

TECH THINGS

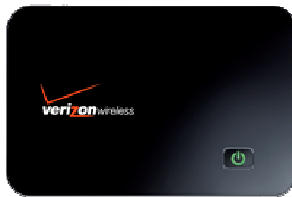
There's a mouse in the house, but it's more than OK!

According to Popular Science magazine, this mouse works where all others fail!



Logitech's Performance Mouse MX works even on glass. It scans the surface for microscopic scratches and dust, then bounces its laser light off these imperfections – not the surface itself – to tell the mouse that you're moving. That means the transparency of the surface or its reflectiveness doesn't matter.

Set up a hot spot wherever you go!



Wired magazine recommends Verizon's "MiFi2200 Intelligent Mobile Hotspot". It has the footprint of a credit card, the thickness of a pencil and you don't have to use VZAccess.

This "instant hot spot" is best for email and browsing and the replaceable battery lasts up to 4 hours & can be revitalized by wall current or USB. Available through Verizon or Sprint.

TECH THOUGHTS



Next best thing to being there!

For managers who have to deal with remote-worker issues, technology is making it easier to communicate and monitor.

Inexpensive software such as: [Wrike](#), [Zoho Projects](#), [5pm](#), [LiquidPlanner](#) and [Basecamp](#) let you assign tasks and deadlines and receive updates when milestones are reached.

If you need the ability for users to collaborate on documents and share files, [Google Apps](#) works.

Current users say you may need more than 1 tool to get all the functions you require, rather than finding one app that does it all.



Web-based teaching tool of the future?

Purdue University has developed [Hotseat](#)...software that allows classroom students to submit questions and comments via the Web or through Twitter, Facebook or a mobile device.

The messages appear on the Instructor's screen, so they can be addressed at the Instructor's convenience. Increased interactivity is the result...especially for larger groups.

It's not on the market (yet!), but it probably won't be long before it *is!*

TECH TALK

A word to the wise about your password...

Make sure it's not vulnerable to a "dictionary attack"!



"Dictionary attacks" come from programs that guess passwords by systematically trying *every* word in the dictionary.

Security experts recommend using a different password for each application. A recent survey indicates that's easier said than done: 81% used the same password for multiple sites and about 33% used the same password for *everything*.

Other recommendations: Two words connected by a number or a full sentence, such as "mary had a little lamb". Or try an abbreviation of a sentence, such as "mhall". Improve it with an "=": "mhall=p" (mary had a little lamb = password).

Alternative? [Password Safe](#), a free program that stores passwords. Companies can manage passwords with [Passlogix](#), [Imprivata](#), [myOneLogin](#)

Why learn it when you can access it any time?



A recent USA Today article about the "iGeneration" warns that kids today are used to having every piece of information at their disposal whenever they need it. Why is important to know? Because they're less interested in *learning* facts/data than in knowing how to gain access to it. The challenge for trainers: kids aren't the *only* ones who think that way these days!