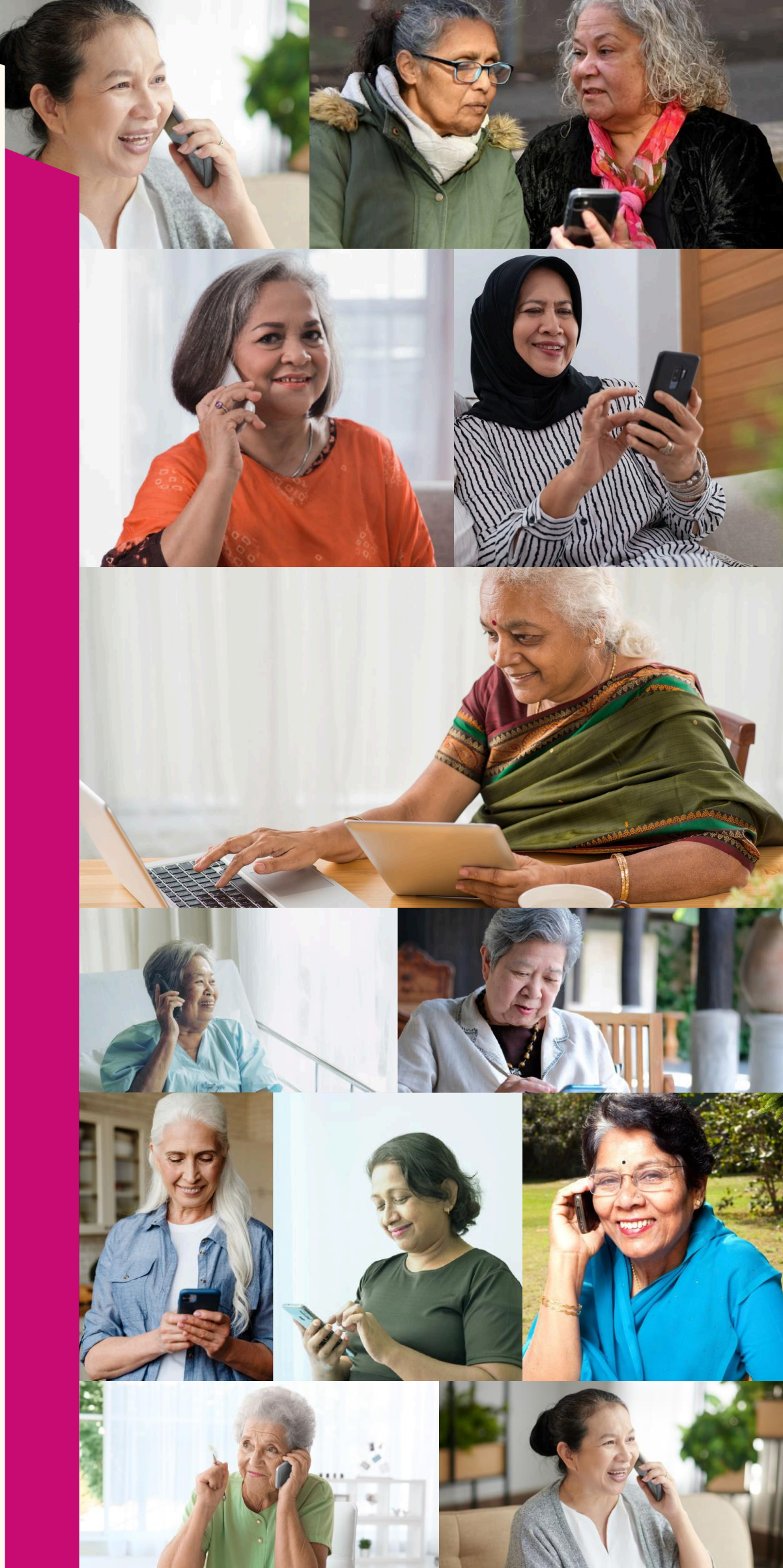


# दक्षिण एशियाई वरिष्ठ महिलाओं के लिए धोखाधड़ी रोकथाम टूलकिट

धोखाधड़ी और ठगी से बचाव





इमिग्रेंट्स विमेंस इन्फॉर्मेशन नेटवर्क (IWIN) ने दक्षिण एशियाई वरिष्ठ महिलाओं की मदद के लिए एक टूलकिट तैयार किया है, ताकि वे ठगी को पहचान सकें और अपनी व्यक्तिगत और धन संबंधी जानकारी को धोखाधड़ी से बचाने के लिए सक्रिय कदम उठा सकें। यह टूलकिट IWIN की वेबसाइट से मुफ्त में डाउनलोड किया जा सकता है। इसके अलावा, कुछ हिस्से उर्दू और पंजाबी में वीडियो के रूप में IWIN के सोशल मीडिया प्लेटफॉर्म पर उपलब्ध हैं। कृपया इसे अपने रिश्तेदारों और दोस्तों को बताइए।



