OTP Fraud – What Is It & How Can You Prevent It?

cyber security risk management fraud protection

Summary: OTP fraud is a new threat that community financial institutions need to know about. One-time passwords (OTP) are intercepted by cyberthieves allowing them access to financial accounts clandestinely. With two-factor authentication more widespread, cybercrime services have seen entry points and cyberthieves have jumped in. Here is a summary of OTP fraud and what you should do about it.

Birdwatching is more popular than we thought. As of 2019, there were 12.82MM birdwatchers in the US alone, or as some call them, twitchers or simply birders. That number increased 4% over 2018, so birds should feel privileged that so many people want to keep their eyes on them.

More than birds, bankers need to keep their eyes on cybercriminals, as there is another way for them to get access to customer accounts. Back in February, KrebsOnSecurity, a security news and investigation organization, alerted readers about a new cybercrime service. KrebsOnSecurity reported that the provider of this service allowed cyberthieves to grab the one-time passwords (OTP) used by a number of websites for a second layer of authentication. While that particular service didn't stay active for long, that doesn't mean this security problem no longer exists. Intel 471, a cyber intelligence company, said recently that it's seeing more of these bad actor services pop up. Here is the latest on this security threat.

OTP fraud. These illicit services assume a cyberthief already has a victim's credentials from some other breach. With two-factor authentication becoming more widespread, thieves have needed more than that. By getting access to OTP, thieves can tap into a victim's financial or other accounts and wreak havoc. These services have been known to attempt access to popular sites, including Amazon, PayPal, and Venmo as well as various large national banks. Some password-gathering services also allow for customization, broadening the scope of potential victims.

How it works. A bot — a software program that performs simple, repetitive tasks — places an automated call to a consumer and directs him or her to enter the code that was just sent to the consumer's mobile device. At the exact same time, the hacker — who has a victim's username and password in hand — requests a code be sent to the victim's phone from a legitimate institution the account holder does business with. The automated call informs the victim that the code is needed to protect against unauthorized account entry — or some similar rouse — when it's actually being used to covertly enter the victim's account.

The right way to use two-factor authentication includes a customer login on a website after which the customer is immediately asked to approve a prompt on their mobile device within a short period of time. Yet, many times the password and one-time code both come through the website, which leaves space for cyberthieves.

What community financial institutions can do

Remind customers. The proliferation of these services underscores why customers need to be reminded never to provide information of any kind in response to an unsolicited call. Community financial institutions (CFIs) need to reinforce this with their customers. They will never call or email to ask them for personal

information, including OTPs. Communicate this through multiple channels so that they are sure to see it and contact you with any questions.

Reminding customers to be vigilant about safe practices is especially important given a wave of mobile phishing scams. A whopping 84% of organizations were subject to mobile phishing scams, according to the Proofpoint 2020 State of the Phish Report. Financial institutions were the most affected, according to the report.

Train employees. It is also prudent to alert employees about these potential risks. According to the 2021 State of Privacy and Security Awareness Report, some employees still need reminding about avoiding risky behaviors. While the report notes that financial industry employees are the most likely to receive training on these issues, deficiencies still exist. For instance, some financial institutions may have halted this type of training amid the pandemic. Twenty-four percent of finance industry employees polled said their employer hadn't resumed security and privacy training after the lockdown in 2020. Also troubling is the 9% of finance industry employees who reported never having received this type of training.

Fraudsters will always abound, but CFIs need to continue to act proactively to mitigate these new risks. Pay careful attention to new scams as they develop and promptly inform customers and staff of these schemes and how to best protect themselves. Protecting them ultimately protects you.

COMPETITIVE AND CONSISTENT LOAN PRICING

Achieve a 360-degree customer relationship view so you can determine the best loan pricing based on your customer data while driving higher bank profitability. Learn more about Profitability FIT.

ECONOMY & RATES

Rates As Of: 11/29/2021 06:18AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.06	0.01	-0.03
6M	0.10	0.03	0.01
1Y	0.22	0.07	0.11
2Y	0.55	0.05	0.43
5Y	1.23	0.05	0.87
10Y	1.55	-0.01	0.63
30Y	1.89	-0.05	0.24
FF Market	**FF Disc**		**IORB**
0.08	0.25		0.15
SOFR	**Prime**		**OBFR**
0.05	3.25		0.07