nigerian government has shown little interest in prosecuting 419 frauds, which is not surprising because corruption is endemic, and the country faces many other serious public order problems.

The Nigerian gangs have been linked to several other murders. The major cons often involve enticing the victim to visit

Nigeria, where he will be entirely within his power. The victim is often told that he does not require a visa to visit Nigeria, and the gang often pays off the customs and immigration officials to allow him into the country. As the U.S. Secret Service puts it,[10] "Because it is a serious offense in Nigeria to enter without a valid visa, the victim's illegal entry may be used by the fraudsters as leverage to coerce the victims into releasing funds."

One scam used by the con-men at this point is known as the **wash-wash**. The victim is taken to a hotel room, where he is shown a suitcase of what appears to have been money before it was covered in some sort of chemical dye. The victim is invited to pick any of the bills and take it to a washbasin, where an amount of scrubbing reveals a $100 bill. The bill is actually counterfeit, covered in washable ink or a combination of petroleum jelly and iodine. The money will be his after he pays for the removal agent. It's the same advance fee fraud in a new guise.

After exhausting every means of tricking the victim out of his money, the gang switches to violence. The victim is kept hostage until the gang is convinced it has drained his wallet completely. Only then is the victim released. In some cases, the gang is nice enough to give the victim a lift to his national embassy, where he can apply for a loan to buy an air ticket to return home. Sometimes the victim disappears.

You might be wondering if there are organizations to help the victims of these schemes. There are.

These investigators will call up victims of 419 frauds to report that the Nigerian police have arrested a gang and offer to use their local knowledge of the banking system to reclaim whatever is left of the stolen money in return for a small fee and percentage of the amount recovered.

Of course, the Nigerian police has not arrested the gang, and the real way the "investigator" got the name is that he is part of the same gang who stole the money the last time. This is re-victimization, or **re-vic fraud**. After all, if they fell for it the last time, they will probably fall for it a second time.

Franchising Fraud

The sheer scale of the 419 scams is self-defeating; it makes no sense to bombard a person with 20 messages a week, let alone

20 messages that look suspiciously similar. Even more peculiar is the fact that would-be 419 scam perpetrators seem unable to learn from the tricks played on them by groups such as 419eater.com who make a sport of them.

The people behind the Web site make fun of would-be perpetrators of 419 frauds by "baiting" them with unlikely stories of their own. Each of the section headings on the 419eater.com Web site consists of a person holding a handwritten sign with the heading. Each is a would-be 419 fraud perpetrator who has been tricked into providing the photograph as "proof" that he is genuine. The trophy room contains hundreds of similar pictures, most showing a different perpetrator. Some show the perpetrators posed in embarrassing positions. One even carries a sign saying "Baiting is my favorite sport."

It is not unusual for a con man to be conned himself, but the tactics used by the scam baiters are as scripted as those used by the perpetrators. The tricks would quickly stop working if the perpetrators were talking to each other. This is itself an interesting fact because most of the scams originate from a relatively small geographical region. The scam would not continue if it was unprofitable, yet remarkably little effort seems to be taken to adapt to the publicity surrounding the scam. The vast majority of the 419 letters follow the original scheme.

An intriguing possibility is that there is a scam within the scam. The people sending the 419 letters might themselves be the dupes of an advance fee fraud, paying for the software tools and mailing lists necessary to set themselves up in a "business" they believe will make them a fortune. The would-be scammer might even be allowed to "earn back" some of his initial investment before being asked to forward a much larger sum.

This hypothesis would explain some of the odder features of the 419eater.com site, such as the fact that many of the photographs are taken in front of the same backdrop. The photographer would surely remark on the curious nature of the signs and warn the scammer that he had been fooled. Unless, of course, the photographer was working with the ring running the fraud within the fraud, and one of the ways that the rings extract money from their victims is to sell them photographs, forged documents, and so on.

Regardless of whether the rise in traditional 419 attacks is due to the fraud rings franchising their underperforming scams or some other reason, the fraud rings have been aggressive in developing new variations on the same theme.

One of these new "products" targets the sale of expensive goods such as luxury used cars through online ads. The vendor lists an expensive car such as a Mercedes on an online used car site for say $50,000 and is surprised to receive an offer to pay $6,000 more than the asking price with the proviso that the vendor forward the additional money to another party such as a shipper or a freight forwarder as part of the deal.

