Educating Customers on the Risks of Gaming Platforms

cyber security business customers digital banking customer experience

Summary: Online gaming platforms have become extremely popular in recent years, with 76% of children under 18 playing regularly and connecting their parents' credit cards and bank cards to their gaming accounts. Financial education about the risks of online gaming payments can add value for young and older customers alike.

Anyone who attended school between 1930 and the end of the 1970s undoubtedly had "Fun with Dick and Jane" books. Dick and Jane, along with their younger sister Sally and their dog Spot, helped generations of children learn by memorizing sight words, with a single new word introduced on each page and no more than five new words in any story. The characters engaged in typical daily childhood activities and the stories became increasingly sophisticated as young readers aged, with the series spanning from beginning readers through ninth grade.

Dick and Jane have been replaced by countless characters in other "I Can Read" books over the decades. While there is no shortage of material available for teaching kids how to read, there is a need for teaching materials for another kind of literacy: financial. Many parents overlook the need to teach children about finance, which can be dangerous in a world where most children play online video games that are linked to their parents' credit cards and bank cards. Community financial institutions (CFIs) can add value for their customers by assisting with financial literacy for children to reduce the risks of online payment fraud.

The Risks of Online Gaming

Video games, particularly online games where people can engage with other players across the globe, have become extremely popular in recent years. These games gained additional traction during the onset of the COVID-19 pandemic, when children could not attend school or play with friends in-person. As of July 2021, 76% of children under 18 years old regularly play video games, according to the Entertainment Software Association. But kids aren't the only people playing games online — 90% of current video game players are over 18 years old. Enabling children to connect to friends and strangers (many of whom could be adults or cybercriminals) in online gaming platforms exposes them to the same risks that adults face online. The financial risks of these activities are hacking and identity theft. Unfortunately, criminals are well aware of the lack of supervision and children's susceptibility in online games, and are more than willing to take advantage of this factor.

According to a recent survey commissioned by Lloyds Bank, 31% of parents of children between the ages of 6 and 15 feel helpless when it comes to protecting their kids from gaming fraud. While 36% of parents are worried about their own finances being tied to such games, 55% of them have linked their credit or debit cards to their children's gaming accounts anyway. Of that group, 25% don't employ any security measures to protect their kids or their personal information. Another 77% of parents allow their children to play online games unsupervised. Not surprisingly, 10% of children have been victims of gaming fraud, and that percentage is expected to rise.

Financial Literacy

The prominence of online gaming and the associated increasing risks for financial fraud offer an opportunity for CFIs to provide financial education for both kids and their parents. These efforts can not only help cement relationships with existing customers, but can also be a way to foster ties and build brand loyalty with the children who will become future customers.

Since the survey found that 38% of parents do not feel they would be able to explain gaming fraud and the risks to their children and 25% don't know how to protect their kids, it is safe to assume that parents will embrace outreach from CFIs regarding online gaming fraud education. Reaching children early with financial education is also important, as recent studies have found that younger generations are far less knowledgeable about finances than their older counterparts.

Reaching Out

CFIs should pursue multiple channels of outreach to educate consumers about the risks of online gaming, from webinars to in-person seminars at local branches. In fact, in-person gatherings are a good way to provide more personal interactions for younger consumers, many of whom are only familiar with online banking services.

Another way to nip the gaming financial literacy problem in the bud is to partner directly with gaming companies. For example, upon seeing the results of their study, Lloyds Bank sought a partnership with Ukie, the UK's trade body for the gaming and interactive entertainment industry. Together, the companies created educational materials to help parents gauge their awareness of online gaming security risks. Some financial institutions are partnering with organizations such as financial literacy app Zogo to put together educational offerings.

If your CFI plans to reach out to customers to educate them on the security risks of online gaming, here are a few things to keep in mind:

- Parents should educate themselves on any **parental controls** available on the games their children play, impose limits on spending, and monitor their children's activities.
- Chat features are one of the most popular ways that hackers target children, so it is important to educate kids about **the risks of revealing information to anyone** they don't know or clicking on links. Scammers also frequently impersonate in-game support and use traditional phishing emails related to gaming or event texts.
- Usernames and **passwords on gaming accounts should be unique** from all other accounts, as cyberattacks often look to gain these details in hopes that people use the same credentials for other accounts.
- Some gaming platforms provide "scrubbing" within their chat functions, which **monitors specific language and blocks links**.
- Parents should actively **monitor their credit cards** for any suspicious activity, particularly any purchases within their child's gaming account.
- Parents should ensure there is **up-to-date antivirus software** installed on the devices used for gaming to minimize hacking risks. To take it one step further, some antivirus programs offer **identity protection or VPN** capabilities to make connections more secure.

CFIs that provide financial literacy on online gaming risks for both their customers and their customers' children can help customers identify knowledge gaps and subsequently lower the risk of their children

becoming victims of online gaming fraud. This can strengthen the relationships CFIs have with their customer bases and build trust with future generations of consumers.

BANKING OUT LOUD: EXTRAORDINARY SALES RESULTS

Check out PCBB's latest podcast, Extraordinary Sales Results: Tips, Mistakes, The Value Equation. The creator of The Value Equation joins us to discuss his sales technique aimed at creating a pathway to extraordinary sales results. You'll hear three tips to boost success at your institution, and three mistakes to avoid.

ECONOMY & RATES

Rates As Of: 09/12/2022 11:55AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	3.08	0.12	3.02
6M	3.52	0.20	3.33
1Y	3.65	0.15	3.26
2Y	3.57	0.08	2.84
5Y	3.46	0.11	2.20
10Y	3.36	0.17	1.85
30Y	3.51	0.22	1.61
FF Market	**FF Disc**		**IORB**
2.33	2.50		2.40
SOFR	**Prime**		**OBFR**
2.28	5.50		2.32