हम IWIN में गरीब और कमजोर समुदायों को पैसे से जुड़ी धोखाधड़ी से बचाने के लिए काम कर रहे हैं। हम समुदाय संगठनों के साथ मिलकर यह सुनिश्चित करते हैं कि दक्षिण एशियाई वरिष्ठ महिलाएं, खासकर जो विदेश से आई हैं, उनके पास अपने पैसे और संपत्ति की सुरक्षा के आसान तरीके हों। हमारा टूलकिट आसान कदमों और सुझावों के साथ उन्हें धोखाधड़ी से बचने में मदद करता है।



# विषय सूची

01

## धोखाधड़ी से बचाव का परिचय

कमजोर समुदायों को लक्षित करने वाली धन संबंधी धोखाधड़ी और जागरूकता का महत्व

02

## धोखाधड़ी को समझना और इसके प्रभाव

धोखाधड़ी क्या है, यह दक्षिण एशियाई वरिष्ठ महिलाओं को क्यों प्रभावित करती है, और धोखेबाज कैसे उनकी कमजोरियों का फायदा उठाते हैं

03

## अनुसंधान का अवलोकन

धोखाधड़ी के वरिष्ठ लोगों पर, खासकर विदेश महिलाओं पर प्रभाव, धोखाधड़ी के सामान्य प्रकार, और आप जो सुरक्षा उपाय ले सकते हैं, उनका संक्षिप्त विवरण।

04

## टूलकिट चेकलिस्ट

सामान्य प्रकार की धोखाधड़ी और इसे पहचानने और रोकने के तरीके

### सामान्य प्रकार की धोखाधड़ी

- फिशिंग / ईमेल धोखाधड़ी
- फ़ोन / वॉयसमेल धोखाधड़ी
- प्रवासी नागरिक/निर्वासन धोखाधड़ी
- लॉटरी/इनाम धोखाधड़ी

### सामान्य प्रकार की धोखाधड़ी (जारी):

- पारिवारिक आपातकाल या ग्रेन्पेरन्ट धोखाधड़ी
- समुदाय या सांस्कृतिक धोखाधड़ी
- टेक सपोर्ट स्कैम

05

## सुरक्षा के लिए वास्तविक सलाह

सतर्क रहने के लिए चेतावनी संकेत , खुद को सुरक्षित रखने के उपाय , और धोखाधड़ी का शिकार होने पर उठाए जाने वाले कदम

06

## धोखाधड़ी से अपनी सुरक्षा कैसे करें

आपके समुदाय और परिवार से समर्थन प्राप्त करने के तरीके और अगर आप धोखाधड़ी का शिकार होते हैं तो क्या करें

07

## आपका धोखाधड़ी परिचयन मार्गदर्शक: चरण-दर-चरण उपकरण

संदिग्ध कॉल्स, ईमेल्स, या अनुरोधों का मूल्यांकन करने और चेतावनी संकेतों की पहचान करने के लिए एक वास्तविक फ्लोचार्ट

08

## संसाधन और समर्थन

विश्वसनीय संपर्क और संगठन जो व्यक्तियों की सुरक्षा में मदद कर सकते हैं और धोखाधड़ी की रिपोर्ट कर सकते हैं



# धोखाधड़ी से बचाव का परिचय

धोखाधड़ी और ठगी किसी को भी प्रभावित कर सकती है, लेकिन वरिष्ठ लोग — विशेष रूप से प्रवासी समुदायों की महिलाएं — खास चुनौतियों का सामना करती हैं।

जैसे-जैसे हम आधुनिक जीवन की जटिलताओं से गुजरते हैं, यह महत्वपूर्ण है कि हम अपनी भलाई को खतरे में डालने वाले संभावित जोखिमों के बारे में सूचित और जागरूक रहें। यह टूलकिट दक्षिण एशियाई वरिष्ठ महिलाओं के लिए एक मार्गदर्शिका है। यह आपको निम्नलिखित तरीकों से अपनी सुरक्षा करने का तरीका दिखाएगा:

## 1. संभावित धोखाधड़ी की पहचान करें

- कभी भी अपने सोशल इंश्योरेंस नंबर (SIN) या अपनी बैंक की जानकारी फोन या ईमेल के माध्यम से साझा न करें।
- मजबूत पासवर्ड का उपयोग करें और संवेदनशील दस्तावेजों को नष्ट करने से पहले उन्हें नष्ट करें।

## 2. अपनी व्यक्तिगत और धन संबंधी जानकारी की सुरक्षा करें

- पैसे या व्यक्तिगत जानकारी के लिए किए गए जल्दबाजी में अनुरोधों के प्रति सतर्क रहें।
- अनजान लिंक या फोन कॉल्स से सावधान रहें जो आपको पुरस्कार का वादा करें या धमकियाँ दें।

