

# 1

## What Drives Cybercrime?

Willie Sutton was a famous twentieth-century bank robber falsely credited with answering the question “Why do you rob banks?” with “Because that’s where the money is.” This saying is so well known it’s sometimes called “Sutton’s Law.” While Mr. Sutton never actually said this, it does explain the basic driver for cybercrime. An enormous number of people are active online, so the Internet is where thieves naturally turn to find victims.

How many people are active online? This Wikipedia chart shows estimates for the global online population by language for 2010.

**Table 1: Top 10 Internet User Populations, by Language**

Position	Language	Internet users
1	English	536,564,837
2	Chinese	444,948,013
3	Spanish	153,309,074
4	Japanese	99,143,700
5	Portuguese	82,548,200
6	German	75,158,584
7	Arabic	65,365,400
8	French	59,779,525
9	Russian	59,700,000
10	Korean	39,440,000

(Source: Wikipedia: Global Internet Usage/Internet World Stats)

The total for all these populations exceeds 1.6 billion users! A close look at Table 1 also reveals that the total Internet population must be bigger. The table omits languages outside the Top 10. Obviously, all speakers of the world's hundreds of other languages aren't as active on the Internet. But we can safely add another 500 million Internet users to the preceding total for a rough guesstimate of 2.1 billion Internet users worldwide. Given a global population of 6.8 billion in 2010, that means just under one of every three people on the planet uses the Internet.

That's a huge pool of potential victims by any standard. Any one of them could be accessible to thieves using any working Internet connection. Because so many people who use the Internet also use credit cards, do their banking, and manage financial accounts online, it's no wonder that cybercrime is prevalent. It's also no mystery that cybercrime rates are going nowhere but up.

# What Exactly Is Cybercrime?

One simple definition of cybercrime is "a crime whose commission involves a computer." A better definition for this book could be "a crime committed using an Internet-connected computer." This broad definition includes any kind of wrongdoing that involves interacting across the Internet. Thus, it covers massive email broadcasts (spam) that involve no other overt criminal activity. It also covers online postings involving libel, defamation, or hate speech, all regarded as criminal in some jurisdictions.

The cybercrimes that provide the focus for this book must be defined more narrowly. We want to dig deeply into various forms of criminal online activity. We are especially interested in attempts to acquire and misuse sensitive information, primarily to rack up ill-gotten gains. This means analyzing attacks or scams of many kinds. Some seek to obtain accounts and passwords for websites. Others attempt to gain access to people's online banking or financial services. Some involve theft of securities or commodities. Some seek to misuse credit cards without notification or permission. Ultimately, the cybercrimes that interest us most are those that supposedly excited Mr. Sutton's interest in banks, too. These cybercrimes go after Other People's Money.

For those inclined to wonder, there's plenty of evidence that cybercrime occurs frequently, no matter how you measure such things. The Internet Crime Complaint Center (IC3) is a joint partnership between the U.S. Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). Look at the following table of complaints received from 2005 through 2009 (it's taken from the IC3 2009 Annual Report).

Table 2: IC3 Complaints Received 2005–2009

Year	Complaints Received	Losses
2009	336,655	\$559.70 million
2008	275,284	\$265.00 million
2007	206,884	\$239.09 million
2006	207,492	\$198.44 million
2005	231,493	\$183.12 million

(Source: [www.ic3.gov/media/2010/100312.aspx](http://www.ic3.gov/media/2010/100312.aspx))

The trend for dollar volume of losses increases every year. The number of complaints dips in 2006 and 2007, then increase substantially in 2008 and 2009. Today, headlines regularly report enormous losses to cybercrime. It’s not unusual to read about tens of millions of dollars lost to single heists, with hundreds of thousands of cybercrimes committed annually. In this book, we explore one interesting and disturbing trend: businesses are bearing an ever-increasing portion of the impact of cybercrime. At the same time, large numbers of individuals experience identity theft plus related financial losses and ruined credit ratings.

Who’s a Target for Cybercrime?

Historically, individuals have been—and remain—key and primary targets for cyber-crime. But with more people targeted at work, individuals who fall prey to cybercrime force employers to suffer and absorb related losses. The short answer to the question that heads this section is “Anybody with an email inbox or who surfs the Web.” That’s nearly everybody who uses the Internet, and you already know that’s more than two billion people!

