RBC Royal Bank

How to retain best practices during these uncertain times

As the COVID-19 situation continues to evolve rapidly, it's important to stay vigilant in protecting your business against potential cyber risks that may emerge. Please take extra precaution to keep your business secure, and protect against fraud. For more information with recommended tips and advice, and how we keep your business safe and secure, please read click here for more information.

We've also shared some common scams and threats to look out for below.

Validate your sources requesting urgent payments

Be wary of urgent requests for payments from what may appear to be an email from a senior member of your organization. In this environment, urgent payments may reference the need to support family members or coworkers.

Be mindful of changing payment templates

Exercise extra caution when receiving requests from your suppliers asking to update your records with new banking information. For example, Vendor email compromise schemes may suggest the vendor needed to invoke business contingency plans.

Protect your business from fraud

Managing duties and administration:

- Continue your daily reconciliation activities
- Review your business audit reports of changes to your systems or processes
- Maintain segregation of duties for creating and modifying payments versus those approving money transfers or release of funds
- Set up dual administration controls to ensure critical user changes are managed by more than one individual

Managing account communications

- Maintain contact with suppliers and employees around new payment requests and account changes (e.g., do not confirm details in an email response, call instead)
- Verify incoming contact information from suppliers for accuracy (e.g. email addresses and phone number)

Recommended Articles: How to Protect Your Business

RBC Fraud Ebook