SP Guard™

Spearphishing Protection for the Enterprise

Enterprises are Under Attack

Enterprises are being attacked like never before, resulting in reports of high-profile breaches on nearly a weekly basis. Spearphishing (fake messages purporting to be from a colleague or business partner) is the primary attack vector, and attackers use human deception to get users to click on messages, leading to stolen credentials or installed malware. Attackers' messages are low-volume, well-crafted and compelling so they can avoid detection and maximize response.

Typical Defenses are Ineffective or Incomplete

Traditional approaches to spearphishing attacks involve filtering out the malicious messages before they reach the user, examining attachments/links for malicious behavior, or training users to spot fake messages. Though each step has value, malicious messages still slip through, resulting in a "toxic trickle" that is mixed in with legitimate messages. Downstream protections such as user monitoring and restricting user privileges either hinder productivity or detect attacks too late.

Users are Unwitting Accomplices

Though the vast majority of email messages are verifiably legitimate, users are faced with a daily wave of indistinguishable messages in their inbox and are left with extreme choices – trust all messages or trust none. With no effective way to distinguish between real and fake, they either plow ahead, risking the organization's safety, or proceed very slowly, impacting their productivity.

SP Guard Turns Users into Defenders

Iconix SP Guard unveils the underlying information about the legitimacy of messages in the inbox by highlighting them with an icon, giving users a tool to easily determine which messages are trustworthy. This allows users to make accurate decisions and prevents attacks from proceeding further into the network.

Icons mark verified messages

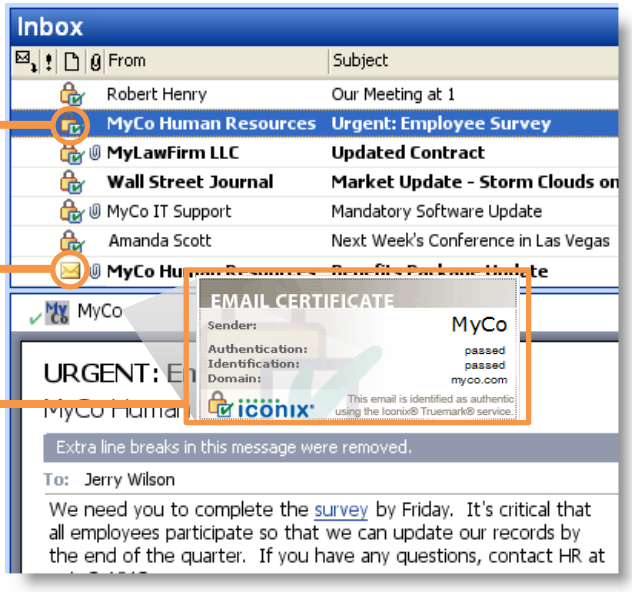
Makes it easy for users to tell real from fake, focus only on non-marked messages

Unverified messages are not marked

Even innocent looking messages from colleagues or internal organizations can be malicious

Rollover provides additional information

Placing the mouse over the icon in the open message presents additional information about the sender



Highlights

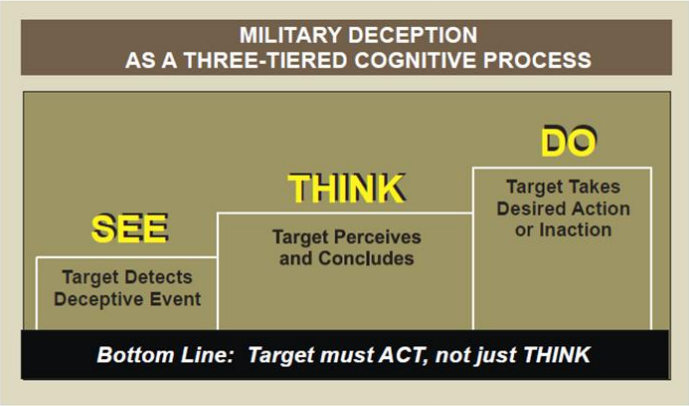
- Visual indicator defeats deception and allows users to process email confidently and efficiently since they can easily determine which messages are trustworthy
- Deflect attacks before they do damage – when users don't engage with fake messages, attacks are stopped early
- Service can be configured to visually verify both internal and external messages

System Requirements

- *SP Guard* plug-in supports Microsoft Outlook 2007/2010/2013 on Windows 7 or later
- Messages to be verified must use email authentication
- Future versions will support additional email clients

Defeating Deception

Advanced Persistent Attacks (APTs) typically rely on deception in the form of "social engineering" as the main entry point into an organization. Innocent-looking messages purporting to be from a colleague or business partner are sent in low volume to specific individuals and contain a compelling call to action. Military planners have summarized this process as follows:



Source: U.S. Joint Chiefs of Staff, JP 3-18, *Military Deception*

By leveraging perceived relevance and urgency clues along with users' email habits, attackers entice victims to engage with messages and give up credentials or become infected. Attackers then use this foothold to move around the network and escalate privileges, often going undetected for months or years. *SP Guard* stops attacks in their tracks by interrupting users' habits with simple visual trust indicators.

Technology Overview

The patented Iconix technology supporting *SP Guard* consists of an Iconix-hosted service and a plug-in that is installed on the user's computer. The plug-in works in conjunction with the user's email client to verify messages and provide visual indicators.

Configuring the service consists of loading domains/addresses into the service's database. Messages from these domains/addresses are then verified at the client using standard email authentication to ensure they are from the purported sender.

Future releases of the plug-in and service will allow additional hosting environments, an option to visually identify suspect messages, and an option to allow users to "crowdsource" feedback regarding suspect messages to IT via a button in the rollover window.

© 2015 ICONIX, Inc. All rights reserved. Iconix, "SP Guard", the Iconix logo are trademarks or registered trademarks of Iconix. While Iconix, Inc. believes that the information in this document is accurate, no warranties are created. Iconix, Inc. is dedicated to constant product improvement; therefore, specifications are subject to change without notice. U.S. Patents issued and pending.

www.iconix.com 255 W. Julian Street, San Jose, CA 95110