



Security Overview

The security of your personal and business data is a primary concern at Newtek Web Hosting and we've invested millions in our infrastructure over the years to be sure your critical information is safe. This document provides a brief overview of some of the security features, policies, and procedures we've implemented to address the everyday security concerns of customers, from the physical security of our datacenter, to our internal controls, and even our hiring practices. We've purposely excluded sensitive information from this document that could be used in illegal or malicious ways against our network or to our customers.

Network Availability

Network availability and uptime is a key attribute for any quality web hosting provider, and we've made it one of our top priorities. It is our policy to have two full tier 1 carriers utilized at levels far below their peak thresholds, which feeds into our fully redundant network infrastructures, allowing for a complete and immediate switchover if one of the carriers became unavailable for any reason.

We also employ redundant power supplies to our network and datacenter operations to ensure your website and related services are available even during a power outage. We use top-of-the-line uninterruptible power supply systems for protection against power spikes and outages, and our multiple 2 Mw Caterpillar diesel generators allow us to function at full capacity for an indefinite period of time.

Server Monitoring

Servers on our shared hosting segment are monitored 24 hours a day, every day of the year, in 5 second intervals. We also use a blend of third party products, in-house developed solutions, and 24X7X365 staff to monitor a multitude of performance related services, including CPU and memory usage, and other items to ensure the stability and reliability of our network and to customer websites.

In addition to monitoring, Newtek Web Hosting has implemented a detailed escalation policy for issues that go beyond that of general server or network issues. In general, we employ secondary and tertiary levels of escalation on all issues, regardless of scope. Support representatives, server operations, and network operations staff are available 24X7X365 to ensure that all issues are dealt with and resolved as quickly as possible.

For dedicated and virtual private servers (VPS), Newtek Web Hosting offers a "managed services" option that handles some of the server monitoring responsibilities and patch management to the server. These "managed services" include the management of updates on all preinstalled software by Newtek Web Hosting administrators, performed on a similar schedule to that of our shared segment, ensuring that they receive updates and fixes in a timely manner. In terms of monitoring, customers can set test pages for a variety of request types, like standard HTTP requests, requests to monitor services (e.g. ColdFusion

and/or ASP), SMTP, POP, and others. These requests can be made at a time interval set by the customer, and then rules are created for how our staff is to react if one of those monitors happens to fail. While several of the solutions to server problems can be handled with simple reboots of servers or services, other courses of action may be required to alleviate issues. The managed services option includes, at no additional costs, reboots of services and restarting of services. However, any additional work on the part of the Newtek Web Hosting staff may incur an additional hourly charge. Regardless, customers utilizing managed services can track any and all services performed on their servers using our WebControlCenter.

Data Protection & Security

One of the best methods to protect your critical data is to be sure you always have reliable backups. All services on our shared hosting segment receive daily backups, including website, database, and email data. Dedicated or VPS customers have the option to add a daily backups option as well. We retain all backups for a two week period, which includes two full weekly backups and then daily incremental backups of all new data added in between.

Virus protection for a network infrastructure is also essential. Therefore, Newtek Web Hosting scans for viruses on all files coming into the shared hosting segment, and runs continuous scans of all servers, regardless of server function. This virus scanning occurs in real time and includes the scanning, quarantining, fixing and/or deleting of emails that come into our network. In cases where emails are deleted or quarantined due to infection by a virus, an email is returned to the sender informing them of the infection.

While securing servers is one step to protecting the integrity of our network, stopping "bad" traffic from reaching the servers in the first place is even more important. Newtek Web Hosting utilizes firewalls and other security features throughout its network. We restrict common ports of attack at our firewall, and these are manual/static changes. Because tens of thousands of packets pass through our network every second, it is not possible to know what type of attack or data is coming in or leaving out network; this is why Newtek Web Hosting implements two types of preventative measures: 1) The first system monitors signatures on common packet types. When a certain signature is detected, an alert is raised. Depending on the threshold limitations set for these alerts, dynamic blocking is done at the firewall to stop the data from continuing to enter our network, and 2) since monitoring types of packets is not enough, monitoring the number of packets from certain locations is incredibly important. While valid packets that are not caught by their packet type will pass through as valid data, an extreme amount of them from one or many locations is considered a Denial of Service attack. We have systems that monitor normal trend of data flow and when unusual amounts of traffic are found, our systems dynamically block the data from the network on the fly.