## 3. आवश्यक होने पर समर्थन प्राप्त करें और निस्संदेह रूप से कार्रवाई करें

- धोखाधड़ी की रिपोर्ट कनाडाई एंटी-फ्रॉड सेंटर या स्थानीय पुलिस को करें।
- यदि आपको धोखाधड़ी का संदेह हो, तो तुरंत अपने बैंक को सूचित करें।





# धोखाधड़ी और इसके प्रभाव को समझना

धोखाधड़ी तब होती है जब कोई व्यक्ति धोखाधड़ी के तरीकों का उपयोग करके पैसे, व्यक्तिगत जानकारी, या अन्य मूल्यवान चीजें चुराता है। धोखेबाज अक्सर उन व्यक्तियों को लक्ष्य बनाते हैं, जिन्हें वे भरोसेमंद या कुछ तकनीकों से अपरिचित मानते हैं। दक्षिण एशियाई वरिष्ठ महिलाओं के लिए, भाषा, सांस्कृतिक प्रथाएं, या समुदायिक संबंध जैसे तत्व धोखाधड़ी की पहचान करना और भी मुश्किल बना सकते हैं।



## यह क्यों महत्वपूर्ण है ?

हमारी समुदाय वार्ताओं से, हमने यह सीखा कि:

- कई धोखेबाज व्यक्तियों के विश्वास, अधिकार के प्रति सम्मान या सामाजिक जिम्मेदारियों का फायदा उठाते हैं।
- धोखाधड़ी से मानसिक तनाव, धन संबंधी चुनौतियां और अकेलेपन की भावना हो सकती है।

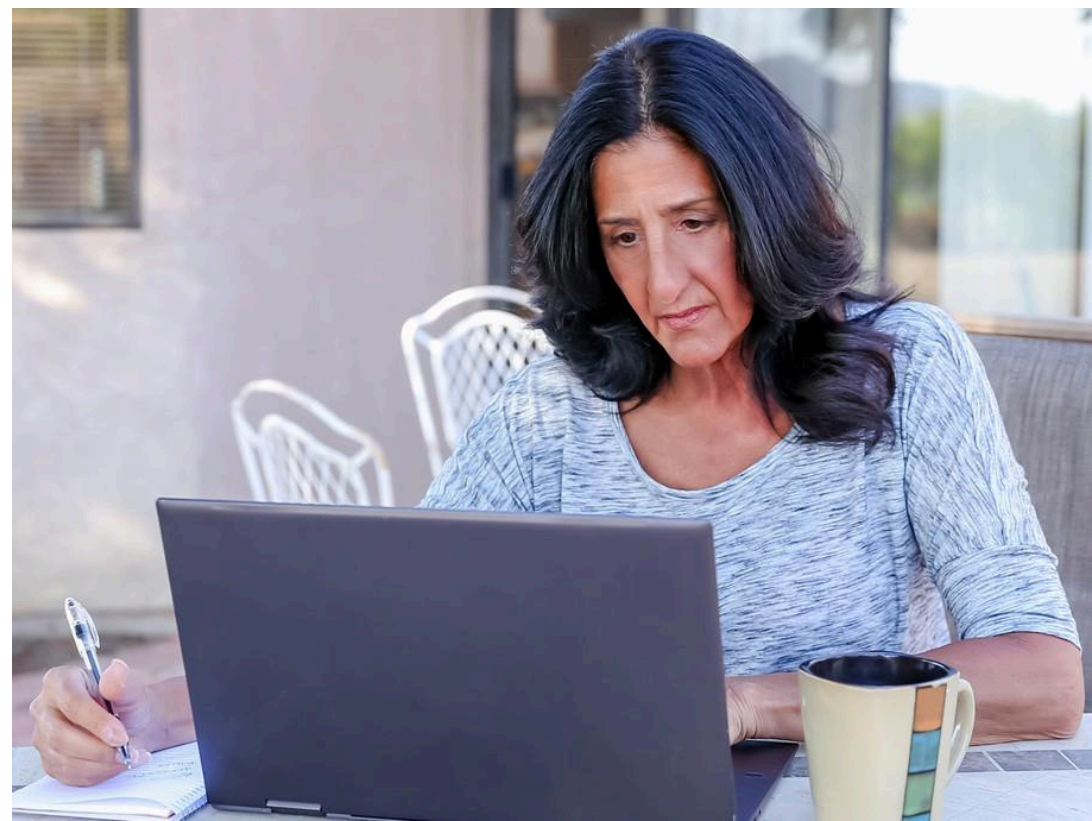


# धोखाधड़ी और इसके प्रभाव को समझना

याद रखें, सतर्क रहना का मतलब होना नहीं है। इसका मतलब है अपनी और अपनी प्रियजनों की सुरक्षा करना।

