

Supported By



TECHLINK

TECHNOLOGY FOR BUSINESS PEOPLE

Home computer network doesn't hack it for business

By Jerry Irvine

Caution: you might have already tripped into a serious security gap created by the type of networking equipment you use.

It's a little recognized hazard. To save money, smaller and medium-sized businesses buy consumer plug-and-play networking equipment over robust enterprise-grade gear, only to end up surrendering higher levels of security, reliability and performance.

Why do businesses make this mistake? Familiarity with networking equipment has risen with American's web access. Companies that traditionally provided enterprise level network devices purchased home networking companies to get a part of this growing market. Their recognized brands are widely available at low cost, leading business owners to falsely assume that the home devices are just as effective as their higher cost siblings. Some enterprise equipment starts at \$300, but home wireless devices can be had for as little as \$39.

Where the threats are

Using home networking over enterprise equipment is like deciding to use a simple dead bolt to protect your business instead of an alarm system. Both devices provide the same basic functionality. But the alarm system assures everything will be there in the morning and alert you should something happen.

Home devices are organized into four prevalent types. Routers/Gateways connect to cable or DSL internet providers; hubs and switches tie multiple computers in the home via a wired network; wireless access points unite computers via WiFi; and NAS (Network Addressable Storage) devices provide shared storage for users.

These products supply the minimum features and benefits necessary to support the average home network, but functionality for businesses falls woefully short.

The average home router/gateway device provides firewall services and allows for automatic configuration allowing PCs to connect to the Internet. For businesses with their own Internet Web pages and e-mail servers, connections from the Internet have to be allowed back in to the business's internal network. This is a major security concern since viruses and malicious applications, like adware, are spread through the Internet. As a result, it is industry best practice to configure a separate network called DMZ (Demilitarized Zone) to redirect traffic coming from the Internet so it can be scanned and checked for dangerous content.

Using home networking over enterprise equipment is like deciding to use a simple dead bolt to protect your business instead of an alarm system. Both devices provide the same basic functionality. But the alarm system assures everything will be there in the morning and alert you should something happen.

When using the aforementioned devices, here's where your business network could fall down by failing to trade up.

Home quality hubs and switches generally require no configuration. But they also don't support security devices which can eliminate malicious applications. While easy and convenient, many users try daisy chaining multiple switches together without understanding the limitations and connectivity problems.

Institute of Electrical and Electronics Engineers (IEEE) standards and configuration requirements limit the number of devices and work stations connected together. Exceed these limits and you'll impact com-

munication and even cause a complete outage. Moreover, connected workstations can transmit viruses and other malicious applications to other devices on the network.

Home-based wireless network devices provide basic security configurations using WEP (Wireless Encryption Protocol) and even WPA (WiFi Protected Access). But automatic configurations frequently fail when connecting PCs to the access points. Upon set up, basic configuration is recommended with advanced security configuration performed later. But, as with most things, this never happens and systems are left wide open.

Wireless connectivity invites potential

Gaining Control

While home networking equipment shortcomings may not present a significant vulnerability, it's what they won't do when viruses, malicious applications, and programs or scripts try to invade your network. Run accidentally or intentionally, these can affect a device, groups of devices or any device connected to a network or the Internet.

Enterprise devices can configure layers of security, giving more access control options that limit users, devices and types of applications that can communicate on the network. Enterprise level devices also allow configuration of secondary devices which can automatically replace primary devices in case of a failure.

Enterprise level devices will do something else home devices can't – monitor the productivity and efficiencies of all the devices tied to your network. With this information, IT professionals can regularly review the systems to assure the business is achieving the levels of service required from its infrastructure.

When designing a business network, use only enterprise-grade gear and research and follow industry best practices to get the highest levels of services at the best price. While cheap and easy to configure, home networking devices could cost you far more than they're worth.

Jerry Irvine is CIO/COO of Prescient Solutions, a virtual Information Technology services company that helps global business clients, local municipalities, schools and governmental agencies maximize technology resources and minimize IT expenditures. He holds many technical designations, including MCSE, MCNE, CCNA, CCNP, CCDA, CCDP, Cisco Wireless Professional. Contact him at jirvine@prescientdev.com.

SAVE BIG ON BUSINESS VOICE SERVICE.

Turn Your Office On™



Sign up for Comcast Business Class Internet now and add phone service for just \$19.95 per line per month.

\$19.95
per month
for 12 months
With qualifying Business Class Internet service

- Unlimited direct-dialed local and domestic long distance calling
- Full featured voice line including Caller ID, Call Transfer and Voice Mail
- Internet speeds up to 16Mbps

Get reliable, high-speed Business Class Internet and we'll add Business Class Digital Voice for just pennies a day. Call now.

1.877.754.0224

Comcast
Business Class

Offer expires July 31, 2008, is only available in wired and serviceable areas in participating Comcast systems (and may not be transferred) and is limited to new Business Class customers. Not available to former Comcast customers with unpaid balances. Offer limited to Business Class Voice and requires subscription to Comcast Business Class Internet 6.0 Mbps or 16 Mbps service. Minimum two-year contract required. Early termination fee applies. After 12 months, or if any service is cancelled or downgraded, Comcast's regular monthly service charge of \$39.95 for each voice line will apply. Service subject to Comcast Business Class Service Order Agreement and General Terms and Conditions. Prices shown do not include equipment and installation charges, taxes, the Regulatory Recovery Fee, or other applicable charges (e.g., international calling and per-call charges). May not be combined with other offers. Business Class Voice, Unlimited package pricing applies only to direct-dialed calls to locations in the U.S., certain U.S. territories and Canada. No separate long distance carrier connection available. Digital Voice service (including 911/emergency services) may not function after an extended power outage. Certain customer premises equipment may not be compatible with services. Internet: Many factors affect speed. Actual speeds vary and are not guaranteed. Not all features are available in all packages. Call 1-877-754-0224 for restrictions and complete details. ©2008 Comcast. All rights reserved.