Trends to be Aware of in Cyber Fraud

cyber security fraud protection phishing

Summary: The tactics that cybercriminals use are ever-changing. Keeping your customers and your institution protected against cyber fraud requires staying on top of the latest trends and making sure everyone knows what to look out for.

Actress Jenna Ortega's portrayal of Wednesday Addams in Netflix's hit show "Wednesday" has soared to unprecedented heights. A scene from the show that features Wednesday wildly flailing her arms about while dancing to "Goo Goo Muck" — a 1981 song by The Cramps — has been mimicked by countless individuals on TikTok, from children to adults and even celebrities.

Just like TikTok trends, the tactics favored by cyber thieves go in and out of style. Protecting themselves and their customers against cyber fraud requires that community financial institutions (CFIs) stay abreast of trends in cyber fraud and educate customers on the methods criminals most often employ, as well as ways to protect themselves from becoming victims.

Cyber thieves are undiscriminating when it comes to identifying potential victims, but there are distinct differences in the approaches they use to trick people within different generational groups into providing access to sensitive personal information or bank account details.

The Most Common Victims: Seniors

Cyber thieves have become particularly aggressive in their efforts to target senior citizens, a group that tends to be significantly less digitally savvy than younger groups. This generation, however, still controls roughly 75% of the country's assets. In 2021, senior citizens 60 and older were dupped out of more than $1.7B to fraudsters, with individuals losing $18,246 on average, according to the Federal Bureau of Investigation's 2021 Elder Fraud Report. That's up 74% from the previous year — an increase attributed to a combination of sophisticated tactics being employed by fraudsters, many seniors' lack of familiarity with digital payments and assets, and the fact that a large number of people nearing retirement have insufficient savings. That key factor makes them more susceptible to promises of outsized investment returns.

With cyber thieves playing on all three of these factors, CFIs should educate customers within this demographic about the most popular tactics cybercriminals use and should look for signs of fraud among this customer group.

One-Time Password Fraud

However, seniors aren't the only age group at risk from the latest cyber fraud trends, necessitating educational efforts and awareness campaigns that span your organization's entire customer base. One method cybercriminals are using to target both elderly customers and younger customers is one-time password (OTP) fraud.

There are multiple ways that criminals seek to gain access to sensitive personal information or accounts. One way they do this is by submitting a request on an individual's behalf that triggers an OTP to be sent to them.

They then call that individual and impersonate a representative of a legitimate organization (such as a financial institution) and ask the account holder to confirm the number they were just sent.

Criminals are getting even more creative. A new OTP scam people are falling prey to involves the delivery of a package to your home, where an individual will impersonate a delivery agent and ask for an OTP in place of your signature. If a recipient says that they haven't ordered a package and don't want it, the agent will insist that an OTP is needed to cancel the order. They'll send what is known as an OTP bot to the recipient's mobile phone. OTP bots are used to trigger the delivery of an authentic OTP code from a legitimate company to the individual's phone, which, once shared with the delivery agent, can be used to hack someone's account.

QR Code Fraud

From fake parking app QR codes used to steal people's credit card information to phony codes for installing malware on an individual's phone, QR code fraud has been on the rise since the onset of COVID-19. The surge of contactless, mobile-initiated transactions during the pandemic meant that people became accustomed to scanning QR codes for things such as paperless menus. Oddly enough, though younger consumers tend to be more tech savvy and familiar with mobile phone apps, a recent study found that they are more likely to fall prey to QR code fraud.

A new QR code scam is also making the rounds abroad and will soon make its way to the US, if it hasn't already. The scam is circulated via email through attached Microsoft Word documents using QR codes and text to make it undetectable by malware programs. The senders claim to be from the Chinese Ministry of Finance, or another governmental entity relevant to the target victim, and reach out to people about government grants they are eligible for. If individuals follow the instructions of the scammers, which ask that they access the QR content through WeChat, then they are directed to a fake electronic grant application used to capture their personal details, credentials, and financial information. This info then gets harvested and either used by the criminals or sold to a third party to be used for future crimes.

Educating Customers

While the above are just a few of the tactics cybercriminals are employing these days, their increasing popularity is something that should be on customers' radars.

The following are a few things CFIs should drive home to customers regarding safety measures:

- Never share an OTP with anyone, and make sure any OTP you use is one you have generated yourself directly through a company's website or app.
- Make sure to type in the URL when accessing any digital content.
- Never click on any unverified link.
- Only scan QR codes that you know are legitimate.
- Don't store any passwords on your phone.
- Do not use public computers to access personal accounts.
- Routinely check your accounts for suspicious activity.

Cyber fraud is constantly evolving and the methods that criminals use are quick to change. CFIs need to ensure that they remain up to date on the latest trends in cyber fraud and that employees know what signs to look for in customer accounts. But most importantly, a CFI can help prevent these fraudulent transactions by helping customers stay abreast of potential threats and educating them on how to avoid becoming fraud victims.

INDUSTRY INSIGHTS FROM PCBB

Love reading the BID? PCBB provides other industry insights in the form of podcasts, white papers, case studies, and other content focused on topics critical to the success of community financial institutions. Check them out today!

ECONOMY & RATES

Rates As Of: 03/14/2023 06:46AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	4.87	-0.01	0.45
6M	4.81	-0.36	0.05
1Y	4.50	-0.51	-0.21
2Y	4.23	-0.59	-0.20
5Y	3.78	-0.41	-0.23
10Y	3.58	-0.34	-0.30
30Y	3.70	-0.22	-0.27
FF Market	**FF Disc**		**IORB**
4.57	4.75		4.65
SOFR	**Prime**		**OBFR**
4.55	7.75		4.56