

By: Fedra Corradi, SEO News Editor

Betting Online, Phishers Training Ground

eBay and banks no longer good enough

Phishing is really taking proportions in the cyber crime universe. After initially targeting only online auction sites and online banks, the trend expands to 'working' on virtual casinos. Security company Symantec has discovered the first examples and deepened its research on the matter, after managing to track back a large number of attacks on small countries to assaults on online casinos. Punters on such sites make much better targets because there is no need for a middle man to be involved, as it is often required with banks, for example. Usually, the target is in another country and the cyber criminal cannot simply send the money into an account abroad. That's where the so-called 'mules' intervene, playing the part of taking the money from the compromised bank accounts and then wiring them someplace else by using hard-to-trace Western Union money transfers, The Register explains. Gambling is the breeding and training ground for such activities. "Phishers can set up online gambling accounts sites using stolen credit card numbers and victims' identities. They can then launder dirty money by exchanging funds through the pots of games they set up amongst themselves," according to the entry on the Symantec site. Even bots can be used for this job, after being programmed to win or lose, and thus transferring the money to a chosen client. The technique used is fairly simple and does not require additional resources other than those used with banks and online auction sites; "phishers could steal players' email information and then forward them spoofed emails claiming that the player has money in his or her account. The message would include a link to a spoofed Web page that requests the user to enter his or her account information. This information can then be used to steal credit card information," Symantec said.