

Online Banking: Expanding the Channel with Convenience and Security

Today's consumers expect financial institutions of all sizes to provide the convenience of online banking; credit unions that do not offer online banking, or that offer cumbersome, difficult-to-use online services, run the risk of losing members to other institutions. Furthermore, every transaction a user conducts online means one less activity for the credit union to process manually; anything which adversely impacts online user experience encourages users to perform activities through manual venues, and can lead to dramatic cost increases for a credit union.

As such, as credit unions consider implementing strong authentication to meet the new NCUA guidelines, it is critical that they consider the true impacts of any new technology introduced to users over both the short and long term. Some technologies – while sound in theory – may cause significant problems over the long term. Some basic considerations include:

- 1) Will users need to re-register or re-enroll? Re-enrollment can seriously frustrate users, as well as dramatically increase the demand on organizational help desks thereby causing the cost of both implementation and long-term management to skyrocket.
- 2) Does the system require users to install special software on each of their computers, carry any security devices or cards, or otherwise suffer an inconvenience that they do not currently incur?
- 3) Does the system perform mutual (two-way) authentication to combat phishing – if so, does the system add any extra steps to the user login process – something can irritate users, and that can ultimately lead to compromised security due to users stepping-through mutual authentication prompts without paying much attention?
- 4) Can the system be undermined by either users seeking to circumvent inconvenience (e.g., quickly stepping through authentication steps by rote without paying much attention) or by criminals (e.g., presenting a broken-image symbol in lieu of a picture in a picture-based mutual authentication system)?

Clearly, human factors will ultimately determine whether a consumer-facing authentication approach succeeds or fails over the long term.

At Green Armor Solutions, we have taken a unique approach to helping credit unions meet the new FFIEC requirements – we call it Maximum Security with Maximum Convenience. A great deal of time and effort was spent researching human behavior, and we developed our Identity Cues Two Factor system to leverage psychology so as to ensure that our offering would deliver full, true two-factor and two-way security – yet in a fashion that is not only maximally effective, but also as transparent and easy as possible for the end-user, and at an affordable as possible for any institution.

One major differentiator of our system is its ease of use – no enrollment process for end-users, no extra steps during login, no security devices to carry, etc. Our patent-pending technology is so simple that users can continue to enjoy working the way they do today – simply typing their usernames and passwords – with no added steps, yet credit unions achieve the security and compliance of true two-factor and mutual authentication.

Furthermore, by leveraging psychology our system is not only more convenient, but also more effective and secure. For example, our mutual authentication system generates visual cues by applying one-way cryptographic functions to user-entered text and a series of organization-specific secret keys. Users can instantly – and almost subliminally – recognize if a web site is legitimate based on the cues that appear; if the correct cue does not appear, it will be obvious to even an untrained user that he/she is not using the real credit union's website. Unique to identity cues is the fact that due to the psychology-based cue design, users do not need to consciously remember a picture, and, unlike systems that rely on assigning users a particular picture, the system cannot be undermined through the use of "broken image symbols," does not allow criminals to check the validity of usernames, and does not require users to share additional secrets with the credit union.



The benefits of Identity Cues Two Factor are numerous: increased member comfort with conducting business online; reduced risk of liability issues and audit problems; compliance with the NCUA guidelines; reduced phishing-related fraud incidents; fewer calls to the credit union's call center; and reduced workloads on the credit union's IT staff.



Joseph Steinberg
CEO

Joseph Steinberg is CEO of Green Armor Solutions, a vendor of information-systems security technologies that leverage psychology to deliver maximum effectiveness with maximum convenience for both users and system administrators. Its current offerings provide strong NCUA-and-FFIEC-compliant two-factor authentication of online users, improve email security, and help combat phishing, pharming, and online fraud through the use of mutual authentication. Prior to joining Green Armor, Mr. Steinberg spent more than four years with Whale Communications (acquired by Microsoft), one of the pioneers of SSL VPN technology. Earlier, he served in senior-management capacities at several product vendors and consulting firms, and worked in technical positions at Citibank and AT&T. Mr. Steinberg earned a M.S. in Computer Science from NYU, and holds a CISSP (Certified Information Systems Security Professional) credential as well as advanced certifications in IT security management (ISSMP) and architecture (ISSAP).