Avast Safe Tech Report

Avast Report Reveals Why Families Must Flip the Script on Cyber Safety

Global Results

"People of all generations are having a harder time spotting scams without help these days as technology becomes more advanced and threats more convincing. Helping our parents and grandparents stay safe online starts with open conversations. Talk with your loved ones about how to practice safe tech and establish a buddy system to check suspicious requests and messages before taking action. Sometimes a quick check in with someone you trust can be all it takes to stop a scam in its tracks."

Leyla Bilge,
Global Head of Scam Research for Avast

"Empowerment - with tools, knowledge and support - is your strongest defense against today's scams and cyber threats."

Practice Safe Tech:

• **Strengthen Password Habits:** Encourage your loved ones to use long, complex passwords across all of your accounts – 15-20 characters with a mix of letters, numbers, and symbols. Avoid using personal information, don't keep passwords written down on paper, and consider using a password manager.

• **Spot the Red Flags:** Tell them to be cautious with unsolicited emails, texts, or calls claiming to be from banks, Medicare, or tech support. Scammers often create a false sense of urgency to trigger quick action.

• **Know the Common Scams:** Talk through the scams they're most likely to encounter, such as phishing, tech support hoaxes, romance scams, grandparent scams, fake software updates, and Medicare fraud.

• **Set Up Smart Safety Tools:** Help install security software, a secure browser and tools like Norton Genie and Avast Scam Guardian that flag suspicious content. Make sure devices and apps stay updated.

• **Make Cyber Safety a Team Effort:** Establish a family safe word so they can make sure it's really you calling and not someone impersonating you. Create a "phone-a-friend" plan for anything that feels off.

Summary of Key Insights

**1.** **Old-School Password Storage is Still Alarmingly Common**

52%

of older adults still write their passwords down on a piece of paper, according to their younger loved ones.

Even more concerning, only **14%** are believed to use a password manager, while **23%** reuse the same password across accounts, **14%** store passwords in notes or documents on their devices and **9%** save them in texts or emails – practices that significantly increase the risk of account compromise.

**52%**

48%
54%
57%
55%
63%
47%
57%
44%
62%
41%
44%
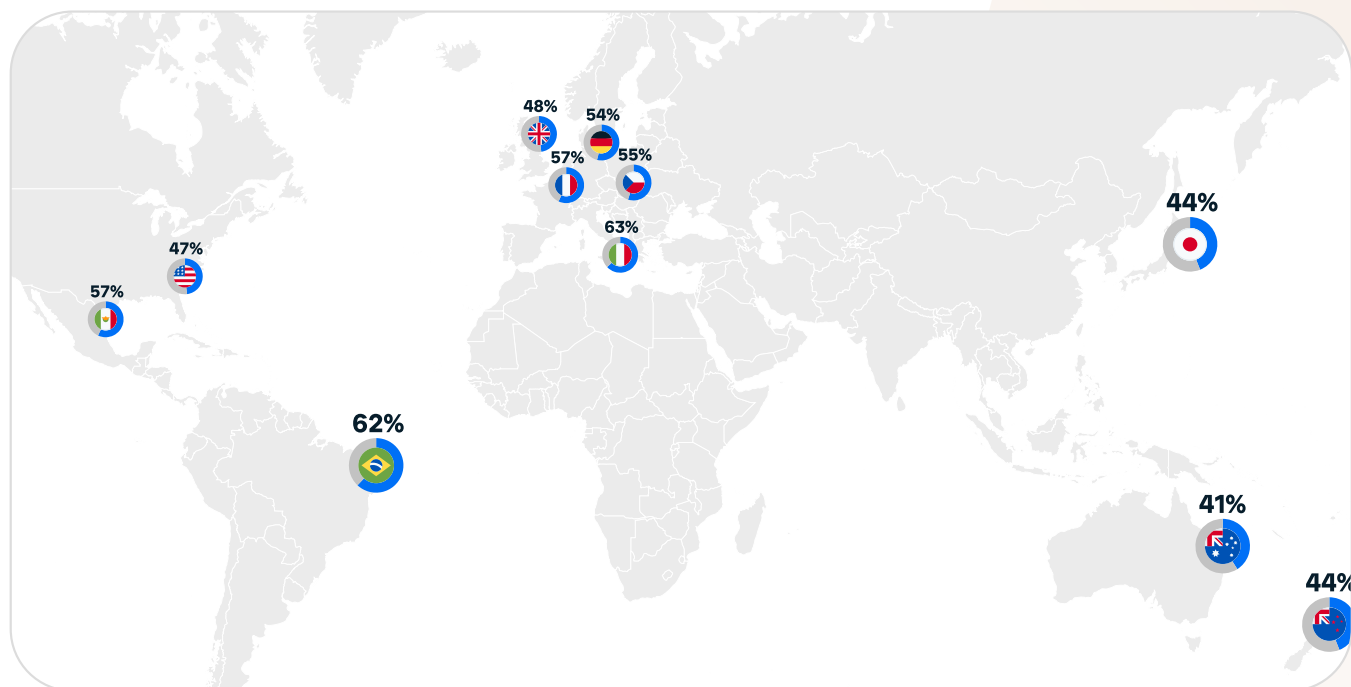
Despite living in an age of biometric logins and password managers, many older adults still rely on pen and paper to store their credentials, according to younger loved ones. From 41% in Australia to over 60% in Italy and Brazil, the habit

