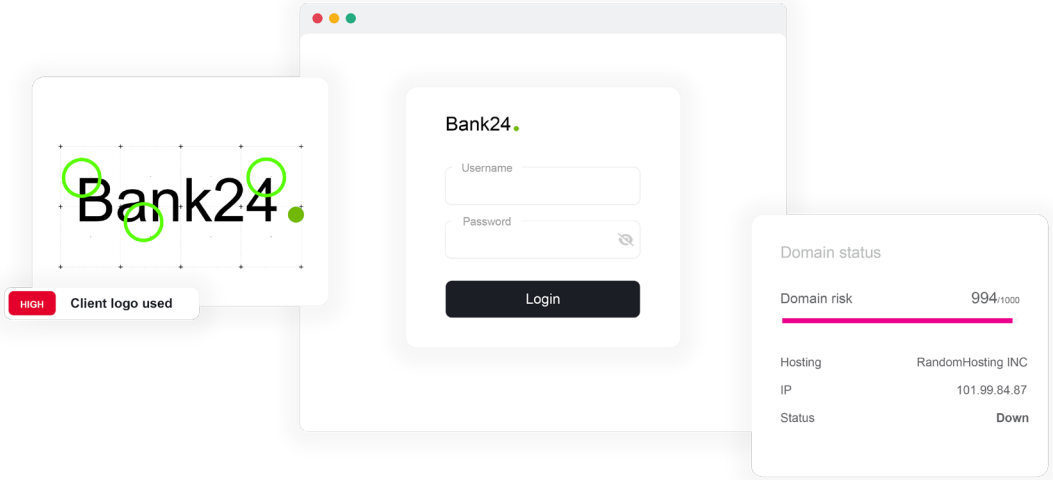
PHISHING DETECTION & MITIGATION.

Evolving Fraud Landscape

With financial institutions facing increasingly evolving threats such as phishing and malware, rapid response is vital. Employing advanced tools and expertise, ThreatMark's **Cyber Fraud Fusion Center** offers comprehensive protection against phishing attacks and brand abuse, reinforcing the overall security posture of businesses in the digital landscape.



Account Takeover Prevention

With fraudsters employing advanced tactics such as remote access intrusions and mobile malware, tackling account takeover (ATO) threats requires a proactive strategy.
By focusing on behavior financial institutions can gain assurance that account access is being made by the rightful user, protecting the customer's treasure and FIs reputation.

Brand Abuse Migitation Service

Institutions face increased unauthorized or malicious online brand and intellectual property use, negatively affecting their reputation. Brand Abuse Mitigation Service works with ISPs and social platforms to eliminate infringing content and take down counterfeit sites. It also allows reporting each site to ThreatMark for an in-depth investigation and site takedown.

DISRUPT FRAUD, GAIN TRUST.

How ThreatMark can Support Financial Institutions

ThreatMark's Cyber Fraud Fusion Center offers organizations an additional cybersecurity service with streamlined operations and a robust defense against phishing and malware, reducing potential financial losses. Through key digital partnerships, we ensure swift threat mitigation with minimal disruptions, optimizing response times to fraudulent activities. Our services enhance return on security investments and proactively hunt threats, safeguarding assets and reputation.

- **Reduced Fraud Costs**
  Expert tools and tactics directly combat phishing and malware, curtailing potential financial losses.
- **Operational Efficiency**
  Quick threat mitigation, due to relationships with key providers, minimizes disruptions and response times.
- **Enhanced Security ROI**
  Maximize the return on security investments by providing an all-encompassing defense.
- **Risk Management**
  Proactive threat hunting reduces unforeseen vulnerabilities, safeguarding assets and reputation.

Advanced Defense

- Integrations with hosting, registrators, and ISVs.
- Cutting-edge technology for multi-channel detection.
- Ensures enhanced detection accuracy.

Swift Response Times

- 6 seconds average time for detection to notification.
- Ensures first measures are effective within 2 hours.

Dedicated Cybersecurity Team

- Provides 24/7 response to incidents.
- Supports and guides on best practices.
- Service activated in less than 5 days.

Proactive Mitigation

- 90:10 ThreatMark Detection vs Client Detection.
- Executes both automatic and manual checks.
- Notifies relevant search engines, hosting providers,

Expert Fraud Analysis

- Investigate phishing sites comprehensively.
- Assesses threat levels and severity.
- Documents findings in detail: IP, source code, etc.

Flexibility

- Adapts and learns continually from new threats.
- No major integration or investment required.
- Serves as a standalone service option.