Wealth Management

# Safeguarding your personal information

At RBC Wealth Management, we maintain rigorous security procedures to ensure that your personal information is safe and secure. Learn more about how RBC protects you, how you can recognize common scams and how to protect your personal information.

Knowledge is often your best defence against fraud.

## Fraud prevention

Fraud detection and prevention activities are part of our normal business activities. RBC has a team of dedicated fraud experts working 24/7 to prevent, detect and investigate fraud, and we work closely with industry associations, government and law enforcement. We invest in emerging and new fraud prevention technologies and maintain rigorous security procedures to ensure that you can do business with us in a safe and secure environment.

## Our due diligence in protecting your account

In rare cases, your email can be "hijacked" or a fraudster may send emails masquerading as you. We take our responsibility to protect your wealth and personal information very seriously. At any time, if we receive an email request with instructions for your account, even if it sounds legitimate, we will follow up with you directly using the phone number on file to confirm the instructions.

To ensure that your privacy and information remain confidential, we will use encrypted email when we correspond with you about personal or account information. Typical correspondence may not need to be sent securely (for example, a message to confirm a meeting) however any account details or investment information communicated by email will be sent to you encrypted.

We may also proactively contact you to confirm that certain transactions going through your account are legitimate. You should request a phone number to validate the call and call us back, using a publicly published number or the number that you have independently verified, prior to providing any information.

## Avoiding email fraud

"Phishing" is a common online scam that involves sending phoney email messages to trick you into revealing your personal information for the purpose of financial fraud or identity theft.

RBC will never, under any circumstances, send you an unsolicited email that includes a link or phone number asking you to update or verify your account details or other personal information. Typical phishing emails will include a phoney

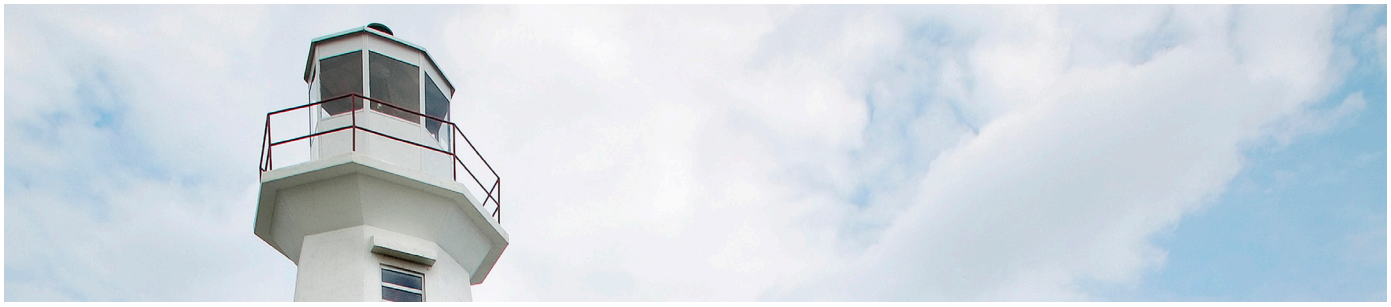
"Phishing" is a scam that involves sending phoney email messages to trick you into revealing your personal information for financial fraud or identity theft.

reason, such as a security breach or contest, as well as a sense of urgency to trick you into responding or clicking on a link.

Don't take the bait – do not click on the links or reply to the message. Remember that these links may take you to a fake or "spoofed" website designed to capture your personal information. The websites often look legitimate and may even contain RBC banners and logos to try to fool you.

RBC will never ask you to provide confidential information, such as account passwords, PIN, Social Insurance Number or other personal information through unsolicited email. If you receive an email requesting such information, do not respond. Instead, please notify us by forwarding the email to phishing@rbc.com. If you believe you have provided your account or other personal information in response to a fraudulent email, contact your advisor immediately or call us at 1-800-769-2511.

**From time to time, RBC will engage in promotional campaigns via telephone, mail and email. If you are ever unsure of any of the information you receive from us, do not respond and contact your advisor.**



# 10 tips to safeguard your assets

In addition to the controls we employ, knowledge is often your best defence against fraud. Following these 10 steps is a simple and effective way to reduce the risk of theft or misuse of your personal and financial information.

Always use encryption when sending confidential information by email, and never store sensitive data in your email folders. Even encrypted emails can be hacked.

### 1. Keep your personal information confidential

An identity thief may go to any lengths to obtain your personal information (even picking through your garbage or recycling bins), so be sure to shred receipts, copies of credit applications, insurance forms, credit offers received in the mail, etc. Get into the habit of clearing your mailbox after every delivery. Ensure you are using a secure, encrypted email to communicate any of your personal or financial information Make sure that your mail is forwarded or re-routed if you move or change your mailing address. Do not give out personal information on the phone, through email or over the Internet unless you have initiated the contact independently and know the person you're dealing with.

### 2. Be aware of billing and statement cycles

If your bills or statements don't arrive on time, follow up immediately to ensure they have not fraudulently been redirected. Review your statements regularly to ensure all transactions are authorized, and review your credit report annually.

### 3. Protect your PIN

Do not reveal your PIN to anyone, including employees of RBC, family members and friends. When conducting a transaction at an ATM or retail (point-of-sale) location, keep your client card within your sight and shield the keypad while you enter your PIN.

### 4. Limit your risk

Review your daily withdrawal limits on your debit card. If you don't need a high daily limit, reduce it. This will help contain fraud by reducing the amount someone can access. Only carry the ID and credit cards that you need; leave the rest (especially your birth certificate, SIN card and passport) at home in a secure location.

### 5. Protect your personal information online

Be cautious in your online activity, especially when using unsecured/ free wireless internet in public locations and when accessing sites with sensitive information, such as online banking.  Make sure your home wi-fi connection is secured with a password.

Never share your passwords, and always use ones that are difficult to guess – with a mix of letters, numbers and characters.

### 6. Be password-smart

Never share your passwords, and always use ones that are difficult to guess. Strong passwords use a mix of letters, numbers and characters, and change frequently. Don't recycle passwords and don't use the same passwords for online banking as you would for other services, such as social networking sites.

### 7. Verify before you click

Verify a message before you take any other action, such as clicking on a link or initiating a transaction. Don't click on any links or open files in emails from people you don't recognize or aren't expecting (this could expose your computer to a password key logger or spyware).

### 8. Encrypt for greater security

Always use encryption when sending confidential information by email, and never store sensitive data about yourself or others in your email folders. Even encrypted emails can be hacked.

### 9. Maintain a suite of software security products

Install a well-recognized security program on all of your devices (computer/tablet/phone), and keep it up-to-date. Beware of pop-up warnings that your computer is infected and instructing you to buy or download software to fix the problem.

### 10. Always log off

Remember to log off and close your browser to prevent others from being able to view your information later.

If you suspect you are a victim of fraud or theft, contact the authorities immediately.

**To learn more about protecting your privacy, visit www.rbc.com/privacysecurity, or contact us today.**