Let’s bring these numbers down to earth. Take one common phishing attack that targets financial professionals at small to medium-sized businesses as an example (see Figure 1-1). An email arrives in Joe Biggs’ inbox at [acmecorp.com](http://acmecorp.com). It appears to originate from an Automated Clearinghouse (ACH) that processes payments for his employer. This message informs him that a payment problem is pending, and that processing has been discontinued. Feeling some concern, Mr. Biggs reads further. Next, he learns that he must provide information about his company’s account for processing to resume. He is asked to click a handy link in the message to provide that information ASAP, so that business can get back to normal. Sounds pretty routine, doesn’t it? It’s not.

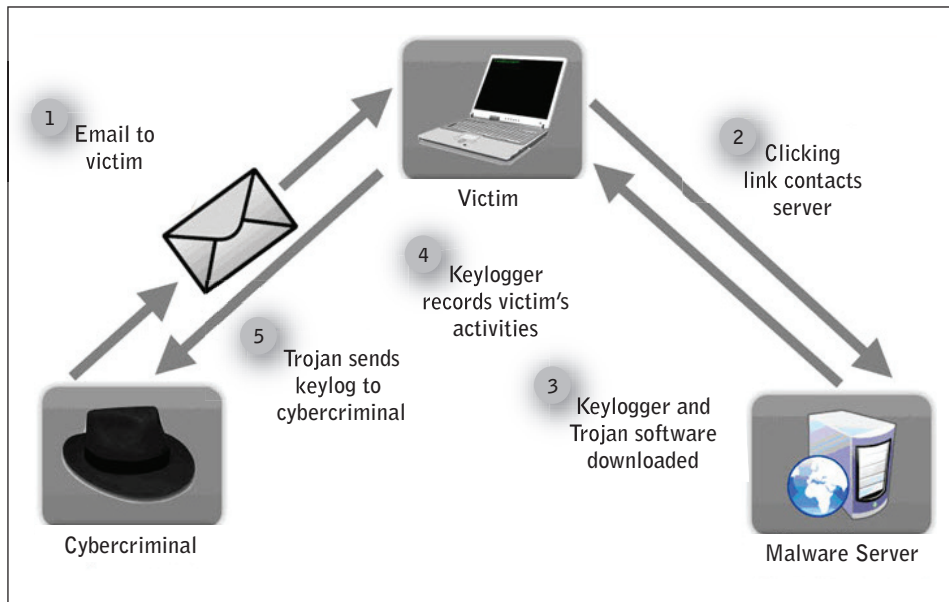
## Definition: Phishing

Phishing takes its inspiration from catching fish. Just as an angler uses a lure to entice the fish to bite his hook, cybercriminals use hyperlinks to draw unsuspecting users to malicious websites. Phishing shares these things in common with its watery inspiration:

- It looks like an innocuous or even legitimate email message, tweet, or Facebook post.
- It seeks to get readers to provide information by responding to the message, or clicking an embedded link.
- It often requests sensitive information about accounts, passwords, or identity.
- The hook gets "set" when a reader responds, even if only to click a link.

Security experts often label phishing as a kind of social engineering. This term describes various techniques used to persuade users to part with information about themselves, credit card or bank accounts, and so forth. The idea is to glean something of value to enable theft. No breadcrumbs and lemon are involved, but the victims often wind up gutted anyway.

If Mr. Biggs does click that link, he is already at risk, even if he provides no information to the web page where that link takes him. That's because simply visiting a phishing page can expose a PC to software downloads. They occur in the background, covertly, without the user's knowledge or consent.



**Figure 1**

How malware gets from a website to a victim's PC.

Cybercriminals who run phishing scams are especially fond of software packages like Zeus, which combine a keylogger with a Trojan to harvest valuable information from unwitting PC users' machines. A keylogger records every keystroke that Mr. Biggs makes on his PC, and the Trojan periodically opens a backdoor to upload that keystroke log. The cyberthieves who planted this malware on his machine will comb that file carefully. They'll grab every account and password combination it contains, along with any sensitive data it might contain. If the bad guys can sniff out an online banking site and use his credentials to log on, they can transfer funds to other accounts right away. Talk about an unfortunate downside of 24/7 online banking services!