Newtek Web Hosting also utilizes a third party to run security and vulnerability audits. These audits include, but are not limited to, port scans, server configuration audits, and other security and vulnerability checks that help ensure that the network and servers we manage are as secure as possible. These audits keep Newtek Web Hosting safe, secure, and PCI compliant. Newtek Web Hosting is also registered as a Safe Harbor with the U.S. Department of Commerce. What this means is that Newtek Web Hosting has met or exceeded certain guidelines for the adequate protection of private and confidential information as defined by the European Union's Directive on Data Protection. More information on Safe Harbor can be found at www.export.gov/safeharbor.

Internal procedures and controls

Newtek Web Hosting takes great care to secure customer data, and that includes internally. Newtek Web Hosting employees only have access to the customer information that enables them to perform his or her job duties to their fullest extent. Using our custom WebControlCenter, we are able to limit access to customer data for all employees. For example, our Customer Service Department has access to billing information pertaining to clients, but they do not have access to the functionality that allows them to change customer site settings, or terminal into customer servers. Our Technical Support staff, on the other hand, has the ability to terminal into servers, but may not necessarily have access to customer billing information. Access to customer data is strictly determined by job role and position within the Newtek Web Hosting employee structure.

We've also implemented a change management policy and procedure to effectively manage and control all internal changes that may affect customers. This includes, for example, any internal request for access to our core systems, and any changes to our website or WebControlCenter. This ensures that all changes that come internally have been properly tested and approved by a Newtek Web Hosting executive before they are deployed.

In terms of hiring practices, Newtek Web Hosting has, and follows, strict guidelines when it comes to hiring. These guidelines are addressed in the Employee Handbook and Non Disclosure Agreement that each employee receives, reads, and is required to sign off on as proof of reading and understanding all of Newtek Web Hosting's policies and procedures. Each prospective Newtek Web Hosting employee is phone screened by the Human Resources staff and then scheduled for in-person or phone interviews with the appropriate hiring manager. Hiring managers may elect to extend the hiring process based on the candidate pool and needs of the company and department. Any candidate who makes it through the interview process receives an extensive background check prior to any offer of employment. The President and Senior Vice President of Human Resources or CEO of the company must approve any request for new hires prior to an offer of employment.

Finally, Newtek Web Hosting has a strict policy for the release and dissemination of customer data that is addressed in both our Terms of Service Agreement and our Corporate Privacy Policy. Newtek Web Hosting does not release, for any reason, any information relating to customers without prior written permission from the customer or without proper authentication and verification of ownership of that data. This policy covers everything from billing and support issues as well as questions from prospective Newtek Web Hosting customers looking for information or references about existing customers (for example, a prospective customer may ask us to provide them with names of our existing clients so they can speak with them. We would not provide any information in this case, and refer the inquiry to our public forum where existing customers may willingly provide their own information.)

Physical Security

Our investment in enterprise-level hardware, data security measures, and network redundancy would be meaningless if we did not have the proper physical security measures in place to protect our assets. Therefore, we have implemented several security measures to ensure the physical security of our infrastructure and customer data. At our corporate office, we employ keycard access to enter the building and to key areas within the building. This ensures that only Newtek Web Hosting employees, or those persons with proper authorization, are able to enter our corporate office.

The Newtek Web Hosting datacenter can only be accessed by authorized Newtek Web Hosting staff with proper keycard, touch pad, and retinal scanning clearance, and well as passage through a bullet-proof, weight sensitive man-trap booth, so that only those employees requiring access to our servers are

granted access. We also utilize manned, third-party security staff at all times, 24X7X365, and a state-of-the-art video surveillance system.

Our datacenter is also located in Scottsdale, Arizona, a geographical area that features a highly stable climate and is nearly free from all natural disaster threats, such as earthquakes, tornados, hurricanes, and landslides. Scottsdale also ranks low among large cities as a target of terrorist or malicious activity.

Conclusion

As we have illustrated, Newtek Web Hosting has implemented many ways to protect customer data, not only at the server level, but at the highest points of our network. All of our precautions, of course, do not ensure 100% protection, and our procedures are ever evolving. It is our goal to continually update our security procedures so that we can provide the most secure web hosting environment possible to our customers.