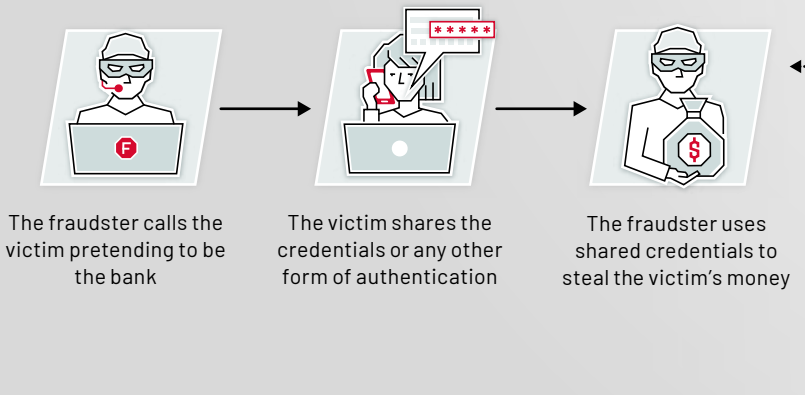
Vishing attacks

Vishing, a compound from voice phishing, is a type of an attack where fraudsters try to convince the unsuspecting users to provide valuable information over the phone.

Situation & solution

- Based on our data, **vishing attacks in the banking sector are on the rise**. These are mainly driven by the pandemic fears and increased usage of multi-channel banking systems with 2FA.
- ThreatMark prevents plain and sophisticated (RAT) vishing attacks. Also, as for any social engineering based attack, it is crucial to educate users to increase vigilance and foster a healthy level of suspicion.

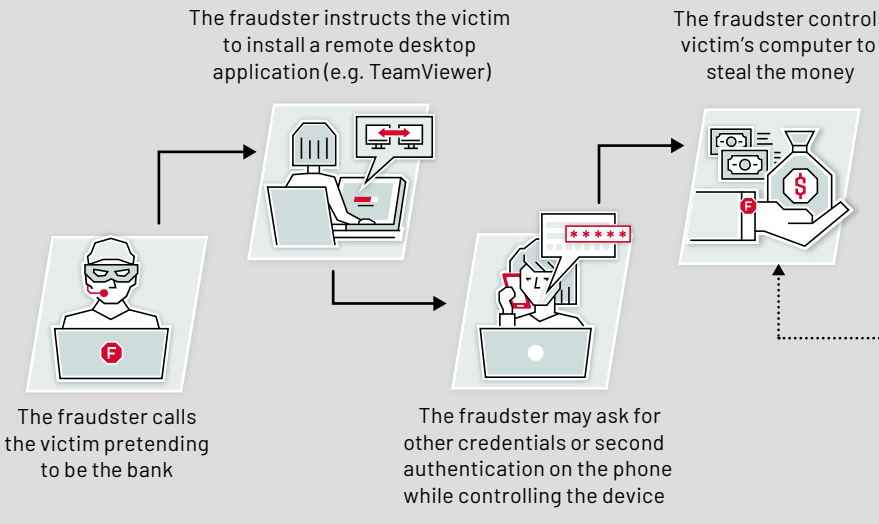
PLAIN VISHING



How ThreatMark prevents it

Even though the fraudster has taken control of the user's credentials, has access to the system and other authentication methods – ThreatMark can recognize that attributes (device, location, browser and behavioral biometrics) are different from the trusted user. ThreatMark can identify these differences as anomalous and alarming.

SOPHISTICATED (RAT) VISHING



How ThreatMark prevents it

ThreatMark can detect Remote Access Trojan (RAT) attacks. So even though the fraudster is using the user's computer, ThreatMark still detects something is different from the trusted user's profile.

Also, fraudsters will send money to an account that was not used previously by the user.

In ThreatMark, these anomalies—in behavior, device & payment—can be used to raise the risk factor and trigger fraud alerts.

www.threatmark.com —— **info@threatmark.com**