The vendor receives a cashier's check for $56,000, which normally clears three days after deposit. The vendor then wires $6,000 to the "freight forwarder" as per the agreement. A few days later, the bank cancels out the credit for the fraudulent cashier's check despite previously reporting it as "cleared." The vendor has lost the $6,000 wired to the "freight forwarder."

Other forms of advance fee fraud include a bogus "National Scholarship Fund" that would pay students scholarships of $2,500 to $6,500 after they had paid a "registration fee" of $100. Loan frauds are also common; the victim is told that he has qualified for a loan that will be paid as soon as he remits his first payment.

Copyright Theft

The one major form of Internet crime I do not try to provide a solution for in this book is theft of copyright work. Theft of copyright works is a major and growing problem. The Internet has led to a major increase in theft of copyright work. If copyright theft continues to grow, it might become impossible to finance the production of feature films costing a hundred million dollars or more.

Copyright is limited by the doctrine of "fair use," and for good reason. Every form of art borrows from others. The tune of *Memories* by Andrew Lloyd Webber sounds remarkably similar to Ravel's *Bolero*. The plot of *The Forbidden Planet* is essentially Shakespeare's *Tempest*. More importantly, the right to earn a living from copyright works is a net benefit to society. The "right" to suppress criticism through control of copyright works is not.

Fair use does not, however, mean that a person who has paid for one copy of a film or an album should be able to share it with the rest of the world for free. Extracting profit due to the content creator by facilitating "exchange" of copyright material is simply not a legitimate business.

I do not deal with the issue of copyright theft because the conditions for success do not exist. Faced with the major threat of Internet copyright infringement, the lobbying organizations for the content owners are still engaged in attempts to obtain retrospective extension of the lifetime of their copyrights. While the representatives of the U.S. recording industry were pleading the need for longer copyright terms and stronger enforcement methods to protect the livelihood of their artists, they slipped a provision into the Digital Millennium Copyright Act (DMCA) of 1999, which effectively transferred rights from the artists to the recording company by retrospectively redefining the status of the work.

The underlying problem here is that the Internet does much more than increase the threat of piracy; it changes the business model for the recording industry. The role of capital is reduced, and distributors will no longer act as gatekeepers. Power has shifted from the labels to the artist. The film industry has already undergone a similar transformation in the 1950s with the demise of the studio system. The recording industry understands that it now faces the same change.

It is not possible to effect a plan to protect against a criminal nuisance without a widespread consensus on the result to be achieved. Such consensus is impossible when neither side of the argument will accept realistic goals. If, however, it is shown that action can be effective against phishing and extortion, there will be much more incentive for both sides in this dispute to come to mutually acceptable terms.

Emerging Threats

Internet crime tends to move from bad to worse. Just as the amateur hackers quickly moved from vandalism to making money, there is always a fringe of crimes where money is not yet the primary motive or the techniques are not yet outright criminal.

Spyware

Spyware is the common cold of the Trojan world. Most spyware will not kill you, but it can make you feel pretty miserable until you get rid of it. And, like the common cold, almost all spyware will make you more vulnerable to more serious forms of infection, and some can ruin your financial health.

The small group of spyware companies clinging to the pretense that they are engaged in an honest business is rapidly dwindling. It is being replaced by worse.

The most benign form of spyware insinuates itself into a Web browser and provides a constant stream of reports on the sites the user is visiting, the pages viewed, and so on. The spyware company constructs a profile of the user from this information and sells it to any buyer willing to pay.

A more intrusive form of spyware called a **cobrowser** or **adware** pesters the user with advertising related to the sites he surfs. If you visit a site on rock climbing, an advertisement for climbing gear or outdoors clothing might appear. If you looked at a TV on one site, you might see an advertisement from a competitor.

The worst type of spyware silently watches the user and reports his most sensitive personal data to the organized crime rings that produced it. This might be used to steal money from the victim directly or to perform an identity theft and apply for a loan in his name.

Today, spyware of the first type has pretty much sunk into the second type, which is rapidly sinking into the third.

The same thing happened with spam. The first spam tried to sell real products. As people stopped buying, the spammers found peddling porn and fake Viagra was the only way to make spam pay. As the second generation of spammers found it increasingly difficult to get legal network access, the gray-market spammers were quickly displaced by the outright criminal.

We could make an effort to distinguish legitimate spyware from the outright criminal, but it is easier to make the propagation of any software intended to resist removal at the direction of the owner of the machine a criminal act. Spyware provides nothing of value to the Internet community.

