# But who's going to set up their own email server?

devblogs.microsoft.com/oldnewthing/20101123-00

November 23, 2010

Raymond Chen

Many many years ago, back in the days when Microsoft's email address had exclamation points, an internal tool was developed to permit Microsoft employees to view and update their Benefits information from the comfort of their very own offices. Welcome to the paperless office! One of my friends noticed an odd sentence in the instructions for using the tool: "Before running the program, make sure you are logged onto your email server." "That's strange," my friend thought. "Why does it matter that you're logged onto your email server? This tool doesn't use email." Since my friend happened at the time to be a tester for Microsoft's email product, he tried a little experiment. He created a brand new email server on one of his test machines and created an account on it called *billg*. He then signed onto that email server and then ran the tool. *Welcome, Bill Gates. Here are your current Benefits selections...* "Uh-oh," my friend thought. "This is a pretty bad security hole." The tool apparently performed authentication by asking your email server, "Hey, who are you logged in as?" The answer that came back was assumed to be an accurate representation of the user who is running the tool. The back-end server itself was not secured at all; it relied on the client application to do the security checks. My friend sent email to the vice president of Human Resources informing him of this problem. "You need to shut down this tool immediately. I have found a security hole that allows anybody to see anybody else's Benefits information." The response from the vice president of Human Resources was calm and reassuring. "My developers tell me that the tool is secure. Just enjoy the convenience of updating your Benefits information electronically." Frustrated by this, my friend decided to create another account on his test email server, namely one corresponding to the vice president of Human Resources. He then sent the vice president another email message. "Please reconsider your previous decision. Your base salary is $xxx and your wife's name is Yyyy. Would you like me to remind you one week before your son's tenth birthday? It's coming up next month." A reply was quickly received. "We're looking into this." Shortly thereafter, the tool was taken offline "for maintenance."

**Bonus reading**: JenK shares her experience with the same incident.

Raymond Chen

**Follow**