Need to Know
MemberOne Credit Union
Staff Newsletter

October 2014: Gone Phishing

This issue of Need2Know comes at an opportune time, in that some of us have very recently experienced this month's topic of discussion: **Phishing**.

Last week, we were made aware of several users receiving a message like the one below:

Concerns were raised as it seemed as if the spam filter hadn't identified the message as spam. This is an example of a Phishing e-mail, where another party uses the identity of a trusted organization (in this case, RBC) to trick users into revealing confidential information, such as user IDs, passwords, and in this case, access to personal financial information.

While spam filters use algorithms to detect elements in messages that can typically be considered spam, they also rely on human input to "teach" the filter how to respond to messages like the one above, which is created to bypass typical spam filter algorithms. Take a look at the image above and note the bottom-most part of the message, which begins with the header **Teach CanIt if this mail is spam**, followed by three links. Answer by clicking the appropriate link and wait for confirmation. This helps the filter to build upon the existing algorithms and do a better job of catching such messages in the future.

Before opening or clicking on any links in an unfamiliar message, ask yourself the following:

- **Do I trust this sender?** Is this someone I know personally? Is this an organization with whom I have regular dealings?
- **Am I expecting the contents of this message?** Is this correspondence dealing with regular business/personal communication? Are the attachments ones that are characteristic of what I would normally receive from this person or similar senders?
- **Does the content look normal?** Does the e-mail address make sense? Is the writing style familiar, or consistent with that of typical business dealings? Is the content a giant image instead of a mix of images and text? If this message is from a corporation or organization, is there a lack of appropriate branding (no logos or images)? Are the links appropriate, i.e., if the sender is supposed to be RBC,

am I being sent a link to an RBC webpage and not something that's masquerading as an RBC webpage? You can tell where link text leads by hovering over it (*without* clicking). A box comes up detailing the link's address, as below:

- **Are they asking for information?** Does the message as you to log into sensitive accounts urgently to check "important information regarding your account", or ask you to verify sensitive personal information (name, address, credit card or SIN numbers, etc.)?

If you come across messages like the one above, the number one rule would be this: **don't click what you don't know**. Use the CanIt links at the bottom of your messages to appropriately designate them as spam, and notify management immediately of your findings.

As a way of tightening our internal IT security, it's important for us to be familiar with the communication methods and formats that are part of our everyday duties. The simple act of *not* clicking on a link, no matter how badly it wants you to, can potentially save thousands of dollars and man-hours in damages not only to operating systems, but to brand loyalty and reputation.