अपने पैसे और व्यक्तिगत जानकारी की सुरक्षा के लिए सरल लेकिन महत्वपूर्ण कदमों की नियमित समीक्षा करना धोखाधड़ी और ठगी से बचाव के लिए एक सक्रिय तरीका है।

हालांकि बैंक और कनाडा सरकार हमें सुरक्षित रखने के लिए विकसित तकनीकी और सुरक्षा की कई परतों का उपयोग करते हैं, फिर भी कुछ महत्वपूर्ण कदम हैं जिन्हें आप उठाकर अपनी सुरक्षा सुनिश्चित कर सकते हैं।



हमें आशा है कि यह संसाधन एक विश्वसनीय साथी के रूप में काम करेगा, जो आपको सूचित निर्णय लेने में सक्षम बनाएगा और आपके परिवारों और समुदायों में खुले संवाद को बढ़ावा देगा।





# अनुसंधान अवलोकन

## वास्तविक सुरक्षा उपाय

### 1. अपने उपकरणों को सुरक्षित रखें

अपने फोन, टैबलेट और कंप्यूटर को सुरक्षित रखने के लिए विश्वसनीय एंटीवायरस और एंटी-मैलवेयर सॉफ्टवेयर इंस्टॉल करें। अपने उपकरणों को नियमित रूप से अपडेट करें ताकि आप नए खतरों से सुरक्षित रहें। अपडेट्स को स्वचालित रूप से इंस्टॉल करने के लिए सेट करें ताकि आप कभी भी महत्वपूर्ण सुरक्षा पैच न चूकें।

### 3. संवेदनशील दस्तावेजों को सुरक्षित तरीके से नष्ट करें

पुराने धन संबंधी या व्यक्तिगत दस्तावेज फेंकने से पहले, यह सुनिश्चित करें कि इन्हें धोखेबाजों द्वारा इस्तेमाल नहीं किया जा सके। बैंक स्टेटमेंट्स, क्रेडिट कार्ड बिल्स, या अन्य दस्तावेजों को जो व्यक्तिगत जानकारी रखते हैं, उन्हें काटकर या फाड़कर नष्ट करें ताकि वे गलत हाथों में न जाएं।

### 2. जो आप ऑनलाइन साझा करते हैं, उसके प्रति सतर्क रहें।

धोखेबाज लोग ऑनलाइन बटाई गई व्यक्तिगत जानकारी का इस्तेमाल करके लोगों की नकल करते हैं या उनके अकाउंट्स तक पहुँच जाते हैं। अपनी सुरक्षा के लिए, अपनी जन्मतिथि, पता, या धन संबंधी जानकारी जैसे संवेदनशील विवरण सार्वजनिक रूप से न शेयर करें। केवल भरोसेमंद व्यक्तियों या संस्थाओं को ही ऐसी जानकारी दें, जिन्हें आपने पहले संपर्क किया हो।

### 4. मजबूत और अनोखा पासवर्ड का उपयोग करें

हर ऑनलाइन अकाउंट के लिए अनोखा और मुश्किल से अनुमान लगाने योग्य पासवर्ड बनाएं, और इनका पुनः उपयोग करने से बचें ताकि सुरक्षा बढ़ सके। अगर आपको लगता है कि कोई पासवर्ड चोरी हो गया है, तो तुरंत उस अकाउंट का पासवर्ड बदलें और जो भी अन्य अकाउंट्स उसी पासवर्ड का इस्तेमाल कर रहे हैं, उनका भी पासवर्ड बदलें।

धोखाधड़ी और ठगी केवल धन संबंधी अपराध नहीं हैं — इनके मानसिक, भावनात्मक और सामाजिक परिणाम भी होते हैं।

फोकस ग्रुप चर्चाओं और हाल की रिसर्च के आधार पर, हमने कुछ सामान्य ठगी के तरीके पहचाने हैं जो खासतौर पर बुजुर्गों, विशेष रूप से प्रवासी महिलाओं को निशाना बनाते हैं:

फिशिंग/ईमेल ठगी

इमिग्रेशन / डिपोर्टेशन ठगी

कम्युनिटी / सांस्कृतिक ठगी

फोन / वॉयसमेल ठगी

लॉटरी/पुरस्कार ठगी

टेक सपोर्ट ठगी

परिवारिक आपातकाल /  
ग्रैंडपेरेंट्स ठगी



# टूलकिट चेकलिस्ट

## धोखाधड़ी के सामान्य प्रकार:

### फिशिंग/ईमेल ठगी

क्या होता है: धोखेबाज फर्जी ईमेल या टेक्स्ट संदेश भेजते हैं, जो एक विश्वसनीय स्रोत जैसे बैंक, सरकारी एजेंसी, या उपयोगिता कंपनी से आने का दावा करते हैं। इन संदेशों में आमतौर पर आपको अपनी व्यक्तिगत जानकारी देने या लिंक पर क्लिक करने के लिए कहा जाता है, जिससे आपकी जानकारी चुराई जा सकती है।