Like the spammers, the spyware outfits are caught between the pincers of legislative and technical measures, which are certain to obliterate their "industry." Even if they manage to stay ahead of the technical measures intended to make it harder for them to infect machines and easier for users to remove infections, legislative action is inevitable. As with the spam "industry," all that will be left is a hard core of spyware operations whose activities are unambiguously criminal.

Terrorism

The Internet has become an infrastructure that is as critical to the running of the modern economy as the telephone system or electrical power. And just as the Internet is dependent on electric power to run, there are complex and increasing interdependencies between the Internet and the telephone and electrical systems.

The threat of cyberterrorism is usually considered in terms of preventing an attack on critical infrastructure. In a recent TV drama, the fictional cyberterrorists performed the highly unlikely feat of successfully disabling every nuclear power station in the U.S. by hacking into the computer system that controls them. In practice, such an attack would be most unlikely to succeed because the nuclear power stations in the U.S. were designed long before the Internet existed, and there is no reason why the computer systems that are used to control them would need to be connected to the Internet.

Bombs are simple but effective means of creating fear and causing disruption. Cyberattacks require considerably greater resources to perform and are much less likely to be effective in achieving these particular ends.

The history of the Red Army Faction (Bader-Meinhof Gang) and similar groups operating in Europe in the 1970s and 1980s suggests that it is more likely that terrorists will turn to the Internet for funding and propaganda rather than as a means of attack. The Red Army Faction financed its activities by robbing banks. Al Qaeda's primary means of finance was the opium trade. Paramilitary groups on both sides of the sectarian divide in Ireland funded their activities through bank robberies and extortion rackets. We must deny these and similar groups the ability to raise funds through Internet crime.

Most terrorist groups already operate Web sites to further their political program, either directly or through sympathetic groups. These Web sites are often the target of attacks by opposing political groups, in some cases disabling the sites completely, but in other cases posting their own propaganda on their opponent's sites.

Often the attacks come from hacker groups that do not consider themselves as terrorists in the conventional sense. But there is a significant risk that actions by these irregular groups might cause escalation of an international incident at a time when the state actors are trying to diffuse the crisis.

A situation of this kind occurred during an incident in 2001 when a U.S. plane struck down a Chinese fighter jet with a missile and was subsequently forced to land in Chinese territory. While diplomats from both countries worked to avert a major crisis, groups of hackers in both countries launched information warfare attacks that threatened to escalate it.

Espionage and Warfare

Intelligence agencies used computer networks to perform espionage long before the Internet existed. The best public account is to be found in Clifford Stoll's book, *The Cuckoo's Egg*. Stoll, an astrophysicist and system manager at the Laurence Berkley National Laboratory, discovered a 75-cent discrepancy in the accounting records on a computer. Investigating this minor discrepancy led to the discovery that the machine was being used as a staging post for attacks on U.S. military computers by German and Hungarian hackers who were selling the results to the KGB.

The use of computer networks to conduct espionage is not new, but the amount of information available to the Internet spy is unprecedented. Equally unprecedented is the ease with which information that at one time might have been regarded as highly sensitive can be obtained from nongovernment sources. Perhaps the most dramatic example of this is Google Earth, which allows anyone to view a satellite picture of virtually any part of the world. Satellite reconnaissance is no longer limited to governments.

Espionage is a national security concern but not necessarily a national security threat. What governments reveal about

themselves is balanced by what they discover from others. A mutual exchange of information can help reduce mutual suspicion and the political instability that can create.

The possibility of cyberwarfare is of considerably greater concern. Paradoxically, governments might be drawn to cyberwarfare for precisely the reason that terrorists are likely to avoid it. By definition, the terrorist seeks to create fear and panic. Governments seek a least-risk means of achieving their political outcomes. Physical violence, even if performed by proxies, carries a high risk of retaliation. Since the end of the cold war, the number of states that actively sponsor terrorism has dropped. The number of states designated by the U.S. as "state sponsors of terrorism" has dropped from seven in 1979 to five in 2007.[11] If a similar list had existed in the 1970s, it would have numbered 15 or more.

Cyberwarfare might provide a new opportunity for belligerent states to engage in low-intensity conflict. As with the use of terrorist proxies, cyberwarfare provides a degree of plausible deniability.

Cyberwarfare is only an attractive mode of attack against an enemy that is sufficiently dependent on a high technology infrastructure to make its loss a serious concern. A country that is only able to provide power for a limited number of hours each day is not going to be brought to its knees by an Internet outage.

