**Used to Be, the Internet Was a Safe Place to Play**

By John Schwartz

THE WASHINGTON POST

WASHINGTON — Why are newspapers full of reports of hackers defacing government web sites and nasty viruses wreaking havoc on computers worldwide?

In no small part it is a cultural problem that goes back to the '60s origins of personal computing and the Internet. Many Internet pioneers were bearded longhairs, academics and engineers whose techno-hippie ethos suffused their new world. They knew one another, were part of a community Trust was the rule. The early Internet was much more about openness and communication than walls and locks. The faults it was supposed to correct were in the machines, not in us: corrupted packets, not corrupted morals.

"Once upon a time, there was the time of innocence," says Clifford Stoll, whose work tracking down European hackers became a popular book, "The Cuckoo's Egg." "Once upon a time, computers were not used except in academia, where there really is nothing that's mission-critical. **Once upon** a time, computers were mainly play toys for the techno-weirds — techie play toys."

In that environment, hacking was part of the fun of what Stoll has called the early Internet "sandbox."

"In that environment, there seems to be a cachet of 'Hey! I wrote a virus! Hee-ho!' In that environment, it seems funny to break into somebody else's computer. ... It seems somewhat innocent to read somebody else's e-mail."

It started with hacking telephone systems. The founders of Apple Computer — Steve Jobs and Steve Wozniak — got their start in business peddling "blue boxes," devices that allowed users to hack the telephone network and make long-distance calls for free. These "phone phreaks" were seen by some as cultural heroes — free spirits striking a blow against the suits, the evil corporations seen as the enemies of spontaneity and creativity.

Once computer systems were connected by networks, "remote hacking was an attractive challenge," Internet pioneer Vinton Cerf recalls via e-mail. "Much of the motivation was like picking locks or scaling walls —just to see if you could do it. Harm was not the objective, most of the time."

"It was a big open playscape for these guys," says Katie Hafner, who has written books about the history of the Internet and about hackers' lives. "The net was built as a completely open community People would actually be offended if files were protected."

There were some early nods to security issues — the fledgling ARPANET, the precursor to today's Internet, required passwords. It was funded by the military, after all. But "the subtext was this was an open community because this was an experiment," Hafner says.

It was built by guys like Jon Postel, the Internet pioneer who died last year. Postel had a vision of an Internet that didn't need a center to survive, a network that could be governed by standards and consensus without ever putting anybody in charge. Utopian? Sure. Vulnerable? Uh-huh.

That culture rejected attempts to create complex, cumbersome computer operating systems that incorporated security from the ground up. Computer security expert Peter Neumann says, "Viruses exist only because of the shortsightedness of subsequent developers who almost completely ignored the security problems" that some designers had effectively solved.

The problem is that the Internet caught on in the biggest possible way. The anarchic, don't-tell-us-how-to-run-our-lives ethic that defined the burgeoning network has retained that early vulnerability. Broader penetration of the Internet into society meant broader penetration of society into the Internet; it became more like the real world, and the real world is a tough place.

A big wake-up call came in 1988 when Robert Morris Jr., then a Cornell University student, released a computer program that single-handedly crashed systems across the Internet. His father, a famous programmer and security expert, was of the generation that had hacked for fun. Morris Jr. didn't mean to bring down the Internet. "His mischief was kind of in the spirit of the net," says Hafner. But by then the Internet was no longer a playscape.

If the net's problem is anarchy, the problem with personal computers is monarchy: Bill Gates. Microsoft "is indeed the evil empire when it comes to robust infrastructures," says Neumann.

Two viruses that recently swept through the world's computers, Melissa and Explore.zip, took advantage of the fact that so many millions of PCs run on a suite of Microsoft's programs. The company's latest offerings include security options — but the options are turned off at the factory. The security measures make computing a little clunkier, and cut users off from some of the bells and whistles that Microsoft writes into its programs. It's as if consumers "said they wanted faster cars," and so the vendors maximize speed by providing "faster cars, but with no brakes and no air bags!" says computer security expert Eugene Spafford of Purdue University.

Today's Internet is a mirror of society Conceived in a spirit of trust and good practical jokes, today it's about money. The frontier is getting settled by corporations worth billions, all of which are promising to sell us our future.

It will be interesting to see if a network strong enough to survive nuclear attack can survive its own success.