SECURE CHANNELS

SUBROSA©

The highly secure, simple, memorable passwordless-authentication system.

ATTACKING THE SOFTEST TARGET

Compromised login credentials are responsible for 80% of data breaches, leading to high recovery costs, regulatory penalties and damaged reputations. Cybercriminals compromise credentials by attacking the softest target in an organization, the people working there. Email phishing and carefully targeted spear phishing are the favored attack vector for unauthorized access, followed by dictionary and brute force attacks on passwords.

Phishing emails contain urgent messages, such as warnings that an account is compromised, tricking recipients into providing their password, clicking on a link or opening an attachment. Spear phishing targets executives or managers with high-level permissions, using extensive research to craft convincing messages. Clicking a link or opening an attachment introduces malware that captures passwords. Poor password hygiene also leads to compromised credentials. Weak passwords are attacked using dictionary words or brute force guessing. Credential stuffing attacks employ lists of reused passwords obtained on the dark web.

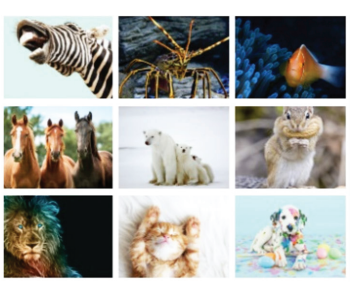
SUBROSA AUTHENTICATION

Secure Channels' patented SUBROSA authentication replaces traditional character-based passwords with secret keys cryptographically generated from grid patterns overlaid on image-based resources, such as high-definition photos. SUBROSA passwords can't be phished, guessed or captured using typical attack strategies. The authentication process is executed on Secure Channel's cloud based SCIFCOM portal.

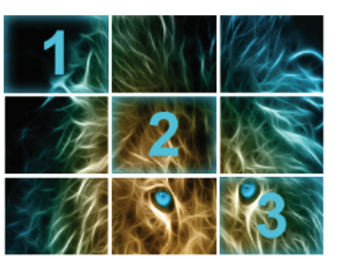
Creating a SUBROSA password is beautifully simple.

STEP 1
Admin defines grid size

STEP 2
Users select their images



STEP 3
Users define a pattern from one or more images

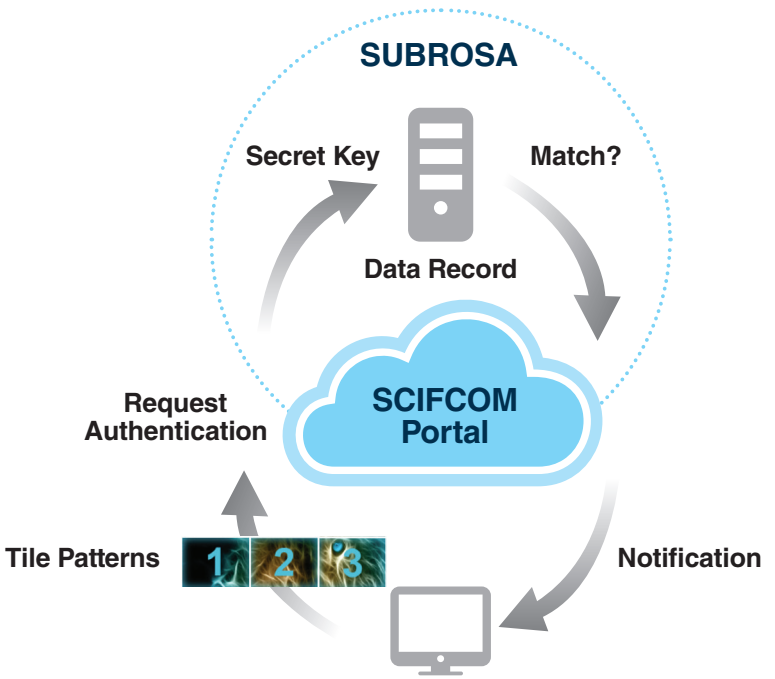


Outcome:
A cryptographically secure secret key

Nothing is stored on the user's workstation when SUBROSA password setup is complete. The user's favorite photos and patterns are easy to remember while password hygiene is effortlessly enforced.

The user only knows the photos and patterns they select with a touch screen or mouse pointer, not the secret key password. Redundant SCIFCOM servers host the encrypted user setups, photos, and data records containing the secret key passwords. The same photos and patterns selected during setup are submitted to the SCIFCOM portal and converted into a secret key to match with a stored data record. The initiating website or application receives the authentication result.

The SUBROSA authentication process:



The application programming interface (API) and software development kit (SDK) easily implements SUBROSA authentication in distributed web applications. Password setup generates API code for adding SUBROSA authentication directly into web pages.

USE CASES

SUBROSA authentication is SAML 2.0 compatible for single sign-on (SSO) authentication and FIDO Alliance compliant.

Standalone Authentication – SUBROSA replaces character-based logins vulnerable to phishing, credential stuffing or brute-force attacks. The platform initiating the login and the application requiring authentication connect to the SCIFCOM portal for the authentication process.

Multifactor Authentication – SUBROSA's image-based password replaces one factor in a multifactor authentication scheme that includes biometrics or a hardware fob. The SUBROSA authentication factor is executed through the SCIFCOM portal, enhancing the security of the login process.

Passwordless/Password Managers – The PIN used by some passwordless login schemes and the master password required by password managers is vulnerable to phishing and brute force attacks. SUBROSA replaces PINs and master passwords, executing authentication through the SCIFCOM portal for enhanced security.