A Smart Risk Checklist For Staying Safe





As Artificial Intelligence transforms the financial landscape, staying safe and resilient is more important than ever.

This checklist is designed to help protect your wealth, reduce risk, and strengthen confidence in your financial decisions.

At The Wong Group, we're committed to providing thoughtful and accurate solutions, an outstanding client experience and performance that delivers peace of mind.

Common Al Scam Tactics



Voice Cloning

Al mimics a trusted voice to request money, gift cards, or a change in banking



Deepfake Videos

Al-generated videos impersonate trusted individuals or celebrities



Phishing Emails

Highly realistic message drive you to share info or click a malicious link



Look-alike websites

Al-built sites mirror real ones to capture logins or payments



High-Pressure Pitches

Urgent messages push you to act quickly without verifying



Unusual Payment Requests

Gift cards, crypto, or wire transfers—often used by scammers



Context mismatches

Timing, tone, or details don't align with prior conversations or processes

Smart Risk Fraud Prevention Checklist



Personal Security

Use strong, unique password

Enable two-factor authentication

Limit personal info shared online



Phone & Voice Safety

Be skeptical of unexpected requests, even if the voice sounds familiar

Use call-screening/voicemail; don't return calls to numbers provided in the message Agree on a simple family/partner "passphrase"

For payment/instruction changes, require a call-back to a published number and dual approval

Online Behavior



Avoid "too good to be true" sites

Don't fall for fake offers



Verify URLs

Type the address or use bookmarks; beware look-alike domains



Use security tools

Anti-phishing in your browser/email; device updates on.



Avoid using Public Wi-Fi

Use cellular or a VPN if needed



Share less on social

Reduces info for targeted scams

Best Practices: Email & Phone Messages

Avoid clicking unknown links

Prevents malware and phishing attacks

Watch for unnatural phrasing

Al-generated messages often sound off

Verify sender identity

Helps confirm legitimacy before sharing info

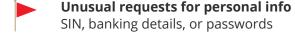
Protect Yourself in the Age of AI: Be Skeptical and Verify

Slow down and question urgency

Confirm identities using a separate, trusted method

Cross-check suspicious messages with known contacts

Red Flags to Watch





Pressure tactics are used to bypass your judgment

Requests for payments that are hard to reverse

Gift cards, crypto and wire transfers are hard to recover once sent

Visual/audio inconsistencies
Be cautious of mismatched lip-syncing, or strange voice tones

What to Do If You Suspect an Al Scam



Pause—don't engage

Pause before clicking, replying, or calling



Secure your accounts

Change passwords, monitor activity, consider freezing your credit



Report the scam

Call the Canadian Anti-Fraud Centre (CAFC) 1-888-495-8501 or your bank



Stay informed

Follow updates from cybersecurity firms and government agencies (CAFC)

At The Wong Group, we're committed to providing thoughtful and accurate solutions, an outstanding client experience and performance that delivers peace of mind.

Contact Us:

thewonggroup@wellington-altus.ca 778.655.2410 #100 - 1450 Creekside Drive, Vancouver, BC, V6J 5B3 Learn more about The Wong Group www.thewonggroup.ca