

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).

NSW GOVERNMENT | Transport for NSW

Verify your identity

Because you are accessing sensitive information. Kindly verify your ID with receiving Email credential to avoid unauthorized access

Select your Email provider

[Redacted Email Address]

Email password for identity verification

Verify

From: Laura Peach <peach_laura@outlook.com>
Sent: Tuesday, July 26, 2022 9:00 AM
To: [Redacted]
Subject: PWS Active Source information confirmation

MassDEP
Massachusetts Department of Environmental Protection

Massachusetts Department of Environmental Protection
PWS Active Source information confirmation
Dear [Redacted]

Kindly verify that below information is correct and up to date by clicking on below button
you can also update your information by clicking the same button if any of the information is wrong.

City Town	[Redacted]
PWSID	[Redacted]
PWS Name	[Redacted]
Class	[Redacted]
Ownership	[Redacted]
Season Start Date	[Redacted]
Season End Date	[Redacted]
Summer Population	[Redacted]
Winter Population	[Redacted]
Mailing Name	[Redacted]
Mail Address	[Redacted]
Mail Town	[Redacted]
Mail State	[Redacted]
Mail ZIP	[Redacted]
Contact	[Redacted]
Phone	[Redacted]
FAX	[Redacted]


[Click here for information confirmation and update.](#)
Note: This secure link will expire after 24 hours.

This message was sent to [Redacted] If you would rather not receive email from this sender you may contact the sender with your request.

information provided is informational, confidential and privileged, and is not for the purpose of providing legal advice. Unless you are the intended addressee (or authorized to receive for the intended addressee), you may not use, copy, disclose, or forward the message or any information contained in the message without the permission of the sender. If you have received this message in error, please advise the sender by reply email and delete the message.

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:

From: Jessica Carter <jessicacarter010@outlook.com>
Sent: Monday, August 22, 2022 8:06 AM
To: [REDACTED]
Subject: Public Water supply (PWS)Information Update.



Public Water supply (PWS)Information Update.

Dear [REDACTED]

Kindly verify if below information is correct and up to date.


Note: This secure verification link below will expire after 24 hours, and if we did not receive your verification / update before the link expire, we will have to revoke your license.

CITY TOWN	[REDACTED]
PWSID	[REDACTED]
PWS NAME	[REDACTED]
CLASS	[REDACTED]
IS CONSECUTIVE	[REDACTED]
OWNERSHIP	[REDACTED]
SEASON START DATE	[REDACTED]
SEASON END DATE	[REDACTED]
SUMMER POPULATION	[REDACTED]
WINTER POPULATION	[REDACTED]
M SERVICE CONNEVTIONS	[REDACTED]
MAILING NAME	[REDACTED]
s	[REDACTED]
MAIL ADDRESS LINE 2	[REDACTED]
MAIL TOWN	[REDACTED]
MAIL STATE	[REDACTED]
MAIL ZIP	[REDACTED]
CONTACT	[REDACTED]
PHONE	[REDACTED]
FAX	[REDACTED]
EMAIL ADDRESS	[REDACTED]

[Click Here to Verify or Update your Information.](#)

DISCLAIMER: The information contained in the message may be privileged and confidential and protected from disclosure. If the reader of the message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by replying to the message and deleting it from your computer. Thank you. Please consider the environment before printing this e-mail.

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.”



City of Evansville
INDIANA

Verify your identity

Because you are accessing sensitive information . Kindly verify your ID with receiving Email credential to avoid unathorized access

Select your Email provider

[REDACTED]

Email password for identity verification

Verify