PHISH HUNTER

Based on Microsoft technology, Phish Hunter creates a barrier that automatically detects and remediates threats that come from Phishing attacks.

Phishing is rapidly becoming the most significant security threat today. Phishing uses well-crafted emails made to convince the recipient of their legitimacy. Countless individuals and organizations have unwittingly wired money, sent tax information, and emailed credentials to criminals who were impersonating their boss, colleague, or a trusted customer. These attacks are compelling and cannot be stopped with traditional email hygiene solutions.

How It Works

Part of Forsyte's four-step approach to phishing defense, Phish Hunter is designed to detect user accounts that have been compromised by utilizing a customizable threat detection engine that monitors user logins to identify anomalies, including risky logins and risky actions. Built on Microsoft technology and hosted in Azure, Phish Hunter leverages Cloud App Security, Azure Automation, and machine learning to stop attacks before they can spread.

By tracking forensic behavioral data, maintaining known attack policies, and logging signs of compromise, Phish Hunter dramatically reduces the time to discover and respond to an attack. User defined threat levels trigger built-in automation and workflow polices that enforce account protection and modification of access policies.

When a threat is detected, policy rules are automatically sent for processing. User's activity is checked against a threat matrix. High and medium risks are sent for action. Alerts are emailed to a user defined distribution list. Remediation can be automated or manually initiated.

OUR FOUR-STEP APPROACH:

Educate & Simulate

Ensure your employees understand and can recognize sophisticated phishing and ransomware attacks and can apply this knowledge in their day-to-day job.

Prevent

Stop users from giving away their credentials before accounts get compromised using a managed Whitelist and a global Blacklist.

Detect

Detect when a user's account has been compromised by utilizing forensic polices to identify account anomalies such as impossible travel and unusual email activity.

Remediate

When threats have been identified, automated remediation occurs to lock down compromised accounts and prevent a lateral spread across the organization.

forsyte I.T. SOLUTIONS

Gold Microsoft Partner

Microsoft

Forsyte IT Solutions is Microsoft's leading provider of Email Security, Identity Management, and Information Protection. Forsyte's team of senior level MCSEs and MCSDs have tackled hundreds of complex and challenging IT projects. At our core, Forsyte's mission is to protect our client's most important assets: their people and their data. As a Microsoft Gold Certified Partner, Forsyte provides expert, high quality, user and data protection solutions to medium and large organizations across multiple industries, including education, state and local government, and the commercial sector.

Contact: 844-587-4535 | info@forsyteit.com | www.forsyteit.com