All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Stupid Security Winner for 2012

In our ongoing efforts to identify and lambaste stupid security practices, we are announcing our winner for stupid security practices in 2012.

This practice has added insecurity to excessive traffic, lost and stolen content, vulnerabilities that needn't be present, and inconvenience to an otherwise simple and easy to use process. It exemplifies why users hate security and how security hates users. If you are offended, likely it is because you are one of the offenders forcing others to use this practice, and likely you are not using it yourself – at least not out of choice. And the winner is...

"Important notices" stored on Web sites with links emailed

Yes, you are the winner! So why is this a stupid security practice? Let me count the ways:

1. Most "important notices" are not really secrets. Why not just send the information?
2. They inevitably require the user to recall a "unique" user identity and password to protect the mass mailed important notice that is not really sensitive at all.
3. They tend to hide the subject of the message, thus requiring unknown follow-on effort for no sensible reason other than that the sender thought it was "important".
4. They often include a URL to the message, thus telling the folks who might intercept the message where to look for "important notices". Let's target ourselves...
5. The Web sites, one after another, get broken into, so the only folks inconvenienced by the multi-step process are legitimate users. The bad guys get and share the secrets.
6. They tend to depend on secure endpoints and SSL encryption, which means we are aggregating risk in these things. And they are failing under the aggregated weight!
7. A simpler solution: Encrypted email with content. Or for things not really confidential, just send the "important notices" in email. Why do complex things when simple works?
8. Spammers can easily take advantage. They spam an "Important notice" and you click on the link, and likely provide a UID and password. A Trojan waiting to happen.
9. Spam filters kill off many of these "Important notices" which means they don't get through. If it's really important, send a real subject with an organization in [brackets].
10. Once we log in, there is inevitably a complex hard-to-use interface. More wasted time.

Of course this is not a comprehensive list, and the order is just the order in which they popped up into consciousness, no ranking is intended or implied. But why waste more time and bits when you, the readers, can add so many more things to this list on your own.

Summary and conclusions

Stupid security should be stopped. But it will likely continue for the foreseeable future. Still, we should all do our part. And now for your part. Add to my list by emailing more bullet items, we will add them in an appendix, attributed to the extent desired. And don't be next year's winner.

