CUSTOMER SUCCESS

symantec™

M&T Bank

Skirting Phishing Scams and Protecting Customers Using Symantec Online Fraud Management

M&T Bank (M&T), a mid-sized financial institution, seeks to migrate as many of its customers as possible to Web banking, while maintaining its trusted reputation among its clientele. A successful phishing attack could derail the bank's plans and damage its brand. After reviewing several options, M&T turned to Symantec for online fraud detection services and other information security solutions. When a real phishing attack occurred, the bank was protected: Of an estimated 14 to 17 million phishing emails sent, only seven people reported receiving them, and no one was fooled into revealing sensitive personal information. M&T was able to shut down the fraudulent Web site in less than eight hours. This quick response prevented any customer losses and preserved the bank's reputation.

Company Profile

M&T Bank (www.mandtbank.com) operates 650 branches throughout New York, Maryland, Pennsylvania, D.C., Virginia, West Virginia, and Delaware.

Industry

Financial

Solution

Information Security

"I have many security vendors, but I have only one to whom I entrust the bank's reputation. That's Symantec."

Matt Speare
Chief Information
Security Officer
M&T Bank

Phishers go after smaller fish

Matt Speare knew it was only a matter of time. As chief information security officer for M&T Bank (M&T), a mid-sized financial institution with 650 branches throughout the mid-Atlantic region, he had seen larger companies such as Bank of America, Citigroup, PayPal, and Amazon.com caught in the phishers' nets, with many unwitting customers disclosing personal information on Web sites that are made to look exactly like the company's legitimate site. He knew that the phishers would eventually target companies of M&T's size—probably sooner rather than later.

Like most other financial institutions, M&T is actively encouraging Web banking, which is more convenient to customers and cost-efficient for the bank. With this emphasis, however, comes an increased need to fortify the bank's defenses against phishing scams and other fraudulent activities. Speare had already set up a closely monitored network of decoys, called honeypots, to serve as an early warning system for pending attacks against the bank, but he needed more comprehensive protection.

Using Symantec Online Fraud Management, M&T Bank shuts down a phishing scam, thereby preserving customers' trust, the bank's reputation, and saving US$75,000 to US$100,000 in response costs

In spring 2004, Speare began investigating his options for online fraud protection, including MarkMonitor and Corillian, but found the offerings inadequate. "It's all about time," Speare explains. "Until I looked at Symantec's offering, I didn't see a service I liked. I need to know what's happening when it happens if I'm truly going to protect our customers."

Symantec offers real-time monitoring and notification

When Speare checked into Symantec's offerings, he knew he had found what he was looking for. Unlike its competitors, Symantec offers real-time notification. Using a probe network and millions of decoy accounts worldwide that are spread out among a vast majority of U.S. and international Internet Service Providers (ISPs), Symantec Online Fraud Management attracts and delivers suspicious emails to Symantec researchers who analyze the messages, identify the fraudulent attacks, and create and automatically deploy anti-fraud filters that allow ISPs to block the emails in question.

Another reason that Speare favored the Symantec solution was the good experience of the bank's Network Deployment Group with Symantec data availability solutions. M&T had been using Symantec Ghost™ Solution Suite since 1998 to quickly deploy reimaging of new desktops and laptops. The solution uses image multicasting to minimize bandwidth and speed the deployment of new images. The bank's network administrators also use Symantec pcAnywhere to manage and update remote user machines. M&T supports these and other Symantec products with Symantec Platinum Maintenance, which features 24x7 support from designated technical contacts and Symantec Advanced Alerting Services.

The combination of the products' feature sets and past history with other Symantec products made Speare's decision easy: Symantec deployed Online Fraud Management for M&T during the last week in March 2005, in what Speare describes as a near instantaneous, incredibly seamless event.

Major phisher tries to net M&T Bank customers

Fast forward one week. It was late on a Friday afternoon. Speare, along with other designated M&T staff, received an email notification from Symantec that a phishing attack was occurring, along with a message to call back for further details that bank management would need to know. Symantec's security experts tracked the phony URL and determined that the server responsible for sending out the fake emails was in Japan. The process of catching the perpetrator was set in motion that very afternoon. "The information that Symantec provided was invaluable," Speare says. "We had set up our own honeypots with mailboxes on the Internet and none of them received

> **"Until I looked at Symantec's offering, I didn't see a service I liked. I need to know what's happening when it happens if I'm truly going to protect our customers."**
>
> **Matt Speare**
> Chief Information Security Officer
> **M&T Bank**

the phony email. Symantec's Online Fraud Management detected more than 14 million fraudulent emails. That showed us how effective Symantec's service is."

Turning the tide on phishers

With the information that Symantec provided about the fraudulent URL, M&T contacted the ISP that was hosting the phony look-alike site and, with the help of a Japanese interpreter, was able to get the site shut down Friday evening just before midnight, within eight hours of the first notification.

How big was the phisher's catch? Seven people contacted M&T to report that they received the phony emails. Four were M&T customers. Three were good Samaritans who wanted to notify the bank. Statistically, that's 0.00005 percent. Best of all, M&T's customers suffered no losses.

