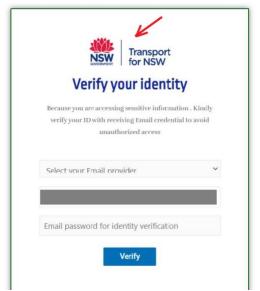
Screenshots for Phishing Campaign Mimics a Primacy Agency Data Validation Request

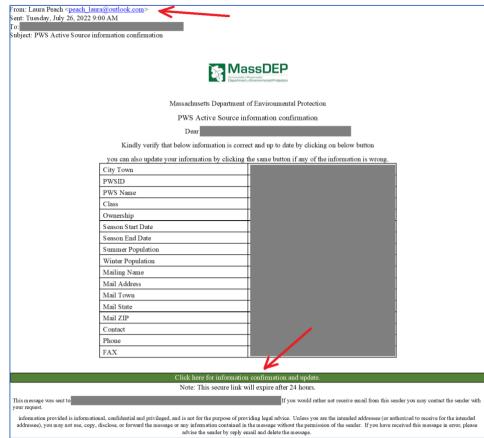
- by Andrew Hildick-Smith

In July, a transient non-community PWS in Massachusetts received an email purporting to be from the Massachusetts Department of Environmental Protection, asking them to kindly verify their PWS information as listed in the email:

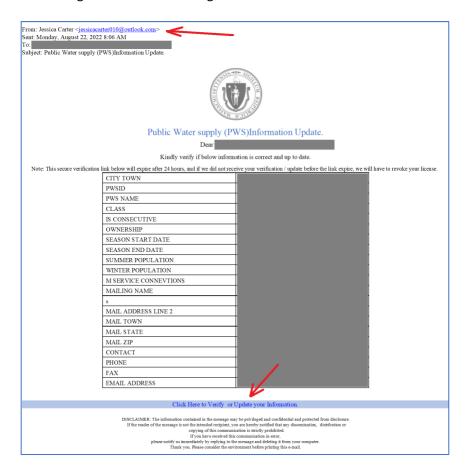
- Note the email source of, "Laura Peach
 <peach_laura@outlook.com>", is not an address the Mass DEP is likely to use and,
- The "Click here for information confirmation and update." bar, displayed an odd destination when you hovered your mouse cursor over the original.

If someone clicked on the aforementioned link – even accidentally – they were presented with a fake login page designed to steal credentials. Note the logo represents a government transportation agency in New South Wales, Australia – not likely to be familiar to a public water supply in Massachusetts (or any other US city or state).





In August, the email went to a community PWS. In the new campaign. The Massachusetts DEP logo was changed to a state seal and some of the wording and data fields changed. Here is the next version:



Like the prior month, please note non-standard/non-business email source and odd link associated with the "Click Here to Verify or Update you Information" bar. Additionally, the destination (phishing) page includes another red flag for someone in Massachusetts, purporting to be the "City of Evansville, Indiana."

