



5 Network Security Tips To Keep Hackers, Viruses & Spyware Away

A network that promises a 99.9% security rate, sounds fairly safe, right? Think again. Consider the 0.1% error-prone situations:

- 12 newborns would be handed to the wrong parents each day
- 880,000 credit cards would have wrong cardholder information on their magnetic strips
- 315 records in Webster's Dictionary will be misspelled
- 18,322 pieces of mail would be wrongly handled every hour

In reality, a 0.1% failure rate can cost thousands of dollars an hour due to a “tiny” compromise in network security. It's crucial to have a robust network security solution in place that boosts productivity, performance and, most significantly, protects your investment.

Equally important, your client's confidential and sensitive information should be safeguarded against any threat from spyware, viruses or hackers. The IT experts have an insider joke “if you want to know something confidential about a person or a company, hack his attorney's or doctor's computer.” No matter which industry you are in, your customers trust you with their proprietary data that can only be protected with solid network security.

Securing a computer network within one office or multi-site offices globally – is not an easy job. It requires expertise in network design, device configuration, and protocols that Celestix is known and trusted for. Additionally, a few of the network security functions that Celestix offers are:

- 24x7 tech support
- Managed services
- Training & professional services
- Access to Celestix Knowledge Base
- Dedicated Technical Support Account Manager (TSAM)
- Periodic security patches, quarterly system health checks, onsite troubleshooting, and more

Here are 5 simple, network security tips to get you started on securing yours and your client's data from being hacked, misused or intercepted:

1. Reducing network presence

Turn off all nonessential network activities (especially those outside the firewall) when not in use such as FTP, file sharing and Telnet.

2. Using encryption software for emails

Using a personal email certificate not only lets you sign your email digitally so that recipients can verify that it's actually from you, but also encrypts your messages so that only the intended recipients can view it.

3. Avoiding common patterns in passwords

The types of programs to crack passwords used by hackers try patterns of words using English and foreign language dictionaries. Avoid those common patterns, use strong passwords.

4. Implementing security patches periodically

Network firewalls cannot prevent hacker attacks that trick people into clicking on dangerous links in their web browsers, hence stay away from clicking on strange links/attachments in email from people you don't know. Implement security patches periodically.

5. Using a strong password and encryption program to avoid data breaches

A combination of a password and encryption program, with the flexibility of protecting individual files to hardware-based full discs on your device is highly recommended. This is to cope with any theft or misplaced laptop computers that can contain your company's trade secrets, financials, marketing plans, and more. This is one of the largest single type of security breaches in today's times.

We can protect your systems 24x7 with our network security solutions that will help you maximize your ROI on the IT infrastructure, and minimize your network downtime. Celestix is the only company that offers a performance-tuned, turn-key Microsoft DirectAccess solution - **CelestixEdge**, for secure remote access for Windows managed and non-managed clients, with the lowest total cost of ownership (TCO). **CelestixFederated**, another network security solution targeted specifically to enable secure federation of user accounts, provides a simple and rapid AD FS deployment. The solution simplifies single sign-on (SSO) and access management for Microsoft Office 365 and numerous other SaaS applications. **Schedule your free 2 hour technical consultation today!**