

17 September 2007

By: Alexandru Dumitru, Security News Editor



[Is Your E-mail Secure?](#)

About mail encryption

This is just like the Dark Ages! You can't send an important message anymore, because you run the risk of having it intercepted and sensitive info being leaked. Remember those movies where the King wanted to send a message to some other royalty, but before it left the castle it was encrypted by some weird old monk? Well, it's the same thing these days, only instead of using pigeons or fast riders to transmit messages people use the Internet.

And how do you secure an e-mail when the Web is such a dangerous place? Well, encryption of course. And now I'm not talking about your basic "Hey, Shirley, check out this cool website!" e-mail; I'm referring to important e-mails that government institutions, or the army, or some companies send – the type of e-mail that if intercepted could cause a lot of trouble. Those are the ones that need protection! So how does encryption work?

Well, let's consider the normal e-mail message that goes from point A to point B. A sends the message, as soon as A pushes the "Send" button, the e-mail gets encrypted once. If B is in the same network as A, then it goes to B without passing through any gateways. B decrypts upon receiving it. But what if A and B are not in the same network and the message goes over the web? Well, then the e-mail has a different route. A sends it and the message gets the basic encryption, then it reaches the gateway. As you might have imagined, a gateway is where info goes in and out of a network. Then, at the gateway, the message will get encrypted once more, after which is sent to the gateway of B. This is called double encryption. The other gateway will decrypt the message once, leaving it in its first network encryption form. Then, that gateway will finally send the message to B that will decrypt the network encryption as well, so that the message can be read by any user. So, it just doesn't go from A to B, it goes from A to gateway_A, over the web, to gateway_B, and then to B.

It may seem complicated, but it's one of the best ways to protect an e-mail. Inside-network encryption is important as well, since hackers will spy on the messages inside a network, not to mention malicious insiders that may try to do the same. E-mail encryption is something that you cannot neglect; sure, it can make the process a little slower, but safety is way more important than speed in this case.