Internet security statement

GWL Realty Advisors Inc. and its affiliates, GWL Realty Advisors Residential Inc. and The Canada Life Assurance Company (“GWLRA”) recognize and respect the importance of security. This Internet Security Statement covers the measures that GWLRA takes to help secure your personal information. This Internet Security Statement is subject to change without notice to you, so we recommend that you review it regularly. By using this site, you acknowledge that you have read and understand this Internet Security Statement as amended from time to time.

Encryption

Encryption technology is designed to secure personal and confidential communications between your computer and GWLRA servers, such that they are protected from being read by any third parties. This is achieved by "scrambling" communications so that they are unreadable by anyone other than GWLRA or yourself. GWLRA web applications require a minimum of 128-bit encryption. You can verify that a GWLRA website is encrypted by looking for the golden lock or key icon along the bottom of your browser window, which is used by most browsers to indicate a secure connection.

Time-outs and automatic log outs

Some GWLRA websites may require you to log in using a username and password. While you are logged in, if you leave your browser window open, GWLRA websites will automatically log you out after a period of inactivity. Similarly, if you close your browser window without logging out, you will be automatically logged out. Both of these measures are designed to protect your information from unintended access by a passerby or different user of your computer.

Fraud

Be cautious of emails, websites and other forms of communications purporting to represent a legitimate company or person and that ask you to provide confidential or financial information. This is called phishing.

The content of a phishing e-mail or text message is intended to trigger a quick reaction from you. It can use upsetting or exciting information; demand an urgent response or employ a false pretense or statement. Phishing messages are normally not personalized.

It is not GWLRA's practice to email you or ask you to provide or confirm your PIN, password, or other confidential or financial information, other than as may occur in response to an inquiry from you. If you receive such a request, or if you have any concern as to the validity of an email from GWLRA, a website claiming to be a GWLRA website, a digital communication claiming to be from GWLRA and its employees, or our online security, please contact our Corporate Security & Investigations team toll free at 1-877-751-3417 or email us.

Please attach any suspicious email in its original form, screenshots in the case of instant messages from other communication platforms, or in the case of a website please include the URL in your notification.

What to watch out for: 4 types of common fraud scams

1. Mystery Shopper Scam

   The fraudsters mail out letters indicating they are a customer survey company that is a division of GWLRA and are offering you a job as a mystery shopper. The letter also includes a realistic looking cheque, which is payable to you.

   If you contact the fraudster, you are given instructions to deposit the cheque and withdraw a portion of that money in cash. Your mystery shopper job is to test the customer service of a money transfer company, and you are also instructed to send a money transfer to a specific person, usually in another country. The original cheque will eventually be returned as a fake and you are out of money from your bank account.

2. Inheritance Scam

   The fraudsters mail out letters using letter head that indicates it's from an investment company that is a division of GWLRA and includes the proper GWLRA address and phone number. Fraudsters follow up with victims by phone, indicating you are entitled to an inheritance from a deceased person who has the same last name. Usually, the fraudsters also include in their mail outs a realistic looking GWLRA cheque payable to you.

   The fraudster advises you this is an advance on the inheritance to pay for the fees to transfer the bank account into your name. You are then instructed to deposit the cheque at your bank and then withdraw cash and send a money transfer to a specific person to cover the fees.

3. Purchase Order Email Frauds

   The fraudsters (posing as a manager at GWLRA) send out emails to legitimate companies. The email requests a price quote and refers to an attachment. Attached is a file marked "purchase orders."

   The attachment is either an attempt to defraud that company of product or the file contains a virus to infect that company's computer. The email address that it was sent from is a generic email, but the information regarding a phone number and address may be correct.

   - Be mindful where you post your resume; scammers use legitimate websites to seek out victims.
   - A legitimate employer will never send funds and request a portion of it back.

- Do your research. A simple search on the Internet can save you thousands of dollars.
- If it sounds to good to be true, it is.

