RESIDENT®

DATA 🔒 SECURITY

AT RESIDENT WE TAKE CYBER SECURITY SERIOUSLY

HERE IS A QUICK LOW DOWN ON THE THINGS WE DO AND THINGS IN THE PIPELINE

Data Security

TWO-STEP VERIFICATION

Two-Step Verification also known as two-factor authentication is an added extra layer of security to your Client database in case your password is compromised. Once set up, every time you sign into the Resident portal on an untrusted device you will receive a security code via email or text, to check that you are you. All our administrative users have two-step verification as standard.

IP ADDRESS RESTRICTIONS

We are currently looking at restricting access to the Resident portal via internet protocol addresses (IP address) which is a numerical label such as 192.0.2.1 connected to a computer network that uses the IP for communication. Only users from a list of approved IP addresses within a Client's own network will be able to login. When a request to the portal is generated from any user, their IP address is evaluated against the allowed list. If the IP address is not on the list, the portal displays a web page with an error code and the user is unable to go any further. Access is automatically denied.

PASSWORDS

When it comes to password management passwords are generated and managed by the user. We will strengthen passwords requirements by the end of 2023 adding upper and lower case letters, numbers, and special characters. Upon request we can set up password refresh requirements which can be any number of days. The most frequently used period is 30 days – so users must update their passwords every 30 days otherwise access is denied until they do.

Humans tend to fall into predictable routines creating passwords based on things familiar to us and easy to remember (we all experience information overload!). Creating unique, strong passwords is easier said than done. Hackers armed only with an email address can use "password spraying" to test passwords on readily available 'common password' lists to see if any work with your email address. Lists of emails are often available on the dark web and people are regularly targeted via phishing scams to harvest their personal data. Here are some tips on creating strong passwords:

1. Use nonsense answers to reset password security questions – you know the ones that ask you your first pet's name, favourite teacher, first school, mother's maiden name

2. Avoid common words and phrases, names, significant dates like birthdays and anniversaries

3. Avoid easy sequential number combinations like 123456

4. Case and numerical substitutions are still easy to guess so use passwords and combinations that are complex and unique

5. Avoid using the same password for everything even slight variations leave you exposed

6. Consider using a password manager which can offer password generation and storing, password health checks, two-factor authentication, form and payment autofill

7. Clear your cookies as these store a wealth of info that hackers can target

8. Learn how to check for spyware apps and software that could be spying on your online activity and harvesting your passwords

Data backup

HOW DO WE BACK UP RESIDENT?

The infrastructure of Resident is using Azure cloud for backups. As a database server we use SQL service (Azure SQL Database). We are able to restore each database 35 days back in the past with accuracy of up to 10 minutes (Automatic, geo-redundant backups).

WHAT HAPPENS IF THE DATA CENTRE EXPERIENCES A CATASTROPHE?

Understanding customer availability expectations is vital to reviewing overall operations for the application. Information stored in the cloud is actually held on servers in data centres. If the whole data centre experienced a major issue Resident would become unavailable. Resident follows Azure's service level agreements but does not have high-availability at the moment. We are planning this with the launch of the next version of the system in 2023/24. High-availability is the ability of a cloud service to remain available by making sure that there is no single point of failure and to ensure a specified level of performance. Based on years of experience, issues with the data centre are rare and short lived so we have never had the necessity of implementing high-availability.

WHAT HAPPENS IF YOUR SERVER WHERE CLIENT DATA IS HELD COMES UNDER A DNS ATTACK?

A DNS attack is a cyberattack in which the attacker exploits vulnerabilities in the Domain Name System infrastructure. Some of the most common DNS attacks are denial-of-service (DoS) and distributed-denial-of-service (DDoS) where attackers flood internet servers with so many requests that they simply cannot answer them all,

and the system crashes as a result. Servers in the data centres can literally fall over. Other types include DNS tunnelling, DNS poisoning and cache poisoning.

In the case of Resident's database server there is no possibility to connect to it or hack it because the whole traffic is separated from it and can only be accessed by dedicated Azure services and the IPs of Resident's administrators.

Protection from attack on our web services is used on App service which provide 24-hour threat management protecting the infrastructure and platform against malware, distributed denial-of-service (DDoS), man-in-the-middle (MITM), and other threats. On top of that our DevOps (Development Operations) team monitor the system for any anomalies.

Data

DO WE RING-FENCE INDIVIDUAL CLIENT DATA FROM OTHERS?

A ring-fence is a virtual barrier that segregates a portion of an individual's or company's data from another's. Yes each managing agent's data is ring fenced in Resident. This means each database is physically separated from others and cannot be mixed.

THE ULTIMATE BLOCK MANAGEMENT SOFTWARE

Resident

Launched in 2014, we are a cloud-based, block management portal designed to simplify and modernise the property management process for both managing agents and those who choose to self-manage.

Our mission is to be the industry-leading, cloud-based, property management platform. Driven by the belief that we can make property management better for everyone by sharing knowledge, striving for transparency of information and encouraging compliance, and by the desire to set the highest professional standards.

Read more

RESIDENT

RESIDENT®

WWW.RESIDENT.UK.COM