The reason that most people do not use crypto

Source: Mailinglist lists.gnupg.org/pipermail/gnupg-users/

On Sun, Jun 09, 2013 at 11:52:32PM -0400, Robert J. Hansen wrote:
The reason that most people do not use crypto is the most trivial one: They don't think they need it.

On 6/9/2013 11:14 PM, Hauke Laging wrote:
This is not supported by the studies. Many people who do not use crypto openly acknowledge that maybe they „should“, in a vague „I really should eat more salads and less meat“ sense. However, they see the risks to themselves as diffuse and distant, and the consequences mild. If you're a political campaign worker and you send an unencrypted email of your contact list, and it gets intercepted by the other side, your screw-up has done enormous damage to your candidate… but you, yourself, will likely never face any real punishment for it.

So, „think I need it“ is a continuous variable. Many people think they need it, sort of, in a small way, but think they don't need it enough to pay the cost of learning to use it.

Provided that potential user X understands his position, the threats to it, and his values w.r.t. [with regard to] those, he may be drawing a reasonable conclusion against which I would not argue.

People don't need to encrypt their grocery lists, except in the sense that it's easier to always do something potentially useful than to make a decision each time. The CIA does not care that I send myself a reminder to get a book on software testing; this is noise, for their purpose, and they'd rather not handle it. Identity thieves do not care to know that I fed the dog this morning, though my wife does. Occasions when I find myself thinking, „I’d better guard this information“ are exceedingly rare.

But that points at the real cost of crypto: you have to think about it. There is no escape; you have to think deeply about slippery things like identity and trust and threat models, and then you have to apply your resulting policies a hundred times a day. Software can relieve large parts of the latter burden; it can do nothing about the former, which is the hardest part.

Mark H. Wood, Lead System Programmer mwood@IUPUI.Edu
Machines should not be friendly. Machines should be obedient.