WealthWisdom

THE PARADOX OF THE DIGITAL NATIVES:

Help Others Protect Against Fraud and Scams

Dale C. Gagnon
Senior Wealth Advisor,
Senior Investment Advisor
613.788.2188
Dale.Gagnon@raymondjames.ca

Emily Gray
Client Service Specialist
613.788.2189
Emily.Gray@raymondjames.ca

Which generation is more likely to fall for online scams? The answer may surprise you. Despite growing up immersed in digital technology since birth, younger generations—often called "digital natives"—are statistically more likely to fall victim to online fraud.[1] This is sometimes referred to as the *"paradox of the digital natives"*: early exposure to digital technologies does not necessarily equate to digital literacy.

Given the growing proliferation and sophistication of online scams, it may be an ideal time to revisit some basic digital safety principles—whether for younger family members or for older adults who may be more vulnerable and in need of support.

Here are six universal tips, which may act as talking points, to help protect against fraud:

1. **Pause before you (re)act.** Scammers often rely on urgency or emotional pressure, although more sophisticated scams have evolved to involve building relationships and trust with a victim over time. However, slowing down can help protect you from making mistakes.

- Be skeptical of messages that pressure you to act immediately—especially those involving money or personal information.
- Use the "Take Five, Tell Two" rule. Take five minutes to think about it, and talk to two people before acting.

2. **Let technology work for you.** Leverage built-in tools and settings to screen out threats. Given our significant daily use of smartphones, here are a handful of ideas relating to mobile phones:

- Let unknown calls go to voicemail. Legitimate callers will leave a message.
- Use your carrier's screening tools. For example, Rogers offers "Call Control," which requires callers to enter a randomly generated number before the call connects. This helps to block automated robocalls.

FOOTNOTES:

1. https://www.news24.com/life/lifestyle-trends/which-generation-is-more-likely-to-fall-for-online-scams-the-paradox-of-thedigital-natives-20250312#; https://www.wsj.com/tech/cybersecurity/young-adult-phishing-scams-social-media-use-bcf7b6ca?; https://www.ey.com/en_us/newsroom/2022/10/gen-z-and-millennials-less-serious-about-cybersecurity-on-work-issued-devices-than-personal-according-to-new-ey-consulting-survey

How Raymond James Ottawa Can Help

If you need support in exploring strategies for teaching financial responsibility, building savings or planning for a financial future, please call the office.

45 O' Connor St Ste 750 Ottawa, ON K1P 1A4
T: 613.369.4600
F: 613.369.4699

- Set up a filter on phones to sort unknown texts into a separate folder to avoid accidental replies and reduce clutter.
- Never reply to unknown calls or text messages—doing so confirms your number is active.

3. **Limit what you share.** The less information you put out there, the harder it is for scammers to target you.

- See what personal data is publicly available. A quick internet search using your name, address or phone number can determine if you have sensitive, publicly-available information. (SEE INSET BELOW)
- Never share personal or financial information unless you're certain of the recipient's identity and the communication channel is secure.
- Reduce your digital footprint. Delete unused online accounts to reduce access in case of a data breach.
- Avoid posting personal details on social media like birthdays, addresses, travel plans or even family member names.
- Set online privacy settings to the highest level.
- Be cautious with online forms or surveys—verify the source first**.**

4. **Use good payment practices.** Be thoughtful about how and where you send money.

- Use payment methods with fraud protection, such as PayPal, when sending funds to unfamiliar recipients. Avoid wire transfers, gift cards or Interac e-transfers for unfamiliar transactions.
- Use separate email addresses or usernames for less-secure transactions to protect your identity online.

5. **Add a layer of personal security.** Proactive steps can make it harder to impersonate you or your loved ones.

- Create a family code word to verify the identity of anyone claiming to be a loved one in distress. If a caller can't provide the code word, hang up.
- Consider using a dedicated email address exclusively for financial and banking transactions.
- For added privacy, some use alternate ("burner") birthdates or slight name variations when registering for non-financial services—to conceal private data and limit exposure of personal information.

6. **Stay informed.** Fraud tactics continue to become more sophisticated and evolve rapidly.

- Follow trusted resources to stay updated on the latest scams. Two trusted resources are the Canadian Anti-Fraud Centre at https://antifraudcentre-centreantifraude.ca/ and the Better Business Bureau at www.bbb.org/ca/news/scams
- If you suspect a scam, report it—you could help protect others. https://antifraudcentre-centreantifraude.ca/report-signalez-eng.htm

Finally, remember that **Raymond James** will never contact you via unsolicited email, text or phone call asking for sensitive information or account details. If you ever have any concerns or doubts, please contact the office.

Staying alert, using smart tools and talking to others can go a long way in protecting yourself from fraud. If you have questions or issues, don't hesitate to reach out—at **Raymond James Ottawa,** your security is a priority.

How Much of My Data is Available Online to Others?

A recent Wall Street Journal article highlighted how marketable your personal data can be after a data breach.[2] How much does your data sell for on the dark web?

- Your credit card number: $6
- Your PayPal account credentials: $100
- Your crypto wallet userID: $350

Managing your digital footprint — including keeping accounts secure, periodically cleansing data and closing unused accounts — is important for maintaining privacy, protecting assets and reducing the risk of fraud.

You may be surprised at what personal data is publicly available. Using Google's free tool, "Results About You," (which Google states it won't use for other purposes), you can view what personal data is publicly available online. The process can take up to several hours. For eligible results, you can select the option to remove the information directly from the search result. You can also use the "dark web monitoring" tool to see how many data breaches your email address and username are associated with.

FOOTNOTES:

2. https://www.wsj.com/tech/personal-tech/data-breach-dark-web-protection-6972f3a6

RAYMOND JAMES®