uring the growth of any business, somewhere between two computers and ten, companies realize the need for a computer network. Computer networking allows multiple computers and devices to communicate and share information and resources, such as all sharing the same main printer.
During the growth of any business, somewhere between two computers and ten, companies realize the need for a computer network. Computer networking allows multiple computers and devices to communicate and share information and resources, such as all sharing the same main printer.

The ability to communicate directly between the computers on your network and share files can greatly increase productivity. There is also a cost-savings associated with the ability to share devices like printers and scanners between several computers. With any connection between computers and other devices, whether wired or wireless, there comes potential security risk. But if you know how to safeguard your network, you can enjoy the convenience and savings without putting your systems in danger.

Risks Associated with Computer Networking

Security First IT works tirelessly to keep its customers’ networks safe from viruses, data loss, and unauthorized intrusions, so we know how to deal with and avoid many of the security issues that can plague company networks.

Some of those risks we protect against every day include:

- Viruses spreading from one computer to another
- Hackers trying to gain access to sensitive company data
- Files being stolen internally by an unauthorized person
- Weak access points like mobile devices or USB drives
- Spyware meant to record keystrokes and other activity
- Unauthorized access by employees to sensitive files
- Inadvertent corruption of data

Keep your personal information highway free of bandits.
The costs to companies from insecure networks are very real. While all businesses may not have a large network security breach as retailer TJ Maxx did in 2007, costing them a reported $8.6 billion, according to reporting by ZDnet, small and medium-sized businesses can also suffer significant losses from unsecured networks.

An article by NueMD, about the cost of stolen health records is very telling. According to the 2016 Cost of Data Breach Study from IBM and the Ponemon Institute, the healthcare industry has a cost of about $355 per medical record that is lost or stolen. Many network hackers look for data that can be used for identity theft, medical records are a prime target.

Strategies to Implement for Secure Computer Networking
Despite all the scary stuff out there, an experienced IT provider can ensure that your company’s computer network is implementing the smartest and best security strategies to stay safe and protected from intrusions. Here are a few of the strategies that experts like Security First IT use to keep their clients’ computer networks safe.

Want to join in the conversation? Talk with us on social media!
Facebook: https://www.facebook.com/securityfirstit/
LinkedIn: https://www.linkedin.com/company/securityfirstit

Hashtags: #networksecurity #computersecurity #cybersecurity #computernet #gatenet cse computer networks #computer networks gate #computer #computer networks course

Staff Expert:
Anton Kioroglo
Anton is the co-founder of Security First IT and our resident expert in networking and cybersecurity.

Find more articles infused with his expertise at:
https://securityfirstit.com/blog/
Layered Defense
Just like a running back on a football team has to go through several linemen and sometimes even the receivers to get the goal line, a layered defense in a computer system has several different checkpoints and security layers to help ensure intruders don’t get through.

Employee Training
Your computer users are your first line of defense against security breaches. Training employees on computer security and implementing systems they can use to ensure they don’t click on a fake email link goes a long way to keeping your whole network safe.

Defined Security Zones and User Roles
No HR Department wants to accidentally have an employee get access to their co-worker’s payroll records. By setting specific security zones and user roles (access limits) correctly, ensuring that no one sees certain files unless you want them to.

Firewalls and Virus Protection
Nothing can replace the security of a strong computer network firewall and virus protection software that scans all devices on your network for any malware or other intrusions. A good IT provider will know the best ones to use.

Disabling Unused Services or Access Points
You used to use a certain contact management software on your computer network, but now you’ve switched to a different one. Have you completely disabled any network access from that old software system? Shutting down unused services and network access points is another important strategy to keep your system protected.

User Device Control
Mobile devices are now being used just as much, if not more than computers. Apps that connect your sales and marketing team to each other or to your customers are accessed from smartphones and tablets more and more. Keeping tabs on those devices and implementing lock-down strategies if they’re lost or stolen is imperative to maintaining network security.

Protect the Master Systems
The main control points of a computer network include the LAN (local area networks), VLAN (virtual local area network), main server hub, and security mechanisms like IPsec (internet protocol security). All these need to have strict access restrictions so only the authorized personnel can access them.
Conclusion
If you have more than one computer or peripheral device, then odds are, you’re going to be relying on a computer network to communicate between them. Networking increases productivity and makes working between multiple desks or offices so much easier. If you implement smart and effective strategies to keep your network safe then you can enjoy the benefits without the pain. Computer security is a never-ending task, so it makes sense to call in an expert to help.

If you implement smart and effective strategies to keep your network safe then you can enjoy the benefits without the pain. Computer security is a never-ending task, so it makes sense to call in an expert to help.