#### उदाहरण:

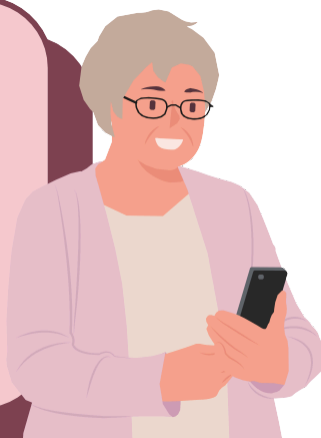
एक ईमेल दावा करता है कि यह आपके बैंक से है, जिसमें कहा गया है कि आपका खाता लॉक हो जाएगा अगर आप अपना पासवर्ड सत्यापित नहीं करते।

#### कैसे सुरक्षित रहें:

अचानक प्राप्त संदेशों में दिए गए लिंक पर क्लिक करने से बचें। संगठन से सीधे संपर्क करके इसकी पुष्टि करें।

### फोन / वॉयसमेल ठगी

क्या होता है: धोखेबाज खुद को सरकार या किसी उपयोगिता कंपनी से बताकर कहते हैं कि आपको पैसे देने हैं या आपकी जानकारी खतरे में है। वे आपको जल्दी में कोई कार्रवाई करने के लिए कहते हैं, जैसे पैसे भेजने या व्यक्तिगत जानकारी देने के लिए।



#### उदाहरण:

फोन कॉल्स आती हैं जो कहती हैं कि वे कनाडा रिवेन्यू एजेंसी (CRA) से हैं और भुगतान की मांग करती हैं या कानूनी कार्रवाई की धमकी देती हैं।

#### कैसे सुरक्षित रहें:

कॉल काट दें और असली संगठन को कॉल करें। अपनी व्यक्तिगत जानकारी जैसे SIN या बैंक विवरण साझा न करें। धमकी देने वाले वॉयसमेल को न सुनें और नजरअंदाज करें।

### इमिग्रेशन / डिपोर्टेशन ठगी

क्या होता है: धोखेबाज यह दावा करते हैं कि आपकी इमिग्रेशन स्थिति में कोई समस्या है और वे आपको डिपोर्टेशन से बचाने के लिए पैसे मांगते हैं। वे आपको डराते हैं कि यदि आपने जल्दी पैसे नहीं दिए, तो आपको देश से बाहर किया जा सकता है या कानूनी कार्रवाई का सामना करना पड़ सकता है।



#### उदाहरण:

"यह इमिग्रेशन विभाग है। आपकी स्थिति की समीक्षा की जा रही है, और आपको डिपोर्टेशन से बचने के लिए तुरंत \$2,000 का भुगतान करना होगा।"

#### कैसे सुरक्षित रहें:

याद रखें कि सरकारी एजेंसियां कभी भी फोन पर भुगतान की मांग नहीं करतीं। किसी भी दावे की पुष्टि करने के लिए सीधे आधिकारिक इमिग्रेशन विभाग से संपर्क करें।

### लॉटरी / पुरस्कार ठगी

क्या होता है: कोई आपको बताता है कि आपने पुरस्कार जीता है, लेकिन उसे प्राप्त करने के लिए आपको फीस का भुगतान करना होगा।



#### उदाहरण:

"आपने एक कार जीती है! टैक्स कवर करने के लिए \$500 भेजें।"

#### कैसे सुरक्षित रहें:

असली पुरस्कार के लिए कभी भी भुगतान की आवश्यकता नहीं होती। उन ऑफर्स से सतर्क रहें जो बहुत अच्छे लगते हैं, क्योंकि वे अक्सर झांसा होते हैं।





# टूलकिट चेकलिस्ट

## धोखाधड़ी के सामान्य प्रकार:

### परिवारिक आपातकाल / ग्रैन्डपेरन्ट्स ठगी

क्या होता है: धोखेबाज खुद को परिवार के सदस्य के रूप में पेश करते हैं और कहते हैं कि वे मुसीबत में हैं, और तत्काल वित्तीय सहायता की मांग करते हैं।



#### उदाहरण:

"नानी, मैं एक्सीडेंट में हो गया हूँ, और मुझे अस्पताल के लिए पैसे चाहिए। आप किसी और को नहीं बता सकती, नहीं तो मुझे मुश्किल हो जाएगी।"

#### कैसे सुरक्षित रहें:

कॉलर की पहचान सत्यापित करने के लिए ऐसे व्यक्तिगत सवाल पूछें जो केवल आपका परिवार सदस्य ही उत्तर दे सके। अन्य परिवार के सदस्यों से संपर्क करें और कहानी की सत्यता की जांच करें।

