www.hcltech.com

Social Engineering and Brand Protection

Organizations are increasingly tapping into the emerging digital technologies such as mobile, social, cloud, and IoT to provide better and more seamless experience to their customers, providers, suppliers, and employees. However, these new technologies come with a newer set of risks, increasing the threat surface. As the digital footprint of organizations increases, so does the touch points or fail points.

Most of the cyberattacks today are manifested through the weakest link in the chain – humans, through what is called Social Engineering. Social Engineering is defined as the use of deception techniques focused on human vulnerabilities in a system designed to manipulate individuals into divulging confidential and/or personal information which is then used for fraudulent purposes or hacking attempts.

Organizations need to aggressively guard themselves against such attacks.

HCL's Business Email Protection Services

Every customer security team is challenged today in their ability to detect, respond, remediate phishing emails and train the users in their organization. Ransomware, phishing attacks are on the rise and with the increase in the variants and the type of malware/ransomware created on a consistent basis, it is essential to detect such payloads quickly, understand the extent and also contain without impacting business operations.

OUR OFFERINGS

Business Email Protection

Phishing simulation

KEY OBJECTIVES

- Simpler management: Single dashboard for understanding phishing status of the entire organization.
- Maintain ownership of your security policy: Customer retains control of their security policy, with HCL assisting in defining it and ensuring it is expertly implemented and maintained.
- Reduce costs: deliver services within budget & take full advantage of Cybersecurity economics.

HCL'S Social Media and Digital Risk Protection Services

Businesses are investing more than ever in social media. Organizations are spending billions on social media advertising. This influx of money has created an ideal setting for cybercrime. Fraudsters create fake accounts to steal data and disrupt business. Some are as simple as unwanted protest accounts. Others might link to phishing and malware. Through fraudulent accounts, criminals can swipe all kinds of personal information: bank logins, credit cards, and even Social Security numbers. Regardless of their methods or goals, fraudulent accounts hurt your brand and your customers. The average enterprise has over 320 social media accounts, making it very complex to manage security and compliance.

OUR OFFERING

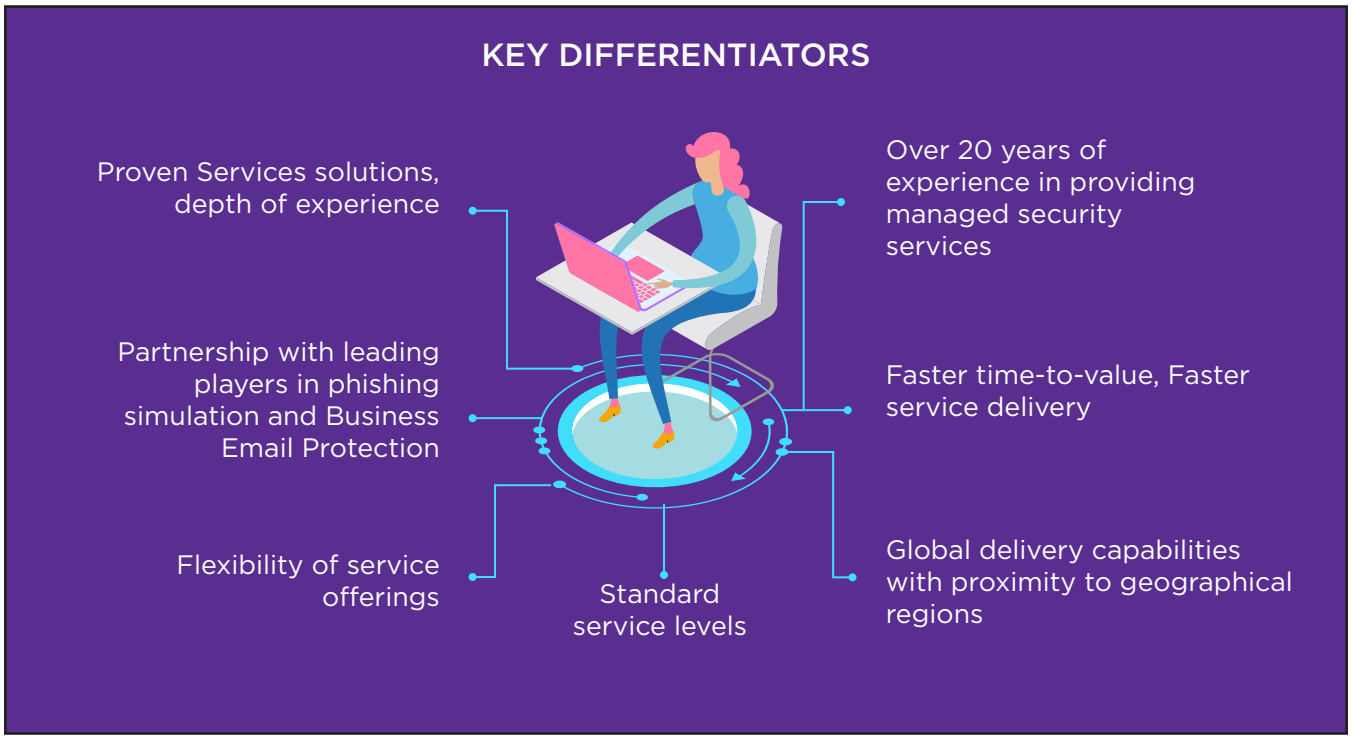
HCL Social Media and Digital Risk Protection Service protects your brands, prevent hacks, and avoid costly compliance violations. The service uses market leading threat intelligence tools to detect advanced phishing and fraud attempts by scanning major social media spaces as well as monitors clear, deep and dark web. Once a threat is identified in real time by threat intelligence tool, HCL CSFC analysts contextualize the threats, then work with you to draft response by removing false positives and adding qualitative risk ratings to prioritize mitigation actions. The service has partial to fully automated response services to take down any threat your organization faces.

KEY OBJECTIVES

- 24x7 monitoring of threats from HCL Cybersecurity Fusion Centre (CSFC).
- Threat intelligence using market leading tool combined with human intelligence to reduce false positives.
- Contextualize alert data at CSFC to assign severity levels to risks ensuring reduced response time to mitigate high risks.
- Automated Takedown Request Submission for threats like suspicious domains, social media page, mobile applications and paste sites.

HCL SOLUTION BENEFITS

- **Extensive Security Coverage to Safeguard Your Brand** - the solution scans variety of cyber spaces like clear, dark and deep web, paste sites and social media pages to gather intelligence and alerts.
- **VIP and Executive Protection** – Service scans online sources to find efforts to spoof or target important people in your organization, then use both automated and human-driven means to take down those threats.
- **Reduced Response Time** – Service Collects vulnerabilities and exploit data from all over and analyzes it in real time to see what poses the biggest risk. Provides real-time assessments of vulnerabilities so that attention can be prioritized and directed right away
- **Automated Response Controls** – Service can automatically validate and reset active credentials if they're found to be leaked.
- **Automated Take Down Requests** – Service analysts initiate automated take down request templates on your behalf to quickly neutralize threats to your brand.



BI-115206307745707-EN00AM
WX-CC6589

www.hcltech.com

Hello there! I am an Ideapreneur. I believe that sustainable business outcomes are driven by relationships nurtured through values like trust, transparency and flexibility. I respect the contract, but believe in going beyond through collaboration, applied innovation and new generation partnership models that put your interest above everything else. Right now 137,000 Ideapreneurs in 44 countries are in a Relationship Beyond the Contract™ with global enterprises helping them reimagine and transform their business . **How can I help you?**

HCL