04/16/2007

To: All CBS Customers

From: Commercial Business Systems

Re: Follow-up to recent email(s) regarding the fraudulent emails and Phishing attempts

As a matter of information, please remember that Phishing scams are designed to “bait” unsuspecting users into giving up personal, confidential, and financial information via a fake web site. It is relatively easy for the perpetrator to mimic a web site (yours, ours, anyone’s). These unscrupulous perpetrators fully understand that the fake site will be detected quickly, and therefore they focus on getting the greatest return in a short time span. In fact, the US Department of Defense has been constantly subjected to fraudulent Phishing attacks. Likewise, the NCUA web site has been duplicated and phished over fifteen times in the last two years. Phishing scams are an unfortunate component of the Internet. All businesses are subject to these scams, not just credit unions and other financial institutions. Please refer to the link that has been published on the CBS Message Center. This information by Microsoft© provides a clear definition and some tips regarding phishing and fraudulent emails. Education and awareness are the keys to your members not succumbing to such fraudulent activity by any unscrupulous element.

Listed below are some CBS responses to probable questions by our customers:

Have checks been made on the security of your Internet Branching site?
Yes. CBS has thoroughly reviewed all access logs at the Internet Branching site and there has not been any unauthorized access to any member’s information. Also, immediately upon notification of any Phishing event CBS reviews all the access logs associated to the Internet Branching site to ensure that there are no breaches of any security. Remember that a Phishing attack is an attempt by the perpetrator “to be given information” by an unsuspecting user.
Several other noteworthy items:
1) the public section of the Internet Branching site logon page is the only page that gets mimicked. None of the internal pages are seen by the perpetrator and therefore are not reproduced.
2) in an attempt to make the “bait” look more authentic, had the perpetrator gained access to the “real” Internet Branching site it is most probable that they would have created a false logon page within the actual Internet Branching hosting area. They were not able to accomplish this so they used various foreign hosting sites to display the mimicked pages.
3) if the perpetrator had gained access to the “real” Internet Branching site it is most probable that they would have used the entire list of email addresses. There is not any evidence to indicate that all email addresses received this Phishing attempt.

Is someone intercepting our email delivery system?
Possibly. Remember that email addresses passing through the Internet are not encrypted and are publicly available, i.e. email is unsecured. Sending an email is similar to mailing a postcard; anyone with the proper technology can see the contents. It is possible that any unscrupulous element could use a “sniffer” program (packet sniffing, packet assembling, etc) that looks at normal Internet traffic and attempts to sift out email addresses. Yet, it is highly improbable that any such sniffing would be limited (i.e. targeting) to just your credit union.

Are a certain group of members targeted? If so, are their email addresses stored in a less secured environment?
It is highly improbable that any Phishing and email sniffing would be limited (i.e. targeting) to just your credit union. There is no way that CBS can determine what any unscrupulous element may have

picked up from normal Internet traffic. However, some CBS customers have informed us that they received telephone calls, from persons that had no association to their credit union, stating that they had received the fraudulent emails. So, it is most probable that this is a random event and nothing that targeted any specific persons or group. Remember that the unscrupulous element is Phishing which is a fairly common method of Internet fraud… gather a list of email addresses and craft emails from a variety of financial institutions in an effort to get personal information from an unsuspecting person.

So how are people targeted? Typically, a mailing list is constructed for this type of Phishing activity through the use of *spambots*. These are small web crawler programs that view Internet traffic for email associations. And because emails have a distinctive format they are easy to find.

Who was more likely to have been identified? Anyone who sends and/or receives emails to/from your credit union. The more volume of emails generated, the greater the chances of being associated by a spambot. Likewise because it's a guessing game, these spambots also make many inaccurate associations and created many inaccurate email addresses (i.e. bounce backs).

Did people outside of our membership receive the phishing email?

It is highly probable that persons outside of your credit union's membership did receive the fraudulent email. Yet, CBS has no way of knowing who received the fraudulent emails as we did not generate the emails. And remember the Phishing perpetrator does not care about membership. Their efforts are to "get a bite" and obtain information.

What is CBS doing to make sure that this does not happen again?

Education and awareness are the keys to not succumbing to such fraudulent activity by any unscrupulous element. CBS has posted warnings on the CBS Message Center and we have recommended that all of our customers have warnings and suggestions posted on the credit union's public web site. There is not anything CBS can do to prevent anyone from sniffing public unsecured email addresses. CBS cannot do anything to prevent anyone from sending emails to your members. Email sniffing and Phishing scams are unfortunate components of the Internet. All businesses are subject to these scams, not just credit unions and other financial institutions. Just as the large banks and NCUA cannot prevent someone from reproducing a shell of their web sites, CBS cannot stop someone from writing a program that mimics your public web sites. Microsoft© has released a study that the best protection lays within the software installed on the client workstations. Internet Explorer 7 has incorporated new features that warn of suspected fraudulent sites. Unfortunately, however, your credit union has little control over the pc workstations that will be used by your members.

CBS has proactively instituted server-side defense measures for such Phishing attacks: In the 4th quarter of 2006 CBS incorporated additional security features into the Internet Branching system. These were provided and installed free of charge and are currently operational in your credit union's Internet Branching system. The Internet Branching login page was segregated from the page that requires a password entry. Each Internet Branching user has to choose a custom image that appears on the password entry page. Also, a challenge question phrase (as selected by the member) appears on the password entry page. There is no question that this additional security succeeded in minimizing the effects of this Phishing episode. Yet, any member that complied with this Phishing scheme and its request for information would have had to ignore the missing graphic, the missing challenge question phrase and the absence of a password entry page. Again education and awareness to your membership are the keys to prevention.

If in fact, CBS' data files were not compromised, how were email addresses "sniffed" from their data?

As stated above, CBS has thoroughly reviewed all access logs at the Internet Branching site and there has not been any unauthorized access to any member's information. There has not been a compromise of any member information unless a member complied with the Phishing scam.