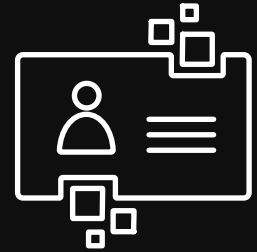


Account Take Over

Account take over is an abrasive event that has significant impact on those affected. The person whose account has been taken over feels violated, their trust in the services they use is diluted and there is often real-world impact in the form of theft or miscreance.

Businesses are under continuous pressure to be vigilant and responsive in their risk mitigation strategies to identify and stop Account Take Over events across their employees and their customers – and in spite of increased awareness and improved capabilities; it is still a daily event.

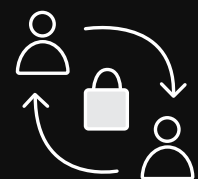
Unlike other approach that are abrasive, point solutions; or provide a confidence level that you are required to then act upon, CIPHERISE fights the problem at its root cause by eradicating uni-directional trust.



The concept of a user having a username and password is history – we replace it with a dynamic digital relationship that defeats account take over.

How does it work?

Standard authentication methods depend upon a user providing credentials for verification to a system when you try to access it. This standard eggshell approach worked 50 years ago, but continuously fails in the modern age. Belt and brace approaches such as two-step, two-factor and multi-factor have tried to solve the problem, but they are generally expensive, introduce extra steps, add friction, and do not actually solve anything.



CIPHERISE takes a different approach – in a single, sub-second action we:

- Confirm the organisation is true and correct to the user.
- Confirm the user is true and correct to the organisation.
- Confirm that the user intends the action.
- Cross check for tampering and manipulation.
- Create an independent, immutable audit trail.

By design, we remove the ability for someone to provide credentials directly to a system and break the chain into two parts. Have someone request an action as a particular identity **and then** the receiving side reaches out and contacts **the owner of that identity** to ensure they are not just **authorised** but **intending** the interaction.

A bit on security



Invented and made in Melbourne, CIPHERISE delivers a new concept called Secure Digital Engagement. It creates a bi-directionally intertwined cryptographic relationship between an organisation and your employees/customers that provides a simple and seamless ongoing capability to perform authentication, authorisation, notification, and digital signoff events.

No usernames

No passwords

No friction

No kidding

About Forticode:

Founded in 2013, Forticode has invested heavily in curious people that wish to not just make a difference, but are prepared to do the hard work associated to researching, testing, failing and persisting until dysfunctional norms can be replaced with a solution.

Two driving goals keep us motivated:

We have a social responsibility to ensure everyone, regardless of demographic, has the right to access modern, digital services without concern, fear, or complexity.

Everyone has a right to privacy but not anonymity.

About CIPHERISE:

CIPHERISE is a mobile-first Sovereign cloud product that replaces the need for people to know usernames/passwords/PINs/mother's maiden name - we eradicate these entirely - nothing to forget - nothing to give away inadvertently.

Users of services Secured by CIPHERISE are no longer potential victims of identity and credential theft whether it be email, SMS or phone-based phishing and many other social and aggressive fraud and credential theft mechanisms.

Contact enquiries@forticode.com for more information