

BusinessForum China

BI-MONTHLY INFORMATION - STRAIGHT FROM THE SOURCE

2|05

March/April 2005

Published By **German Industry & Commerce China** | Shanghai

▶ www.bfchina.cn

Main Topic

China's Information and Communications Market

Marketing

Virtual Marketing

WTO

Great Opportunities - The Impact of WTO on China

Staying Connected ... Safely



Thomas Parenty
Managing Director
Parenty Consulting Limited

The timing for the trip couldn't be worse. There are acquisition negotiations, you're close to signing a new distributor, and you're putting the finishing touches on the plans for a new product line. All this, and yet a series of critical meeting requires that you leave home in the next 20 minutes to catch an early morning flight. Fortunately traffic isn't too bad and you have a few minutes for a cup of coffee in the airline lounge before boarding. You take advantage of the wireless hotspot there to download your emails so you can go through them on the flight. After you check into your hotel, you connect your laptop to the hotel room's high speed Internet connection to send off the emails you finished on the flight and get up to date on what has happened in the interim. A corporate attorney has sent you a revised term sheet for the proposed acquisition and the VP of Product Development has sent you the latest rollout schedule for the new product line. After sending off your email replies, you logon to your bank's website to check balances and pay a few bills. The following day, in a break between meetings, you stop by a cyber café for another check on email.

The worst case scenario: by the time you get back to your hotel room that evening one competitor knows your new product plans, another the details of the acquisition, and your bank account is empty. And by morning your voicemail box will be full of messages from irate customers in response to the insulting email that came from you. And all of this took place even though your anti-virus software is up to date, your laptop is free of spyware, and you have a personal firewall. How could this happen?

Let's start with the wireless hotspot in the airport lounge. All of the information going to and from your laptop is traveling through the air, much like the broadcast transmissions from radio stations. Anyone with the right radio can tune in. In this case the right radio is any wireless-enabled computer or PDA (Personal Digital Assistant) with a "Sniffer" program, such as Kismet, Ethereal, or NetStumbler. These programs are available for free on the Internet

and they allow anyone in the lounge to tune in and see all of your web browsing and email.

As bad as this might be, what's worse is that in most cases they'll be able to capture the username and password you used to access your email account. This means that they'll be able to read your email and even send an email impersonating you, long after you finish your coffee and board the plane. And if you use the same password for other accounts, such as online banking, they'll have access to those, as well.

When you plug the network cable in your hotel room into the back of your laptop, you are exposing yourself and your company's information to a similar, though lesser, threat of interception as was present in the airport lounge. All of the communication going between your computer and the Internet first goes through the hotel's local network. This means that anyone, such as hotel staff, who have access to the hotel network have access to your information. This is analogous to the hotel waiter having your credit card when he is processing your bill. He is probably honest, but there is still a risk.

So what can you do to protect yourself?

Encrypt the information you send over the Internet. Encryption is a mathematical process of scrambling information so that anyone who intercepts it won't be able to understand it. There are many different encryption solutions available today and the most comprehensive one for the corporate user is the VPN (Virtual Private Network). A VPN encrypts all of the information between your laptop and your corporate network so that everything you do, from sending email to accessing other corporate applications, e.g. CRM (Customer Relationship Management), is protected from prying eyes.

Without a VPN you have to look to protecting yourself on a case by case basis. For email, this may mean that the best you can hope for is to protect your password. Yahoo!® Mail, for example, provides two modes for logging on,

standard and secure. The default mode offers good, but not foolproof no protection for your password. At the Yahoo!® Mail login page there is also the option to use the secure mode. When you click on “Secure” you are taken to a new login page that is protected by SSL (Secure Sockets Layer) encryption for complete protection. If you look in the Address Bar you’ll see that it begins with “https://,” where the “s” means secure. In some browsers, such as Internet Explorer on Windows, a padlock in the lower right hand corner of the window also indicates that encryption is being used. Once you login, however, there is no more encryption to protect the confidentiality of your email. If you look at the Address Bar you’ll see that the “s” has disappeared and the beginning of the address now looks like “http://.” This won’t prevent intruders from reading your email, but it will prevent them from being able to use your email account in the future, or using your password in other circumstances, such as online banking. In contrast, the email passwords on netease.com, sina.com, and sohu.com are completely vulnerable.

What about the safety of online banking?

By and large this is a relatively safe activity because bank websites provide SSL encryption to protect all of your banking activity and not just the logon process. Of course you should verify this by checking for “https://” at the beginning of the Address Bar on every page. The protection of your bank balance thus de-

pends on the protection of your password. This means you should never use your bank password anywhere else, such as for email or another website, where it is not protected. Nor should you disclose your password in reply to any of the numerous “phishing” emails, that claim to be from your bank.

The security risk in a cyber café is much greater than either at an airport lounge or hotel room, because you are using someone else’s computer and you have no way of knowing what malicious software is running on it. Of particular concern are keystroke logging software that records everything you type, including bank account and email passwords. Since this information is being collected as you type it, no form of encryption can protect it. You are completely vulnerable and there is nothing you can do to protect yourself. Cyber cafés are great places to catch up on some web browsing, but not places for serious work.

Fast, convenient access to the Internet is necessary not only for conducting business, but also for taking care of many of the bookkeeping chores of a busy life. As with every aspect of life, there are risks and the effort you spend to protect yourself and your company’s information should be based on the value of that information and the damage that would result from its theft or destruction. In order to make that decision you first need to know what the risks are and how to mitigate them. ■

PROFILE

Thomas Parenty is Managing Director of Parenty Consulting Limited (Hong Kong). For over twenty years, Mr. Parenty has advised governments and corporations on the development and use of information security technologies to increase productivity and innovation, while reducing costs and risk. In particular, his consulting practice helps companies protect and leverage their intellectual property and helps governments protect information relating to public health and safety. Mr. Parenty has testified five times before the United States Congress on global competitiveness, national security, law enforcement, and encryption. A former employee of the U.S. National Security Agency, he is the author of Harvard Business School Press’ Digital Defense: What You Should Know About Protecting Your Company’s Assets.

CONTACT

Parenty Consulting Limited | 39/F | One Pacific Place | 88 Queensway | Admiralty | Hong Kong
Tel: (852)2273 5730 | Fax: (852)2273 5999 | www.parenty.com | thomas@parenty.com