Lesson Three

Key point: useful sentences for establishing business relationship
Difficult points: Letter writing on establishing business relationship
Requirement:
By the end of this lesson, you should be able to have a good command of

- e-commerce terms given in the lesson
  useful sentences in letters of establishing business relationship

By the end of this lesson, you should be able to

- know the situation of the cybercrime
  tell of the ways to defeat snooping
  share your experience to against hackers

A Crime Wave Festers in Cyberspace

by Bob Tedeschi

Abstract: Cybercrime has long been a painful side effect of the innovations of Internet technology. Spurred by a tightening economy, the increasing richness flowing through cyberspace and the relative ease of such crimes cybercrime has now reached a considerable scale.

Key words: cybercrime; Internet technology; technically skilled thieves

Cybercrime, long a painful side effect of the innovations of Internet technology, is reaching new dimensions, security specialists say. Spurred by a tightening economy, the increasing richness flowing through cyberspace and the relative ease of such crimes, technically skilled thieves and rank-and-file employees are stealing millions if not billions of dollars a year from businesses around the world, according to consultants who track cybercrime.

Thieves are not just diverting dish from company bank accounts, these experts say. They are pilfering valuable information such as business development strategies, new product specifications or contract bidding plans and selling the data to competitors.

"Criminal activity on the Internet is growing—not steadily but exponentially, both in frequency and complexity," said Larry Ponemon, chairman of the Ponemon Institute, an information management group and consultancy, "Criminals are getting smarter and figuring out ways to beat the system."

The number of successful, and verifiable, worldwide hacker incidents this month is likely to surpass 20,000 above the previous monthly record of 16,000 in October, as counted by mi2g, a London-based computer security firm. Others have also offered dire estimates, although the dollar amounts are difficult to verify or compare because the definitions of loss vary so broadly. Part of the challenge in quantifying the problem is that businesses are often reluctant to report and publicly discuss electronic theft for fear of attracting other cyber attacks or, at least, undermining the confidence of their customers, suppliers and investors or inviting the ridicule of their competitors. In one survey of 500 computer security practitioners conducted last year by the FBI and the Computer Security Institute, a trade group, 80 percent of those surveyed acknowledged financial losses resulting from computer breaches. The computer professionals took part in the survey on the condition they and their organizations would not be identified. Among the 223 respondents who quantified the damage, the average loss was $2 million. Those who had suffered losses of proprietary company information said each incident had cost an average of $6.5 million, while financial fraud averaged $4.6 million an incident.

One of the best-known cases of corporate computer crime involved two accountants at Cisco Systems, who after pleading guilty were each sentenced in late 2001 to 34 months in prison for breaking into parts of the company's computer system they were not authorized to enter and issuing themselves nearly $8 million in company stock.

But it is nearly impossible to identify the companies that have incurred the biggest losses, because of corporate reluctance to discuss what anonymous surveys have found to be a growing problem.

Computer security specialists who help protect these companies said the attacks were hitting major banks, telecommunications companies and other *Fortune* 500 companies and included a great variety of attacks. "If people found out how astoundingly large this problem is, they'd be shocked," said James Hurley, an analyst with Aberdeen Group, a technology consulting firm. Hurley said one client, whom he declined to identify, suffered a $500 million case of electronic theft last year. Other consultants also recently recounted numerous examples of electronic thefts, but, like Hurley, they omitted company names because of confidentiality clauses in their contracts. Some examples, all provided by consultants who had seen the damage, include these: Last summer, someone hacked into the treasury system of a U.S. financial services company and transferred more than $1 million to what investigators presume to have been personal accounts. The company suspects it was an employee because of the inside knowledge required to gain access to the system. The investigation is continuing, but the employee's identity is still unknown.

In November 2001, a New York brokerage house noticed an intruder in its network from overseas but did not know the nature of the intrusion. When a security form tracked him, they saw that he was removing trading information on Euros and using that data to compete with the firm while trading in markets in the Far East. The estimated damage was in the millions of dollars. Last spring, hackers broke into a U.S. $-based bank's database and gained access to accounts of wealthy customers. Millions of dollars was transferred overseas. The bank managed to undo most of the transfers, but total losses, including a security clean-up, were more than $1 million.

