BANC OF CALIFORNIA | TOGETHER WE WIN™

ACCOUNT TAKEOVER FRAUD

A higher incidence of account takeover fraud requires a higher level of caution.

Fraudsters have developed startlingly sophisticated techniques for infecting and taking over accounts.

Account Takeover, or ATO, is a form of payment fraud that targets electronic transactions. Fraudsters perpetrate the scam by gaining access to your systems and generating fraudulent electronic payments, usually ACH batches or Wires. It is closely related to Business Email Compromise (BEC), which revolves around phishing emails and "spoofed" email accounts.

Scammers are getting more sophisticated all the time. They patiently study their targets and the businesses they interact with, learning all they can about them so they can execute their scams without detection.

Account takeovers start with obtaining account data and conducting targeted phishing scams.

Account takeover attacks begin with fraudsters obtaining personal data, often starting by purchasing data leaked in a previous breach. They use that data to create targeted phishing scams to gain access to accounts.

One of the most common phishing scams is when the scammer impersonates the target's bank, or some other trusted entity, and sends an urgent alert via email, text or phone, which requires immediate action. The action takes the target to a fake banking portal that installs malware.

Malware can take over your account, so you need to be careful about actions that can infect your devices.

There are different types of malware. However, most are designed to do one thing: capture their victims' banking credentials so criminals can take over their account. Some do it by redirecting the victim to a malicious website, some intercept everything the victim types, while others can even modify transaction details.

Malware is typically downloaded inadvertently by visiting risky websites or by opening attachments, apps or even program updates without verifying their sources. For example, if you get a pop-up notice to update Flash®, do not respond to it. Instead, go to the Adobe® site and check there for updates.

As mobile banking becomes more popular, mobile banking trojans are becoming more prevalent.

Mobile banking is convenient and enables you to access your account anytime, from anywhere. With the right protections and precautions, it is safe.

Keep in mind that fraudsters are becoming better at replicating bank interfaces with so-called overlay attacks that push the actual app to the background, overlaying a fraudulent one that looks just like the real thing. Once that happens, fraudsters can redirect fund transfers to their own accounts.

Man-in-the-middle attacks put fraudsters between you and the bank to hijack your communications.

Man-in-the-middle attacks can come from malicious public hotspots and through mobile banking apps with insufficient protections. An effective mobile banking app has safety features to ensure there is a secure connection for the transfer of mobile banking data.

EQUAL HOUSING LENDER FDIC

BI06W1120