

18 September 2008

By: Lucian Constantin, Web News Editor



Alaska Governor and republican vice-presidential candidate Sarah Palin  
The Midnight Ride

## [How Sarah Palin's E-Mail Account Got Hacked](#)

*Vice-presidential candidate Sarah Palin had gremlins going through her e-mail*

A media storm started as the e-mail account of Alaska Governor and republican vice-presidential candidate Sarah Palin got hacked yesterday. Lots of sites reported that a group of hackers got access to the account and posted samples and screen shots of the content online. By other accounts, a single person was responsible and the group of hackers, known as Anonymous, is really an online amusement discussion board.

### The why

Earlier this year, a public records request prompted Palin's office to refuse disclosing around 1,100 e-mail messages citing "exemptions for deliberative process, executive privilege, attorney/client privilege, privacy, and personnel". E-mails that are related to government business should be public records according to the law; however, it was uncertain whether Palin was using her Yahoo account to conduct such official business.

Other officials also expressed concerns regarding communication transparency being hindered by using personal Yahoo accounts and so her gov.palin@yahoo.com e-mail address transpired in the media. "Some of her aides also routinely use Yahoo, but even messages sent from one private account to another should be public, if they concern public business", said assistant attorney general Dave Jones for the [Anchorage Daily News](#). "The difficulty is finding out if they exist," he added.

### The where

Some reports attribute this illegal action to a person associated with a supposed hacking group that goes by the name of Anonymous. The same group is also known for its "battle" with the Church of Scientology. By other accounts, this is completely flawed. Anonymous is not an organized group, "it is people using the umbrella of a web discussion board for cover to be as offensive, funny, strange, or whatever as they want," says a [user](#) who monitors the board. The board in question is called /b/ and is hosted on 4chan, an "image-based bulletin board where anyone can post comments and share images".

The notorious /b/ board is used by all sorts of people for their own amusement and "their sense of humor runs the gamut from sick to cruel to merely strange". The people who post here generally do so under the "Anonymous" account, hence the "group"'s name. According to the same account, a member of this board was responsible for this e-mail hacking incident and this board is where the original screen shots were posted. "Anonymous is not a group of hackers. Anonymous is more like gremlins," he concluded.

### The how

After original threads on this subject had been deleted by the board's moderators, someone who took responsibility for the illegal action posted the whole story in which he explains why and how he did it. The individual in question posted under the name of rubico and the e-mail address associated with the post is rubico10@yahoo.com. According to him, he used social engineering to get into the account and it took him no more than 45 minutes to do it.

He used Yahoo's password recovery feature and got the answers to the security questions by doing online research. "Birthday? 15 seconds on wikipedia, zip code? well she had always been from wasilla, and it only has 2 zip codes (thanks online postal service!)," he says. According to him, the most difficult question to find the answer for was the "where did you meet your spouse?". "I found out later through more research that they met at high school, so I did variations of that, high, high school, eventually hit on Wasilla high," explains rubico. He then claims to have changed the password to "popcorn" and posted it on /b/ after reading all the e-mails, so that the other users could have fun with the account.

#### The what

Some of the screen shots of Palin's e-mail messages and contacts leaked on other websites after threads on the subject started to be closed down on /b/. They showed mostly personal messages and pictures. Even if some e-mails were addressed to or came from other officials like Alaska Lieutenant Governor Sean Parnell or Amy McCorkell, a member of Governor Palin's Advisory Board on Alcoholism and Drug Abuse, it is questionable if the messages exceed the personal level.

"Don't let the negative press wear you down! Pray for me as well. I need strength to 1. keep employment, 2. not have to choose. Lately I just pray may God's will be done. I am trying to learn patience and listen to God," writes Amy McCorkell in one of the e-mails. The lack of anything really incriminating is also confirmed by rubico. "I read though the emails&hellip; ALL OF THEM&hellip; before I posted, and what I concluded was anticlimactic, there was nothing there, nothing incriminating, nothing that would derail her campaign as I had hoped, all I saw was personal stuff, some clerical stuff from when she was governor&hellip;. And pictures of her family," he writes with clear disappointment.

#### The consequences

This is unarguably an illegal action, a crime which could cost rubico, if he is the real offender, years behind bars. Even though rubico says he initially considered this more like a joke, he realized the implications of what he did and got scared. "Earlier it was just some prank to me," he says and later adds, "I panicked, i still wanted the stuff out there but I didn't know how to [share] all that stuff, so I posted the pass on /b/, and then promptly deleted everything, and unplugged my internet and just sat there in a comatose state".

It looks like he did not bother to cover up the browser address bar in the screen shots, which might end up costing him, because according to the pictures, he used a proxy service called Ctunnel. People use this service to anonymously access e-mail services like Yahoo! Mail or Gmail or sites like YouTube or MySpace. The owner of Ctunnel, Gabriel Ramuglia, claims that because most of the session strings (a random string of characters) in the URL appear in the pictures, he might be able to track it. "Since they were dumb enough to post a full screenshot that showed most of the URL, I should be able to find that in my log," he commented for [The Register](#).

If rubico is telling the truth when saying that "yes I was behind a proxy, only one," then this should make things very easy for the authorities, as Ramuglia declared that he would most likely provide the log information, which stores the user's IP address, if he is contacted by law enforcement officials.