

## **Tech Savy – Let's go Phishing – By Amy Markin**

I have had a fair amount of experience with computers, and I realize that some of our members have not, so for that reason, I thought I'd share a tip or two in this newsletter. I do have previous experience working indirectly for the worlds largest online auction center to draw from.

This edition, I would like to draw your attention to email Scams. I'm sure we all have come across an email from a stranger, asking us for money, or to follow a link and enter our password, or to open an attachment.

Some places in the world are very lax regarding internet law and scam and are prime centers of origin for emails that are scams. Phishing is a term used for such an email that has the purpose of 'Fishing' for your data.

### **What to watch for:**

#### **-Email asking you to click on a link within the email and enter your password, or even simply asking for your password**

If you are required to update your information on a website that you use on a regular basis, go to the actual site to log in. If a site that requires a password to use it has the power to change that password, why would they ask you for yours?

Example: An email from eBay asks me to review and update my mailing address by clicking on this link. It would be best to go to [www.ebay.com](http://www.ebay.com) to log in, to see if this looks true. It's a good idea not to follow links in email addresses asking for passwords, because it is easy for a scammer to duplicate the look of a valid website but have a slightly different web address that collects your data. Many people fall victim to this, as it looks valid on the surface. Most responsible online companies, such as eBay, encourage you to forward any questionable email to them so that they may assess the email for you, and let you know if it is a valid email or not. If you ever receive a questionable email from the CPCA office, please feel free forward it to me: [admin@cpc-rpc.ca](mailto:admin@cpc-rpc.ca).

#### **-Email that pressures you to open an attachment**

If an email is pressuring or urging you to take an action, think about why this party is contacting you by email, and not by telephone. Are they calling you Sir or Madame instead of addressing you by your first name?

Example: This scenario happened to me very recently and inspired this article. I received an email, appearing to be from the Better Business Bureau, a real organization. The email was well written, with appropriate grammar and tone, and urged me to open the attachment. It's never a good idea to open an attachment from an unknown source, because usually this attachment will contain some type of Malware or virus.

#### **-Email asking you for money**

If an email is asking you to make a payment, think about how legitimate this is. If someone asks you to transfer money via Western Union, this can also be a warning sign.

Western Union money transfers cannot be refunded, so this is an ideal transaction for a scammer.

Example: Here is an example of another recent email that I have received. Apparently, there is a man that wants to make me a business offer, because I have been specifically chosen, and he will send me thousands of dollars, if only I can wire him the initial \$1000 fee to cover the administrative costs. There are so many variations of this type of email. If a VALID company, individual or organization wishes to give you money, it is going to require more documentation than just an email.

### **Tools that you can use**

1. [www.snopes.com](http://www.snopes.com) is a good site to use to see if there is an ongoing scam regarding an email you have received.
2. [www.google.com](http://www.google.com) is an easy tool to use, enter some keywords, or the subject line from the email in question, and see what results come back to you.
3. **Ask a friend** if they find the email fishy-a computer savvy friend is a good choice here, or even **a co-worker, or a computer technician** at your work.
4. **Your own eyes** – Some of us aren't perfect at spelling, but scammers often have poor grammar, and don't check their spelling. They often will choose the wrong form of a word to fit the sentence, so use that as a potential warning sign.
5. **The CPCA Facebook Group** – Chat with your colleagues online and see if what they think. A couple of weeks ago, there was an email going around about a woman from outside of Canada (or a man) in some cases, looking for counseling. One member posted about this on Facebook, and others came forward having received the same email.

### **Above All!**

Take a moment to think about the email, does anything feel wrong to you?

### **Lastly:**

What I gave you is a very short overview to increase your awareness of how you can spot a scam, and also give you some tools to identify them. The link below is from Wikipedia and goes on to further describe Phishing. You don't need to live constantly in fear but being aware may prevent you from problems down the line.

<http://en.wikipedia.org/wiki/Phishing>