



Community Bank attacks phishing away from home with BrandProtect

One mid-western U.S.-based community bank has always adopted a proactive approach to online protection for its customers. So when the bank began receiving notices of a phishing attack on another bank with the same name, it decided to leverage the anti-phishing resources it had in place to stop the activity at its source. Using StrikePhish™ services from BrandProtect, it was able to neutralize the attack on the other bank and ensure its own reputation remained intact.



As with most financial institutions today, online banking has become an integral part of the organization's service to its customers. As such, the bank's Information Technology (IT) department has always been very proactive in adopting technologies to prevent fraud and unauthorized access to information.

Other phish in the sea

In early 2008, the bank began receiving complaints of a phishing attack. However, the attacks – which were growing exponentially each day – were targeted at another bank with the same name in another state. According to the bank's Security Director, "As far as phishing attacks are concerned, the volumes were unbelievable. Although it wasn't our bank, a lot of customers that were receiving [the fraudulent emails] felt that it was directed at us."

As a result, the bank's website was being bombarded with reports from all types of customers – from large corporations to students – of phishing emails appearing in their inboxes. "We ended up spending a lot of time responding to the complaints in order to clarify that it was not our bank and to redirect their complaints to the appropriate bank," says the spokesperson. "We even provided an email link to the other bank's site so they could lodge their complaint with the right company."

While the bank's IT department continued to respond to the flood of incoming emails, it repeatedly contacted the other bank to check their progress on dealing with the attack, he adds. "Every day we were getting more and more emails. At its peak, we were getting 30 to 50 reports a day. The problem was escalating exponentially, and it seemed that nothing tangible was being done to stem the tide."

It became evident that even though the attack wasn't directed at the bank, the organization felt its reputation would suffer adverse effects from all the phishing activity. Its own customers were feeling it was responsible for allowing the attack to continue.

Taking charge of a phishing crisis

The bank decided rather than simply responding to emails and providing links to reports it was time to take the situation in hand. It turned to BrandProtect to deal with the phishing attack at its source. "It was a little out of the ordinary, since the attack was directed at another bank; but the job of handling the phishing email complaints was consuming a lot of our IT resources. We knew BrandProtect had the resources to do the job," explains the Security Director.

The bank was already a user of BrandProtect's StrikePhish service since the fall of 2007. This

turnkey offering provides community banks and credit unions with a complete end-to-end program to protect against phishing attacks and web-linking threats. Based on BrandProtect's enterprise-level phishing solution, StrikePhish is tailored to meet the specific security needs of credit unions and community banks, at an affordable price. Services include rapid response to deal with phishing attacks, 24x7 response to abuse email, incident response guidelines, weekly link checking and customer communications.

"When we first looked at an anti-phishing solution, BrandProtect came highly recommended says the Security Director. "They had a reputation for being industry leaders and very proactive." The bank had worked with BrandProtect on an earlier minor phishing situation involving a single site in Korea. Although the bank had identified the site in question, the IT department had been spending considerable time trying to disable it with no results. "It was like climbing uphill and running into roadblocks every day," explains the Security Director. When BrandProtect took on the problem, the site was taken down within 48 hours.



Community Bank attacks phishing away from home with BrandProtect

For more information:

www.brandprotect.com

onlinesales@brandprotect.com

1.866.721.3725



“That minor situation really showcased BrandProtect’s capabilities,” he says. “The bank’s IT department was extremely impressed with BrandProtect’s success.”

When this latest phishing attack surfaced, the first thought was to bring BrandProtect on board to deal with it. “We realized that we could either assist the other bank or wait for them to fix it,” says the Security Director. “This very well could have been us, so we looked at how we would deal with it ourselves and what resources would be available to deal with the attack. We knew right away that we needed to get BrandProtect involved.”

Phished out

Within a day of putting BrandProtect on the problem, “It was absolutely amazing,” he says. “All of a sudden the phishing emails just stopped. It was like someone turned off a faucet. The change was so obvious that our IT department executives were checking internally to see if anyone had received any additional phishing reports - they thought something was wrong.”

When he contacted BrandProtect, the Security Director discovered that it was already in the process of taking the sites down. Within a week, the targeted phishing sites were a thing of the past.

Today, BrandProtect continues to monitor for any new sites to ensure that the attacks do not resurface.

He notes that while the bank’s IT department has been successful in managing activities of this type that are US-based, “We learned from the Korea incident that when the phishing attack is from overseas, it becomes quite a problem for us to disable a site. BrandProtect on the other hand has the experience and the connections to understand where the attacks are coming from and is able to negotiate with other regions to deal with these sites.”

What also impressed the bank’s management team is the fact that BrandProtect “has the ability to deliver on what they say they can deliver. They have the resources, the quality staff and the expertise behind them. A lot of vendors out there promise everything but can’t always deliver. BrandProtect can – and does.”

As the relationship evolves, the bank plans to use BrandProtect for more extensive domain monitoring and link checking. “They offer so many options beyond just phishing services. We’ll definitely be looking at more opportunities as we continue to grow.”

He adds that approaching the latest phishing crisis from their end was in the best interests of the bank and its customers. “We decided to undertake the job because of the reputational risk. That is extremely important in our industry. If a customer is concerned about how we are conducting business and safeguarding their information, they will go elsewhere. We certainly didn’t want that to happen.”

About BrandProtect

As the leader in internet reputation management, BrandProtect empowers organizations to gain control over how they are represented online by uncovering and mitigating the issues that put their reputation at risk and erode customer trust. BrandProtect’s Response Services help detect, uncover and mitigate brand and trademark infringement issues, phishing attacks, web traffic diversions, website integrity issues and defamatory discussions. BrandProtect was the first company of its kind to be offered full membership by the Forum for Incident Response and Security Teams (FIRST). It also has relationships with more than 4,000 Internet Service Providers globally, accounting for more than 90 percent of the traffic flowing across the internet.