If Mr. Biggs does provide the information requested on their web page, the thieves don't need to bother with a keylogger and Trojan software. They can simply try out the information he provided, and see what it gets them.

"But wait!" you're probably thinking, "Does anybody really fall for this kind of thing?" A surprising number of people do fall for such scam. In fact, about one in five people in ordinary user populations is typical.

---

*KnowBe4.com has run surveys at various types of firms and observed success rates of 20 to 22 percent for its own simulated phishing attacks.*

---

A PCMag.com Security Watch article, "Phishing Effectiveness: 35 Credit Cards in 5 Hours" (1/28/2011), confirms this 1-in-5 ratio. This story reports how Internet security firm ESET discovered and monitored an obvious and crude phishing site in Latin America. The site was up and running for five hours on January 20, 2011. Of the 164 users who accessed the site, 35 users (about 21%) provided account information by filling out a form on the phishing page. This explains why online scams are so prevalent, and why new variations keep popping up. Users keep falling for such scams, and these sites produce "free money" like clockwork!

## A Million Stories for a Million Scams

Let's take a quick sample of warnings and reports of scams from the IC3 website. It displays the ingenuity and resourcefulness that cybercriminals bring to online scams:

- **Emails containing malware sent to businesses concerning their online job postings:** Companies download resumes only to become infected by malware payloads. The malware harvests sensitive data for transmission to cyberheisters. This is surely a sinister way to fight unemployment!
- **Fraudulent ACH transfers connected to malware and work-at-home scams:** Infected email attachments or drive-by downloads on malicious web pages harvest corporate banking credentials. This enables cybercrooks to access bank accounts and make fraudulent funds transfers. Poor people seeking to generate income while working at home fall prey to account harvesting that costs them money instead.

## 6 Chapter 1

- **Pop-up advertisements offering antivirus software pose threat to Internet users:** Users respond to bogus virus discovery and repair offers, to help them get rid of viruses they don't really have. These users waste money on worthless software. Worse, their machines fall prey to malware that can harvest sensitive data and cost them even more of their money.
- **Fraudulent email claiming to be from DHS and the FBI Counterterrorism Division:** Readers who download a purported speech by Osama Bin Laden get malware instead. Thieves can then harvest and download sensitive data. Instead of keeping up with terrorism, readers get ripped off.

---

## Drive-by Downloads and their Potential Risks

A drive-by download is a transfer of software from a web server to an unsuspecting client. It occurs in the background with no notification when a user visits some particular web page. The “drive-by” term means that a user need only access the page to be subject to the download. Such downloads usually include malware when some kind of scam or attack is underway. Because such downloads can install themselves on the systems on which they take up residence, this lets attackers put specific types of malware of their choosing on victim machines.

What kind of malware is in a typical drive-by download? Two items are common. The first is called a “keystroke logger.” It records every keypress a user makes on his or her machine into a special file called a keystroke log. The second is a class of software called “Trojans” (short for Trojan horses, after the famous ruse that got the Greeks gain into the city of Troy in The Iliad). Trojans can access the Internet, and ship a keystroke log off to some recipient address. Cyberthieves comb the log for sensitive information. If they find accounts, passwords, or other information they can use to impersonate authorized users, they'll steal their money.

---

Other phishing attacks recently reported from various sources include the following:

- Cyberthieves attempt to collect bogus payday loans. Disturbingly, these attacks feature lots of sensitive data about potential victims (social security numbers, addresses, bank accounts, credit card balances, work history, and more).
- Numerous foreclosure-related scams seek to trick people in danger of losing their homes to waste their money on false remedies for their troubles.
- Email account renewal scams ask for credit card and other account information to cover a purported but non-existent annual renewal fee.
- Countless bank account and credit card information request scams ask users to provide account details for hundreds of reasons, ranging from “database problems” to totally fabricated “security checks.”

For every online account access or transaction where money changes hands, there's at least one scam that seeks to divert some of those funds into the wrong hands. For really popular forms of online financial activity, there are bound to be scads of such scams.

