**Federal Deposit Insurance Corporation**
550 17th Street NW, Washington, D.C. 20429-9990

**Financial Institution Letter**
**FIL-64-2005**
**July 18, 2005**

# "PHARMING"

## Guidance on How Financial Institutions Can Protect Against Pharming Attacks

**Summary:** The FDIC is issuing the attached guidance to financial institutions describing the practice of "pharming," how it occurs, and potential preventive approaches. Financial institutions offering Internet banking should assess potential threats posed by pharming attacks and protect Internet domain names, which – if compromised – can heighten risks to the institutions.

**Distribution:**
FDIC-Supervised Banks (Commercial and Savings)

**Suggested Routing:**
Chief Executive Officer
Chief Information Security Officer

**Related Topics:**
GLBA, Section 501b
FIL-77-2000, Bank Technology Bulletin, November 2000
FIL-27-2004, Guidance on Safeguarding Customers Against E-Mail and Internet Related Fraud, March 2004
FFIEC Information Security Handbook, Issued November 2003
Interagency Informational Brochure on Phishing Scams, Contained in FIL-113-2004, Issued September 13, 2004
Putting an End to Account- Hijacking Identity Theft Study, Issued December 2004

**Attachment:**
Guidance on How Financial Institutions Can Protect Against Pharming Attacks

**Contact:**
Senior Technology Specialist Robert D. Lee at Rolee@fdic.gov or (202) 898-3688

**Note:**
FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2005/index.html.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (1-877-275-3342 or 202-416-6940).

## Highlights:

- "Pharming" is the process of redirecting Internet domain name requests to false Web sites to collect personal information. Information collected from these sites may be used to commit fraud and identity theft.
- The attached guidance explains how pharming occurs and recommends strategies for protecting financial institution Internet domain names from a successful pharming attack.
- The effectiveness of an insured institution's Internet domain name protection program should be addressed in periodic risk assessments and status reports presented to the institution's board of directors.

# Guidance on How Financial Institutions Can Protect Against Pharming Attacks

The Federal Deposit Insurance Corporation (FDIC) has prepared guidance for financial institutions on the risks posed by "pharming" and strategies that can help mitigate those risks. "Pharming" is the practice of redirecting Internet domain name requests to false Web sites in order to capture personal information, which may later be used to commit fraud and identity theft. While pharming is similar to phishing in that both practices try to entice individuals to enter personal information on a fraudulent Web site, they differ in *how* they direct individuals to that site:

- **Phishing** – as in fishing for confidential information – is a scam that encompasses fraudulently obtaining and using an individual's personal or financial information. In a typical case, the consumer receives an e-mail appearing to originate from a financial institution, government agency or other entity that requests personal or financial information. The e-mail often indicates that the consumer should provide immediate attention to the situation described by clicking on a link. The provided link appears to be the Web site of the financial institution, government agency or other entity. However, in "phishing" scams, the link is not to an official Web site, but rather to a phony Web site. Once inside that Web site, the consumer may be asked to provide a Social Security number, account numbers, passwords or other information used to identify the consumer, such as the maiden name of the consumer's mother or the consumer's place of birth. When the consumer provides the information, those perpetrating the fraud can begin to access consumer accounts or assume the person's identity.

- **Pharming** refers to the redirection of an individual to an illegitimate Web site through technical means. For example, an Internet banking customer, who routinely logs in to his online banking Web site, may be redirected to an illegitimate Web instead of accessing his or her bank's Web site.

Pharming can occur in four different ways:

- Static domain name spoofing: The "pharmer" (the person or entity committing the fraud) attempts to take advantage of slight misspellings in domain names to trick users into inadvertently visiting the pharmer's Web site. For example, a pharmer may redirect a user to **anybnk.com** instead of **anybank.com**, the site the user intended to access.

- Malicious software (Malware): Viruses and "Trojans" (latent malicious code or devices that secretly capture data) on a consumer's personal computer may intercept the user's request to visit a particular site, such as **anybank.com**, and redirect the user to the site that the pharmer has set up.

- Domain hijacking: A hacker may steal or hijack a company's legitimate Web site, allowing the hacker to redirect all legitimate Internet traffic to an illegitimate site. Domain names generally can be hijacked in two ways:

    - Domain slamming: By submitting domain transfer requests, a domain is switched from one registrar to another. The account holder at the new registrar can alter routing instructions to point to a different, illegitimate server.
    - Domain expiration: Domain names are leased for fixed periods. Failure to manage the leasing process properly could result in a legitimate ownership transfer. In this instance, trade name laws usually must be invoked to recover lost domains.

- DNS poisoning: The most dangerous instance of pharming may be domain name server (DNS) poisoning. Domain name servers are similar to Internet road map guides. When an individual enters **www.anybank.com** into his or her browser, Domain Name Servers on the Internet translate the phrase **anybank.com** into an Internet protocol (IP) address, which provides routing directions. After the DNS server provides this address information, the user's connection request is routed to **anybank.com**. Local DNS servers can be "poisoned" to send users to a Web site other than the one that was requested. This poisoning can occur as a result of misconfiguration, network vulnerabilities or Malware installed on the server.

  There are 13 root DNS servers for the entire Internet, which are closely protected and controlled. Most requests are directed by the local DNS server before they reach a root DNS server. However, if a hacker were to penetrate one or more of these root servers, the Internet could be severely compromised.

**Detection and Prevention**

Consumers and businesses can take several steps to prevent pharming attacks:

- Digital certificates: Legitimate Web servers can differentiate themselves from illegitimate sites by using digital certificates; Web sites using certificate authentication are more difficult to spoof. Consumers can use the certificate as a tool to determine whether a site is trustworthy.

- Domain name management: Financial institutions should diligently manage domain names by ensuring that the domain names are renewed in a timely manner. Institutions also should investigate the possibility of registering similar domain names. In addition, many registrars offer domain locks[1] to prevent unauthorized domain slamming. For more information about managing domain

[1] Generally, if someone wants to transfer a domain name, he or she would make the request at the registrar's Web site. The domain may then be intentionally or unintentionally transferred to the person making the request. If the name is locked, the request is automatically denied. If the owner of the domain name wishes to transfer the name, he or she would have to unlock the domain name before proceeding.

names, refer to FIL-77-2000, which includes a *Bank Technology Bulletin* informing banks about the risks related to poor domain name management and recommended best practices.

- DNS poisoning: Insured financial institutions should investigate anomalies about their Web site to ensure that DNS poisoning attacks are addressed promptly. For example, if **Anybank'**s domain was hijacked, it would immediately stop receiving normal Internet-related requests. The drop in Internet traffic should alert technology staff at **Anybank** to the problem, which the staff should then investigate.

- Consumer education: The financial institution should recommend Internet banking customers install current versions of virus detection software, firewalls and spyware scanning tools to reduce computer infections, and should stress the importance of regularly updating these tools to combat new threats. The institution also should educate consumers about how to know when they are connected to a trusted site instead of a spoofed site.

**Conclusion**

Financial institution domain names are critical and valuable financial institution property that should be protected. Financial institutions and their Internet banking customers may be vulnerable to data and financial loss if domain names are misused or otherwise redirected. Practices to monitor and protect domain names should be regularly reviewed and updated as part of a financial institution's information security program.