SUBMISSION NO. 6

Submission - Inquiry into Cyber Crime

This submission comments on two sections of the Terms of Reference, d) and e) and comes about from my experience as an Australian consumer in trying to report an instance of Cyber Crime being hosted in Australia, and having nowhere to report it to on a Friday evening and being advised to wait until business hours on the following Monday morning, thereby seeing the scammers operating freely over a complete weekend.

The scam was a typical phishing scam targeting E-gold as the target, in September 2006. E-gold was the then internet's then largest electronic currency site and had been in operation for over 10 years.

Terms of Reference specifically being commented on:-

d) Measures currently deployed to mitigate e-security risks faced by Australian consumers:

- *Education initiatives*
- *Legislative and regulatory initiatives*
- *Cross-portfolio and inter-jurisdictional coordination*

e) Future initiatives that will further mitigate the e-security risks to Australian internet users.

Overview & Background of the Reason for this Submission

To an Australian consumer there is no inter-jurisdictional coordination. Further, there is no intra-jurisdictional coordination within the Australian Federal Police. The phishing site which I was trying to submit a crime report for had a domain name of wwww-e-gold.com, (the real site being: www.e-gold.com). The domain was being hosted in Australia by Melbourne IT, a major, and the original, Australian domain name registrar.

At 18:45 on Friday 15th of September 2006, the same day wwww-e-gold.com was registered, I called Melbourne IT to try and get them to be proactive and do something about the domain, e.g. suspend it, but they gave me the typical corporate response, "*there is nothing we can do; send your complaint to policy@melbourneit.com and it will be dealt with during office hours*". I advised them that criminals don't work office hours, and that this scam will be ongoing overnight, and over the weekend and it will be trapping people for all that time worldwide, until they get to it, and if I am going to go to the trouble of reporting it, it will be to the Australian Federal Police, as the local NSW Police just weren't interested, as it was "cyber crime".

In calling the AFP, I had to be persistent to them to take my report. It took about 15 calls to the main switchboard in Canberra, 0262567777, with the advice each time, "*to call back during office hours*", as the anonymous AFP staff, (they had refused to give me their name or location), kept taking the easy way out by hanging up on each of my calls. I was advised that it "*wasn't particularly an important crime compared to terrorist acts, drug running etc*" and I was threatened with arrest myself if I called back again. I would have thought they could have at least taken the complaint, and maybe even humored me that it would be looked in to, even if they shelved it until Monday morning. Providing a basic level of service would have been the easy way out, instead of hanging up on each of my 15 calls.

Eventually, on the 16th call, when put through to a more senior officer, I was advised to lodge an online complaint with the AFP's Australian High Tech Crime Centre, AHTCC, at www.ahtcc.gov.au (whose site was discovered to be faulty). I was just getting nowhere. Even today, the AHTCC's website asks people not to report crimes to them, but instead report the crime to "*your local State or Territory police, or to the Australian Federal Police (AFP)*" thereby restarting the whole process.

I gave up trying to report the said phishing crime and I ended up making a complaint to the ACT Ombudsman, who sided with the AFP, in saying that reporting Cyber Crime 24/7, was unreasonable expectation.

It is therefore my submission that the following should be considered:-

- That the Australian Consumer have a clear and well publicized 24/7 "place" to report cyber crime to, either via phone, email, or online form submission and are educated in the process, ala terrorism

fridge magnets.

- That is be considered a reasonable expectation that reporting Cyber Crime is 24/7.
- That the State and Territory police be educated in where to direct the Australian Consumer when they call to report Cyber Crime, or coordinate with the AFP once a local complaint is taken. At the moment the local police in NSW just aren't interested and need to be educated in what to do with Cyber Crime complaints (as do the AFP front line officers themselves).
- The the AFP need to take responsibility for, and educate themselves, in accepting all Australian cyber crime complaints and be the central place of coordination, 24/7. Gone should be the days when the Australian Consumer is fobbed off, or hung up on due to lack of interest.
- The the AFP take responsibility for, and educate themselves that the AHTCC is not the place to send Australian Consumers to report crime.
- That legislation be passed to allow for domain registrars be directed to suspend domain names suspected to be involved in Cyber Crime and that the onus be on the domain owner, not the AFP, to prove that no Cyber Crime is involved if the domain owner wishes to have their domain name reinstated. This is allow for speed in stopping the routing of phishing links in emails.

David Ready

David Ready: The author has been involved in the IT industry and data transmission for 26 years, and with the internet for 19 years in many capacities and is very experienced in many of its uses. The author was responsible for installing the first ever global VoIP link between Chatswood and Canberra in 1994. This submission is forwarded by the author as an individual Australian Consumer.