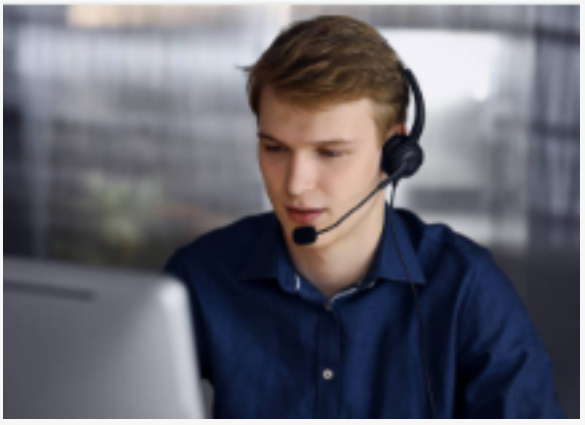
Digital thieves using OTPs to run scams: Cyber-Forensics.net shows safe internet and transaction practices

One-time password offers a secure mechanism to log into user networks. But scammers are sending fake texts with bogus OTPs to steal personal information.

Cyber-Forensics.net



Cyber Forensic Specialist

SOFIA, BULGARIA, March 3, 2022 /EINPresswire.com/ -- Digital payments are catching pace, particularly in uncertain times like Covid-19. People have witnessed technological evolutions in the past few years. But the rise of digital acceptance has also led to increased cyber threats. A new kind of financial fraud is catching momentum across nations. In the wake of 790 OTP-based reported scams tricking account holders of more than $13 million, authorities are out to issue urgent warnings.

There have been calls for law enforcement agencies to intervene in various forms. Last month, Cyber-Forensics.net, a cyber forensics service for online scam victims, dealt with hundreds of similar consumer complaints.

A 78-year-old Kansas resident fell victim to a cyber fraudster who posed as a Telecom company executive and sought to privy bank details. According to police, the senior citizen received a message that his phone services would be discontinued if the user failed to verify his documents. The citizen fell prey to the con artist's gimmick and shared his card details only to receive an OTP. Subsequently, the senior citizen realized he was duped and lost $5676.

Chief analyst at the firm, Timothy Benson, took a look at the case and said authorities need to ask three questions to move forward:

 Prevention: What can be done to prevent individuals from falling victims to such scams?
 Accountability: Who is responsible when a scam like this occurs worldwide, and how can victims vindicate their fundamental rights to security?
 Loss allocation: In situations like these where no one is at fault, besides cybercriminals, who should bear the financial losses?

> OTP-based scams are usually an arms race between the defenders and the attackers, and the defender needs to succeed 100 percent of the time."
>
> *Timothy Benson*

Preventing OTP-based Scams:

Typically, there are two broad categories of measures that bank account holders or internet users can take to avoid becoming prey to OTP-based scams: Technological and Behavioral.

Technological measures:

It is essential to get rid of short messages and OTPs sent to registered mobile numbers that contain bogus links. Use certified platforms like Google to make an online payment. Never share a computer screen with anyone online claiming to give proper instructions.

Secondly, use secure identification verification measures. For instance, any platform doesn't clear payment without asking the account holder to confirm the transaction details. Make sure to double read the amount to be paid and check the bank's name.

Use governmental secure online systems to login. It makes sense that all government platforms usually require integration with highly-secured digital services that will enable only authorized people to use the system. This ensures that scammers cannot break into the bank's account by simply guessing the password or getting access to the potential victim's OTP details.

Using government-authorized digital infrastructure may also be more secure because each bank service usually has a set of its biometric data repository to facilitate safe access and create data privacy complications to stop cyberattacks further.

Third, banks and customers should use automated scam detection software. Such software helps individuals to identify suspicious calls and messages.

While banks may also have integrated internal fraud detection tools, for example, freezing an account with suspicious activity automatically within a defined period, individual account holders can download paid tools.

However, fund recovery company Peter Thompson thinks "the downside with automated bank protection measures is they can end up making the situation frustrating for customers, as they are subject to friction and ask overwhelming questions."

Another problem is that "OTP-based scams are usually an arms race between the defenders and the attackers, and the defender needs to succeed 100 percent of the time."

Behavioral measures:

There are many aspects in behavioral measures like educating users about the scams through law enforcement websites and scam alerts. Thus, bank authorities also need to send cautionary tips for safe bank transactions from time to time.

The solution for organizations is to collaborate with behavioral experts and develop ways to approach users cleverly to pay attention.

The best way is to use visual attention because, just like scams, infographics are less wordy.

Another possibility is to keep track of online scams prevalent around. Most users dismiss the importance of reading about the number of scams making the rounds on the internet. It can keep people on their toes and aid in identifying the red flags before being tricked.

What to do when someone falls victim to an online OTP- based scam and loses money?

Cyber forensic intervention is most appropriate when efforts are directed at fund recovery. It increases the chances of recovering those lost funds. Proper authorities can align their business goals with consumers' problems. For example, Cyber-Forensics.net is a cyber firm that helps online scam victims recover their money lost in any scam.

Another reason to involve fund recovery services is that they can put pressure on the banks to disclose the exact details of the transactions. Investigative agencies can assess whether the victims stand a chance to make viable claims. They help victims prepare reports that bank or government authorities may require to comply with banking secrecy laws and prevent inadvertent disclosure of the anti-fraud techniques that scammers may exploit in the future.

Secondly, if the victim does have a viable claim, banks can be held responsible for returning the total amount. The fund recovery company make the process quick and affordable.

But ensuring to choose the right fund recovery companies to make informed decisions can impact whether the victims will get their money back or not. Cyber-Forensics.net generally receives positive reviews.

About Cyber-Forensics.net

Cyber-Forensics.net is committed to providing the most accurate tracing service for victims of online scams. Cyber-Forensics.net empowers and simplifies the process of tracking down the cyber-criminals and assists in recovering the funds and creating an atmosphere for a negotiated settlement. Cyber-Forensics.net commonly deals with Bitcoin scams and Forex withdrawal problems. For more information, please visit https://cyber-forensics.net.

Peter Thompson

Cyber-Forensics.net
+1 917-920-6613
email us here
Visit us on social media:
Twitter
