Random Character Authentication - Easy as ABC

Intuitive logon technology that's got that 'get it' factor

PIN PHRASE

Delightfully simple. Deceptively secure. By fusing 'something you have' with 'something you know' and rendering them inseparable, PINphrase prevents reverse engineering and increases logon security.

Traditional 2 Factor Authentication is based on the concept of pairing 'something you have' (a token) with 'something you know' (a PIN or password) with the intention of identifying users.

Challenges arise when that 'something you have' is used by an unauthorised individual. Or if the 'something you know' becomes compromised – a PIN is hacked by keystroke loggers for instance.

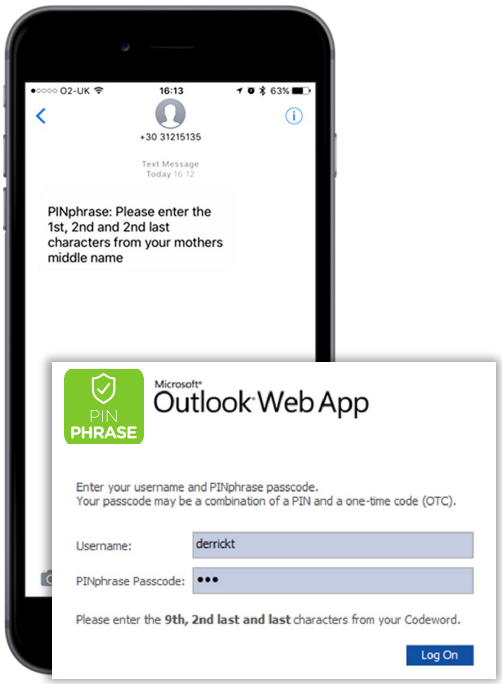
PINphrase eliminates both risks by utilising randomised questions and characters that are meaningless to anyone other than the user for which they are intended. Since answers are never divulged in full, they remain private throughout the logon process.

How it works

1. Your security team creates a pool of questions: a mother's maiden name, a memorable place or date, or a favourite sports team. At the same time, it also specifies the minimum number of questions users must answer and the minimum number of characters that must be entered during logon.

2. For the initial logon, users are provided with a temporary codeword to use. After which each user is asked to provide answers to a selection of the generic questions set up by the administrator. These answers are stored by the server.

3. To generate a logon phrase, the system randomly selects one or more questions from the pool of authentication questions completed. It also selects characters from those answers using a patent-pending algorithm which is derived from OATH technology.



Features and highlights

- No need to carry hardware tokens
- Securely logon on to Windows desktops from any location
- Cost effective - especially compared to hardware solutions
- Secure access to internal and cloud-based applications
- 1.5 and 2 Factor Authentication
- Real-time or pre-sent token delivery via SMS or email
- Web-based operator portal for day-to-day operation of IT helpdesk
- Self-service AD password reset
- Rapid user provisioning (thousands in minutes)

Authlogics

Random Character Authentication - Easy as ABC

PIN PHRASE

Fewer account lockouts mean significant helpdesk savings

Say you have stored the answer 'Samantha' as your first pet's name. The PINphrase way of asking you to logon might be: 'Please enter the 1st, 4th, 5th and 2nd last characters of your pet's name.' to which your answer is 's a n h'.

4. Upon logon, the system never prompts for the entire answer, but rather random letters from one or more random answers. With this, the users sensitive is never revealed in its entirety only random and relatively meaningless characters within.

A token so simple it's child's play

With PINphrase, users don't need to remember anything new; the system uses information they already know and are not likely to forget. It's not even important for users to answer the questions correctly or truthfully, they just need to be able to recall the answer supplied.

Since answers are not passwords, there is no need to combine alpha-numeric, mixed cases or punctuation marks – a huge plus when it comes to user recall. This translates into less account unlocks and resets, leading up to 40% savings for helpdesk budgets,

And because the entire answer is never entered all at once, it's impossible for cybercriminals to work out responses by observing or capturing logons.

De facto Standards

The combination of standards-based OATH and de facto authentication methods results in a hybrid approach that provides strong security and retains ease of use and low cost of ownership.

The questions can be displayed on either a web logon page in your browser for 1.5 Factor authentication, or on a mobile phone by means of email or SMS for full 2 Factor.

PINphrase is proving to be the answer to many organisation's security concerns and suit many usage scenarios.

Open Authentication (OATH)

The Initiative for Open Authentication (OATH) is a collaborative effort of IT industry leaders aimed at providing a reference architecture for universal strong authentication across all users and all devices over all networks. Using open standards, OATH will offer more hardware choices, lower cost of ownership, and allow customers to replace existing disparate and proprietary security systems whose complexity often leads to higher costs.

- Emergency override access
- SMS flash and message overwrite functionality
- Active Directory or LDAP database storage (no schema extensions)
- RADIUS and Web services interface for universal integration
- FIPS 198 and 180-3 compliant
- Based on OATH technology

About Authlogics

Award-winning authentication experts Authlogics are committed to assisting IT managers improve security while making it easier for users to access their information. Authlogics focuses on helping your business transition away from password-driven environments, while increasing your security posture and compliance to policy.

PINphrase is one of the core components of the Authlogics product suite, an enterprise-ready authentication and management platform designed to fit seamlessly into existing Active Directory environments or as a standalone solution.

Authlogics has been designed to integrate with most systems from remote access solutions to application specific requirements via standard interfaces such as RADIUS and Web Services. It is quick to deploy, easy to maintain and manage with tools such as web-based user self-service and helpdesk operation portals. Authlogics also includes Windows Desktop Logon functionality to allow for online and offline access to Windows

Authlogics

www.authlogics.com | sales@authlogics.com | +44 1344 568 900 | +1 408 706 2866