Wealth Management (A Special Report) --- Get-Rich-Quick Schemes That Target Young People Online Proliferate: Many scams can seem surprisingly legitimate to those who spend a lot of time on social media

Narula, Svati Kirsten . Wall Street Journal , Eastern edition; New York, N.Y. [New York, N.Y]. 15 Nov 2021: R.1.

FULL TEXT

LaNiah Moon had just moved out of her college dorm and into her parents' house in February when she received a direct message on Instagram from a woman named Maya, offering her an opportunity to "make some quick cash." Ms. Moon, 22 years old, had lost her on-campus job the year before when the Covid-19 pandemic began, and was taking classes remotely from home in Chicago while also looking for a job. She says Maya told her that if she gave her $150, she could "flip" it into $1,500.

Although Ms. Moon was a bit skeptical, she says that Maya had several thousand followers on Instagram, including a "mutual" -- someone Ms. Moon also followed -- which gave the woman's profile an air of legitimacy. She also saw pictures of Maya posing on top of a car and says that vision of success played a role in her gullibility.

"I think I was just really, really vulnerable at that moment," says Ms. Moon. "I thought, 'I'm going to just send this and see where it goes.' " Ms. Moon sent the money via a mobile-payment service.

The cash-flipping scam Ms. Moon fell for is one of dozens of ways that swindlers steal money from young adults after first approaching them on social-media platforms. While such scams have been proliferating for years, there was a sharp uptick in 2020 as people started spending more time online amid the pandemic.

Cybersecurity experts say millennials and Generation Z are particularly susceptible to these scams because social media is so integral to their lives. More than older generations, they use these platforms to forge relationships, gather information, shop, espouse political views, conduct business and more. A strong sense of familiarity lends legitimacy to everything they do and see on these platforms -- and swindlers know how to take advantage of this.

The lightning speed with which money can be exchanged also puts young people at risk -- they often realize they've been scammed mere minutes after a transaction they can't undo.

A young adult may not fall for the email from the prince promising them money, says Alethe Denis, a cybersecurity consultant and social engineer who studies how psychological manipulation can lead to security breaches, but "what they're maybe not considering is that somebody who is in their direct messages on LinkedIn promising a job that sounds too good to be true" also can't be trusted.

Today's most common scams fall into three categories: online-shopping deals and product giveaways in which the goods are never delivered; offers of free cash or too-good-to-be-true investment opportunities, sometimes involving cryptocurrency; and fabricated romances, says Satnam Narang, a research engineer at the cybersecurity firm Tenable who has been studying social-media scams since 2007. No platform is exempt from these schemes, he says.

Brand or celebrity impersonation is at play in many of these cases, says Mr. Narang, adding that a direct message on Twitter from someone impersonating a celebrity that says, "You've won my Cash App giveaway!" could look

legitimate at first glance.

The use of hashtags on social media can make it particularly easy for bad actors to target a certain audience, says Jane Lee, a fraud-prevention adviser at digital fraud-prevention firm Sift. Scammers, for example, can use a hashtag like #fashion or #cybermonday to tailor malicious posts for people who are following those topics.

It can be particularly easy to manipulate users with personal information, such as where they go to school, what their goals are, and who they spend time with -- all information that young people share freely on their social-media profiles. "Scammers succeed by approaching a victim with information about the individual that engenders trust that the scammer is legitimate," says Linda Miller, an antifraud risk manager and principal at Grant Thornton, an accounting firm in Washington, D.C.

The rise of social-media influencers and content creators is another overarching factor in the proliferation of scams targeting young people online, cybersecurity experts say. Young people see social media as a legitimate place to run a personal business, and scammers take advantage of this by offering to help them gain followers or land endorsement deals.

So what can be done? Ms. Lee advises people to closely scrutinize the profiles of users they're interacting with for the first time. Instagram, Facebook, Twitter and TikTok "verify" certain users by appending blue check marks to their usernames to signal that their identities have been confirmed.Ms. Lee also suggests reviewing the historical content posted by the user in question. "Real users are more likely to have a history of organic posts, while fake accounts often appear to be newly created, solely for the purpose of posting scams or monetizing content," she says.

Stacey Wood, a psychology professor at Scripps College in Claremont, Calif., who discusses fraud with her students, says they tell her that when they receive a direct message on Instagram from someone they don't know, they immediately check the "bio" of the sender. One marker of authority is the number of followers, Prof. Wood says, though her students note that bots are often employed to increase that number artificially.

One solution, Prof. Wood says, might be a tech one such as "adding a flag, or indicator of risk -- like I get email banners warning me of suspicious emails."

Michal Strahilevitz, a marketing professor at St. Mary's College of California who studies behavioral economics, says the most effective way to combat such scams is education. Young adults especially don't like being tricked or cheated by "older people who are assuming they are naive and less bright due to being younger," he says. So educating them on how to spot a scam, as well as the risks of sharing their private information online, "can be very impactful," he says.

Content creator Samantina Zenon, age 31, was just trying to grow her business when a fake marketing agency reached out to her offering to help her gain 100,000 new followers and a blue verification check mark on Instagram. The agency had a website touting partnerships with several major beauty brands, including brands that Ms. Zenon knew.

Ms. Zenon signed a contract and sent $1,500 to the marketing agency through Venmo, and never heard from anyone at the agency again. The agency's website disappeared soon after, and Ms. Zenon discovered that the address on the contract she signed was nothing more than an empty parking lot.

Her hard-earned lesson: "If it sounds too good to be true, most likely it is," she says.

Ms. Narula is a writer in Santa Fe, N.M. Email: reports@wsj.com

Credit: By Svati Kirsten Narula

DETAILS

Subject:	Young adults; Marketing; Legitimacy; Mobile commerce; Celebrities; Computer security; Pandemics; Social networks; COVID-19; Fraud; Series &special reports; Wealth management
Business indexing term:	Subject: Marketing Social networks Wealth management
Publication title:	Wall Street Journal, Eastern edition; New York, N.Y.
First page:	R.1
Publication year:	2021
Publication date:	Nov 15, 2021
Publisher:	Dow Jones &Company Inc
Place of publication:	New York, N.Y.
Country of publication:	United States, New York, N.Y.
Publication subject:	Business And Economics--Banking And Finance
ISSN:	00999660
Source type:	Newspaper
Language of publication:	English
Document type:	News
ProQuest document ID:	2597411678
Document URL:	https://www.proquest.com/newspapers/wealth-management-special-report-get-rich-quick/docview/2597411678/se-2?accountid=44910
Copyright:	Copyright 2021 Dow Jones &Company, Inc. All Rights Reserved.
Last updated:	2021-11-16
Database:	U.S. Major Dailies