"A bank of similar size to us, located in a major U.S. city, suffered a similar attack," Speare recalls. "Without a filtering and notification system in place, they received hundreds of phone calls and thousands of emails. With Symantec Online Fraud Management protecting M&T, we received seven emails and no calls. I can't argue with that type of return."

Tangible cost savings of a repelled attack

Though M&T was able to shut down the phony site the same day the phisher sent out the deceptive emails, the bank immediately prepared its call center, Web banking center, and branch offices to respond to any calls or complaints that came in during the following week. But Speare knows it could have been much worse.

"Without Symantec's service in place," Speare asserts, "I probably would have had to deal with as many as 200 customers who unwittingly gave out personal information, help them establish a fraud alert, offer to pay for a fraud alerting service in order to maintain them as loyal customers, and pay for dedicated staff to assist these customers going forward." All in all, Speare estimates that he saved between US$75,000 and US$100,000 with this attack alone. "I can tell you that this single event easily paid for the first year of Online Fraud Management."

Beyond the cost savings in dealing with each specific attack, Speare estimates that Symantec Online Fraud Management saves the bank approximately $50,000 annually, on an ongoing basis, because the staff time previously dedicated to fraud monitoring is now freed for more valuable tasks.

Less calculable, but no less important, are M&T's reputation, brand, and customer loyalty—all of which rest on a foundation of trust. The time and skill required to establish this trust can be shattered in an instant. "It's difficult to quantify this, but there certainly would have been

SOLUTION AT A GLANCE

Business Drivers

- Encourage customers to use online banking services
- Build trust with current and prospective e-business customers
- Minimize exposure to brand damage from phishing attacks

Technology Challenges

- Detect attempts at phishing attacks as soon as they occur
- Block phishing attacks by working with major ISPs
- Shut down fraudulent phishing sites before customers can be defrauded

Solution

Highly responsive fraud detection and antivirus solution from Symantec

Symantec Products

- Symantec AntiVirus™ Corporate Edition
- Symantec Ghost™ Solution Suite
- Symantec pcAnywhere®

Symantec Services

- Symantec Online Fraud Management
- Symantec DeepSight™ Alert Services
- Symantec Platinum Maintenance

Symantec Enterprise Licensing

- Symantec Elite Program Enterprise Licensing Agreement

BUSINESS VALUE AND TECHNICAL BENEFITS

Increased Fraud Detection/Prevention

- Almost complete blocking of phishing emails; in one instance, an estimated 14-17 million emails sent, with only seven complaints from customers
- Phishing site shut down in less than 8 hours from detection

Brand Protection

- Preserve reputation as a conservative, community-based institution that looks out for its customers' best interests

Return on Investment

- 100% ROI upon first phishing attack

Cost Savings

- Saved US$75,000 to US$100,000 in staff resources and customer loss coverage that would have been spent responding to phishing attack
- Saved 1,000 hours in staff time monitoring potential attacks
- Approximate $50,000 in annual savings for staff time previously dedicated to fraud monitoring

"The information that Symantec provided was invaluable. We had set up our own honeypots with mailboxes on the Internet and none of them received the phony email, but Symantec's Online Fraud Management detected more than 14 million fraudulent emails. That showed us how effective Symantec's service is."

Matt Speare
Chief Information Security Officer
M&T Bank

institutional damage to M&T had the phishing scam not been detected as quickly as it was," Speare notes. "You can't put a price on reputation. The bank loses relatively little directly and immediately, but it loses much in the long run. I have to do what I can to protect M&T's reputation as a conservative, community-based institution. I think we are much more successful in protecting the brand, and in being able to focus our efforts on getting as many fraudulent sites as possible shuttered."

Beyond protection: enhancing reputation through education

One of Symantec's newest offerings in Online Fraud Management is customer education. This security resource, which can be co-branded with financial institutions, helps customers understand Internet security risks, assess their exposure to these threats with free online security assessments, and obtain Symantec Security products at a discount to protect their desktop computers.

