Subject: **Quiz: Can You Spot the Phishing E-Mail?**

According to Get Cyber Safe, a program sponsored by the Canadian government, 156 million phishing e-mails are sent each day, and approximately 80,000 people are lured into providing their personal information to fraudsters as a result.

Given the prevalence of these scams, and the serious ramifications of falling victim to them, it's critical that you be able to identify them at a glance. But can you? This quiz from Dell offers a risk-free way to measure your phishing IQ. Give it a try!

Tips for recognizing phishing e-mails
A great feature of this quiz is the detailed explanation it provides as to why each example is legitimate or not. If you didn't do as well as you'd hoped, be sure to click on **Why?** in the column on the right side of the page to learn more about what you may have overlooked.

And as you look to protect yourself from phishing scams in the future, you'll want to heed these tips:

1. **Pay close attention to branding and the use of grammar in any unsolicited e-mail that you receive.** If you notice misspellings and awkward formatting, you are onto some red flags that scream "phishing." Still, be aware that many phishing attempts are well done and extremely believable. (All the more reason why you should always be wary of requests or messages from unknown entities.)
2. **Make it a habit to enter the address of any banking, shopping, auction, or financial transaction website** in your browser **yourself** and don't depend on links displayed in any e-mails you receive. To be safe, don't click on any links in the e-mail either. Just enter the address directly in your browser window.
3. **Be sure to check your bank, credit, and debit card statements regularly** to ensure that all transactions are legitimate.
4. Valid messages from your bank or from an e-commerce company generally are personalized, while **phishing e-mails typically are *not*—but they can be.** For example, if a fraudster has your e-mail address, it's very possible that he or she has your first and/or last name as well; therefore, a phishing message could indeed be personalized. So don't use the notion of personalization as your only validator. When in doubt, always call the entity that supposedly sent the e-mail to confirm its legitimacy.
5. **Under no circumstances will our firm ever request your passwords via e-mail**, nor should you provide this information to any other entity that may ask for it.

A little bit of awareness goes a long way. Following the above-mentioned tips, asking questions, and being aware of even the slightest discrepancies in the unsolicited e-mails that you receive will help you mitigate your risk of falling victim to these scams.

Rest assured that we are always concerned about information security, and we will strive to keep you up to date on new security threats, as well as potential solutions to help protect your information. If you have any questions, please contact us.