Financial Intelligence Agency
BERMUDA

ALERT

Phishing and Vishing Scams Targeting the Elderly (Bermuda)

June 26, 2026

Introduction

This typology identifies a persistent fraud threat in Bermuda involving phishing and vishing (imposter scams) that primarily target elderly individuals. The activity combines social engineering techniques with remote access technology to bypass traditional banking safeguards and gain unauthorized access to victims' accounts.

In the reported cases, criminals impersonate legitimate institutions (e.g., banks or service providers), manipulate victims into granting device access, and gain the ability to execute fraudulent transactions directly from compromised accounts.

Financial abuse of seniors is a matter of significant public interest due to the need to protect older persons, one of Bermuda's most vulnerable populations, from financial exploitation. Through this typology, the Financial Intelligence Agency seeks to raise awareness of the risks and indicators of senior financial abuse, enhance its detection, and support preventative, investigative, and reporting efforts by financial institutions and other relevant stakeholders.

Modus Operandi (Execution Pattern)

This typology is informed by intelligence reported to the FIA, including **42 SARs/STRs** reported by all banking institutions in Bermuda during January 2023 and June 2026. The reported activity provides a focused view of how phishing/vishing scams affecting elderly persons are being detected, reported, and escalated within Bermuda's financial sector, and highlights the importance of broader vigilance across reporting entities.

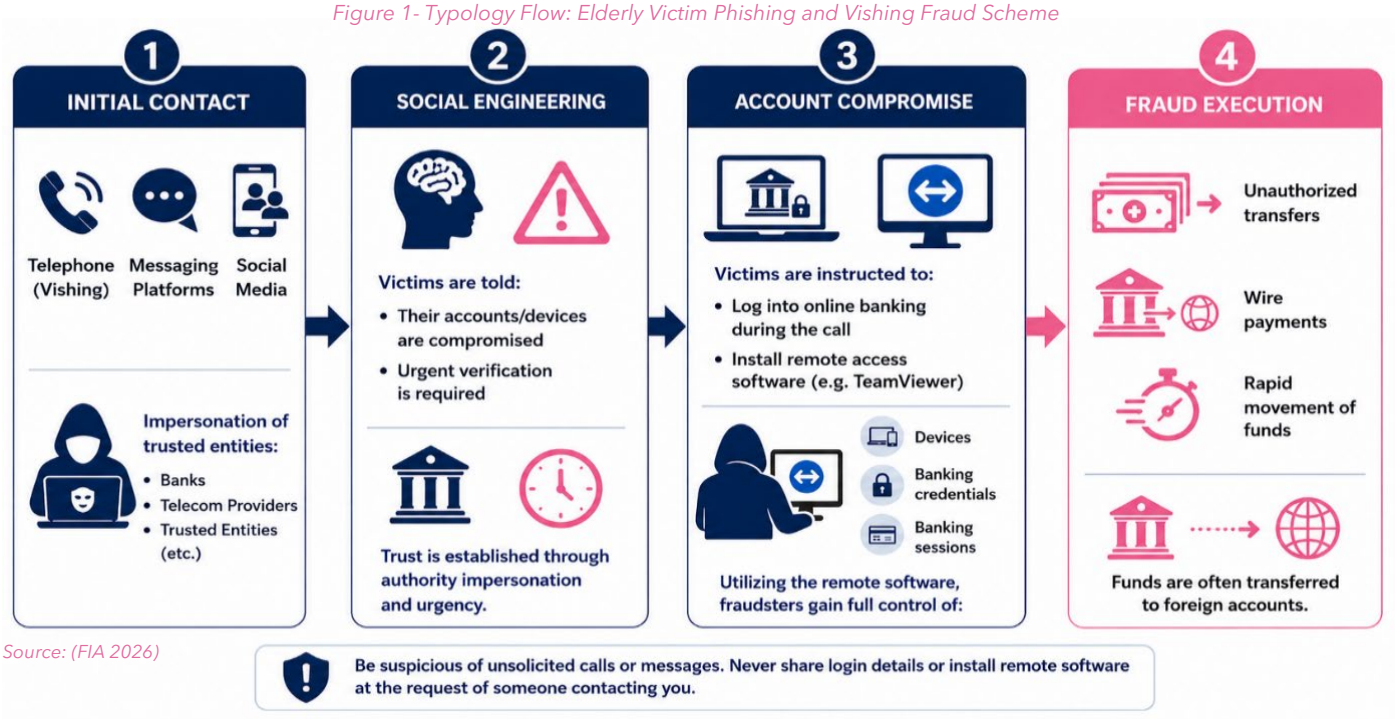
Analysis identified a recurring four-stage fraud scheme involving initial victim contact, social engineering, account compromise, and fraud execution, through which perpetrators impersonate trusted entities, gain unauthorized access to victims' devices and banking credentials, and facilitate the movement of illicit funds.

