

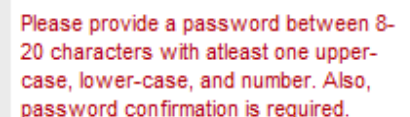
[TrustDefender](#) comments on the US Government's draft plan to secure online identities

5th July, 2010: *In a draft plan released recently by the cybersecurity co-ordinator and special assistant to the US president, Howard Schmidt, the White House laid out the plans for a yet-underdeveloped, voluntary identification system to combat the rise of online transaction crimes. The Government's aim is to enable individuals to voluntarily obtain a secure credential, such as a smart identity card, from public and private sector providers. Under the plan, this credential would be used for online authentication when banking, accessing electronic health records, sending email and making online purchases.*

Online security expert [Andreas Baumhof](#), Chief Cyber Security Officer of [TrustDefender](#) reviews the draft plans and comments:

"At TrustDefender it is our job to research highly sophisticated banking malware and we welcome the initiative of the US government to improve the situation for online consumers; however the current plan is missing critical key points. The draft plan (title: "National Strategy for Trusted Identities in Cyberspace") focuses solely on an online identity and forgets that the identity is only the first step in an online transaction. It fails to address the issue of security within the transaction. It's like installing a highly secure front gate, but leaving the picket fence around it as it is.

"For example with my online identity a bank can verify it is me, however the fraudsters today don't even attack the identity, they are after the transaction I conduct after I am authenticated which is where the real money is. The way in which online identities are currently managed is a total mess. From a consumer's perspective every single website requests you to register, but each website has different rules to what information they collect and more importantly how the password should be configured (eg. minimum 6 characters, minimum 8 characters, minimum 1 number, minimum of one uppercase character, and so on). This is very confusing and frustrating for users, but also for the enterprises because people can't remember their passwords. From an enterprise perspective, on each transaction, the authenticity of the newly registered person has to be verified. However there are no processes to check that the provided identity is actually legitimate. So we definitely need an interoperable framework to improve this situation."

A red-bordered box containing a red exclamation mark icon and the text: "Please provide a password between 8-20 characters with atleast one upper-case, lower-case, and number. Also, password confirmation is required."/>

Please provide a password between 8-20 characters with atleast one upper-case, lower-case, and number. Also, password confirmation is required.

"The scope of the Government's strategy is to provide a framework and standardisation within the different identity providers and identity solutions so that they are inter-operable. While this could solve the problem for internet users of having many different logins it would only be realistic for low-value transactions, e.g. an individual could use the same login for both their eg. Yahoo and Google accounts.

"For high-value transactions however – such as online banking transactions - I fail to see how this federated identity system would work. We have seen numerous failed efforts so far here in Australia as when it comes down to the details, financial institutions struggle to share valuable information between them because there is no business driver to do so. They almost view it as sharing their intellectual property, e.g. banks would be fearful that if a customer can login with the same identity verification to another bank, customer loyalty might be negatively impacted."

“To make matters worse, an interoperable ‘Identity Ecosystem’ could actually also have a negative impact as it introduces a risk that hasn’t been there before and thus provides a new attack vector for the fraudsters. First of all it introduces third-party dependencies. If the service of the identity provider is down, you can’t login and a bank wouldn’t want that to happen. But more importantly today, if an attacker wants to hack your gmail account and your Hotmail account, he needs to ‘hack’ two completely different services and systems. In the suggested ‘Identity Ecosystem’, if an attacker takes over a computer with a Trojan, he has access to all interoperable sites straight away.”

“What the US Government needs to do is to focus on the entire transaction process – from the moment a user logs onto a web service provider (such as online banking) to the moment they log off - as the current plans only intend to move the country towards a better personal identity system. It will not have the desired impact on how valuable online transactions are going to be performed more securely, which means malware and Trojans will still be able to take advantage and reap havoc on the worlds online fraud record. Trojans like URLZone¹ don’t even attack the identity at all. They wait until the user is fully authenticated and then they take over and strike. I can’t see how this new draft would prevent a Trojan like this from doing its nasty work.”

What the Government needs to do is address how cyber criminals are attacking users online to generate reported losses of \$560m² in the US alone in 2009. However everybody agrees that this is just the tip of the iceberg with the ACCC valuing a direct cost of \$1bn³ to the community, which costs money, wastes time and destroys brand credibility.”

“So in conclusion, the Government have missed an opportunity to deliver a plan which addresses where the malware and cyber criminals actually are and have limited the scope to simply securing identities. With this current plan the perpetrators of cyber crimes can still sleep safely at night – which worries the hell out of me.”

To view the draft plans please visit http://www.dhs.gov/xlibrary/assets/ns_tic.pdf or visit the Government’s website for comment <http://www.nstic.ideascale.com/>

For more information visit:

www.trustdefender.com and www.trustdefender.com/blog

For any further media information or an interview contact:

Sharon Ghatora, Taurus Marketing

Phone: +61 2 9415 4528 or +61 416 890 648

Email: sharon.ghatora@taurusmarketing.com.au

Notes to editor:

1. TrustDefender Labs analysis of URLZone <http://www.trustdefender.com/blog/2009/10/08/urlzone-a-desaster-waiting-to-happen/>
2. FBI http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf
3. The Australian Bureau of Statistics recently found that around 1 in 20 Australians fall victim to some sort of consumer fraud each year, with a direct cost to the community of around a billion dollars.” from <http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub46.pdf>



About TrustDefender

TrustDefender is the worldwide leading provider of 'real-time risk based online transaction security solutions' to safeguard consumer, financial institution and business online transactions. TrustDefender's revolutionary technologies enable users to verify its security health state, perform a memory forensics analysis and secure their mobile computing device in real-time - before and during any Internet transactions.

At the same time, TrustDefender provides real time feedback on the security health of their computer. Best yet, the user does not need to be a security expert to use this technology. Most importantly, for the first time, the financial institution has real-time information that they can use to better protect transactions from compromise and also allows the enterprise risk managers to finally get a real time risk profile of their customer base.

The Enterprise Server incorporates a real-time risk-scoring engine that together with the rules and policy engine is always in control and can give the financial institution a server-side tool to mitigate the risk on both ends and includes an extensive Auditing and Reporting module. TrustDefender is the world's first security solution which enables online businesses to integrate the home user or end user's PC into one overall security chain.

TrustDefender was founded in December 2005 after the founders discovered the traditional security model was broken – **and decided to fix it.**