### समुदाय / सांस्कृतिक धोखाधड़ी

क्या होता है: ठग धार्मिक या सांस्कृतिक आयोजनों के दौरान विश्वास का फायदा उठाकर दान के लिए अनुरोध करते हैं।



#### उदाहरण:

एक झूठी चैरिटी दीवाली या रमजान के दौरान योगदान के लिए कहती है।

#### कैसे सुरक्षित रहें:

दान देने से पहले चैरिटी के बारे में जांच करें। केवल जानी-पहचानी और सत्यापित संस्थाओं को ही दान दें।

### टेक सपोर्ट धोखाधड़ी

क्या होता है: आपको एक कॉल या पॉप-अप आता है जिसमें कहा जाता है कि आपका कंप्यूटर खतरे में है, और आपको "मदद" के लिए भुगतान करने को कहा जाता है।



#### उदाहरण:

एक पॉप-अप संदेश दिखाई देता है, "चेतावनी: आपका कंप्यूटर संक्रमित है! अब इस नंबर पर कॉल करें।"

#### कैसे सुरक्षित रहें:

अनचाहे पॉप-अप से नंबर पर कॉल करने से बचें। तकनीकी समस्याओं के लिए विश्वसनीय स्थानीय मरम्मत सेवाओं का ही उपयोग करें।



# सुरक्षा के लिए वास्तविक टिप्स:

## धोखाधड़ी को पहचानने और बचने के लिए कदम:

### धोखाधड़ी के संकेत जिन पर ध्यान दें

**जल्दी कार्रवाई करने का दबाव:** ठग जल्दी भुगतान या निर्णय लेने के लिए जोर दे सकते हैं।

**गोपनीय जानकारी की मांग:** ठग आपसे पासवर्ड, पिन या बैंक विवरण जैसी व्यक्तिगत जानकारी मांग सकते हैं।

**गोपनीयता बनाए रखना:** ठग आपको दूसरों से इस मामले के बारे में बात करने से रोक सकते हैं।

### अपनी सुरक्षा कैसे करें

**रुकें और सत्यापित करें:** थोड़ा समय निकालें और सोचें। किसी भरोसेमंद व्यक्ति से संपर्क करें और स्थिति की समीक्षा करने के लिए उनकी मदद लें।

**व्यक्तिगत जानकारी साझा करने से बचें:** अपने बैंकिंग विवरण और पहचान से जुड़ी जानकारी को निजी रखें।

**विश्वसनीयता जांचें:** कॉल करने वाले व्यक्ति या संगठन की पहचान हमेशा सत्यापित करें, जवाब देने से पहले उनकी जानकारी की जांच करें।

## सुरक्षा के लिए वास्तविक टिप्स:

### 1. व्यक्तिगत जानकारी की सुरक्षा के लिए वास्तविक टिप्स:

- ऑनलाइन अकाउंट्स के लिए मजबूत पासवर्ड या पासफ्रेज़ का उपयोग करें।
- व्यक्तिगत जानकारी वाले दस्तावेज़ों को नष्ट करें।
- सोशल मीडिया पर अपनी व्यक्तिगत जानकारी बहुत कम और सावधानी से साझा करें।

### 2. वित्तीय जागरूकता:

- अपने बैंक स्टेटमेंट्स को नियमित रूप से जांचें ताकि किसी भी असामान्य गतिविधि का पता चल सके।
- कभी भी अजनबी लोगों को वायर ट्रांसफर या प्रीपेड कार्ड के जरिए पैसे न भेजें।
- किसी चैरिटी को दान करना चाहते हैं, तो सुनिश्चित करें कि वह प्रमाणित और वैध हो।

### 3. तकनीकी सुरक्षा:

- अपने डिवाइसों के सॉफ्टवेयर को समय-समय पर अपडेट करें।
- अपनी डिवाइस की सुरक्षा के लिए अच्छे एंटीवायरस सॉफ्टवेयर का उपयोग करें।
- किसी भी अजनबी ऐप को डाउनलोड करने से बचें और संदिग्ध लिंक पर क्लिक न करें।

## सुरक्षित रहने के लिए चेकलिस्ट:

☐ व्यक्तिगत या धन संबंधी जानकारी मांगने वाले किसी भी व्यक्ति की पहचान सत्यापित करें

☐ बैंक स्टेटमेंट्स को नियमित रूप से जांचें ताकि अनधिकृत लेन-देन का पता चल सके और धोखाधड़ी को जल्दी पहचाना जा सके।

