

Pharming

The scam popularly known as 'phishing' – email messages trying to deceive you into surrendering personal information over the Internet – today is well known. Competing with it more and more for headlines is a newer scam: pharming.

Illinois National Bank wants to take a moment to offer you information about pharming, in our ongoing effort to keep our customers informed about issues that could impact their online banking experience.

Phishing requires victims to voluntarily visit a criminal's website; pharming simply redirects victims to fraudulent websites without assistance. Pharming subverts a basic service of the Internet known as the 'Domain Name Service,' or 'DNS.' Each machine connected to the Internet knows the location of one or more DNS servers. This service translates a human-friendly URL name such as www.illinoisnationalbank.com, into an IP address, which is a unique number that has been assigned to each web server on the Internet.

To execute pharming, suspects first must gain access to the DNS server used by many people, such as the server of an ISP. Once accessed, the suspect will replace the IP number for the financial institution's URL with the IP number of his or her fraudulent website. When this occurs, any person using that DNS server will be redirected, silently, to the fraudulent website.

The good news is pharming requires either an unpatched software/server vulnerability to exist on the DNS server itself, or the criminal needs an insider at the ISP or financial institution to make unauthorized DNS server changes. This is rare.

Please be assured that Illinois National Bank manages and updates its DNS server's software to maintain a high level of security. We maintain the highest standards; our customers are protected from pharming that would result from a compromise of our DNS server.

If you are suspicious about our website, you may submit an email to abuse@illinoisnationalbank.com. You may also contact our customer service department by email at customerservice@illinoisnationalbank.com or by phone at 217-747-8766.

If you are suspicious about a website, consider contacting the FBI's Internet Fraud Complaint Center at www.ifccfbi.gov.