



COMPUTER TROUBLESHOOTERS

Global NEWS

® May 2004

*“Local service,
global strength”*

Computer Troubleshooters of Southwest Austin

6034 Abilene Tr.
Austin, TX 78749

PHONE:
(512) 394-9115

FAX:
(512) 301-1754

E-MAIL:
dbryce@comptroub.com

See us on the Web!

at:

www.comptroub.com

*“Thousands of businesses
around the world depend on
Computer Troubleshooters”*



Global strength

Newsletter produced by
Pat Chesters

www.computertroubleshooters.co.nz

Internet Related Scams

The old fair ground scams like find the lady or the 3 cups may be long gone, but they have been followed with new up to the minute scams using the internet, e-mail or even the old “invoice” trick with a modern slant.

Phishing

Phishing (pronounced fishing) has been brought to our attention with people in both the northern and southern hemispheres recently falling for the scam. This is an example of Phishing: You get an official looking e-mail from your bank. It will contain text like **“This e-mail was sent to you by YourBank server to verify your e-mail address. You must click the link below and enter in the small window your ATM/Debit Card number and PIN”**

The unsuspecting customer clicks on the link and is taken to a web site that looks like their banks site, where they type in the details as requested. What happens next . . . the creator of the site, (which is an excellent copy of the real banks web site) has your bank details and within seconds



has emptied all of the money out of your bank account. The Anti-Phishing Work Group (APWG) has stated that Phishing is increasing at up to 60% per month in 2004.

You should be very suspicious of any e-mail that asks you to supply login or personal information of any kind.

The “looks like an invoice” scam.

Many of you will have come across this one in the past. The old trick where you receive in the post some papers that look like an invoice. The scammer is hoping that a busy office will miss that it is not a real invoice and pay over the money.

The new version of this invoice scam is to send a domain name registration to a company that already

owns a domain name. The registration looks like a reminder to renew your domain name, it has a due date as you would expect and you must pay the annual or bi annual fee to keep ownership of your name.

In fact it is trying to sell you a **new** domain name virtually identical to the one you already own, you have to read it very carefully to spot the difference. It would be very easy for a busy office to pass this through for payment as they don't want to lose the rights to their domain name. It even includes a pay by credit card payment slip. If confronted the scammer just says they are selling domain names – which of course is a legitimate business.

So when renewing your domain name registration ensure it is yours and not a similar one you are paying for.



Australia



Canada



Dominican Republic



Republic of Ireland



Hong Kong



Kuwait



Mexico



Netherlands



New Zealand



Portugal



Singapore



South Korea



South Africa



United Kingdom



USA