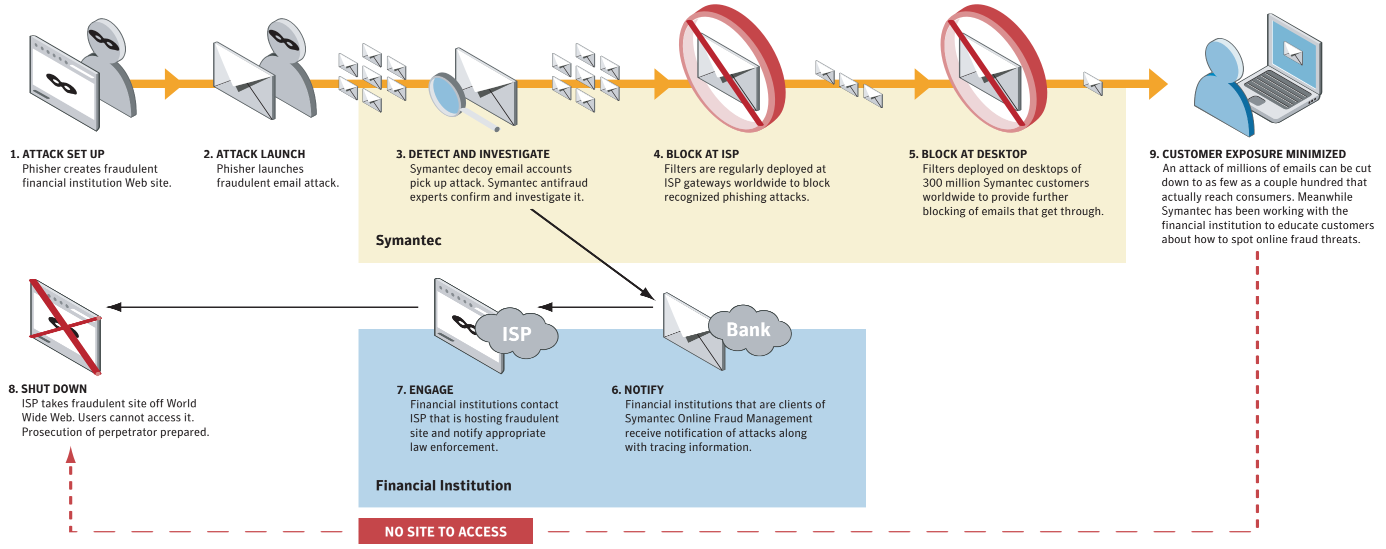
M&T decided to take advantage of this service and began rolling out the resource center in September 2005. Notes Speare, "It enhances our reputation among our customers who then tell non-customers about the added benefits we provide."

Adding to the security breakwater

M&T is also in the process of beefing up its security with Symantec AntiVirus™ 10 Corporate Edition software, which provides real-time virus and spyware protection, and automatic removal, for enterprise servers and workstations. M&T chose AntiVirus 10 because of Symantec's rapid response to new viruses and signatures in the wild, its high frequency of updated signatures, and the automated distribution of those signatures, which simplifies administration. For Speare, speed was once again the distinguishing factor. "Symantec is more responsive than any of the other vendors in that space."

To add another layer of protection, M&T also recently implemented Symantec DeepSight™ Alert Services to provide proactive notification of threats to M&T's internal operating systems and applications. Using a worldwide network of more than 20,000 registered sensors in 180 countries, DeepSight Alert Services provides a view of security risks including vulnerabilities and malicious codes, technical analysis of these threats, and recommendations on best practices for keeping systems protected. For Speare, a main benefit of DeepSight Alert Services is its customization. "It saves us time by

How Symantec Online Fraud Management Works



1. ATTACK SET UP Phisher creates fraudulent financial institution Web site.

2. ATTACK LAUNCH Phisher launches fraudulent email attack.

3. DETECT AND INVESTIGATE Symantec decoy email accounts pick up attack. Symantec antifraud experts confirm and investigate it.

4. BLOCK AT ISP Filters are regularly deployed at ISP gateways worldwide to block recognized phishing attacks.

5. BLOCK AT DESKTOP Filters deployed on desktops of 300 million Symantec customers worldwide to provide further blocking of emails that get through.

6. NOTIFY Financial institutions that are clients of Symantec Online Fraud Management receive notification of attacks along with tracing information.

7. ENGAGE Financial institutions contact ISP that is hosting fraudulent site and notify appropriate law enforcement.

8. SHUT DOWN ISP takes fraudulent site off World Wide Web. Users cannot access it. Prosecution of perpetrator prepared.

9. CUSTOMER EXPOSURE MINIMIZED An attack of millions of emails can be cut down to as few as a couple hundred that actually reach consumers. Meanwhile Symantec has been working with the financial institution to educate customers about how to spot online fraud threats.

notifying us of vulnerabilities for only the systems we run at M&T," he notes.

Symantec Elite Program lowers TCO

M&T purchased its Symantec products and services under the Symantec Elite Program Enterprise Licensing Agreement, a two-year contract that simplifies administration, provides volume discounts, and includes upgrade protection and technical support.

An ongoing partner for critical information security

In the several months since the initial attack, M&T has experienced one additional phishing scam—this one smaller, with almost 500 emails detected. There was zero impact on customers, and the bank was quickly able to shutter the illicit operation. And with additional attacks virtually guaranteed in the future, M&T will continue to realize value from its Symantec information security solution.

How satisfied is Speare with his bulwark of Symantec services, products, and support? "I have many security vendors, but I have only one to whom I entrust the bank's reputation. That's Symantec." ■

> **"A bank of similar size to us located in a major U.S. city suffered a similar attack. Without a filtering and notification system in place, they received hundreds of phone calls and thousands of emails. With Symantec Online Fraud Management protecting M&T, we received seven emails and no calls. I can't argue with that type of return."**
>
> **Matt Speare**
> Chief Information Security Officer
> **M&T Bank**

[1] Gartner research study, May 14, 2004
[2] http://www.pewinternet.org/PPF/p/1068/pipcomments.asp