



# CFE Federal Credit Union:

## Protecting Customers Against Phishing and Other External Threats

### Acceleration

Beyond the fraud losses that result from a successful phishing attack, the loss of consumer confidence in the online channel can be even more detrimental. When CFE Federal Credit Union came under attack, they enlisted the help of the RSA FraudAction™ Service. RSA immediately shut down over 20 fraudulent sites, some in less than 30 minutes. This quick action enabled CFE Federal Credit Union to minimize their fraud losses and accelerate user confidence in their online service.

RSA recently sat down to talk with Kevin Dougherty, Sr., Vice President of Information Services at CFE Federal Credit Union, a \$1.1 billion financial institution based in Orlando, FL. In 2006, CFE was the target of an extensive phishing attack that literally contributed to the shutdown of its online banking site. Here, Kevin discusses the experience and offers advice to other financial institutions on how to effectively handle a phishing attack.

**RSA:** Prior to CFE Federal Credit Union being a target, what steps had you taken to educate your members about phishing and the possibility of an attack?

**Dougherty:** CFE has always taken a proactive approach to customer education. For example, we had messages on our website that stated we would never send an email requesting personal information. In addition, even though we had never come under attack before, we had incident response processes in place should one ever occur.

**RSA:** Was there a particular incident that you believe prompted a phishing attack against CFE?

**Dougherty:** We were in the process of a broad campaign offering an upgrade to our credit card portfolio. As part of our communication strategy and because our members are used to going online to gather information, we put a lot of information on our website about the new credit card offer. Fraudsters got a hold of this and used our own messaging against us.

**RSA:** What was the first sign that something was wrong?

**Dougherty:** We were starting to receive calls in our call center from members stating that they were getting emails about a new offer and it was coming from one of our board members. We immediately started to do more research and put a message on our website and phone system to make members aware of the incident. Communication to staff and members is vital to the process.

**RSA:** What happened next?

**Dougherty:** Later that afternoon, we got a call saying our website and home banking site was down. At first, we didn't make the connection and just thought it was a problem with our provider. At that point, though, we had actually come under a denial of service (DoS) attack. The fraudsters were trying to shut down our site so that we couldn't communicate with our customers.

**RSA:** At this point, how did you react?

**Dougherty:** One of the first things I did was to call a colleague that I knew had only recently gone through the experience. When I explained to him what was happening, he immediately replied, "Do you have a shutdown service?" I wasn't familiar with any shutdown services nor how they could help. My colleague ended up recommending we contact RSA. We got RSA on the phone and within a few hours had a contract signed.



The Security Division of EMC



**RSA:** Did the attack continue to get worse?

**Dougherty:** Yes. As soon as we'd get one IP address blocked, another would spring up. By the next night, I got a call from our network provider saying we were being flooded with about 400,000 packets per second which essentially rendered our technology useless. We made the decision to blacklist our site for the night.

The following day, we decided to bring the site back up. At this point, we were now getting flooded with 600,000 packets per second. The DoS attack had escalated to a distributed denial of service attack (DDoS). In working with our telecom vendor, we discovered they were coming from zombie computers all over the Internet. We finally traced the source to a server operating out of Virginia.

**RSA:** Once RSA became involved, how were they able to help you?

**Dougherty:** RSA essentially became our "trusted advisor." They provided us with guidance on exactly how the process would evolve and told us how long we should expect it to take. RSA immediately set up a web abuse box so that members and non-members could directly forward the emails they were receiving to its Anti-Fraud Command Center to perform forensics. The abuse box was key to helping them shut down the phishing sites. RSA was able to shut down over 20 sites, most in less than 30 minutes. Some were being hosted in Europe and while they took a little longer to shut down, RSA had the relationships and knew the process.

**RSA:** Once the attack was under control and the sites shut down, what other steps did you have to take?

**Dougherty:** We had to alert the appropriate government agencies, such as the FBI, about the attack and submit a suspicious activity report (SAR) detailing the incident.

**RSA:** What are some of the lessons learned from having gone through a phishing attack?

**Dougherty:** Personally, I reached out to another colleague that had the same experience for advice and I found that very helpful. More importantly, though, customer communication is critical. As we were unable to provide information to our members through our website, the first thing we did was to send them a letter via first class mail to let them know what was happening. We received very positive feedback from our members concerning the level of communication we maintained throughout the incident.

**RSA:** What advice would you offer to other financial institutions that may become a target for fraudsters?

**Dougherty:** Even if you may think you have all the pieces in place, it is still wise to re-evaluate the protection and processes you have. You can never be too prepared. Once again, the most important thing is communicating with your customers effectively. Throughout the attack, we had one person in the organization act as the spokesperson to ensure we provided a consistent message, had one external voice.

Also, I'd recommend that financial institutions, regardless of their size, employ the outside help of an anti-phishing and shutdown service – even as a supplement to existing in-house capabilities. Not only do they have the global resources and relationships to ensure quick blocking and shut down, thus minimizing the effect of a phishing attack, it is valuable to leverage their experience in dealing with these threats on a daily basis.



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

The Security Division of EMC

RSA, FraudAction and the RSA logo are registered trademarks or trademarks of RSA Security Inc. in the U.S. and/or other countries. EMC is a trademark of EMC Corporation. All other trademarks mentioned herein are the property of their respective owners. ©2007 RSA Security Inc. All rights reserved.

CFEFC CP 0307