Phonexa™

Our Data Security & Protection Policy

Phonexa is equipped with multiple robust layers of virus-resistant firewalls and data protection tools to ensure security. As a company that respects and upholds strict privacy regulations, data security is our topmost priority.

Data Protection

3 Independent Levels of Intrusion Prevention

Cloudflare Web Application Firewall[1]: Cloudflare's enterprise-class web application firewall (WAF) protects your Internet property from common vulnerabilities like SQL injection attacks, cross-site scripting, and cross-site forgery requests with no changes to your existing infrastructure.

Google Cloud Firewall: The GCP firewall lets you allow or deny traffic to and from your chosen internet-connecting devices. This firewall provides an impressive level of protection at the virtual networking level.

Internal Firewall: As an added layer of protection, we've implemented our own internal firewall to secure internal network traffic and closely monitor all abnormalities.

3 Independent Layers of DDoS Prevention

Cloudflare[2]: Cloudflare's network capacity is 15x bigger than the largest DDoS attack ever recorded. With 15 Tbps of capacity, it can handle any modern distributed attack, including those targeting DNS infrastructure.

Google Cloud[3]: The Google Cloud Platform deploys detection systems, implements barriers, and absorbs DDoS attacks by preventing hackers from overwhelming or disabling access to your end users.

Automated IP Ban System: Since DDoS attackers use multiple hosts to launch a large-scale attack their targets, Phonexa's sensitive Automated IP Ban System has been implemented to ban any and all IP addresses that pose even a remote threat to the system, mitigating all risks of a full blown DDoS attack.

Encrypted Client-to-Service Channels

Client-server communications have been heavily encrypted for maximum data security. Rest assured that all traffic passing between you and the Phonexa server will be protected by multiple layers of encrypted algorithms.

Virus-Resistant Software

On top of the three powerful firewalls and DDoS prevention methods in place, we've also tamper-proofed our software to make it more resistant to attacks, resulting in the system becoming a smaller target for attackers overall.

CIPP/US Certified Staff

Phonexa's key personnel are Certified Information Privacy Professionals and possess an understanding of global concepts of privacy and data protection law and practice. The global industry standard for professionals in the field of privacy, CIPP helps organizations strengthen compliance and risk mitigation practices.

[1] **Cloudflare Web Application Firewall:** https://www.cloudflare.com/static/media/pdf/cloudflare-datasheet-waf.pdf
[2] **Cloudflare DDos Prevention:** https://www.cloudflare.com/media/pdf/cloudflare-two-pager-ddos-protection-rate-limiting.pdf
[3] **Google Cloud DDoS Prevention:** https://cloud.google.com/security/overview/whitepaper

Security

3-Step Account Security Protection

For added gateway protection, users go through a 3-step login process, including the initial password submission, one-time token authentication and a PIN passcode.

- Valid Passwords are 8 to 32 characters in length with no spaces , include upper and lower case characters, include at least one numeric digit, and include at least one special character such as - . , @ : ! $ /.
- Passwords are case sensitive.
- Do not select a password that is similar to the Company Name.
- We recommend changing the password every 30 days and Phonexa's Two-Factor Authentication.

Two-Factor Authentication

Keep the bad guys out, even if they steal your password through malicious software. Phonexa secures your account by requiring a mandatory second login step. Two-Factor Authentication protects against phishing, social engineering and password brute-force attacks and secures your logins from attackers exploiting weak or stolen credentials.

Flexible ACL System

The ACL, or access control list, is a list of permissions attached to individual operations. Phonexa’s flexible ACL System allows for combinable user roles, an additional password layer for modules with sensitive data, and the ability to fine-tune system privileges on the individual user level.

Brute-Force Password Attack Prevention System

Also known as brute-force cracking, this specific attack uses trial and error to decode encrypted data through extensive effort. To combat brute-force attacks, Phonexa’s system creates captcha for each login and automatically locks the account after a certain amount of failed login attempts, notifying the administrator of the activities.

PCI DSS Compliant[4]

The Payment Card Industry Data Security Standard is a set of policies and procedures intended to optimize the security of transactions and protect against the misuse of personal information. PCI DSS ensures a secure network, encryption of sensitive data including banking information and Social Security numbers, among other enforcement measures.

[4] **Payment Card Security Policies:** https://phonexa.com/resources/payment-card-security-policy.pdf

Reliability

3-Level Manual Testing

- Penetration Testing
- Trustwave Security
- Independent Ethical Hacker(s)

**Phonexa does not grant third parties access to production servers for penetration testing and similar services. All tests are performed on isolated (sandboxed) instances containing test data only.*

Automated Health-Checks and System Testing

An automated system assessment is performed regularly to actively combat potential problems. These sensor automations embody our goal to stay proactive in maintaining a bug-free, healthy and productive system.

Updates and Maintenance Time Windows Tailored to Clients Priorities

As a consistent theme for Phonexa’s fully customizable platform, you have complete control over the updates and maintenance time frames.

CONTACT

818-800-0000

sales@phonexa.com