bfore.ai

Case Study

Volksbank

Protecting customers while saving remediation costs

PreCrime Brand

Situation

Brand is an extremely valuable asset, and customers count on Volksbank doing their best to protect the relationships.

The growing threat from phishing and impersonation campaigns was among the largest risk to handle for the bank security team and had become unmanageable.

With an estimated average cost of 42.000€ per each account breached, an investment to bring improvement is quickly justified.

Impact

Volksbank Banca Popolare - is a trusted regional bank in Italy. They cater both to individuals and small/medium businesses and have built their reputation over decades. Each phishing email that tricks a customer causes multiple costs:

- The loss of funds due to account access and unauthorized withdrawals
- The time wasted in handling the incident response and customer escalation
- The personnel busy with analyzing the breach and checking for other victims
- The cost of securing against further criminal activity

TL;DR

- The brand is a key asset for any company, as it represent the trust and values.
- Each breach has average cost of 42.000€
- Bfore.Ai PreCrime Brand was configured configured to protect all brand and domains owned by the bank.
- More than 20 active threats stopped in less than a week
- Reduction of false alerts by 98%
- Increase in threat detection by 60%

About Bfore.Ai

The first truly predictive security solution. We help organizations prevent intrusions and data exfiltration by predicting vectors of future attacks, the information is used in #PreCrime for Network - predictive cyber threat intelligence to upgrade existing security solutions (firewalls, DNS resolvers, anti-phish filters, proxies, etc.) with foresight.

bfore.ai

Key takeaways

Proactive Brand Protection to safeguard customers

Less than 4 hours from prediction to takedown

95% of counter measures completed in lessthan 24 hours

Zero victims

<0.05% false positives

Set Up

Volksbank has 2 main branded domains to protect. Alerts were configured to be sent by email immediately as predictions are made. A semi-automated countermeasure and proactive takedown service was selected.

The fully software-as-a-service capability offered by bfore.ai provides alerts automatically when predictions identify future vectors of phishing and scams.

The security team at Volksbank requested countermeasures and proactive takedown to be validated manually on working days, and fully automated during weekend, a period of increased malicious activity.

> *We truly love Bfore.Ai PreCrime,they give us the superpower to protect our customers by stopping threats before they start.*
>
> **Petra C. - Chief Information Security at Volksbank**

The Results

Bfore.Ai engaged in a Proof of Value lasting 15 days, and the results were immediately visible :

- Reduction of false alters by 98%
- Increase in threat identification by 60%
- Alerts shared at least 72 hours earlier than malicious activity started
- Time to takedown down to less than 24 hours in most occurrences
- More than 20 takedowns completed in less than a week

Moreover, since PreCrime for Brand is active phishing attacks have seen a reduction in volume. PreCrime technology is now helping Volksbank Security team keep their customers and brand safe against malicious domains. PreEmption activity is initiated on demand during working hours, and automatically when the security team is off-work.

The team is now also implementing PreCrime for Network to complete predictive protection.