How Can I Protect My Company Against Threats?

Instances of phishing emails, phone calls, and other attacks are on the rise. As fraudsters become more sophisticated in their ways of phishing information from their victims, it is more important than ever to practice safe online banking.

If you believe you have received a phishing email or a phone call that appears to be from RBC:

Email:

1. Do not action the email or click on any of the links.
2. Immediately forward it to phishing@rbc.com and then delete it.

Phone call:

1. If the caller claims to be calling from RBC or claims to be an RBC employee and asks you for sensitive personal information, such as your PIN or RSA SecurID Token value, hang up immediately.
2. Report the call to RBC Express online banking support at **1-800-769-2535**.

Important: *If you suspect anyone else knows your RBC Express Sign In ID and/or Password, or your RSA SecurID Token is lost or stolen, immediately contact your Service Administrator or RBC to have your Sign In ID locked.*

For RBC Express online banking support please call **1-800-769-2535**.

How to Identify Phishing?

RBC will never ask you for your RBC Express password or token value through unsolicited email or phone call. RBC Royal Bank will also never send an email or text message that asks clients to provide, confirm or verify personal, sign in, or account information.

Phishing emails or other types of phishing attempts are becoming more sophisticated and can be tricky to spot. To help you spot phishing and fake websites, see the tips under “Recognizing it” on RBC’s Phishing Resource site.

What Does Phishing Look Like?

Example #1

An employee will receive an email that appears to be from RBC Royal Bank. It may even have the right logo and a seemingly credible business purpose such as to verify information or approve a banking function. Typically the email will contain a number of links that mimic actual links on the Bank’s online websites. The phishing email may even provide a direct link to what appears to be the RBC Express Online Banking sign in page. ***Once clicked, the fraudster uses these links to infect the recipient’s computer.***

Example #2

You receive a phone call from an impostor posing as an RBC employee and asks you for your token number as your token is seemingly “out-of-sync”. The name that is displayed on the caller ID shows

“RBC” and has a valid RBC phone number associated with it. Unbeknownst to the victim that the caller is an imposter, they provide their token value over the phone, and a payment is approved and released immediately. Frauds of this nature often remain undetected longer, making the recovery of funds more difficult.

What Else Can I Do to Protect My Company?

1. **Always verify payment instructions**
   Always take additional steps to be certain of the origin of payment instructions. Be just as wary of phone calls asking for confidential information as emails requesting confidential information and be aware that Caller ID information can be “spoofed” by fraudster to make it appear as if the call is coming from the genuine person/company.

2. **Report potential security breaches**
   Immediately inform your Service Administrator if you suspect anyone else knows your Sign In ID and/or Password, or if your RSA SecurID Token is lost or stolen. The Service Administrator is to advise RBC immediately.

   *For RBC Express online banking support please **call 1-800-769-2535**.*

3. **Remember to sign out**
   Be sure to always Signoff and close your browser. This will prevent others from being able to access your online banking session.

4. **Safeguard your password and token**
   Use passwords that are difficult to guess and change your password frequently. Always safeguard your token. Never share your password or token with anyone.

5. **Be wary of pop-up windows, especially those that request financial or identification information.**
   Avoid clicking any "action" buttons within a suspect pop-up window.

6. **Keep your computer healthy**
   To protect against software vulnerabilities, it is very important to frequently check your operating system and web browser vendor websites for software "patches" and updates.

7. **Use antivirus software**
   Antivirus software can protect you from potentially damaging viruses that can enter your computer without your knowledge. Always use up-to-date antivirus software that is capable of scanning files and email messages for viruses.

8. **Use firewalls**
   A firewall creates a barrier between your computer and the rest of the Internet. It can help to protect against malicious attacks and block certain types of data from entering your computer.

9. **Use anti-spyware**
   Anti-spyware helps prevent unwanted software being installed on your computer without your knowledge. Anti-spyware also helps prevent slow computer performance.

10. **Use anti-spam software**
    Spam is a growing source of computer viruses. Use up-to-date anti-spam software along with your antivirus software. If you receive spam, remember this: don't try, don't buy and don't reply. Just delete it.

RBC Express Best Practices

RBC Express online banking combines the convenience of online banking with state-of-the-art security features that are designed to protect your business and financial information. These security features can be combined with the steps outlined above to help you better protect your company.

The “Guide to Securing Your Online Banking” is available through the Resource Centre once you have signed into RBC Express online banking. It will walk you through the mandatory and optional security features offered by RBC Express online banking. It also provides recommended options and helpful hints to ensure your company is taking full advantage of all the available security features. RBC recommends that your company review this guide on a regular basis to ensure you are leveraging the most up-to-date security features that are best for your company.

If you have any questions about what security features are best for your company, please contact your RBC representative.