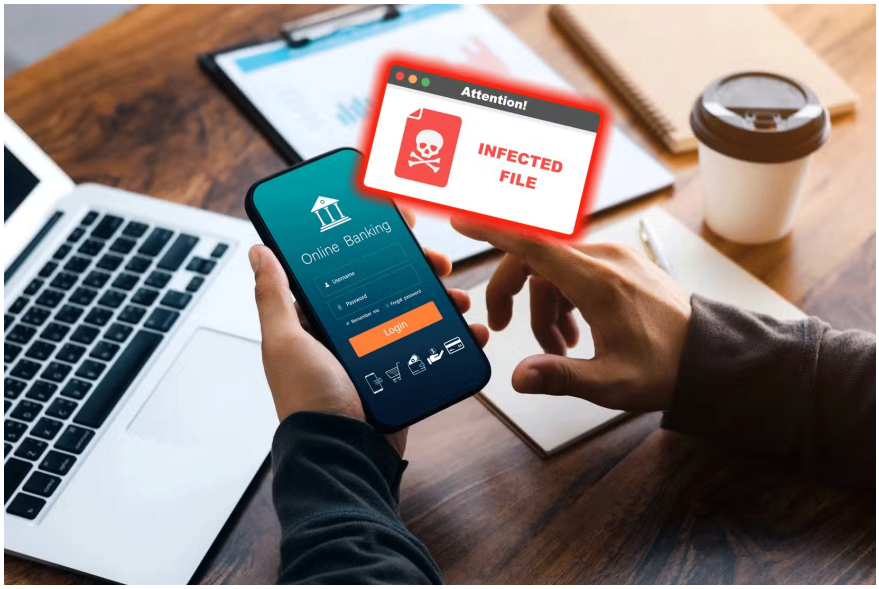
5 common methods hackers use to hack bank accounts

With so many people turning to online banking, it's no surprise that cybercriminals are looking to hack bank accounts.

With so many people switching to online banking, it's no surprise that cybercriminals are looking to hack bank accounts. What's surprising, however, is that these individuals will go to any lengths to gain access to your finances. Here's how someone can hack your bank account and how you can stay safe.

1. Mobile banking Trojan



Fake banking apps have become an easy way to hack bank accounts. This attack involves hackers creating a copy of a legitimate banking app and uploading it to third-party websites. When you download the app, it prompts you to enter your username and password. If you enter your details, they are sent to the hacker.

A more stealthy version of this attack is a mobile banking Trojan. These aren't disguised as official banking apps; instead, they're often completely unrelated apps with a Trojan installed inside. When you install an app, the Trojan scans your phone for banking apps.

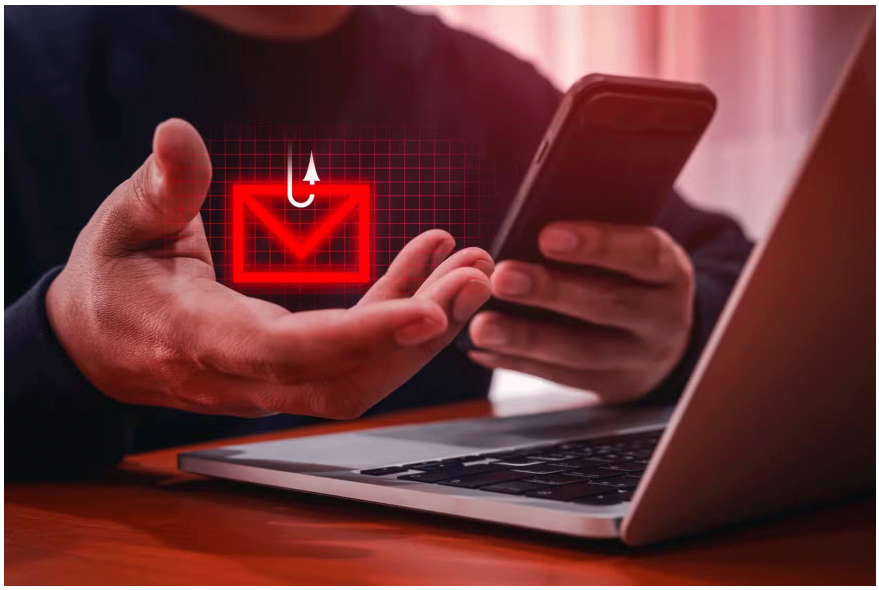
This type of malware plays an integral role in the entire process of hacking bank accounts. When it detects that the user has launched a banking application, the malware will quickly create a window that looks exactly like the

application you just launched.

If done smoothly enough, the victim won't notice the swap and will enter their details into a fake login page, which will then be sent to the malware author.

Banking Trojans often need SMS verification codes to access your accounts. To do this, they often request SMS reading permissions during installation to steal the codes as they appear.

2. Phishing



Hackers have stepped up their efforts to trick people into clicking on fake links as the public becomes more adept at phishing tactics. One of their worst tricks involves hacking into attorneys' email accounts and sending fraudulent emails from a previously trusted address.

The attack is devastating because it's so hard to spot the scam. The email address will be valid, and the hackers may even address you by name. This is exactly how one unfortunate homebuyer lost £67,000, according to The Guardian, despite replying to a valid email address.

3. Keylogger

Have you ever seen someone's password by looking at what they typed into their keyboard? Keyloggers are the digital version of that. They often come with malware and work silently in the background.

Every time you type something on your keyboard, a keylogger sends data back to hackers. It may not seem dangerous at first, but if cybercriminals notice you typing in the URL of your bank's website, followed by something that looks like your username and password, they can use that data to break into your account.

4. Man-in-the-Middle Attack

Sometimes, hackers will target the communication between you and your bank's website to get your details. These are called Man-in-the-Middle (MitM) attacks, and the name says it all: It's when hackers intercept the communication between you and a legitimate service.

Typically, a MitM attack involves monitoring an unsecured server and analyzing the data that passes through it. When you send your login information over that network, the hacker 'sniffs' your information and steals it.

However, sometimes hackers will use a technique called DNS cache poisoning to change the website you visit when you type in a URL. DNS cache poisoning means "www.yourbankswebsite[dot]com" will instead redirect you to a copycat website owned by the hacker. This website will look exactly like the real website; if you're not careful, you'll end up giving your login information to the fake website.

5. SIM Swap

SMS authentication codes are a big problem for hackers. Unfortunately, they have ways to bypass these checks — and they don't even need your phone to do it!

To perform a SIM swap, a hacker will contact your network provider, pretending to be you. They will say that they have lost your phone and want to transfer your old number (which is your current number) to their SIM card. This is one of the most widely used methods to hack bank accounts using phone numbers.

If they succeed, the carrier will remove your phone number from the SIM and install it on the hacker's SIM. This can often be done using a Social Security number, which someone can get through a data breach or the owner accidentally gives them.

Once they have your number on the SIM card, they can easily bypass SMS code protection. When they log into your bank account, the bank will send an SMS verification code to the hacker's phone instead of yours. They can then log into your account unhindered and take your money.

similar articles on tips and guides. Thank you for reading and for following us regularly.