

## தொலைபேசி பாதுகாப்பு குறிப்புகள்

### கவனியுங்கள்...

- உங்களுக்குத் தெரியாத தொலைபேசி எண்களிலிருந்து வரும் அழைப்புகள் மற்றும் குறுஞ்செய்தி (SMS)/செய்திகள்
- உங்களை உண்மையிலேயே மகிழ்ச்சியடையச் செய்யும் அல்லது பயமுறுத்தும் ஒரு செய்தி
- விரைவாகச் செயல்பட உங்களை வற்புறுத்தும் ஒரு அழைப்பாளர் அல்லது குறுஞ்செய்தி (SMS)/உரை
- இணைப்பைக் கிளிக் செய்யச் சொல்லும் ஒரு குறுஞ்செய்தி (SMS)/உரை
- அழைப்பாளர் பேசத் தொடங்குவதற்கு முன்பு தாமதம் ஏற்பட்டால்
- அழைப்பாளர் துஷ்பிரயோகம் செய்து அச்சுறுத்தினால்
- பணம் அல்லது தனிப்பட்ட/ரகசியத் தகவலுக்கான எந்தவொரு கோரிக்கையும்



### அதை செய்யாதே!

- உங்கள் SIN எண் (Social Insurance Number), வங்கித் தகவல் அல்லது பயனர் பெயர் (username) மற்றும் கடவுச்சொல் போன்ற எந்த ரகசியத் தகவலையும் கொடுக்க வேண்டாம்.
- பணம் அனுப்ப வேண்டாம்.
- கொடுக்கப்பட்டுள்ள இணைப்புகளைக் கிளிக் செய்ய வேண்டாம். குறுஞ்செய்தி (SMS)/உரைக்கு பதிலளிக்க வேண்டாம்.

- உங்களுக்குக் கொடுக்கப்பட்ட எண்ணை அழைக்க வேண்டாம், அல்லது உங்கள் தொலைபேசியில் திரும்ப அழைக்கும் அம்சத்தைப் பயன்படுத்த வேண்டாம்.

## என்ன செய்வது

- துண்டிக்கலாம் அல்லது தெரியாத அழைப்பாளரை குரல் அஞ்சலுக்கு பெற அனுமதிக்க செய்க.
- எண்ணைத் தடு.
- உங்களுக்குப் பிடித்தமான ஒருவரைப் பற்றி கவலையாக இருந்தால், அவர்களின் எண்ணைக் கண்டுபிடித்து அழைக்கவும்.

## நினைவில் கொள்ளுங்கள்

- மோசடி செய்பவர்கள் மிகவும் தந்திரமானவர்களாக இருக்கலாம், மேலும் உங்களை ஏமாற்ற அனைத்து முயற்சிகளையும் செய்வார்கள், அன்புக்குரியவர்களைப் போல ஆள்மாறாட்டம் செய்வது உட்பட.
- அரசாங்கமும் வங்கிகளும் உங்களை அழைத்தால் தொலைபேசியில் தனிப்பட்ட தகவல்களைக் கேட்பதில்லை. நீங்கள் அவர்களை அழைத்தால், உங்கள் அடையாளத்தைச் சரிபார்க்க அவர்கள் இந்தத் தகவலைக் கேட்கலாம்.
- உங்களுக்கு அழுத்தம் கொடுக்கும் ஒரு நிறுவனம், உங்கள் வணிகத்திற்கு தகுதியற்றது.

## நீங்கள் என்ன பார்க்கவோ கேட்கவோ முடியும்

- **உதவிக்கான வேண்டுகோள்:** உங்களுக்குத் தெரிந்த ஒருவர் போல் தெரிகிறது. அவர்களுக்கு உண்மையிலேயே உங்கள் உதவி தேவை. பொதுவாக அவர்களுக்கு பணம் தேவை. நீங்கள் உதவவில்லை என்றால், அவர்களுக்கு ஏதாவது மோசமான விஷயம் நடக்கும் என்று உங்களுக்குச் சொல்லப்படும்.
  - அழைப்பவர் அல்லது குறுஞ்செய்தி (SMS) /உரை அனுப்புபவர்:
    - உங்களைப் பற்றியும் உங்கள் குடும்பத்தினரைப் பற்றியும் தனிப்பட்ட தகவல்களைப் பகிர்வதன் மூலம்