persists across continents—highlighting a global tension between digital security best practices and the comfort of analog methods. These patterns reflect deeper cultural attitudes toward technology, trust, and habit change.

## 2. Over Half of Older Adults Have Fallen Victim to Online Threats

51%

of people with older loved ones said their elders have fallen victim to online threats ranging from scams **(25%)** and financial fraud **(18%)** to data breaches **(15%)**, malware infections **(15%)** and even identity theft **(10%)**. These numbers reveal just how vulnerable older adults are in today's digital world – and why proactive cyber safety measures are more important than ever.

50%

0%

25%	18%	15%	15%	10%
Scams	Financial Fraud	Data Breaches	Malware Infections	Identity Theft

![Avast logo] Avast
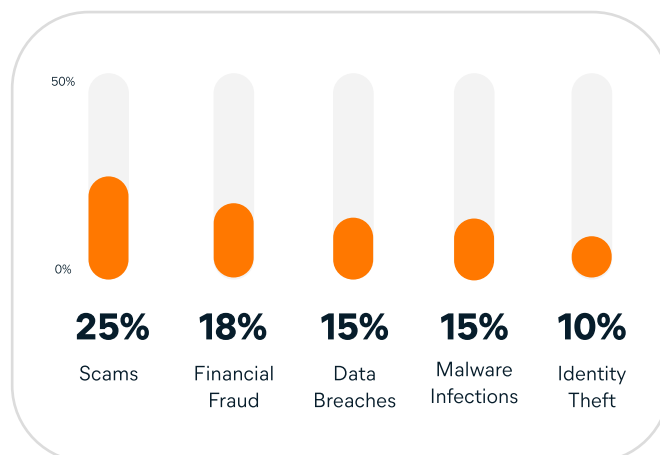
Some of the most common scams targeting older adults are:

- **Tech Support Scams** – Pop-up calls claiming a virus is on the device.
- **Phishing** – Emails or texts pretending to be from legitimate organizations like banks or Medicare.
- **Fake Invoice Scams** - Fake payment requests, often imitating legitimate companies or service providers
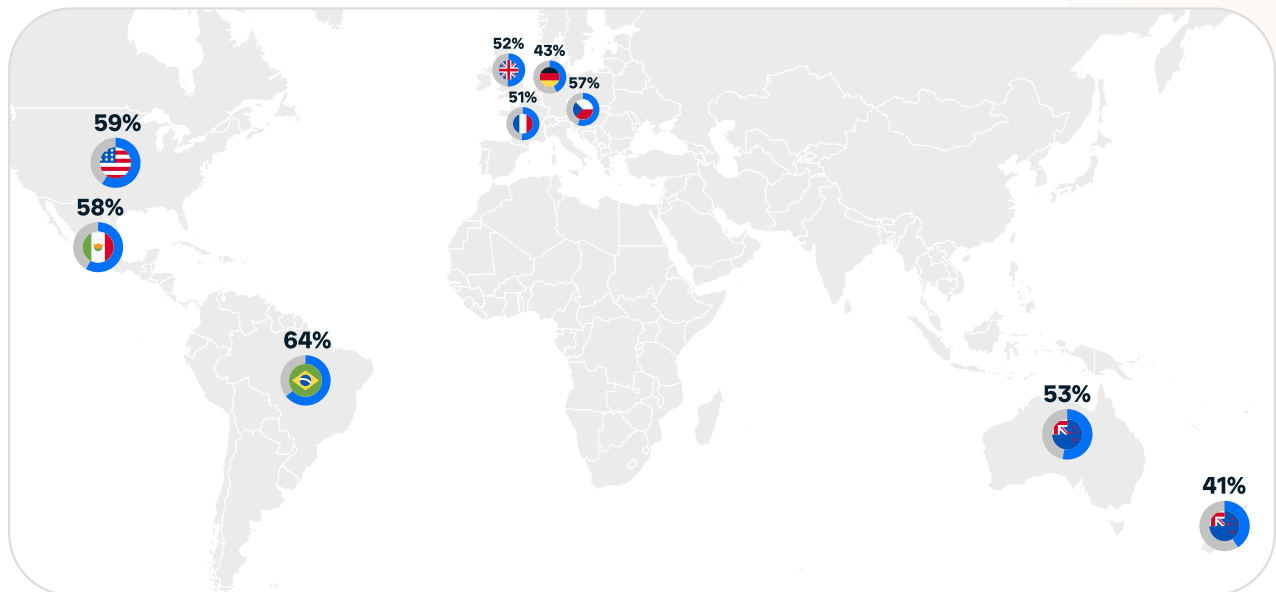
Cybercrime isn't just a local problem – it's global too. Across the globe, older adults are falling victim to online threats at alarming rates—but how often it happens, and why, varies by region. From cultural attitudes toward technology to differing levels of digital literacy, the data reveals a powerful story about how scams exploit generational and regional gaps in cyber awareness.

3. People Are on High Alert for Senior Scam Risks

74%

say they're concerned their older loved ones could fall victim to an online scam, reflecting ongoing concerns around online risks. This concern speaks to the perceived vulnerability of older adults and the increasing importance of family involvement in online safety.

4. Confidence in Scam Response Remains Low

Only 35%

of people say they definitely know what to do if they fall victim to a scam – highlighting the major gap in digital preparedness.

5. Helping Seniors Online is More Dreaded Than the Dentist For Some

19%

of consumers with older loved ones say they'd rather go to the dentist than help them navigate the internet – a clear sign of how challenging and frustrating these tech support moments can be.
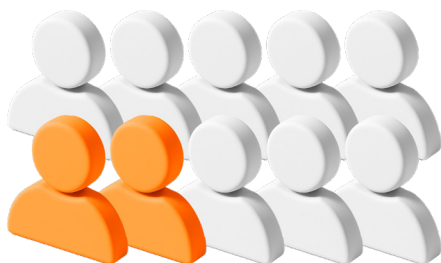
Key takeaways

Cyber safety isn't a one-time lesson– it's an everyday habit. Just like locking your doors or testing your smoke alarms, staying safe online should be second nature. Make it a family priority: schedule regular tech check-ins, be the trusted source for guidance and remind your loved ones – there's no such thing as a silly question when it comes to staying safe online, only missed chances to protect yourself.