Stage 1: Initial Contact

- Fraudsters contact victims via:
  - Telephone (vishing) originating from domestic, international and unknown numbers through mobile/landline devices
  - Messaging platforms e.g. WhatsApp
  - Social media e.g. Facebook
- Perpetrators impersonate trusted entities (banks, telecom providers, technology support services, government or investigative agencies etc.).

In some instances, victims become willing participants in money mule activity after responding to fraudulent employment advertisements. These individuals receive what they believe are salary payments from fraudsters; however, the funds originate from elderly victims' accounts held at domestic banks.

Figure 1- Typology Flow: Elderly Victim Phishing and Vishing Fraud Scheme



Source: (FIA 2026)

Be suspicious of unsolicited calls or messages. Never share login details or install remote software at the request of someone contacting you.

Stage 2: Social Engineering

- Trust is established through impersonation of positions of authority and urgency.
- Victims were transferred on calls between multiple fraudsters. In some cases, victims communicate with fraudsters up to ten days.
- Victims are presented with one or more of the following situations:
  - Accounts/devices are compromised
  - Urgent verification is required
  - A driver's licence image is needed.
  - A standing order requires review.
  - Victims must call a number displayed in a pop-up message.
  - Funds must be transferred to another account.
  - An IP address issue has been detected.
  - A virus has infected the victim's computer.
  - Technical assistance is required.
  - Online banking registration is necessary.
  - Remote access software must be installed.
  - Online banking credentials or token codes need to be reset.
  - The bank's legitimate telephone number should be blocked.
  - Security codes generated from banking tokens must be provided.
  - The caller is part of an overseas investigation team.
  - Victims must assist in identifying rogue employees by performing "dummy" transactions.
  - Cash should be withdrawn and transferred through MoneyGram.
  - Charges relating to Amazon purchases or loans need verification.
  - Funds should be moved to a "safe account."
  - Demo or test transactions are required.
  - Victims' accounts are being used in money laundering investigations.

Stage 3: Account Compromise

- Victims are also often instructed to undertake one or more of the following:
  - Log into online banking during the call
  - Install remote access software e.g. TeamViewer
  - Delete pending transactions.
  - Provide account numbers and banking information.
  - Disclose login credentials.
  - Leave devices unattended after granting access.
  - Click malicious email links.
  - Permit funds to move through their accounts.
  - Make payments to release items allegedly held in the Bermuda Customs Department.
- Utilizing remote software, fraudsters gain full control of:
  - Devices
  - Online banking credentials and sessions
  - Active banking sessions

Stage 4: Fraud Execution

- Criminals are able to freely conduct:
  - Unauthorized transfers
  - Wire payments
  - Rapid movement of funds
  - Use of victims as witting or unwitting money mules.
  - Installation of firewall or remote management tools.
  - Control of accounts used to receive and transfer illicit proceeds.
  - Transfer of funds to foreign and domestic bank accounts shortly after account compromise
- Funds are often transferred to foreign and domestic bank accounts shortly after compromise
- Victims are often assured that:
  - The bank will replace any stolen funds.
  - Fraudulent transactions will be reimbursed.
  - Accounts will be protected from further loss.
  - Any conflicts that the victims have had with bank staff or family members with accounts at the same bank will be reviewed.

Key Characteristics

- Fraudsters engage victims via telephone calls, messaging platforms, or social media and impersonate trusted institutions, including banks or service providers.
- Impostors claim that customers' accounts or devices are compromised and require remote access for verification.
- Victims are persuaded to provide access to their online banking platforms through the installation of remote access software.
- This access allows criminals to take control of devices and accounts, facilitating unauthorised transactions, transfers, or wire payments and rapid depletion of funds under false pretences.