Until recently, the ephemeral nature of Internet vulnerabilities has made cyberwarfare impractical. It is not possible to stockpile weapons for a cyberattack as if they were tanks, planes, or bullets. A cyberweapon has an unknown and short shelf life. Maintaining a cyberwarfare capability would require constant research and development. One approach for the country looking to develop a cyberwarfare capability is, therefore, to acquiesce to if not actively encourage the growth of Internet crime rings so that their technical skills may be called upon should this be required. Evidence is beginning to emerge that might suggest that this is happening.[12]

Pedophile Rings

Phishing is real crime, and a lot of money is lost, but as a banker who used to be a policeman on a homicide squad pointed out to

me once, "It is only stuff." The worst effects of the online world are what can happen to people, not their money.

The positive effects of the Internet vastly outweigh the bad. The Internet is bringing information on sanitation and healthcare to slums around the world. It's giving the poor and the oppressed a voice in political systems from which they have been excluded. And the Internet has played a key role in the exposure of numerous abuses of children by pedophiles.

The threat of Internet pedophile rings was the first serious Internet crime that the mainstream media took seriously. The reports make it easy to believe that the Internet is filled with pedophile predators plotting to rape and murder children, a lawless frontier where law enforcement is impotent.

Fortunately, the truth is rather different; law enforcement was taking the problem of Internet pedophiles seriously before the first reports reached the mainstream media.

There will always be Internet sites offering pornographic material that offends the sensibilities of some government or other. Magazines sold openly on the shelves of newsstands in Germany would still result in a jail sentence if found in a UK home.

The material of concern for the purposes of this book is not what might merely offend but that which is universally prohibited, in particular explicit photographic or video depictions of prepubescent children in penetrative sex acts.

Internet pornography is a large, highly profitable, legal business. Child pornography is a threat to that business. The same is probably true albeit to a much lesser extent of the professional Internet criminal. Child pornography is a considerably greater risk than bank fraud; it is only going to be an attractive crime if it is considerably more profitable than the alternatives.

In 1995, the FBI began Operation Innocent Images, which tracked pedophile use of the Internet. FBI agents monitor online chat forums for criminal activities. Just as people who try to hire a hit man by responding to advertisements in the classified section of *Soldier of Fortune* magazine invariably end up talking to undercover law enforcement officers, pedophiles attempting to "groom" a victim in an online chat room are likely to receive a similar surprise.

In 1998 law enforcement agencies in 13 countries arrested 107 members of the Wonderland pedophile group. Police seized three quarters of a million images, many of which depicted sexual acts with minor children. Seven British members of the club received jail sentences of between 12 and 30 months, one received a 12-year sentence for rape, and another member committed suicide before the trial.

Even though the Wonderland club was extensive, its primary purpose was perversion rather than profit. Members of the club swapped images and videos. To join, a prospective member had to provide a large number of original images.

The breakup of the Wonderland gang and subsequent police operations demonstrate that the Internet does not allow pedophiles to operate without fear of prosecution. The members of Wonderland were caught despite attempting to use sophisticated encryption technology.

The use of technology cuts both ways; the most sophisticated Internet criminals can use technology to conceal their activities, but Internet technology also makes it easier to identify Internet criminals with ordinary skills or less. Even the most sophisticated Internet criminal only needs to make one mistake to get caught.

The Internet allows groups of all kinds to operate on a much larger scale than previously but does nothing to change the risks inherent in operating any criminal operation on a large scale. The more members that a criminal organization has, the greater the risk that one of the members will be caught with information that incriminates other members of the group.

The existence of the Wonderland club had been revealed by forensic examination of computers seized in an earlier 1996 investigation into a pedophile ring called The Orchid Club, which led to 19 defendants receiving sentences ranging from 12 months to 30 years.

Internet pedophiles remain a serious problem, but it is the only Internet crime problem that can be regarded as being under some measure of effective control.

The arrest and prosecution of Internet pedophiles demonstrates that Internet crime can be investigated and controlled. It *is* hard to get law enforcement in another country to investigate a case involving computer hacking, but pedophilia and bank fraud are a different matter.

Offline Safety

Online dating poses many risks, only some of which are criminal matters. The real safety concern is not what happens online. There are few places safer than the Internet; risks to life and limb occur only if the participants meet offline. Online chat rooms can result in emotional injuries, but there is no risk of physical harm unless online activities cross into the offline physical domain.

