Risk Alert: Phishing continues to be a concern for Credit Unions

Consumers used to worry about phishing but now business owners, including credit unions also need to watch for this event as businesses are now being targeted.

Phishing through the use of e-mail can lead to financial loss as well as the loss of personal information; it can also lead to reputation loss as members can lose confidence in using email to communicate with their credit union. It can also impact the productivity of the “phished” employee.

Organizations often ignore or minimize phishing assuming their spam filter will detect phishing or that employees can easily tell when it occurs but unfortunately, this is not always true. Credit unions need to look at challenges in staying ahead of phishing techniques and outline a frame work to incorporate anti-phishing actions into existing processes.

What can a credit union do to affectively address phishing?
A credit union can consider implementing an effective anti-fraud solution using innovative technology specifically designed to combat phishing along with providing consistent and accurate communication.

- **Use current technology to help detect fraud**
  Spam filters, which are specifically designed to let legitimate email into your corporate network, will not stop phishing email that looks identical to the real thing. An effective anti-phishing solution must be able to analyze a variety of message attributes that set phishing email apart from spam and legitimate email.

- **Develop internal controls for handling phishing email**
  Phishing email should not be placed into quarantine with spam and allowed into your corporate network where your employees might remove it from quarantine and act on it. An effective anti-phishing solution must be able to segregate phishing emails immediately from other types of unwanted email and offer your IT department the option of deleting them at the perimeter of your network, before they have a chance to reach any recipient.

- **Establish a comprehensive Email Security Policy that includes an anti-phishing solution**
  An effective risk solution should offer a number of options that align with other corporate security processes. You may want a paper trail of all attempted phishing attacks or general alerts about new types of phishing as they emerge. You may want to consider linking to a broader network of security entities that provide frequent fraud alerts about current attacks, trends and emerging fraud techniques. This will allow your IT Department adequate information and lead time to address the attack(s) and defend against intrusions before they occur.

- **Educate your employees and volunteers on phishing techniques**
  The more your employees know about how they are being targeted and what they should do when they suspect email phishing, the more likely they are to take appropriate action when you are hit by a phishing attack. An effective anti-phishing solution needs distinct phishing reporting protocol so that administrators can be kept aware of trends, make necessary modifications at the network level. If tied into a local alert network, these attacks can be reported to other entities that are part of your security network, both inside and outside your organization.

By understanding phishing as a distinct and sophisticated type of email threat, and by seeking solutions designed specifically to stop phishing email, you can protect yourself and your organization. Not only does an integrated solution reduce administration and increase efficiency, it also allows you to analyze the sources of greatest threat and respond accordingly.