Overview of Identified Phishing and Vishing Fraud Case Characteristics

Common Characteristics of Elderly Victim Fraud Cases

CHARACTERISTIC	TREND
Victim Profile	
Age Range	65–93 years
Gender	Males & Females
Nationalities	Bermudian
Place of Residence	Bermuda
Notable Factors	• Elderly and vulnerable individuals • No indication of complicity (unwitting victims) • Some cases involve joint accounts • No powers of attorney or guardianships noted • Multiple persons transferred funds to the same beneficiaries and countries
Geographic Exposure	
Origin	• Bermuda
Destination of funds	• United States • Thailand • Hong Kong • Peru • Mexico • Romania
Linkages	• Foreign individuals, • companies, and • bank accounts
Remote Access Software utilised	
Software	• TeamViewer • AnyDesk • UltraViewer
Financial Impact	
Range of amounts stolen	• From BMD/USD 1500.00 • to BMD/USD 725,412.00
Transaction patterns	• 0–19 transactions per case • Some cases involved only attempted fraud. • Rapid depletion took place once access was gained.
Total recovered	• Unclear, as recuperated losses were not often quantified in reports. • Not all recall efforts successful
Timeline	
Fraud occurrence:	• August 31, 2021 – March 12, 2026
Reporting period	• January 1, 2023 – June 8, 2026

Source: (FIA 2026)

- Victims may be either unwitting or, in some cases, witting participants.
- Links were identified to foreign individuals, companies, and bank accounts, indicating broader international connections and cross-border financial activity.

Mitigating Measures

Preventative Controls

- Stronger transaction verification protocols
- Enhanced device authentication measures
- Real-time wire screening and blocking tools

Monitoring & Detection

- Behavioural monitoring for anomalies
- Identification of social engineering patterns
- Increased scrutiny for elderly client transactions
- Record value of funds recovered and unrecovered

Customer Protection

- Awareness campaigns targeting vulnerable populations
- Education on:
  - Phishing/vishing risks
  - Remote access threats
- Encouraging direct verification with banks
- Coordinating awareness efforts through the Bermuda Ageing and Disability Services.

Frontline Intervention

- Staff engagement when suspicious behaviour observed
- Escalation procedures for vulnerable customers

Takeaways

This typology highlights several key lessons for financial institutions, supervisory authorities, law enforcement, and other stakeholders involved in preventing and detecting elder financial exploitation.

- **Social engineering** remains the primary enabler of the fraud. Fraudsters establish trust through authority impersonation, urgency, and the appearance of legitimacy, often persuading victims that they are assisting a bank, service provider, or investigative authority.
- **Remote access tools** significantly increase the risk of account compromise. Once installed, these tools allow fraudsters to control victims' devices,

access online banking sessions, and execute transactions directly.

- Victims may **unknowingly facilitate their own compromise**. In several cases, victims approved transactions, shared credentials, installed software, or followed instructions without realising they were acting on fraudulent directions.
- **Early intervention by financial institutions is critical**. Behavioural monitoring, frontline questioning, transaction holds, recall attempts, and rapid suspension of online access can reduce losses where suspicious activity is identified quickly.
- Recovery outcomes are uncertain and **should be better recorded**. Not all recall efforts were successful, and reporting should more consistently capture attempted fraud, actual losses, recovered funds, and unrecovered funds.
- Money mule activity remains a key feature of the typology. **Fraud proceeds may be moved through domestic and foreign accounts**, including accounts held by individuals or entities that may be witting or unwitting participants.
- **Public awareness and direct verification are essential**. Elderly and vulnerable customers should be encouraged to verify suspicious calls, messages, or pop-ups directly with their bank using known contact channels before taking any action.

Conclusion

The analysis of the identified fraud typology highlights a highly coordinated and evolving scheme that relies on impersonation, social engineering, and remote access technologies to exploit vulnerable individuals, particularly the elderly. Across all cases, perpetrators systematically established trust, created urgency, and manipulated victims into authorizing actions that ultimately resulted in account compromise and significant financial loss. The consistency of execution patterns, coupled with cross-border fund movement and the use of money mules, underscores the sophistication and adaptability of these schemes, as well as the ongoing challenges faced in detection and prevention.

Moving forward, the insights derived from this information should support enhanced awareness, stronger preventative controls, and improved detection capabilities across financial institutions and related stakeholders. It is essential that suspicious activity is reported promptly, as early intervention can significantly reduce financial losses and disrupt fraud networks. Equally important is the need for continued public education and vigilance, particularly regarding the protection of personal and banking information, cautious engagement with unsolicited communications, and verification of any requests involving financial transactions. Strengthening collective awareness and encouraging timely reporting will be critical in reducing the impact of these fraud schemes and safeguarding vulnerable populations in Bermuda.

-END-

Statistical Disclaimer:

The report's statistics are based on SARs and STRs submitted to the FIA between January 1, 2023 – June 8, 2026. These reports reflect suspicions from reporting entities and do not confirm the existence of criminal activity. The data is intended for analysis and may change as new information or investigations arise. While reasonable steps are taken to ensure accuracy, the FIA relies in part on information provided by reporting entities and other third parties and cannot independently verify all underlying data.

Disclosure-2615-26 (PROJ0001-2025)