Despite widespread expressions of concern, safety appears as an afterthought in many popular books on Internet dating—a few chapters thrown in at the end. Heaven help the reader who starts dating before finishing the book!

The boundary between the online and offline world is an important safety control. Strictly speaking, the online world is not anonymous and never has been. An online **avatar** is a pseudonym, an *alternative* persona, a mask that is to be worn by its unique owner.

Maintaining the pseudonymity offered by online interactions allows participants to reduce the risk that the boundary between the online and the offline world will be broken without their permission. It also increases the risk of physical harm if those boundaries are breached.

The boundary between the online and offline worlds may sometimes be breached without permission. It takes some skill to hide effectively online. Occasionally, an involuntary breach leads to serious consequences. More often, the connection between the online and the offline world is made voluntarily. The point of online dating is to meet people after all.

Internet stalkers are a real risk for women in particular (and also for men). The risk of an unwanted pregnancy or contracting a sexually transmitted disease is considerably higher. A study of online dating by Dr. Paige M. Padgett at the University of Texas reports that "Seventy-seven percent of respondents who met an online partner did not use condoms for their first sexual encounter".[13] None of the online dating guides I read made mention of condoms or birth control either.

If you are a woman and you meet an Internet criminal in person, you may have worse to fear than crime. While researching this topic, I went to an airport bookstore and asked if she had any books on online dating safety. Immediately she handed me

a book and said, "It's not the Internet, but you should warn women about the men who read this."

After reading the book, I agree. A how-to guide for lounge lizards,[14] the book advises men to peacock (that is, dress like a pimp), frequent places where lots of women congregate, and attempt to attract them through "demonstrations of high value" (that is, project a huge ego). The only counterintuitive part to the process is the idea that the man should demonstrate a high value relative to the woman by expressing a lack of interest in her and talking her down. Feminists will be disappointed to discover that the guy who insists that the woman buy her own drinks might well be a misogynist intent on establishing a high relative value rather than a champion of equality.

There is a curious mismatch between the shallowness of the pickup lines presented and the use of technical jargon. The mismatch is explained when it is realized that many of the terms used come from writers who are not generally regarded by mainstream psychology and whose theories are of the type that explain rather too much and predict rather too little.

Looking at the work a little closer, I noted some curious similarities between the self-styled "seduction community" and the activities of the online vandals who preceded the rise of the professional Internet criminal. Both groups display the same ego-centricity and obsessive use of jargon as a substitute for understanding, the same outlandish claims made for their success in applying their expertise. Finally, unpicking the wider social circle, I recognized some names of notorious (and some not so well known) Internet criminals.

In retrospect, it is obvious that someone specializing in "social engineering" would attempt to apply his skills for sexual advantage. As with all advice from such circles: *Caveat emptor*. If the author of a book openly boasts about his success in manipulating people, he is almost certainly attempting to manipulate his readers too.

Key Points

- Internet crime is a serious problem that causes real economic damage and major losses for the victims.

- The principle vectors for Internet crime are spam and zombie botnets.
  - Spam allows the Internet criminals to reach a large audience. The spam may be a direct solicitation for a criminal fraud or part of a larger scheme.
  - A zombie is a computer that has been taken over by a criminal. A botnet is a network of zombie computers controlled by a criminal.
    - Computer criminals use compromised computers to hide their tracks in the same way that bank robbers use stolen cars as getaway vehicles.
    - Turning a computer into a zombie allows the criminal to effectively steal the computer while the owner still pays for the electricity and network connection.
- Internet crimes are typically variations of traditional crimes—often confidence tricks.
  - Phishing is stealing credentials, usually credit card numbers or usernames and passwords for online bank accounts.
  - Carding is the process of turning stolen credentials into cash.
    - Package reshippers receive stolen goods and forward them on to the criminal gangs.
    - Money movers perform money laundering.
    - "Mules" are recruited into these schemes through online advertisements for work-at-home schemes.
  - Internet criminals also operate protection rackets.
    - If the victim refuses to pay, his site is targeted by a denial of service attack.
  - Advance fee frauds induce the mark to pay an upfront fee in the hope of realizing a large profit.
    - The letters that offer to share $20 million are advance fee frauds.
    - Other variations include lotteries that ask for an upfront fee and re-victimization fraud.
    - The victims of these scams are often seniors with large retirement savings.
  - Terrorists are unlikely to use the Internet for political direct action, but Internet crime may be an attractive means of raising money.