4. Fake job postings scam

   On various websites and social media there have been fake job postings for a customer service representative position working from home. The job posting looks legitimate, but the reply link is to an email address instead of connecting directly to our official careers website.

   Typically, the fraudster will reply to you by email and request to conduct a job interview using a chat related app (e.g., WhatsApp, Google hangouts), and send you a realistic looking job offer. The fraudster may send you a fake cheque using the chat app to pay for a Laptop and software required for the job, and instruct you to deposit the cheque using your cell phone. This cheque is not legitimate. The fraudster may then instruct you to provide personal information, and to send funds via an e-Transfer or other method.

   Please note that we will never request payment or funds from a new hire as a condition of employment. If you see a job advertised, go to our official careers website and check to see if that job is actually posted. Any legitimate job posting will link directly to our company web site.

For information on various types of email fraud, please visit the email fraud / phishing page on the RCMP website.

The Canadian Anti-Fraud Centre has published some tips on how to protect yourself:

For more information, visit the Canadian Anti-Fraud Centre.

If you have lost money because of a fraud, contact your local police.

You may also contact our Corporate Security & Investigations team toll-free at 1-877-751-3417 or email us.

.

Other security measures

GWLRA engages in a number of other security activities to help ensure the safety and privacy of your personal information. This includes adopting measures to help secure our computers against hacker attacks and virus activities by a number of different means. We monitor our website, servers, email, and data 24 hours a day to help us immediately identify and rectify any problems. Note that all emails and attachments sent to the organization may be scanned for viruses by a third-party service provider. Scanning may take place outside of Canada.

Security tips you can use

You can also contribute to the security of your information by following a few straightforward principles: For GWLRA sites requiring a password:

- Pick a password that is unique and hard for others to guess. A strong password includes a combination of upper- and lower-case letters and numbers. Avoid passwords such as family or pet names, birthdays, or words found in dictionaries.
- Memorize your password, and don't tell it to anyone. Remember no one from GWLRA will ever call or e-mail asking for your password.
- If you think anyone has had access to your password, change it immediately by logging in and clicking the Your Profile tab. From the Your Profile section, follow the simple instructions to change your password.
- If you are using a computer in a public place (such as an Internet café, or an open desk at work), ensure that no one can see you type in your password, log off when you are finished using the site and clear the browser's cache.
- Run current anti-virus software and anti-spyware software on your computer. This helps ensure your computer is free of malicious programs such as viruses, worms and spyware (snooping software that collects and shares confidential information on your computer with a third party without your consent).

- After using a GWLRA application, clear your browser's cache and then close it. The cache is where a browser keeps copies of the web pages you have recently visited. By clearing it, you help ensure no one else can view these pages, including the next website you visit.

Cookies and Web Beacons

When you visit our website, your computer may be offered “cookies”. Cookies are small text files that are stored on your computer or mobile device when you visit a website. The next time you visit our website, we may use the information stored on your cookie to make your visit easier and to help us to make continual improvements so that we can update our pages to stay relevant and useful to you.

GWLRA uses two types of cookies: session cookies, which are temporary cookies that are erased when you close your internet browser and leave our website, and persistent cookies, that remain on your computer when you close your internet browser and leave our website. Some cookies are used to allow you to browse our website and to see certain features, while others are used to provide information on your browsing to allow us to improve our website, and for advertising-related purposes during future visits.

Our website uses “first party cookies” which are set by the website that is being visited in order to preserve your settings (e.g., while on our site) and “third party cookies” which allow third party features or functionality to be provided on or through the website (e.g., through advertising and interactive content and analytics). GWLRA uses first- and third-party cookies.

Web beacons are also referred to as “pixel tags”. They are embedded in a web page and are not usually visible to you the user. Web beacons or pixel tags are used for many of the same purposes as cookies and they allow GWLRA or its agents on GWLRA’s behalf to gather aggregate statistics about website usage patterns, including how many times a link or a page on a website is visited.