BANK FRAUD AWARENESS

In 2021 over 2.8 million fraud reports in USA. Banks are combating fraud by implementing advanced technologies such as machine learning, artificial intelligence and biometrics.

TOP 10 BANKING FRAUD TRENDS IN 2023:

- Technical support. Scammer poses as representatives from legitimate tech company by call or email claiming that your computer has a virus or issue. Scammer will ask for remote access to your device to fix the problem and during that time will steal your personal and financial credentials.
- Mobile SIM swap. Fraudster will take over your mobile phone number in a SIM swap scam by posing as you and convinces your wireless provider to transfer your number to a new SIM card he controls. The fraudster now has access to your phone number, all phone calls and text messages. Access to any two factor authentication linked to your number can be used to access bank accounts and credit cards.
- Account takeover. The scammer gains access to your bank or credit card account or credit card by posing as you and providing enough personal information to pass security measures. They will then change pin codes/login information. They can then drain your account, make unauthorized purchases and take out loans in your name.
- Bank insider. A bank employee that has access to your account number and login details can skim off small amounts of your account. If it is a large account the scam can go unnoticed for a long time. The employee can possibly sell the account information. You must be on constant vigilance to prevent or stop this crime.
- Phishing. Fraudsters sends email or texts posing as a legitimate institution such as your bank. They request personal information

or login details. These communications often contain links to fake websites that look like the real thing. Once they have the details they can commit identify theft or gain access to your accounts.

- Man-in-the-middle. Another type of phishing is pharming attacks. Scammer will insert themselves between the victim and a legitimate institution. They might intercept communications or redirect you to a different website. They will then collect login information for their own gain.
- Business email compromise. The scammer will pose as someone in authority within a company. They will send an email requesting a transfer of funds to a particular account that they control. An example is a fraudster will pose as a vendor and send an invoice to a victim requesting payment. The victim may be an employee and not realize that it is fake and send the amount.
- Investment scams. The fraudster convinces the victim to invest in amazing opportunities. They may promise high returns with little risk by using false information or pressure tactics. The crypto-currency market has proven to be a inviting for these types of frauds due to lack of regulations.
- Push payment social engineering. The scammer will convince the victim to send them money through social engineering tactics. These can range from posing as a government agency requesting payment for fake fines to impersonating a family member needing an urgent funds transfer. Can be an individual requesting funds due to a disaster or could be a fake charity requesting donations.
- Romance scams. Scammer will crate a fake social media profile and start an online relationship with the victim. Ultimately, they will convince them to send money. They may start by catfishing, using a fake identify and photos and gradually gain the victims trust over time.