HOLVI

CASE STUDY

Holvi Pushes a Proactive Security Strategy to **Protect Customers with Netcraft**

netcraft

Customer Overview:

Industry: Holvi is a financial institution focused on business banking and account services for self-employed professionals and SME businesses across Europe. They offer core services in nine countries and support international transfers to more than 50 countries.
Headquarters: Helsinki, Finland
Company Size: 100–200 employees
Use Cases: Phishing URLs, Google Ads impersonation, brand infringement, and fake bank URLs

Challenge:

Waiting on Providers: Holvi's security team was manually detecting and removing impersonation threats across the web. Each week, analysts spent three hours identifying phishing URLs, fraudulent ads, and fake bank sites. After submitting takedown requests to providers, they faced long queues, which increased the window of victimization and was often already too late with shutting down the attack before the high-traffic periods. When there were not questions about site credibility, takedowns would typically take 12-18 hours.

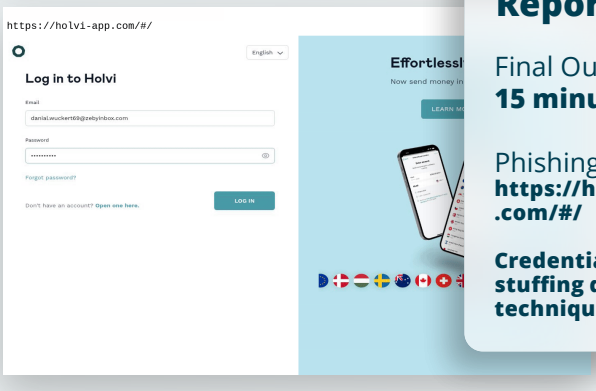
Targeted Phishing Campaigns: Operating across multiple countries and languages added complexity in identifying malicious URLs and ads. Threat actors used geographically targeted ads towards customers of certain cities, countries, and kilometer radiuses making the identification of these URLs and ads harder to capture.

Redirect Link Logic: Addressing impersonation Google Ads was particularly challenging. Ad clicks could redirect users to benign or malicious sites depending on location or device, making it difficult to identify and track genuine threats.

Netcraft Reported

Final Outage: **31 minutes**

Phishing URL: **https://holvi-krediet.be/**



Netcraft Reported

Final Outage: **15 minutes**

Phishing URL: **https://holvi-app.com/#/**

Credential stuffing discovery techniques

> "We knew phishing would be a problem towards our customers as it is the number 1 attack method used by threat actors. After a discussion with the rest of leadership, we decided to be as proactive as possible in an attempt to reduce the negative effects of phishing towards our customers. This led to searching for an anti-phishing and IP violations tool. The goal was to preserve Holvi's reputation with current customers and potential new customers."
>
> — Ronald Clark, CISO

Brand Protection: Recognizing the need for greater speed and coverage, Holvi's Security team evaluated Netcraft after hearing positive feedback from peers and online forums.

Solution:

Global Coverage: Netcraft's extensive proxy network enabled worldwide detection, bypassing cloaking tactics cybercriminals use to hide threats in certain regions or on specific devices.

> "Before, we relied on manual web searches, community reporting and other forms of detection, but with Netcraft we see things before they are reported." —Ronald Clark, CISO

Rapid Takedown Speed: Netcraft's zero-false-positive approach ensured providers prioritized takedown requests, dramatically reducing response times.

Advanced, Automated Detection: Netcraft's technology automatically followed ad redirects, uncovering hidden malicious sites, typosquatting domains, and lookalike URLs that manual methods missed.
Recognizing the need for greater speed and coverage, Holvi's Security team evaluated Netcraft after hearing positive feedback from peers and online forum.

Impact:

Partnering with Netcraft enhanced Holvi's threat-response process:

Each analyst regained roughly **three hours per week**, about **150 hours per year per analyst**, to focus on other high-value security initiatives like SIEM and XRP projects.

