



“Having Catbird is the equivalent of having a dedicated security team complete their rounds every 15 minutes, 24 hours a day, 7 days a week, 52 weeks a year.”

EXECUTIVE SUMMARY

Ohio State Bank needed to protect their website from pharming/hijacking and defacement. By deploying Catbird’s DNS Pharming/Hijacking Monitor and Web Page Defacement Monitor, they secured their site against two of the most damaging types of attacks that financial institutions face. As the bank grew, they added other Catbird Monitors in order to lock down their firewall, protect their email system, and secure their entire network from every known type of hacker attack.

THE NEW BANK ROBBERS

When national banks started moving into Marion, Ohio, Ohio State Bank started refocusing on what community banks do best—offering the same range of services that larger banks do, while providing their customers with the highest possible levels of convenience and value. One of their first moves was to expand their e-banking services, so that customers could check their balances, pay their bills, and make transfers through the web.

The move into online banking can be a risky step for a bank to take. Hackers, often affiliated with organized crime groups, have become experts at “pharming” or “hijacking” websites. In a pharming, a hacker reroutes unsuspecting visitors from a legitimate website to a phony “look-alike” site. Thinking they’re on the original site, customers enter their confidential information, which hijackers then use to make purchases, drain accounts, or even steal identities.

In addition to these financially motivated hackers, recreational hackers pose a major risk to any online venture, seeing it as a challenge to deface a company’s website by altering or replacing the content. For both types of hackers, banks are a primary target, and the risk to a bank’s reputation – and consequently its bottom line—are severe.

GUARDING THE BANK

Ohio State Bank uses a local firm to host their website, and outsources its e-banking services to a well-known third-party vendor. The routing points between Ohio State Bank and these critical partners provide a particularly dangerous opening for hackers attempting to interfere with their business. To protect their site, Ohio State Bank uses Catbird’s full suite of monitors, including the DNS Pharming/Hijacking Monitor and Web Page Defacement Monitor

DNS hijackers exploit Internet routing protocol vulnerabilities which are inherently insecure. The DNS Pharming/Hijacking Monitor works by taking a snapshot of all of Ohio State Bank’s DNS records. It then compares the snapshots with current DNS records every 15 minutes, every day of the year. If they don’t match, Catbird sends an alert to the system administrator’s email or pager so they can resolve the problem immediately.

The Web Page Defacement Monitor protects the bank’s site by establishing “baseline content” —approved content for the Web site. The Defacement Monitor then compares the baseline content to Ohio State’s live site every 15 minutes, every day of the year. When a mismatch occurs, it means there has been an unauthorized alteration to the site. Catbird immediately alerts the system administrator so they can remedy the problem.

“We’ve reduced the risk of our website being hijacked or defaced to a ‘very low’ rating, thanks to Catbird’s continuous active monitoring,” says Phil Hotz, Ohio State Bank’s Director of IT Security. “Our Board of Directors takes our Web security very seriously. I explained that traditional vulnerability tests were like sending a security guard to your house once or twice a year to see if your windows and doors were closed. Having Catbird is the equivalent of having a dedicated security team complete its rounds every 15 minutes, 24 hours a day, 7 days a week, 52 weeks a year.”

THE CHALLENGE

When The Ohio State Bank began offering online banking services, their central concern was the security of their website. In particular, the rising tide of website pharmings and defacements threatened both the reputation of the bank and the security of their customers’ confidential data.

THE SOLUTION

Ohio State Bank chose Catbird’s full suite of monitors, including the DNS Pharming/Hijacking Monitor and Web Page Defacement Monitor, to protect their website. Catbird’s fully-automated monitors scan the bank’s website every fifteen minutes, 24/7, 365 days a year, to ensure that it hasn’t been defaced or hijacked.

GROWING WITH CATBIRD

Ohio State Bank started out in 1988 as Marion Bank, with one branch and approximately 9 million dollars in assets. By 2005, they’d expanded throughout central Ohio and renamed themselves The Ohio State Bank. With over ten times their initial assets, and a much larger and more geographically distributed client base, they found themselves facing all the challenges of running a wider and more complex network.

As Ohio State Bank grew, they continued to add Catbird Monitors in order to protect their network. They now deploy the full suite of Catbird Monitors, which in addition to protecting the bank from every major type of hacker attack, also safeguards its email system, greatly simplifies its compliance with regulatory audit requirements, and monitors the performance of its website and e-banking services to ensure that customers are receiving the highest level of service.