## A Case of Criminal Culture

Criminals often learn their tradecraft from other criminals, sometimes through direct contact and outright mentoring, and other times through observation of what kind of crimes prove most successful. Cybercrime is a booming growth industry because it combines many characteristics that are especially appealing to criminals, including:

- **No physical risk:** Crime can be a dangerous business, particularly mugging or other forms of armed robbery. Cybercrime involves no direct contact with victims, and hence poses no physical danger to its perpetrators.
- **No proximity:** Criminals must interact with their victims to commit their crimes. Working through the Internet lets criminals interact with potential victims from anywhere in the world, with no real-world contact needed, in a way that virtually guarantees preserving their anonymity.
- **Work when you want:** Sending email or putting up web pages requires no real-time interaction with victims. A victim chooses to read an email or visit a web page whenever he or she wishes. The criminal need only check for resulting information harvests, and be ready to act fast once potentially valuable information is available.
- **Tremendous opportunity:** The sheer size of the Internet user community lets criminals experiment with scams. They know they need to score only with a small number of emails or clicks to reap sometimes significant gains. It's easy to generate tens of thousands to millions of email messages, and post tweets or Facebook pages to large audiences. They'll do anything to draw users to their malicious websites.
- **Small effort, big rewards:** Until the Internet came along, scamming required significant effort and finesse to generate earnings. It also involved real physical risk and close proximity to victims. Modern criminals need invest only small amounts of time and effort to run Internet scams, but can easily reap thousands of dollars in return.

Cybercrime is easy to do, involves little or no risk for criminals, and lets them work when and how they want, from any location in the world. If that sounds like an ideal job to you, think how it sounds to those with few scruples and a yen to make a quick and dirty buck.

## Cybercrime Learning and Lore


There's more to cybercrime than ease, low risk, convenience, and payoffs. There's a learning curve to climb, and a need to master the tools of the trade. Lots of successful scams breed imitation. Once a cybercrook learns how to run a scam, performing

## 8 Chapter 1

variations or refining targets involves little additional effort. Younger crooks can watch and learn easily and quickly from older, more experienced ones. After that, they can quickly get scams of their own going, too.

You already read about the Zeus toolkit, which combines a keylogger and a Trojan to make it easy to obtain and harvest accounts, passwords, and other sensitive information from unwary users. Zeus is just one of many toolkits that cybercriminals can use to package malware downloads that “phone home” to report on the user data they gather. For someone motivated by the illicit returns these tools can generate, spending a few days learning to use them is a modest investment with a “pot of gold” waiting at the end.

By watching others launch and manage scams, cybercriminals quickly learn how to scam. They will formulate their own scam scripts, distribute emails (or Twitter feeds, or Facebook pages, or...), and post web pages, then sit back until results send themselves back for further action. For cybercrime, further action involves separating victims from their funds: unauthorized fund transfers, illicit credit card outlays, crooked epayment collections, or other ways to access account balances as cybercrooks see fit.



**It takes only one or two trips around the block with a more experienced cybercrook for trainees to catch on, and then start running scams for themselves.**

### Variations on a Scamming Theme

So far, we’ve explored a basic and simple scam: create an email to provoke user action, harvest access information in response, then use that information to steal from victims. This takes little computing sophistication, and is simple to implement. A scam appeal, be it email, Twitter feed, Facebook page, or whatever, is broadcast to as many addresses as possible, and cybercrooks sit back and wait for a response.

But then, there are various elaborations on this scheme. In keeping with complex scams from the pre-Internet era, cyberthieves may research a specific group of victims. Then, they’ll tailor a scam that’s focused on and effective for a narrower audience. Thus, for example, ACH scams target financial or accounting professionals at small to medium-sized firms. There’s work involved in putting together a hit list, but professional association membership lists and websites, and even online phonebooks make it easy to identify such people. These folks are most likely to handle electronic banking for companies where they work. Thus, they’re most likely to have (or provide) the account information and passwords necessary so cyberthieves can hijack those accounts and redirect funds as they please.



