Solution Guide:

Basic voice phishing



Modus Operandi (MO)

Attackers trick victims into willingly sharing credentials with them.

Phone call to victim

Convince victim to share credentials

Use credentials to commit fraud



• Mimic bank or other known institute

- Build trust
- Psychological tricks
- Practical in-app guidance
- Request password and 2FA code
- Transfer money
- Order goods with different shipping address (often with 1-click payment)

18K

94M

Voice phishing victims in NL*

Lost to voice phishing in NL*

Voice phishing is a form of APP fraud where fraudsters call their victims and pretend to be the bank. They convince their victims to share their credentials (e.g. to 'solve an issue') and then use the acquired credentials to transfer money or order goods.

Realtime Visibility

Manage fraud risks from the earliest stage using layered detection.

Behavioral risk:

On-call while opening banking app

Behavioral risk:

- Navigational timing anomaly
- Typing rhythm anomaly
- Device orientation anomaly
- Switching to 2FA app while on-call

Behavioral risk:

- Location anomaly
- Browser anomaly
- Form filling anomaly
- Navigational timing anomaly
- Mouse anomaly
- Typing rhythm anomaly

Using ThreatFabric's Fraud Risk Suite, every step in the fraudster's attack attempt is detectable using one or more detection layers. Our unique integration of technical and behavioural detection layers will lead to early warnings and a high signal-to-noise ratio. Combined with internal knowledge, it allows our customers to stop fraud attempts before people become fraud victims.









Realtime risk events & scores, fraud alerts, reports, etc.

Demo?

Contact us for

a demo or trial!



+31 (0)20 8950650



info@threatfabric.com



PII, account, address book, transactions, (order) history, interests, and more.

Fraud team & systems

* Bank fraud stats in the Netherlands (2021) - CB