

[Home](#) » [News](#) » [Tracking Devious Phishing Web Sites](#) » [Full Text](#)

ACM TECHNEWS

Tracking Devious Phishing Web Sites

October 19, 2009



Machines involved in a flux trick "don't belong to the miscreants, they belong to you and I and our grandmothers," says Minaxi Gupta, an assistant professor of computer science at Indiana University.

Credit: Indiana University

Internet security experts have discovered that many phishers are using a trick called a flux, which allows a fake Web site to rapidly change its URL, making it difficult for defenders to block phishing sites or warn unsuspecting users. New research has found that about 10 percent of phishing sites are now using flux.

Indiana University professor Minaxi Gupta says that because phishers often have access to thousands of hijacked machines they can quickly move a site around the Internet, protecting it from security professionals while keeping the fake site operational. To use a flux, phishers must control a domain name, giving them the right to control its name server. The phisher can then set the name server so it

directs each new visitor to a different set of machines, rapidly cycling through the thousands of addresses available within its botnet. If the name server also is moved to different locations on the Internet, it is particularly difficult for defenders to pinpoint a central location where the fake site can be shut down.

Gupta has identified several methods for detecting a flux and suggests that flux detection should be incorporated into the domain name system itself, because only a fraudulent site is likely to use a flux. There are some legitimate reasons for using a flux, but a legitimate flux looks different from a flux on a botnet. Shortening the detection time of phishing sites by even a few hours can make a major difference and make the scams less profitable for criminals, Gupta says.

From *Technology Review*

[View Full Article](#) 

Abstracts Copyright © 2009 [Information Inc.](#) , Bethesda, Maryland, USA