The weak economy is partly behind the rise in cyber crime, said Richard Power, global manager of security intelligence for Deloitte Louche Tohmatsu, a business management consultancy. "In times of economic hardship, crime always increases," he said. "The more that money flows into cyberspace, the more criminal activity there'll be."

Corporations, meanwhile, are struggling to keep pace. With budgets and personnel stretched thin, companies that added many new technologies to their computer systems during the dot-corn build-up now find themselves lacking the resources to secure those systems against break-ins.

Part of the problem is that cyber crime is much harder to detect than crime in the physical world. "The vast, vast majority of virtual crimes right now never get caught or prosecuted, where you have some chance in the real world," said Dan Fanner, chief technology officer of Elemental Security, a computer security firm in Silicon Valley. "It is extraordinarily hard to prove anything using digital evidence."

Electronic crime is difficult to detect because it is so often an inside job. Security experts say the fastest-growing type of cyber crime involves theft of intellectual property—the pilfering of a company's plans for major projects, for instance, or marketing schedules and budgets stolen by an employee and sold to a competitor.

John Pescatorc, an analyst with Gartner Inc., a technology-consulting firm, estimated that in 70 percent of computer systems intrusions that resulted in a loss, an employee was the culprit.

In other industries, losses have become so widespread that accounting specialists are starting to call for fuller disclosure of cyber crimes by corporate victims, saying that customers and shareholders should know more about the losses and risks. Ponemon, the consultant, said companies often concealed the losses in their balance sheets. "It'll be recorded in different accounts that wouldn't have the same level of scrutiny as a loss," he said.

Such cover-ups do not allow for "a clean picture about how expensive it is to have to deal with fraudulent or criminal activities," Ponemon said. "This is becoming a very material part of the business model, so it deserves its own disclosure. That way, people can make better business decisions—whether to demand better controls or better technology or different precautions."

A securities lawyer cautioned against holding companies to a higher standard for disclosing cyber security breaches in all cases, lest they attract copycat attacks. "Sometimes it's more socially responsible to disclose, because it could multiply a company's losses by 20," he said.

But Jay Ehrenreich, senior manager of the cyber crime prevention and response group at Pricewaterhouse Coopers, said requiring broader disclosure of cyber crimes "makes a lot of sense and is something shareholders should demand". Still, he does not expect corporations to easily give in to such demands.

"A lot of times companies don't want to know what was taken," Ehrenreich said. "They just want us to find what the problem was and close the door, because there's a cost to finding out what was actually taken."

New Words

cyber-	前缀；有计算机或因特网的含义
cyber space	n. 电脑空间；网络空间
cyber crime	n. 网络犯罪
cyber attack	n. 网络攻击
spur	v. 刺激；鼓舞；鞭策
the rank-and-file	n. 普通老百姓；普通成员
pilfer	n. 小偷小摸
exponentially	ad. 按指数地（增长）
figure out	v. 想出；弄清
FBI	n. （美国）联邦调查局
practitioner	n. 开业者；实践者
fraud	n. 欺骗；诡计；假货；骗子
anonymous	a. 匿名的
brokerage house	n. 经纪行
break into	v. 强行进入；闯入
disclosure	n. 揭发；透露；被公开的秘密
victim	n. 受害者；牺牲者
shareholder	n. 股东
scrutiny	n. 仔细检查；监视

Sentence Explanations

Spurred by a tightening economy, the increasing riches flowing through cyberspace and the relative ease of such crimes, technically skilled thieves and rank-and-file employees are stealing mil-lions if not billions of dollars a year from businesses around the world, according to consultants who track cyber crime.