உங்கள் நம்பிக்கையை உருவாக்குகிறார் (அவர்கள் அதை சமூக ஊடகங்களில் கண்டுபிடித்தனர்)

- உங்கள் குரல் அக்கறை கொண்ட ஒருவரைப் போல கேட்கிறது (இது AI ஆக இருக்கலாம்)

- **அச்சுறுத்தல்:** அழைப்பவர் அல்லது குறுஞ்செய்தி (SMS) /உரையாடல் ஆக்ரோஷமாகவும் கோருவதாகவும் உள்ளது. உங்களிடம் கூறப்படலாம்:

- அரசாங்கம் அல்லது ஒரு சட்ட சேவை உங்களைத் தொடர்பு கொள்கிறது.
- நீங்கள் உடனடியாக நடவடிக்கை எடுக்கவில்லை என்றால் மிகவும் மோசமான ஒன்று நடக்கும்.
- நீங்கள் ஒரு வலைத்தளத்தைப் பார்வையிட வேண்டும், அல்லது உங்கள் SIN எண் (Social Insurance Number) அல்லது வங்கித் தகவல் போன்ற ரகசியத் தகவலைப் பகிர வேண்டும்.

- **நல்ல செய்தி!** அழைப்பவர் அல்லது குறுஞ்செய்தி (SMS)/உரை அனுப்புபவர் உங்களுக்காக ஒரு சிறந்த சலுகை இருப்பதாகவோ, நீங்கள் ஒரு போட்டியில் வெற்றி பெற்றதாகவோ, அல்லது உங்களிடம் பணம் வருவதாகவோ கூறலாம். நீங்கள் கேள்விகள் கேட்டாலோ அல்லது தாமதப்படுத்தினாலோ அவர்கள் ஆக்ரோஷமாகவோ அல்லது துஷ்பிரயோகம் செய்யவோ கூடும்.

உங்களிடம் இவ்வாறு கூறப்படலாம்:

- விரைவாகச் செயல்படுங்கள்
- இணைப்பைக் கிளிக் செய்யவும் அல்லது எனது தனிப்பட்ட விவரங்களை வழங்கவும்.

- **உதவி வழங்குதல்:** அழைப்பவர் அல்லது குறுஞ்செய்தி (SMS)/உரை உங்கள் வங்கி அல்லது கணினி சேவை என்று உங்களுக்குச் சொல்லலாம்.

உங்களுக்கு இவ்வாறு கூறப்படலாம்:

- உங்கள் சாதனம் அல்லது கணக்கு ஹேக் செய்யப்பட்டுள்ளது ("சமரசம் செய்யப்பட்டது") ("compromised")
- உதவி பெற, நீங்கள் ஒரு இணைப்பைக் கிளிக் செய்ய வேண்டும் அல்லது நபரின் விவரங்களை வழங்க வேண்டும்
- நீங்கள் தாமதப்படுத்தினால், உங்கள் நிதி அல்லது சேவைகளை இழப்பீர்கள்

## அது உங்களுக்கு நடந்திருந்தால்

- உங்கள் பயனர் பெயர் (username) மற்றும் கடவுச்சொல்லைப் பகிர்ந்து கொண்டால், உடனடியாக அவற்றை மாற்ற முயற்சிக்கவும்.
- நீங்கள் வங்கி அல்லது கிரெடிட் கார்டு தகவல்களைப் பகிர்ந்து கொண்டால், உடனடியாக உங்கள் வங்கியை அழைக்கவும்.
- காவல்துறையினரிடம் புகார் அளிக்கவும் மற்றும் [Canadian Anti-Fraud Centre's online reporting system](#) அல்லது தொலைபேசி மூலம் [1-888-495-8501](tel:1-888-495-8501).
- உங்களுக்கு என்ன நடந்தது என்பதை உங்கள் நண்பர்கள் மற்றும் குடும்பத்தினரிடம் சொல்லுங்கள், அதனால் அவர்களுக்கும் அது நடக்க வாய்ப்பு குறைவு.