☐ अनपेक्षित ईमेल या टेक्स्ट में लिंक या अटैचमेंट पर क्लिक करने से बचें

☐ संदिग्ध गतिविधि की तुरंत रिपोर्ट करें

☐ अपनी चिंताओं को भरोसेमंद दोस्त या परिवार के सदस्य से साझा करें

☐ अजनबी कॉल को वॉयसमेल पर जाने दें





# धोखाधड़ी से अपनी सुरक्षा कैसे करें:

धोखाधड़ी से बचने की शुरुआत जागरूकता और सरल कदमों से होती है। यह पृष्ठ आपको सुरक्षा, सहायता और सामुदायिक शक्ति के लिए व्यावहारिक टिप्स और संसाधन प्रदान करता है ताकि आप सुरक्षित, समर्थ और सशक्त रहें।



## आपके समुदाय और परिवार से समर्थन:

### परिवारिक संबंधों को मजबूत करना:

- धोखाधड़ी और ठगी के बारे में परिवार के सदस्यों से खुलकर बात करें। इससे वे सतर्क रहेंगे और धोखाधड़ी के संकेतों को पहचानने में सक्षम होंगे।
- अगर किसी बात को लेकर आपको संदेह या उलझन महसूस हो, तो अपने परिवार के सदस्यों से मदद और मार्गदर्शन मांगें। वे आपकी स्थिति को समझने में मदद कर सकते हैं और सही कदम उठाने के लिए आपको प्रोत्साहित कर सकते हैं।

### समुदाय में जागरूकता बढ़ाना:

- अपने समुदाय में धोखाधड़ी से बचने के लिए कार्यशालाओं और सेमिनारों में भाग लें। यह आपको धोखाधड़ी से बचने के नए तरीके सिखाएंगे। जो भी जानकारी और सलाह आपने धोखाधड़ी से बचने के बारे में सीखी हो, उसे अपने समुदाय के अन्य लोगों के साथ साझा करें।

### अगर आप धोखाधड़ी का शिकार होते हैं, तो क्या करें:

- **संपर्क को समाप्त करें:** विनम्रता से उस व्यक्ति या संगठन से संपर्क बंद करें। किसी भी और जानकारी को साझा करने से बचें।
- **जानकारी इकट्ठा करें:** सभी ईमेल, संदेश या अन्य प्रमाणों को इकट्ठा करें। यह भविष्य में धोखाधड़ी की रिपोर्ट करने में सहायक हो सकता है।
- **धोखाधड़ी की रिपोर्ट करें:**  
कनाडाई धोखाधड़ी निरोधक केंद्र: 1-888-495-8501  
वरिष्ठ सुरक्षा लाइन: 1-866-299-1011  
साक्ष्य इकट्ठा करें: सभी संचारों को प्रमाण के रूप में इकट्ठा करें। यह रिपोर्टिंग प्रक्रिया को सरल बनाता है और भविष्य में धोखाधड़ी के खिलाफ कार्रवाई में मदद करता है।

धोखाधड़ी रोकथाम एक साझी जिम्मेदारी है। अपने व्यक्तिगत जानकारी को सुरक्षित रखना सीखें, समुदाय से समर्थन प्राप्त करें, और यदि आपको कोई धोखाधड़ी का संदेह हो, तो तुरंत कार्रवाई करें।

याद रखें, धोखाधड़ी की रिपोर्ट करना आपके समुदाय के अन्य लोगों को बचाने में मदद करता है और धोखेबाजों को रोकने में सहायक होता है।





इस गाइड का उपयोग किसी भी संदिग्ध कॉल, संदेश, या अनुरोध का मूल्यांकन करने के लिए करें। इन कदमों का पालन करें ताकि आप चेतावनी संकेत को पहचान सकें, जानकारी की पुष्टि कर सकें, और धोखाधड़ी से बचने के लिए सही कदम उठा सकें।

संदिग्ध कॉल्स, ईमेल्स,  
या संदेशों का मूल्यांकन  
करने के लिए इन कदमों  
का पालन करें:

क्या यह  
धोखाधड़ी  
है?



अनुरोध का  
मूल्यांकन  
करें



चेतावनी  
संकेत की  
पहचान करें



रुकें और  
सत्यापित  
करें



कार्यवाही  
करें



क्या वे भुगतान  
की मांग कर रहे  
हैं?

क्या वे आपकी  
व्यक्तिगत जानकारी  
मांग रहे हैं?

**अनुरोध का मूल्यांकन करें**

- अगर आपसे पासवर्ड, सोशल इंश्योरेंस नंबर (SIN) या बैंकिंग जानकारी मांगी जाती है, तो इसके प्रति सतर्क रहें। यह एक बड़ा चेतावनी संकेत हो सकता है कि कोई धोखेबाज आपके व्यक्तिगत डेटा को चुराने की कोशिश कर रहा है।
- गिफ्ट कार्ड्स या वायर ट्रांसफर के माध्यम से पैसे भेजने से बचें
- अगर अनुरोध भावनात्मक प्रतीत हो, तो पहले किसी और से सत्यापित करें
- थोड़ा रुककर यह आकलन करें कि स्थिति तात्कालिक या अप्रत्याशित महसूस हो रही है या नहीं, क्योंकि ठगी अक्सर दबाव का फायदा उठाते हैं।
- उदाहरण: आपका बैंक कभी भी फोन पर आपका PIN नहीं पूछेगा।

क्या वे आपको  
कार्रवाई करने  
के लिए दबाव  
डाल रहे हैं?