Even more sophisticated scams have been documented. After a particularly successful account harvest, a group of cyberthieves ran various electronic funds transfers against the victim company's accounts. At the same time, another group mounted a denial of service attack against the target company to prevent their servers from accessing the Internet until after the first group had absconded with their ill-gotten funds. This prevented any automatic notifications from reaching their intended recipients until it was too late to deny or disallow those illicit transfers.

---

## Definition: Denial of Service (DoS) Attack

On the Internet, a denial of service attack takes servers or networks out of play. Basically, such attacks involve overwhelming specific servers with so much traffic that they can't do their normal jobs. If a server is totally busy doing something, it can't do anything else. In the preceding paragraph, cyberthieves drowned the servers that would normally issue fraud alerts to account holders and security personnel in huge volumes of bogus network traffic. This prevented the servers from sending those alerts to the right people. In turn, this allowed other thieves to complete a series of fund transfers that siphoned money out of the company's bank accounts.

---

## Internet, and the Money Is Easy

The Federal Deposit Insurance Corporation (FDIC) protects individual citizens' accounts against theft and fraud. What makes attacks against businesses particularly insidious is that corporate and commercial accounts in the United States are uninsured—likewise, in most of the rest of the world. Also, business accounts tend to accumulate much larger balances. Where FDIC insurance is limited to \$250,000 per depositor per insured bank, corporate balances often exceed this limit substantially. Because they do, they are prime targets for cyberthieves.

Once a cyberthief gains access to an online bank account, he or she often changes account settings to enable money transfers to other accounts. Favored techniques here include authorizing electronic funds transfers (EFTs) where such transfers are not already authorized. Sometimes a cyberthief authorizes international funds transfers when existing account settings may only permit funds to be transferred to other U.S. banks.

---

*Favorite offshore transfer destinations for cyberthieves include Bulgaria, Romania, the Ukraine, the Baltic Republics, Russia, and Nigeria, among others.*

---

Sometimes cybercrooks transfer money multiple times, in an effort to lose the wire trail from the source to the ultimate destination. In such cases, they may open temporary accounts just to receive stolen funds. Those accounts will be closed once the funds

move closer to their ultimate recipients. Occasionally, cybercrooks recruit local confederates to set up accounts, and receive and forward stolen funds. This further obscures the money trail that EFTs leave behind. Fund transfers may involve intermediate hops in countries with lenient banking laws, and where depositor anonymity is favored over criminal prosecution and restitution of illicit gains.

## **Offshore Has Definite Virtues, and Vices**

Many cyberthieves set up operations in countries where law enforcement for cybercrime is lax, lackadaisical, or simply absent. Some countries choose not to prosecute such acts. Their leaders perceive no “local harm” involved for operations that funnel hard currency inside their borders with all the fiscal benefits that a ready and steady cash flow can provide. Other countries may be subject to graft and corruption. This offers a safe haven to cybercriminals, so long as local authorities and power brokers get a “fair share” of the proceeds.

The Internet is mostly insensitive to location and geography. This makes committing cybercrime possible, if not absurdly easy. Criminals just set up shop where their offenses are ignored, tolerated, or treated as a source of income. This also makes it difficult for law enforcement in the United States, the European Union, and other areas to track down and prosecute perpetrators. Even in these circumstances, the FBI and other law enforcement bodies sometimes mount long-term, sophisticated “sting-and grab” operations. They will snare and then capture particularly glaring offenders and try them in U.S. courts. Once cybercriminals get into that system, things usually turn out differently, and much less happily for those found guilty.

## **Avoid Exposure to Avoid Losses**

The old saw goes “An ounce of prevention is worth a pound of cure.” Where cybercrime is concerned, users who avoid clicking email, Twitter, or Facebook links avoid the possibility of drive-by downloads that can infect their systems with malware. In turn, this skips the part where accounts and passwords get harvested. That prevents cyberthieves from using their information to steal, either from individuals or business concerns.

The motto at KnowBe4.com is “Think before you click,” which savvy readers should internalize for themselves as “I think before I click.” If there’s no click on the questionable link, there’s simply no opportunity for a scam to succeed. Nor is there any way for cyberthieves to get their paws on a system, to harvest accounts, passwords, and other sensitive data.