据追踪网络犯罪的咨询人员提供的信息，经济环境的恶化、网络空间上流动财富的日益增多，以及网络犯罪相对容易，造成每年数十亿，至少数百万美元从全球各个企业中被技术娴熟的窃贼和普通员工窃走。句子中 Spurred by…引起一个分词短语做状语，表示原因。

Exercises

1．Tell of the ways to defeat snooping.

2．Share your experience to against hackers.（Read the following Reading Material first.）

Skill Training

Business Letter Writing (I)

书信是电子商务活动中进行沟通的最主要手段之一。在本课和以下四课中，我们将给出一些书信案例和常用句型。关于书信的结构和格式，在此不做赘述。只要灵活掌握常用句型，写出一封规范的书信并不困难。

先熟悉一下一般书信正文常用的开头语句和结尾语句，然后再看各种不同内容的书信。

Commonly-used Opening Sentences and Closing Sentences of Letters 一般书信正文常用的开头语句和结尾语句

1．Commonly-used Opening Sentences 常用的开头语句

（2）表达“兹致函给您，通知您……”的句子

I beg to inform you that …

I am writing to you to ask about…

I am glad to tell you that…

（2）表达“收到贵方 X 月 X 日来函，内容悉知”的句子

Thank you for your kind letter dated 6th.

Your kind letter of July 30 arrived this morning.

Your favor of the 5th inst. has come to hand and its contents have been duly noted.

注意：① 表示 X 月 X 日来函可有两种方法 a. 用介词 of；b. 用过去分词 dated。

② kind 在“letter”前常用，以示客气；favor 用在信函文字中就是指书信。

（3）表达“迟复为歉”的句子

I must apologize for my delay in replying your recent letter.

I beg thousand pardons for not having written to you sooner.

2．Commonly-used Closing Sentences 常用的结束语句

在书信正文的末尾，常常表达盼回信、表祝愿和代问或嘱笔问候等意思，这种意思可以用句子表示，也可以用短语表示。用句子表示时，末尾用“.”；用短语表示时，末尾用“，”。

（1）表达盼回信的句子或短语

I hope to hear from you soon.

Hoping to hear from you soon,

Awaiting your early reply,

Your kind early reply will be appreciated.

（2）表示祝愿的句子

With best regards,

Wish you the best of health and success.

Much love to you and your family,

（3）表达转达或嘱笔问候

Say hello to Joe.

Please remember me to your brother.

My mother joins me in love to you.

Letters of Establishing Business Relations　书信（建立业务关系）

建立业务关系是从事商务活动最初始的活动，通过书面语言建立这种关系主要是依靠商务信函（电子邮件）来沟通。撰写这种信函时，首先要告诉对方我方是如何获悉对方信息的，并表示我方有意与对方建立业务联系的愿望。其次需要介绍我方企业的性质、基本业务情况、经营范围、分支机构、品牌等等，必要时也可向对方提供资信证明人，以便对方了解我方的资信情况。有时，还可说明希望推销什么商品或希望购买什么商品，以便对方按要求着手准备。

下面是一封希望建立业务关系的书信例子：

China National Import & Export Corp.
Shanghai Branch
Shanghai
China

July 18, 2004

M & D Co.
211 Exhibition Road
London SW7 2PG
UK

Dear Sirs

Your company has been introduced to us by Messrs. Freeman & Co. Ltd London, England, as a prospective buyer of Chinese cotton piece goods. As this item falls within the business scope of our corporation, we shall be pleased to enter into business relations with you at an early date.

To give you a general idea of the various kinds of cotton piece goods now available for export, we enclose a brochure and a sample-cutting booklet. Quotations will follow upon receipt of your specific enquiry.

We look forward to hearing from you soon.

Faithfully yours,
Wang Lin

Encl. 1. a brochure of China National Import & Export Corp. Shanghai Branch
2. a sample-cutting booklet

Useful Sentences

1．Having had your name and e-mail address from… we avail ourselves of this opportunity to write to you and…

2．We are a Sino-American joint venture specializing in the export of household electrical appliances.

3．The American Consulate in Shanghai has advised us to get in touch with you concerning...

4．Will you please send us your catalogue and price list for...

