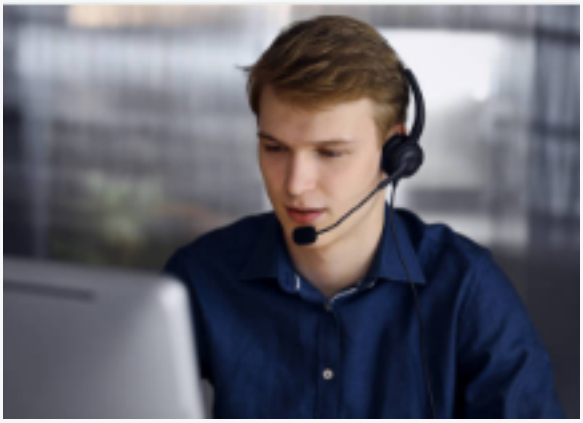
Digital Banking Frauds becoming a billion dollar industry: Cyber-Forensics.net shows technology-based prevention steps

Digital banking frauds account for 33% of all digital crimes in the United States. Experts say the right adoption of technology can help evade severe damage.

Cyber-Forensics.net



Cyber Forensic Specialist

SOFIA, BULGARIA, August 19, 2022 / EINPresswire.com/ -- Digital transformation in banking has accelerated partly due to the pandemic and partly because of multiple players in the market focusing on digitization. Governmental policies and new startups have led to a surge in revolutionizing the financial landscape.

However, with technological advances, scammers have their plans to advance too. Fraudsters are busier than ever. Digital platforms have allowed them to identify various money-making techniques. And online fraud is becoming more and more frequent.

As per the latest media reports, scammers target online bank customers, convincing them to give out their internet banking details, mobile numbers, and OTPs to carry out various fraudulent transactions.

Cyber-Forensics.net, a cyber forensics service for online scam victims, says that until a few years ago, digital banking fraud was a small industry where scammers just stole modest sums.

But today, digital banking fraud has become an enormous liability, causing billions of dollars of losses annually. These scammers target vulnerable individuals caught in the middle of digital adoption—for example, senior citizens.

According to Timothy Benson, a fund recovery expert at the same firm, criminal groups may use sophisticated tools to execute several online banking-related frauds.

What happened?

Giving a twist to phishing techniques, digital fraudsters have begun developing a new way of

> Digital banking fraud has caused a serious challenge to the reputation of banks. Criminal hackers are employing broader methods of financial fund exploitation.”
>
> *Timothy Benson*

tricking consumers. Now they are using a web-based application that pushes out notifications to warn internet banking users that they are about to become targets of a phishing attack.

Thus, they need to secure their account. A fake representative from a bank calls the target and asks for an OTP to ensure the user's account. Then, these malicious actors take control of the accounts and steal all the funds.

As per estimates, hackers have stolen millions in cryptocurrencies since the start of the year and other financial assets by breaching the bank accounts of internet bankers.

Earlier this month, a network platform that allows users to exchange crypto tokens confirmed that thousands of account holders had been affected by these digital frauds.

Peter Thompson, who offers expert counseling on how to recover cryptocurrency, says, "Digital banking fraud has caused a serious challenge to the reputation of banks. Criminal hackers are employing broader methods of financial fund exploitation."

Digital banking fraud has caused a severe challenge to the reputation of banks. Criminal hackers are employing broader methods of monetary fund exploitation. And the ways these tricksters acquire to steal money are difficult to predict. Enabling a secure end-to-end transaction can help victims stay protected longer.

How to avoid becoming a victim of scammers asking for ransom?

While in most of these cases, it is hard to avoid becoming a victim. But still, users can avoid giving scammers the upper hand by following the mentioned steps.

 Don't receive incoming calls from strangers. Users don't need to learn each area's pin code. But the minimum they should do is check the pin code of where they reside and nearby locations.

 Callers or text senders can go to extreme lengths to stay connected when they try to hack the user's account. Usually, a few seconds on the call are sufficient to determine if the conversation has any relevance. Hang up quickly if it's not an important call.

 Never share any banking credentials or OTP. No matter how closely related the person claims to be.

 Understand when the conversation has become a threat.

 Never pay a ransom. It is better to involve law enforcement.

What to do if scammed into a digital banking fraud?

 Seek immediate help by reporting the issue at a nearby police station. Irrespective of how a victim was targeted, lodge a file to ensure a case is registered. Also, write emails to bank branches and credit card companies.

 In the case of scams related to banking, it is advised to report the issue to concerned banks, cyber cells, and third-party payment apps on the phone.

 Register what happened: In most cases, scammed victims are clueless about what possibly led them to become victims of a scam. Thus, it is recommended that you note down the order of events. Keep screenshots, texts, and numbers.

 Report fund recovery services: Bringing fund recovery services on board in case of a huge loss is a viable option as the local police may not have the right tools and equipment to deal with scammers hiding behind advanced computers.

 Investigators at fund recovery are typically able to collaborate with financial institutions, lawyers, the FBI, Interpol, and other legal teams to pin down the perpetrators.

How to report the matter?

As bank users usually operate their accounts using an internet connection, it is best to contact financial institutions as quickly as possible.

Victims may consider emailing the entire incident or registering an online complaint by visiting the online complaint websites.

Taking a print-out of the incident report and visiting the designated authorities in person

How can fund recovery services help victims?

One of the reasons scam victims involve fund recovery services when they are targeted by digital banking fraud is to recoup the lost amount. But other than this, there are a few more reasons, including:

 They offer accurate financial counseling.
 Help uncover the faces of the cheaters.

 Offering emotional support
 They help bring out a clear status of the progress.
 This will give an accurate idea of whether the lost money is recoverable.
 Also, provide information about other online scams causing financial damage.

But be careful while searching for a recovery service. There may be fraudsters who claim to help victims but have plans to track victims again. This is often called a "funds recovery scam."

Because of their exaggerated and sugar-coated talk, it can be difficult to distinguish a genuine service. Remember, scammers train themselves in the art of manipulation. Any sign of absolute guarantee of return of funds is definitely fraud. A real fund recovery company will give you detailed instruction how they operate and will answer questions in with honesty and integrity.

Make sure to identify the red flags or, better yet, check online reviews on multiple platforms. For example, several reviews on online discussion platforms and company review platforms recommend Cyber-Forensics.net as a highly suggested name.

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
