

Minimising online fraud

RIVA RICHMOND show what you can do to protect yourself when shopping online

LAST year, 92 million people bought things online using credit cards, debit cards and services like PayPal and Google Checkout. Millions of others paid bills and wired money electronically from bank accounts with just a few clicks.

Despite the apparent popularity of all these services, they still cause nagging anxiety for many of us.

We wonder, how secure are these payment systems? What if someone steals my account numbers and goes on a wild shopping spree or bleeds my savings dry?

Deciding which online payment method to use would seem to be a simple matter of picking whichever offers higher security. But the wise consumer also weighs the legal protections in the case of theft: the best security and the lowest liability don't necessarily go together.

Here's the lowdown on the risks associated with the most popular ways to pay online:

CREDIT CARDS

After you hear some of the horror stories, using a credit card online may seem as risky as Russian roulette. Crooks can and frequently do capture card numbers by sneaking malware onto home computers or by tricking people into revealing numbers in "phishing" schemes in which people unwittingly type in the numbers on fake sites. Some thieves hack shopping sites.

There are a few precautions everyone should take. First, look for signs of quality security at sites you use, like logos or seals, from security providers like VeriSign and McAfee, said Aleksandr Yampolskiy, director of security at the luxury shopping site Gilt Groupe. To check that a seal is legitimate, click on it to make sure it takes you to the verification page of the security service.

Also make sure that "https" appears in the address bar, because that indicates that digital transmissions from the site are



being encrypted. Yampolskiy said.

Security seals, however, are just a starting point, not a guarantee that a site is secure. They affirm only that it has met specific criteria set by that security service. And the lack of a seal doesn't necessarily mean a site is risky. So use common sense when deciding which merchants to do business with. For instance, it isn't wise to shop at a site you reached by clicking on a spam e-mail. If you're suspicious of a site, run its name through a search engine and see if there are complaints from other shoppers.

SSL encryption, which is indicated by the "s" in "https" in the address bar and a padlock icon in the lower right-hand corner of the browser, is your best insurance against theft of your data while it's being transmitted.

Sending your personal data across a network is a key moment of vulnerability, said Robert Zigweid, a senior security consultant at IOActive, which helps companies secure their sites and networks. Responsible sites will automatically use "https" on pages where sensitive information is sent and received.

If you get a pop-up or other warning that something is wrong with a site's

SSL certificate, "back away," said Tim Callan, vice president at VeriSign.

Professional, well-put-together sites do not tend to have certificates that are expired or have other problems.

And since shady sites can use encryption, too, also check the address bar for a bit of green or the site owner's name written in green. (Recent versions of major browsers all now use green in some way to indicate the existence of another layer of security called an extended validation SSL certificate). It indicates that the site you're visiting has been vetted and belongs to a legitimate company, and not a phishing site. You will certainly see green on larger e-commerce sites and on bank sites.

None of this encryption will help you if you're infected with malware known as keylogger. It captures your keystrokes and images from your screen and then sends them to hackers. Your only real line of defence is to use security software and install all the updates from that software and all the other software you use.

Password-management software can also help. This stores your login information and, typically, the personal data used in Web forms in an encrypted place on your computer. You can

For extra protection against having your card number stolen, consider using one-time credit card numbers for online purchases, which you can often set up with your card number

then enter this sensitive data onto Web site forms without retyping it.

Now that you are frightened enough, here's the good news about online payments: There is little to worry about using credit cards online, because the risk of loss from unauthorised charges, by law, is almost nil.

"The strongest protections are when you pay by credit card," says Carole Reynolds, a senior lawyer at the Federal Trade Commission. Under the Truth in Lending Act, consumers' maximum

liability for unauthorised use of their credit card is only US\$50 (RM160), and when a card is used online, it's zero.

If you report fraud quickly, banks will typically reverse the charges rapidly and without much fuss, though in these tight times banks are scrutinising fraud claims more closely, says Avivah Litan, a payment-fraud expert at research firm Gartner.

For extra protection against having your card number stolen, consider using one-time credit card numbers for online purchases, which you can often set up with your card provider.

DEBIT CARDS

Using debit cards online is a bit riskier. These transactions, which draw directly from your bank account, are subject to a different federal law, the Electronic Fund Transfer Act. This law provides considerable protection from liability, but the level of protection diminishes as time passes.

If you report unauthorised charges on a debit card within two business days of discovering the problem, your liability is limited to US\$50 offline and zero for online transactions, Reynolds says. If you neglect to do that, but report the loss within 60 days of the date your bank sent the

statement listing the bogus transactions, your liability is capped at US\$500 for offline transactions and remains zero online. If you miss those deadlines, however, you could end up in a bigger mess. Reynolds warned that your liability could be unlimited.

PAYMENT SERVICES AND BILL PAYMENT

Shopping online using services like PayPal, Google Checkout and BillMeLater offer some useful additional security because you entrust your sensitive account information to one company and not to every online store you may buy something from. This can be a good idea, especially if you frequently buy from little-known merchants that may not have top-notch Web defences.

But Litan warns that if your PayPal account is used fraudulently, it may be harder to get your money back than if you use a credit card.

For those who pay bills online, note that, like debit cards, online bank accounts — savings, checking and other personal "asset accounts" — are covered by the Electronic Fund Transfer Act, so your responsibility for unauthorised transactions is limited, depending on when you discover and report fraud.

So even if your computer becomes infected with a malicious programme and thieves are able to steal your password and plunder your bank account, you will get your money back if you catch it quickly. Litan says it's a good idea to set up automatic bill payments with your bank, as opposed to individual billers like the gas company or the day care provider, because banks and their payment processors are generally better at protecting data than merchants. — NYT