> "Holvi's four-person distributed security team previously conducted periodic manual web searches across different regions to identify phishing sites and malicious ads." —Ronald Clark, CISO

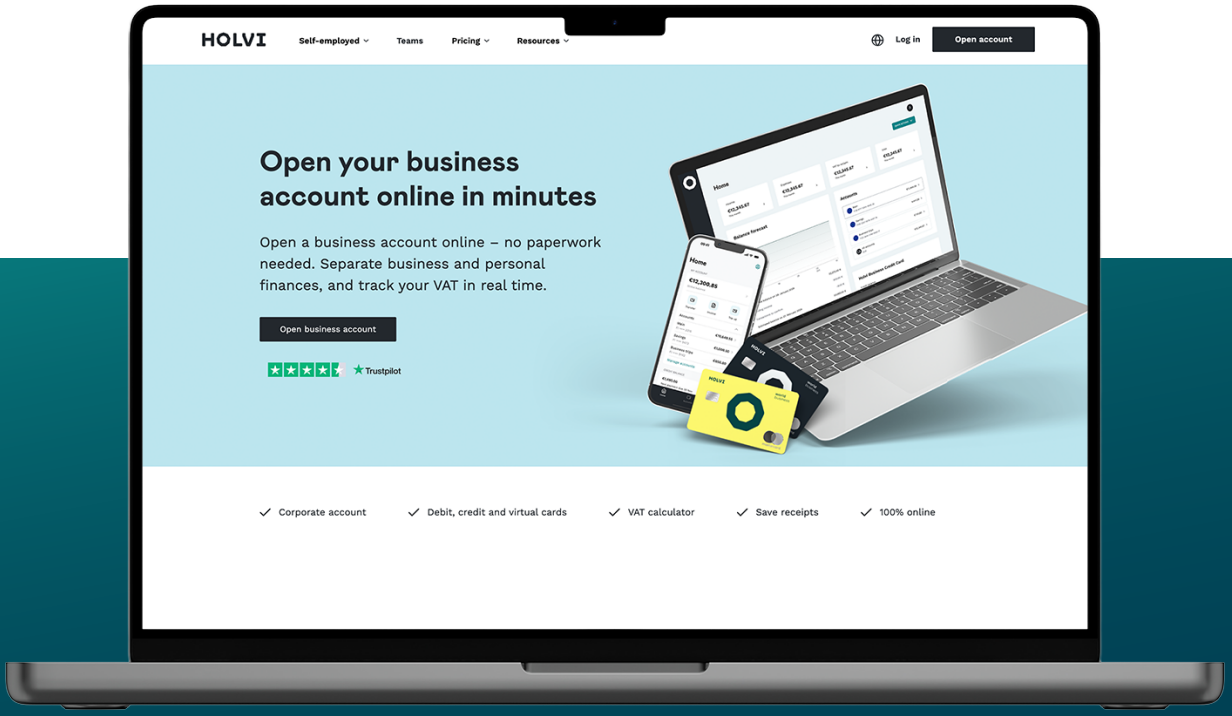
Gained confidence knowing the team isn't missing threats, moving quickly, and automating response – 24/7 availability means the team has their evenings and weekends back.

> "Monday morning workflows have improved – Netcraft email alerts now provide weekend threat detection summaries, eliminating the need for manual web scouring." —Ronald Clark, CISO

> "Usually, on Monday mornings we're scouring the web to see if anything new has popped up, but now we just have an email waiting for us letting us know that Netcraft identified x number of threats and we can get an overview in the dashboard." —Ronald Clark, CISO

Holvi's customers were better protected from phishing and credential theft, reducing the risk fraudulent data collection.

Threat detection became more effective across geographies, with Netcraft bypassing anti-cloaking measures to reveal attacks limited to certain cities or regions.



Key Results:

$35K
saved annually

Time savings: 3 hours a week per analyst with a team of 4 analysts
(150 hours/analyst annually)

$56/analyst hour at 624 hours a year = $35k saved in manual labor costs

~2
hours

Average phishing URL availability reduced to **~2 hours**

~2.4
hours

Cloudflare takedown times averaged ~2.4 hours

Why Netcraft?

> Netcraft can get our phishing mitigations actioned faster than we were able to ourselves, minimizing the window of victimization for our customers. With Netcraft, my team can take a breather on identifying web phishing and focus on other security initiatives, working towards being more proactive than reactive to these attacks."
>
> — Ronald Clark, CISO at Holvi

Summary:

By adopting Netcraft, Holvi turned a manual process into a fast, automated, and globally effective operation. Their security team now spends less time chasing providers to take down phishing URLs and fraudulent ads, and more time on proactive initiatives that strengthen Holvi's overall security posture.

netcraft

Connect with Netcraft today for greater speed and global reach at scale.