Cyber Fraud Economics, Scam Types and Potential Measures to Protect U.S. Seniors: A Short Review

Niroop Sugunaraj, Akshay Ram Ramchandra, Prakash Ranganathan
School of Electrical Engineering and Computer Science (SEECS)
University of North Dakota
Introduction
Source: statista.com, 2021

• Steady rise in internet users.
• Increase in users of all age groups.
• Under 20% to over 70% since 2000.

Fig. 1: Number of internet users by year globally.

Fig. 2: Number of internet users by year - USA

Fig. 3: Percent of user age group by year.
Elder Fraud

Source: IC3 elder fraud reports, 2021

• Illegal or improper use of an older adult’s funds, property or assets.

• 21.5% of frauds account to elders.

• 92k + victims in 2021.

Fig. 4: 2021 Reports of Fraud by Age Group.
Elder Fraud Statistics
Source: IC3 elder fraud reports 2021

Total number of victims over 60 years of age, by year

Fig. 5: Total number of victims over 60 years age, by year by year
Scam Types

Source: IC3 elder fraud reports, 2021

![Bar chart showing scam types by number of victims - Over 60 years of age](image)
Fig. 10: Top 5 Scams by total loss – over 60 years of age

Source: IC3 elder fraud reports, 2021
Sophistication in Scams

Fraudulent activities have achieved a degree of sophistication:

1. **Fake notifications impersonating corporations such as USPS, UPS, Amazon, and FedEx (Raybould, 2021).**
2. **Counterfeit admission tickets to high-profile events such as concerts.**
3. **Celebrity impersonators who ask for personal information to deliver “gifts” (Witman, 2019).**
4. **Artificial intelligence (AI) to mimic voices/faces to solicit money (Brewster 2021) or confidential data.**
5. **Evasion of detection tools such as Google Safe Browsing (Raybould 2021).**
6. **Social Engineering**
7. **Fraudulent Online Surveys**
Typical Mediums and Signs of Elder Fraud

Urgent requests or threats:
- Urgent and pressurizing requests for money transfer? Sounds like a classic scammer's tactic.
- Email or SMS asking you to verify personal information over the phone.

Bogus activity:
- Unexpected charges, checks, or credit cards transactions you didn't initiate.
- Really good offers for prizes and gifts; it's likely too good to be true.

Fig. 11: Mediums/Vectors of Elder Fraud.
Tech Support

Source: IC3 elder fraud reports, 2021

Medium:
• Pop-up.

Fraudulent transactions are made by:
• Wire transfer to overseas accounts
• Prepaid cards
• Mail cash

Methods of execution:
• Impersonate well-known companies
• Offer support for non-existent problems

Fig. 12: Total loss by tech support per year.
Romance/Confidence

Source: IC3 elder fraud reports, 2021

Medium:
- Voice call
- SMS
- Email
- Social Media

Fraudulent Transactions are made by:
- Wire transfer to overseas accounts
- Mail cash

Methods of execution:
Romance:
- Assume fake identity
- Gain trust
- Extort

Confidence:
- Panic calls at odd hours

Fig. 13: Total loss by confidence/romance per year.
Sweepstakes
Source: IC3 elder fraud reports, 2021

**Medium:**
- Letters
- SMS
- Email
- Voice calls
- Social Media
- Wire transfer to overseas accounts
- Mail cash

**Fraudulent Transactions are made by:**
- Wire transfer to overseas accounts
- Mail cash

**Methods of execution:**
- Congratulate on winning a fake contest
- Ask victim for payment to claim prize

![Total loss by Sweepstakes/Lottery scams by year](Fig. 14: Loss by lottery scams per year.)
Phishing/Impersonation

Source: IC3 elder fraud reports, 2021

Medium:
- Letters
- SMS
- Email
- Voice calls
- Social Media

Fraudulent Transactions are made by:
- Wire transfer to overseas accounts
- Mail cash
- Prepaid cards

Methods of execution:
- Pretend to be a government official
- Make physical / Financial threats

Total loss by Impersonation scams by year

Fig. 15: Loss by phishing/impersonation scams per year.
Investment

Source: IC3 elder fraud reports, 2021

Medium:
- Letters.
- SMS.
- Email.
- Voice calls.
- Social Media.
- Mail cash
- Prepaid cards.

Fraudulent Transactions are made by:
- Wire transfer to seas accounts
- Methods of execution:
  - Foster trust.
  - Target similar groups.
  - Offer little to no risk for high returns.

Fig. 16: Loss by investment scams per year.
Prevention/Mitigation

1. **Setting “healthy” passwords**
   - Upper case/lower case alphabets, numbers, and special characters.
   - At least 12 characters long.
   - Unique and non-personal.

2. **Multi-factor authentication (MFA)**
   - Two or more authentication methods.
   - Biometric/token based.

3. **Antivirus software**
   - Scans computers to keep them free from malicious software.
   - Keeps itself updated with latest rules for detection.

4. **Pop-up blockers**
   - Safe browsing.
   - Browser extensions.

5. **No caller ID apps**
   - Detects reported scam/spam callers.
   - Examples: TrueCaller, Eyecon.

6. **Federal Trade Commission Blacklists**
   - Helps restrict tele-marketing calls.
<table>
<thead>
<tr>
<th>Organization</th>
<th>Service Type</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office for Victims of Crime (OVC)</td>
<td>Helpline</td>
<td>Assists older adults with reporting crimes.</td>
</tr>
<tr>
<td>Internet Crime and Complaint Center (IC3)</td>
<td>Reporting</td>
<td>Collects reports on internet crime.</td>
</tr>
<tr>
<td>Federal Trade Commission (FTC)</td>
<td>Reporting</td>
<td>Steps to take by which one can get back their money.</td>
</tr>
<tr>
<td>National Center on Elder Abuse (NCEA)</td>
<td>Assistive</td>
<td>Deals with 6 type of elder abuse, including financial abuse. Can conduct investigations in as little as 24 hrs.</td>
</tr>
<tr>
<td>Office of Inspectorate General (OIG)</td>
<td>Reporting</td>
<td>Scams or crimes typically reported to the SSA. impersonation, misuse of SSN by terrorist groups/activities.</td>
</tr>
</tbody>
</table>
References


References


statista.com (2022)

IC3 elder fraud reports https://www.ic3.gov/
Questions