Help Protect Your Customers Against Generational Fraud

cyber security fraud protection Gen Z

Summary: While fraudsters will try any and all methods across every generation, certain practices for each generation typically bear the most fruit. CFIs should be aware of the types of online fraud that each generation is most susceptible to, then educate their customers on ways to not fall prey.

Bestowing catchy names onto generations is a relatively new phenomenon. A century ago, Gertrude Stein coined the term “Lost Generation,” for those who lost their lives during World War I. But it wasn’t until 1991 with the book “Generations,” by Neil Howe and William Strauss that naming generations became popular. Most of the names that the theorists coined stuck, such as baby boomers.

Now, generation names are routinely used in research, not only for marketing, but for pretty much any way an organization relates to both employees and customers. This includes determining how fraudsters might target each generation within a financial institution’s customer base.

Fraud Traps by Generation

Depending on whether you’re a baby boomer, Gen Xer, Millennial, or Gen Zer, fraudsters are finding ways to lure you into their trap based on your generation’s habits and preferences.

Baby boomers, for instance, are susceptible to robocalls about healthcare, taxes, or social security. Older people without companionship are also liable to fall prey to catfishing scams — more so than younger generations. Baby boomers tend to use Facebook far more than Gen Z — only 32% of teens between 13 and 17 use Facebook — so they are more likely to openly talk about relationship woes that leave them vulnerable to romance scams on the site.

The younger generations can often be lured by instant gratification tactics. Fraudsters send them ads for illegitimate products and services. Users then unwittingly grant access to the fraudster, who subsequently demands money from them.

Gen Z is also particularly susceptible to fraud tactics through social media and chatbots. Millennials, on the other hand, are vulnerable to phishing through targeted text messages that disguise themselves as shipment tracking or other automated messages.

The Cost of Generational Fraud

According to a report by fraud prevention firm SEON, Gen Zers saw the largest increase of any generation for online fraud victimization from 2019 and 2020. Perhaps not surprisingly, baby boomers with more established incomes suffered the highest losses. There was a 116% increase in online fraud victims under 20 during that time — more than any other generation. Their collective losses totaled about $70.98MM in 2020, or about $3K per person. For 20- to 29-year-olds, the average loss was $2,789. On the other hand, people between the ages

of 50 and 59 suffered the most, with an average loss of $9,864, with those 60 and older following close behind with an average loss of $9,174.

How to Protect Your Customers

Here are some ways that your institution can help **keep customers from falling prey to online fraud** — no matter their age.

Technology. Your institution can employ machine learning to analyze customer transaction data to determine whether there are patterns of online fraud within each generation. For example, if your institution has more baby boomer customers than younger customers, you might be on the lookout for tactics such as lottery and sweepstakes scams or spoofing scams, compared to student loan scams that typically target younger generations.

To minimize customers getting lured in by fake ads, particularly the younger generations, your institution should encourage strong security methods like multifactor authentication or biometrics whenever possible. You should also verify links and sites before exchanging any account details, as well as the identity of the person or entity that is part of the financial transaction.

Education. Let your customers know about the various types of fraud that they may be most susceptible to and how to avoid becoming a victim of an attack. You can instruct them what signs to look for that an email or ad or phone call is fraudulent.

These cautionary steps will help strengthen your institution's relationships with your customers and position your CFI as a trusted partner in the event that fraud does happen. Financial institutions should be transparent and communicative about why customers are experiencing a certain degree of friction with access or transactions, and continuously introduce new techniques to educate and increase customer awareness.

New methods for generational fraud are something that your institution must be constantly monitoring. Make sure you are mitigating the potential for attacks by employing technology and educating your customers.

YOUR TRUSTED PARTNER FROM COAST TO COAST

PCBB provides high-quality, competitively-priced solutions with personalized service. Designed to help community financial institutions thrive, our services include: cash management, international banking, lending, and advisory services. Contact us to learn more.

ECONOMY & RATES

Rates As Of: 02/01/2023 08:14AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	4.70	0.28	0.28
6M	4.80	0.04	0.04
1Y	4.66	-0.01	-0.05
2Y	4.20	0.00	-0.22
5Y	3.60	-0.02	-0.40
10Y	3.50	-0.01	-0.38
30Y	3.63	0.00	-0.34

FF Market	FF Disc	IORB
4.33	4.50	4.40
SOFR	**Prime**	**OBFR**
4.31	7.50	4.32