5．Will you please quote price CIF San Francisco for the following items in the quantities stated...

6．We are also interested in your terms of payment and in discounts offered for regular orders.

7．Your Commercial Counselor's Office has referred us to you for establishing business relations with your corporation.

8．We wish to introduce ourselves to you as a state-owned corporation dealing exclusively in light industrial goods.

9．With a view to expanding our business at your end, we are writing to you in the hope that we can open up business relations with your firm.

10．In order to extend (to increase) our export business to your country, we wish to enter into direct business relations with you.

Exercises

1．Try to write 10 commonly-used opening sentences and 10 commonly-used closing sentences.

2．You work in a company dealing in the import and export of local product. Please try to write a letter on establishing business relationship to a company in Australia.

Reading Materials

Hackers Are Enemy Number One on the Internet

Abstract: The Internet and Internet users can be targets for hackers. This article presents several ways to defeat the hackers.

Key words: hacker; ways to defeat the hackers; an up-to-date virus scanner; constant password changes

Until comparatively recently the opportunities for criminal activity on the internet have been low. However, the volume of business done on the Internet is growing rapidly, as people order books and other products and makes money transactions. All this is creating temptations for hackers.

Hackers are often young people who are obsessed by computers. They use them to prowl the Internet, looking for ways to break into computers systems run by banks, telephone companies and even government departments. They look for examples of credit cards and try to steal the numbers.

Recently in America, hackers have been caught testing the security system at the Pentagon, headquarters of the American Defense Department. But still the hackers persist often for a dare "because it's there" although with what success nobody really knows.

Hackers rarely admit to a successful break-in. The first indication of a security breach may be when a customer discovers a fraudulent money transaction on a credit card account. It is harder to check on somebody misusing an online connection unless there is a massive download of information which would alert the consumer.

The use of credit cards to buy things on the Internet converts the issue of Internet security into one of general security, says Michael White, multi-media product manager for Clear Communications.

"You've got to know your vendor, you just don't give your credit card out to anybody," he says. "And in the same way that you should regularly change your credit card access number, you can defeat hackers by regularly changing your Internet password. If you don't, it's like leaving the bank vault door wide open."

When it comes to creating your password, he recommends including a few punctuation marks and numbers rather than relying on letters in the alphabet.

"A hacker tries to break in using a standard computer program (ironically it can be bought online using a credit card) which is just looking at the 26 characters in the alphabet. Hackers move all the letters around, trying to find the correct combination, which makes up a password. While the possibilities are vast, you've got to remember the speed at which a computer works."

"The movie version of the guy sitting there typing in combinations is nonsense. It looks good but in fact you have a bit of software to do it. That's what's known as 'brute force' cracking. You aren't using anything clever. You're just bashing away at it like using a hammer on a lock until it breaks… but if you add punctuation marks and numerals to a password it makes it that much harder."

Hackers can also be defeated by the sophistication of encryption, or scrambling the information, which Internet service providers give those who give computer users access to the Internet.

While inside an Internet service provider's system, a customer's password is useless to a hacker.

But if a customer accesses his or her service from another Internet service provider, for example when retrieving e-mail, then it may be possible for the name and password to be viewed by an outsider. The way to beat this is to regularly change passwords.

Telecom media communications manager Glen Sowry says that when it comes to security of credit cards, the Internet offers a higher standard than many others whose honesty is taken for granted.

For example, few people think twice about giving a credit card number over the phone and many are equally careless about what happens to the carbon copy when completing a transaction over the counter.

Some customers may inadvertently reveal their passwords to hackers via what is known as a Trojan horse form of virus. These are attached to documents or messages being received, and lodge in a computer's hard drive. Next time the customer logs on to an Internet service provider the virus reveals where it is and the password to anyone who is prowling the Net looking for such information. They can then tap in.

