NORTHWEST TITLE COMPANY

5 WAYS TO BE CYBER SECURE

With so much of our lives being occupied in the "digital world", we need be diligent about staying a step ahead of the fraudsters. They are hard at work to conceal their identity, while they attempt to find ways to gain access to your private information through the internet.

- **Technology has its limits.** As "smart" or data-driven technology evolves, it is important to remember that security measures only work if used correctly. Smart technology runs on devices such as smartphones, laptop computers, wireless printers, and other devises such as home security systems and smart locks. Take proper security precautions and ensure correct configuration to wireless devices to prevent data breaches.

- **Be up to date.** Keep your software updated to the latest version available. Maintain your security settings to keep your information safe by turning on automatic updates so you do not have to think about it, and set your security software to run regular scans.

- **Social media is part of the fraud toolset.** By searching Google and scanning social media sites, cybercriminals can gather information about you and people you are connected to. Avoid oversharing on social media and do not conduct business, exchange payment, or share personal identification information on social media platforms.

- **It only takes one time.** Data breaches do not typically happen when a cybercriminal has hacked into an organization's infrastructure. Many data breaches can be traced back to a single security vulnerability, phishing attempt, or instance of accidental exposure. Be wary of unusual sources, do not click on unknown links, and delete suspicious messages immediately.

- **Follow these simple tips when creating a password:**
  - » Create a password with eights characters or more and a combination of letter, numbers, and symbols.
  - » Use a long passphrase. Such as a news headline or even the title of the last book you read. Then add in some punctuation and capitalization.
  - » Avoid using common words in your password. Instead, substitute letters with numbers and punctuation marks or symbols. For example, @ can replace the letter "A" and an exclamation point (!) can replace the letters "I" or "L".
  - » Get creative. Use phonetic replacements, such as "PH" instead of "F". Or make deliberate, but obvious misspellings, such as "enjin" instead of "engine". Use "VV" instead of "W".
  - » Unique account, unique password. Use different passwords for different accounts and devices so that if attackers do guess one password, they will not have access to all of your accounts.
  - » Use stronger authentication. Always opt to enable stronger authentication when available, especially for accounts with sensitive information including your email, credit card, and bank accounts. For example, it could be a one-time PIN texted to your mobile device, providing an added layer of security beyond your password and username.

IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT YOUR SETTLEMENT AGENT.