Avast

6. Younger Generations See Red Flags in Older Adults' Digital Behavior

36%

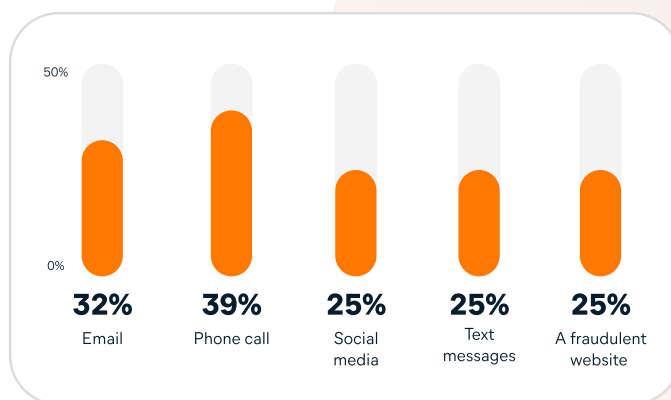of people believe their older loved ones' online behavior is risky, pointing to these specific habits:

- **73%** say they click on **suspicious links**
- **59%** say they **answer calls from unknown numbers**
- **54%** say they **overshare personal information**
- **49%** say they **respond to texts from unknown numbers**
- **45%** say they **use weak passwords**
- **44%** say they **download unknown apps**

7. Phone Calls Are a Top Way Scammers Reach Older Adults

While scams can strike through emails texts and social media, phone calls remain one of the most common entry points for fraud and identity theft. Its familiarity – and frequent use – makes it an especially effective tool for scammers looking to exploit trust and trick victims into clicking.

32%	39%	25%	25%	25%
Email	Phone call	Social media	Text messages	A fraudulent website

8. Talking with older loved ones about their online safety can be a real challenge.

84%

Of adults have tried talking to their older loved ones about risky online behaviors or scams. Many who believe their older loved ones engage in risky online behavior are sounding the alarm - warning them about clicking suspicious links

(85%), answering unknown calls **(80%)**, oversharing personal information **(78%)** and responding to random texts **(77%)**. They are also cautioning against downloading unknown apps **(73%)** and using weak passwords **(68%)**, highlighting a widespread effort to help protect older adults from scams and digital threats.

84%

9. **Despite Warnings, Almost Half of Older Adults Aren't Listening.**

Only 52%

of older adults who were warned by younger loved ones about online risks changed their habits.

Among younger adults who offered online safety advice to older loved ones, **16%** said their advice wasn't understood, **13%** reported their older loved ones said they'd change but didn't, **11%** said their concerns were dismissed as overreacting and **3%** said their older loved ones simply ignored them – highlighting the challenges of bridging the generational gap in online safety.

52%

10. **Gen Z Steps Up to Protect Older Generations Online**

69%

of Gen Zers have helped their older loved ones avoid scams. As digital natives, Gen Z is stepping up, helping protect their parents, grandparents, and more with warnings about scams, suspicious links and risky behavior.

69%

11. Digital Know-How is a Family Affair

Nearly

1/3

(27%) of people with older loved ones have taught them something about staying safe online within the past week – proving that digital security is becoming a regular, real-time conversation across generations.

12. When Scams Strike, Loved Ones Step In

85%

of family members have stepped in to help older loved ones recover after falling victim to a scam.

This support came in many forms – **56%** guided them through what steps to take, **49%** reported the scam to authorities and **35%** contacted financial institutions on their behalf. Some even went further, with **15%** helping cover financial losses and **14%** attempting to track down the scammer. of family members have stepped in to help older loved ones recover after falling victim to a scam.

85%

56%	49%	35%	15%	14%
Guided through steps	Reported the scam	Contacted financial institutions	Covered financial losses	Tried to track the scammers

"As online threats become more sophisticated, it's vital that we treat cyber safety as a shared responsibility across generations. A simple conversation can help prevent a devastating scam and empower families to navigate the digital world more confidently together."

Jorij Abraham,
Managing Director of the Global Anti-Scam Alliance (GASA)

avast.com