क्या कॉलर  
अजनबी है?

**चेतावनी संकेत पहचानें**

- ठगी कार्रवाई करने के लिए दबाव डालते हैं और देरी के लिए परिणामों की चेतावनी देते हैं।
- अज्ञात भेजने वालों या कॉल करने वालों से सतर्क रहें, जो धमकी या अत्यधिक मित्रवत व्यवहार का उपयोग करें।
- स्थिति को गुप्त रखने से मना करें—यह एक बड़ा चेतावनी संकेत है।
- जो ऑफ़र "बहुत अच्छे लगते हैं," जैसे कि लॉटरी जीतने का दावा, वे आमतौर पर ठगी होते हैं।

किसी  
विश्वसनीय  
व्यक्ति से पूछें

आधिकारिक  
चैनलों से संपर्क  
करें

धोखाधड़ी  
की रिपोर्ट  
करें

संपर्क समाप्त  
करें

**रुकें और सत्यापित करें**

- अपना समय लें; ठगी आपको जल्दी करने के लिए दबाव डालते हैं।
- संस्था से सीधे संपर्क करें, आधिकारिक नंबरों या वेबसाइटों का उपयोग करके।
- किसी परिवार के सदस्य, दोस्त, या समुदाय से सलाह लें।
- आनलाइन अनुरोध की जांच करें (जैसे, "CRA धोखाधड़ी" खोजें) ताकि आपको ज्ञात धोखाधड़ी के बारे में जानकारी मिल सके





## कृपया हमारी मूल्यांकन करें!

हमें बताएं कि आप क्या सोचते हैं।

आपकी राय हमारे लिए बहुत महत्वपूर्ण है। कृपया इस टूलकिट पर अपने विचारों के बारे में संक्षिप्त सर्वे पूरा करें:

स्कैम टूलकिट सर्वे

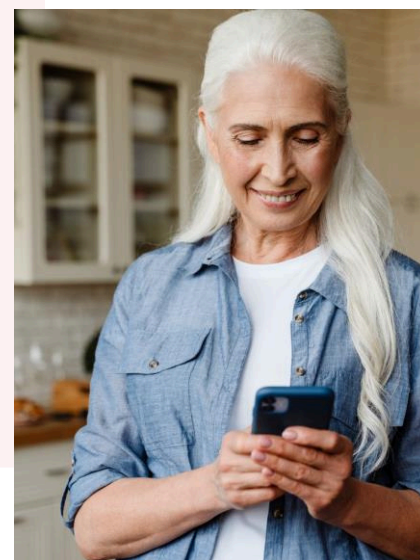
-

## आभार

हम अपने फोकस समूहों के सभी प्रतिभागियों का धन्यवाद करते हैं, जिन्होंने अपने समय और इस शोध में अमूल्य योगदान दिया। उनके फीडबैक के बिना यह टूलकिट संभव नहीं हो पाता। हम अन्सा तलत (कार्यक्रम समन्वयक) और ह्यूमन एन्डेवर का भी धन्यवाद करते हैं, जिन्होंने फोकस समूहों की व्यवस्था की।

## वित्तपोषण

इस टूलकिट के विकास और प्रकाशन को कनाडा सरकार के न्यू होराइजन्स फॉर सीनियर्स प्रोग्राम (NHSP) से प्राप्त वित्तपोषण ने संभव बनाया। इसमें व्यक्त किए गए विचार जरूरी नहीं कि वित्तपोषक के विचारों का प्रतिनिधित्व करें।



हमसे संपर्क करें!

✉ info@iwinca.ca

🌐 www.iwinca.ca

हमसे संपर्क करें और हमारी सदस्यता में शामिल हों!

वित्तपोषित:

Canada



अस्वीकृति

IWIN ने प्रकाशन के समय सही और अद्यतित जानकारी प्रदान करने का प्रयास किया है। हालांकि, इस संसाधन को वित्तीय और कानूनी सलाह के रूप में नहीं लिया जाना चाहिए। वित्तीय निर्णयों से संबंधित सभी निर्णय व्यक्तिगत विवेक पर निर्भर करते हैं। इस दस्तावेज़ में व्यक्त किए गए किसी भी विचार IWIN या उसके किसी साझेदार या वित्तपोषक की नीतियों या दृष्टिकोणों का प्रतिनिधित्व नहीं कर सकते।