

Microsoft launches global antiphishing initiative
Will set in motion more than 100 legal proceedings

News Story by China Martens

MARCH 20, 2006 (IDG NEWS SERVICE) - Microsoft Corp. today unveiled a global initiative to crack down on cybercriminals who engage in phishing. The company said it will set in motion more than 100 legal actions against phishers in Europe, the Middle East and Africa (EMEA) by the end of June, according to a [release](#).

Phishing attacks use spam to entice Internet users to visit what appear to be legitimate e-commerce Web sites but are in fact phony sites controlled by cybercriminals. Users are encouraged to enter personal data such as passwords and bank account or credit card details, which the criminals can then exploit to commit crimes.

Neil Holloway, president of Microsoft EMEA, introduced the company's Global Phishing Enforcement Initiative (GPEI) at a technology debate in Brussels hosted by the European Internet Services Providers Association (EuroISPA) and co-sponsored by Interpol.

Three years ago, the main problem centered on spam, Holloway said. But over the past 12 months, phishing has become "the next wave of cybercrime," he said.

The aim of GPEI is to better coordinate and expand on Microsoft's previous antiphishing moves. The vendor said it will work with law enforcement agencies, different industries and governments with the mission of improving consumer education, increasing the number of cybercriminal prosecutions and identifying more ways to combat phishing by using technology.

Of the more than 100 planned legal actions against phishers in EMEA, 53 are already under way, including actions against alleged cybercriminals in countries including Austria, Egypt, France, Morocco, Spain, Turkey and the U.K., the release said.

When Microsoft identifies a suspect phishing site, it notifies the Internet service provider hosting it, said Jean-Christophe Le Toquin, a Microsoft attorney who is working on the phishing cases. Microsoft will provide URLs or e-mail addresses affiliated with the scam to law enforcement officials, he said.

So far, prosecutions have been few, but the number of cases is growing. At least one phisher -- based in the U.S. but whose site was hosted in Austria -- pleaded guilty in December, Le Touquin said.

Law enforcement officials are still adapting to cybercrime's increasing demands and the complications when it crosses international borders, said Bernhard Otupal, a crime intelligence officer at Interpol in Lyon, France.

"If a country is running a huge case, it's often the last thing to think that another country might have a similar issue," Otupal said.

Interpol runs training courses for officers in areas such as botnets, which a criminal can use to take control of thousands of computers in different countries to attack other computers.

Phishing attacks are growing, according to an online poll conducted by security firm Sophos PLC in February. The survey of 600 business users determined that 22% of PC users receive at least five phishing e-mail messages every day.

Some companies are employing measures to combat online fraud attempts. MasterCard International Inc. started a program two years ago, said Walter Hansen, vice president of security and risk services, who is based in Waterloo, Belgium.

MasterCard has a contract with NameProtect Inc., a digital fraud protection company, to troll the Internet for credit card numbers and phishing sites, Hansen said. MasterCard also contacts the Internet service providers associated with those sites, he said.