The two ways to defeat such snooping are:

1) to have an up-to-date virus scanner which can recognize the invader and delete it

2) to constant password changes

Shopping on the Internet is likely to be the way of the future for many people. The main sites like Amazon.com probably the biggest and most successful bookshop online, which does millions of

dollars of business daily secure a customer's credit card by scrambling. Dell Computers in the US does the same and reports it is doing $14 million a day of business online. But if a company does not have that scrambling facility then sending a credit card number by e-mail is more risky.

The warning against hackers is out there. And the answer is obviously to choose tricky passwords and change them frequently and to watch who you pass your credit card details to.

Notes

hacker	n. 黑客（私自存取计算机中资料的人）
transaction	n. 办理；处理
temptation	n. 引诱；诱惑
breach	v. 破坏；不履行
prowl	v. 悄悄行动
alert	a. 警惕的；警觉的
fraudulent	a. 欺骗的
estimate	v. 估计
disclosure	v. 揭发；泄露
brute	a. 残忍的；没有理性的
bash away	v. 猛力冲击来砸坏
sophistication	n. 复杂；篡改
encryption	n. 密码
scramble	v. 使混杂
retrieve	v. 重新得到；追溯；检索
inadvertently	ad. 偶然地；无意地
snoop	v. 持续而秘密地寻找或调查
scrambling facility	n. 扰频设备
tricky	a. 狡猾的；复杂的；靠不住的

Victoria Beckham Joined Her Husband David for the Appearance on CCTV

Abstract: Victoria joined husband David for the appearance on CCTV. She introduced several models wearing dresses from her Victoria Beckham fashion line.

Key words: Victoria; Beckham; CCTV

She is known for her extremely slim figure and permanent scowl. And Victoria Beckham was showing off her svelte frame to maximum effect on Sunday as she appeared on a Chinese TV show.

The star looked rail-thin in a chic red dress, with black cuffs and collar detail.

The star's long brown hair was tied in a low ponytail and she wore spiky black heels and smoky brown eye make-up as she joined husband David for the appearance on China Central Television.

Cheerful Victoria later even flashed a rare smile for David, who immediate posted the extraordinary snap on his Facebook page: "See, I told you she smiles," he wrote, alongside a laughing picture of Victoria lying down.

Earlier the famous couple had appeared together on the talk show, with David looked typically dapper in a grey double breasted suit and matching tie.

Victoria introduced several models wearing dresses from her Victoria Beckham fashion line as David looked on proudly.

The beautiful brunette landed in China on Saturday and was given a warm welcome by local fans at the airport before hitting the shops.

The attention was well received by Victoria and she thanked her fans via Twitter by posting: "Thank you to my amazing fans here in Beijing, what a welcome!!!"

She jetted into join husband David who is on a promotional tour of the country to promote the sport as the Ambassador of Chinese football.

Useful Terms and Definitions

Network

1. A system of autonomous computers connected to each other for data transfer and communications. A network requires two or more computers, networking software (also called the network operating system), network adapters, and cables. Examples of network operating systems include Novell NetWare and Windows for Workgroups. Networks are useful when several users must share resources, such as data or printers. 2. The source of most computer problems in business computer systems.

Wholesaling

A wholesaler is an intermediary between the producer and the retailer. His main functions are: l. "Breaking of bulk", that is, buying in large quantities from the producer and selling in small quantities to retailers; 2. Warehousing, that is, holding stocks to meet fluctuations of demand; 3. Helping to finance distribution by allowing credit to retailers although paying his own suppliers promptly; 4. Sometimes preparing a commodity for sale by grading, packing, and branding the goods.

Since wholesaling is an essential part of the work of distribution, the elimination of the wholesaler simply means that the work of wholesaling must be undertaken by someone else—the manufacturer or the retailers. Large-scale retailers generally buy direct from manufacturers, but in the case of multiple shop organizations, this merely means that they themselves must undertake the business of warehousing and distribution of stock to their branches. Manufacturers of many branded goods too prefer to undertake the distribution of their products to retailers to ensure that they reach the maximum number of retail outlets. However, more than one wholesaler acts between the manufacturer and the retailer, this is justified only if the complexity of distribution for that particular commodity requires it.