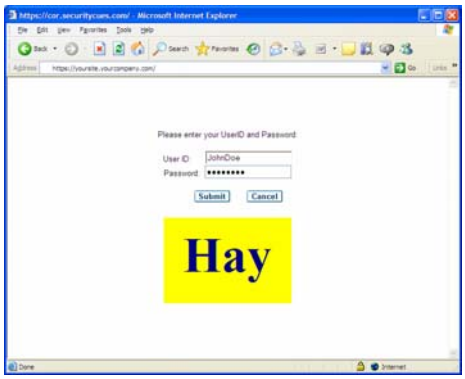
Identity Cues Two Factor™ & Two Way Authentication

Maximum Security with Maximum Convenience

Identity Cues Two Factor is a unique, user-friendly authentication system that both strongly authenticates users to an online system as well as informs users whether they are interacting with a legitimate web site or with a criminal's clone site. As the most user-friendly two-factor (and two-way) authentication system available today, Identity Cues Two Factor typically requires no user enrollment, no extra steps during the login process, no devices to be carried, no user training, and little ongoing maintenance.

Authentication using passwords or "secret" answers to questions poses serious risks — if an unauthorized party obtains a password or answer he can gain inappropriate access to sensitive resources. Two-factor authentication – in which users must possess a physical device in addition to knowing a password – is a far more secure. In fact, the Federal Financial Institutions Examination Council (FFIEC) has instructed US-based financial institutions to implement two-factor authentication for all online account access.

But, two-factor authentication can be inconvenient for users. It also does not adequately address the issue of phishing, and is usually vulnerable to man-in-the-middle attacks (such as those recently leveraged by criminals to successfully breach financial institutions that use two-factor authentication). With phishing costing American businesses over $1-billion annually, and with targeted corporate phishing (also known as spear phishing) causing significant breaches of sensitive corporate information, two-way authentication – in which systems prove their identity to users – is crucial.



Identity Cues Two Factor exceeds FFIEC guidelines and delivers both two-way and two-factor authentication in the most user-friendly fashion.

Maximum Security

True Two-Factor Authentication - Identity Cues Two Factor delivers true two-factor authentication. It never relies on users answering questions (whose answers can often be obtained by criminals) in lieu of a two-factor sign on.

Protection against Man-In-the-Middle Attacks Unlike other two-factor authentication systems, Identity Cues Two Factor protects against man-in-the-middle attacks – using dual defenses.

Two-Way (Mutual) Authentication - A unique combination of technology and psychology proactively informs users whether or not a website is legitimate. Visual cues are optimized per the human recognition process in order to ensure maximum effectiveness.

Maximum Convenience

Easiest two-factor authentication for users - Identity Cues Two Factor requires no user enrollment, no software downloads, no secrets to be remembered, no devices to be carried, and no extra steps to be endured during login.

Support for Numerous Web Environments Identity Cues Two Factor runs on numerous platforms, easily scales to meet the needs of organizations of all sizes, and requires little ongoing maintenance.

Simple: Identity Cues Two Factor is delivered as software that easily integrates with existing web sites. True two factor authentication takes place behind the scenes, and obvious cues enable all users to instinctively recognize whether or not they are interacting with an intended legitimate business.

Effective: Identity Cues Two Factor delivers true two-factor and two-way security without requiring users to make a conscious decision as to whether they are accessing a legitimate website. Psychology leveraged in the design helps ensure effectiveness even when users do not pay attention to visual cues.

Secure: Patent-pending technology authenticates users as well as the computers they use for access. Users type their login names & passwords as they always have – with no added steps. When a user accesses from an unknown machine a one-time password is required for access; the one-time password can be sent to the user via an email message, an SMS to his cellphone, or generated by a third-party product such as a hardware token.

Identity Cues Two Factor generates visual cues to prove the veracity of websites; cues are generated by applying one-way cryptographic functions to user-entered text and a series of secret keys. Only the genuine site can generate the proper cue for any particular user; if no cue or an incorrect cue is displayed, it will be obvious to even an untrained user – and even to users not paying attention – that something is wrong with the site.

Identity Cues Two Factor also offers double protection against man-in-the-middle attacks, cueing users when a site is legitimate, and warning them when it is not.

"Sometimes the easiest answers are the best."
John Dix, Editor-in-Chief of *Network World*, describing Identity Cues

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