Tip of the Month - February, 2013
Criminals Disguised as Cupid for Valentine's Day

The following extracts were taken from an article published by "Privacy Rights Clearing House." Bahamians will do well to heed the good advice given.

Valentine Day comes in the month of February each year. In the week leading up to Valentine's Day, many consumers are feeling hopeful, romantic, and generous – feelings online criminals prey on in order to scam you. Most online scams fool you into clicking on malicious (dangerous) links.

It is very easy to get duped into clicking on a malicious link. If you click on a malicious link, you will most likely be taken to a site that tricks you into providing personal information that can then be used to steal your money, or even worse, your identity. Clicking on a dangerous link could also cause malware to automatically download onto your computer.

Malicious links may look like they were sent by someone you trust, such as:

• A friend or someone who you know.

• A legitimate-looking company selling a product or service.

• A bank or other business that you have an existing account with.

Most people think that malicious links arrive by email. But, criminals are finding even sneakier ways to trick you into clicking on a dangerous link. You could receive the malicious link in an instant message, a text message, or on a social networking site like Facebook or Twitter.

Love is the theme each February. The criminals will be disguised as friends or companies appealing to your romantic side. For example, you may be sent a link by an online flower store selling a dozen roses at a steep discount. Maybe a friend sends you a link out of the blue for aphrodisiacs. Or perhaps the hotel you just booked a getaway with says there was an error with your account and is asking for your credit card number.

Malicious links are hard to spot. They often:

• Are ever-so-slightly misspelled versions (1) of well-known URLs.

• Use popular URL shortener sites to hide the real URL (2).

• Use simple HTML formatting to hide the real URL. This is the most common method for emailed dangerous links. You think you're clicking on a trustworthy link, but you are redirected to a dangerous link.

To protect yourself from malicious links, consider the following tips:

• Do not click on a link that appears to be randomly sent by someone you know, especially if there is no explanation for why the link was sent, or if the explanation is out of character for the sender (i.e. horribly misspelled or talking about what a great deal they discovered).

• Do not click on a link that was sent to you by a business you don't know that is advertising a great deal. Instead, perform an online search for the business, make sure it's legitimate, and go directly to the business' website to find the deal yourself.

• Do not click on a link that was sent to you by a business you have an existing account with. Either go to the business' site yourself, or call up the business and confirm the legitimacy of the link. (Note that some businesses may require that you verify your email address as part of a registration process, which requires you to click on a link contained in an email. Typically, the link will be emailed to you immediately after you register online with the business. It's a good idea to check your email right after you register with a business.)

So, this Valentine's Day don't let more than your heart get stolen and think before you click!

For more information on this and any other data protection concern you may have, please email us at dataprotection@bahamas.gov.bs or visit our website www.bahamas.gov.bs/dataprotection.

Remember "Privacy is the Best Policy"

Links:

(1) http://blog.mcafee.com/consumer/cyberattack-via-msn-references-facebook-hi5

(2) http://www.stopthehacker.com/2010/02/19/analyzing-url-shorteners/