

# “PHISHING ATTACK DEFEATED. CLIENT’S BRAND PROTECTED. IT’S ALL IN A DAY’S WORK!”



## NEUSTAR OFFERS COMPLETE THREAT PROTECTION FOR TOP-LEVEL DOMAINS

**IDENTIFY** phishing, malware and other malicious activity within your TLD.

**INVESTIGATE AND REPORT** on all threats.

**TAKE ACTION** to stop threats and safeguard your brand.

“When criminals used a TLD’s domain for a phishing attack on a major bank, they were ready and protected by Neustar’s Registry Threat Mitigation Service” says Jeff Neuman VP of Neustar Registry Services. Neustar offers top-level domains (TLDs) a complete solution for identifying, investigating and mitigating malicious activity. “A threat that comes from a site within your TLD doesn’t just hurt consumers, it damages your brand.”

Continues Jeff, “To steal valuable data, the criminals had sent emails to lure bank customers to a bogus site. These emails looked exactly like ones the bank might send — it’s a very common phishing tactic and often times it works. Once on the site, customers were asked for personal information like Social Security Numbers and date of birth, plus account numbers, PINS and expiration dates.”

Adds Jeff, “The attackers aimed to steal identities, transfer funds and misuse credit cards. Besides hurting the bank’s customers, they would have tarnished the TLD’s positive reputation that was earned by maintaining a safe top-level domain. The TLD’s brand was at risk, so Neustar sprung into action. To protect the TLD, time was of the essence.”

### “WE HAD EVERYTHING WE NEEDED TO MITIGATE THE THREAT.”

“When the attack first happened, our threat-detection service issued an alert,” says Jeff. “Our team investigated to see if the domain was hosting malicious content. Once we confirmed the threat, we sent a notice to the registrar, which in turn contacted the registrant, or domain owner. The registrant was able to identify and remove the malicious content — effectively shutting down the phishing operation.” Banking customers were safe — and so was the TLD.

According to Jeff, comprehensive protection and experience make the difference. “Our detection uses external and internal data feeds, along with reported incidents and private security sources,” he says. “We conduct our investigations quickly and accurately, so the TLD client knows the story right away. And when we mitigate, we collaborate with the client’s team, including securely handling complaints and requests for action.”

He adds, “**To keep their good names and customers, TLDs need be ready. By proactively getting protection, this TLD continues to be a trusted leader in the domain name space.**”