Identity Cues for Email™
Believe what you see. Trust what you know.

Email-related fraud such as phishing poses serious risks to any organization conducting business online, as well as to companies that provide their employees with web-based remote access to business systems. In the United States alone, over $1 billion is lost annually to phishing and email-related fraud in which crimes are committed using personal information obtained from people transacting business online through the use of fraudulent emails that mimic those of legitimate business. Furthermore, sensitive corporate information may be compromised by criminals using access credentials garnered by phishing attacks.

Key Benefits

Protection Against Online Fraud
Identity Cues for Email helps protect against online fraud without inconveniencing users with additional processes or complicated technology. Companies can reduce fraud-related losses without suffering collateral damage arising from user dissatisfaction.

Leverages Technology and Psychology
A unique combination of technology and psychology proactively informs users whether or not an email message is legitimate. Visual cues are optimized per the human recognition process in order to ensure maximum effectiveness with minimal user effort.

No User Training Required
Obvious cues enable all users, even those are not technically savvy, to instinctively recognize whether or not an email that they have received is genuine.

Safe Usage of Email for Communication
Identity Cues for Email allows organizations to safely use email as a mechasmism for communicating with customers, partners, and employees.

Non-Intrusive
Identity Cues for Email requires no user enrollment, or client-side software downloads. Users can continue to read email with whatever email software they like – users are not burdened with any changes to the way that they receive and read email messages.

Consistent User Experience
Identity Cues for Email works from all computers, including when users access email from home pcs, work pcs, handheld devices, borrowed pcs, or public kiosks. It delivers the same visual experience when users use an email client or a webmail interface.

Support for Multiple Languages
Cues can contain letters, words, phrases, or numbers – using any alphabet supported by email systems.

Support for Numerous Environments
Identity Cues for Email interfaces with all standard mails servers and easily scales to meet the needs of organizations of all sizes.

Low Total Cost of Ownership
Identity Cues for Email requires little or no ongoing maintenance.

Identity Cues protects your company, customers, and employees from phishing, pharming, online fraud, and "brand spoofing."

Identity Cues for Email is a unique, user-friendly system that displays a specific easily-recognizable visual cue at the top of every email message sent by your organization; the cues will identify to even untrained users whether emails that they receive are really from your organization or may be phishing emails from a criminal.

Simple implementation: Identity Cues for Email is delivered as mail server software that installs easily onto your network; all messages directed through the server will have cues added to them. Users do not need to be trained, no enrollment is necessary, and no steps are added to the login process.

Effective technology: Identity Cues for Email provides visual cues that leverage proven psychology and technology in a fashion that protects users without requiring them to make a conscious decision as to whether or not an email message is legitimate.

Secure: Identity Cues for Email's patent-pending technology generates visual cues by applying one-way cryptographic functions (hash functions) to user email addresses (or other user information) and a series of secret keys known only to the organization deploying Identity Cues. Based on the result of the calculations, various elements of a cue are selected and added to email messages. Cues vary between users, but a particular user will see the same cue on every email message that he receives from the organization. Only the genuine mail server can generate the proper cue for any particular user, and if no cue or an incorrect cue is displayed, it will be obvious to even a novice that something is wrong with the email that he or she has received.
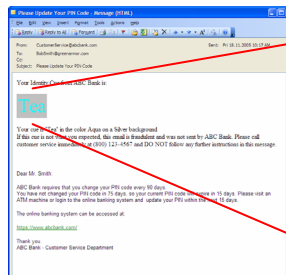
"Sometimes the easiest answers are the best."
John Dix, Editor-in-Chief of *Network World*, describing Identity Cues in a June 2005 editorial

Green Armor Solutions Inc. – +1 (201) 801-0383 – www.greenarmor.com – info@greenarmor.com