



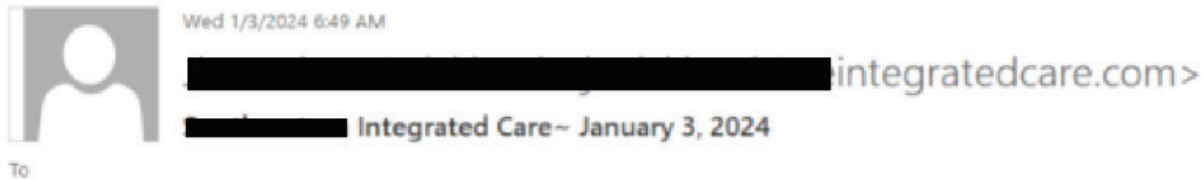
# URGENT

## NOTIFICATION FOR PROVIDERS

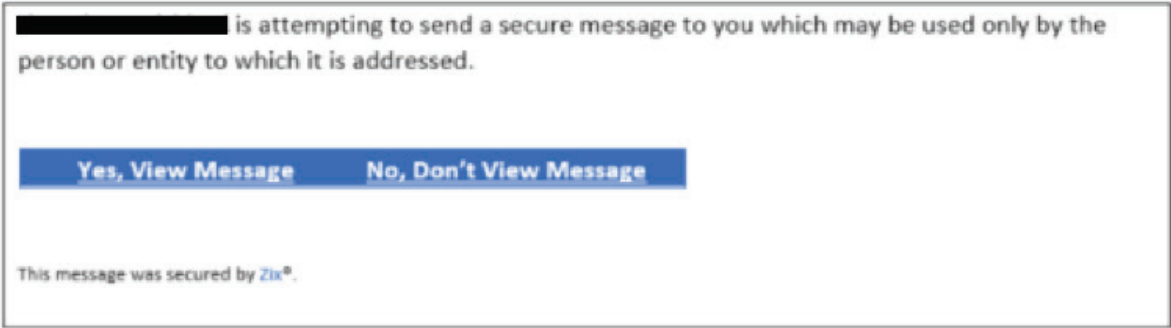
### ATTENTION PROVIDERS

Trillium Health Resources is seeing and also hearing of from other MCOs a malicious email that appears to be a **Zix secure message** from several entities including provider organizations. The link does not take you to Zixmail, but to an Evernote site which contains a link to a document that prompts you to enter a username & password. This is a malicious site that will harvest your user information and compromise your account.

Please see the screenshot below. **Please DO NOT OPEN.**



This message was sent securely using Zix®



The reader is hereby notified to follow the authentication required by Zix® and disallow any dissemination, distribution or copying of this e-mail is prohibited. If you have received this email in error, please notify the sender by replying to this message and delete this e-mail immediately.

**If you have opened this email & clicked the link/entered your username & password, please change your password immediately and enter a helpdesk ticket with your organization.**

**IT Staff: If you have seen this email in your organization, please follow your protocols for a compromised account which should, at a minimum, include the following:**

- 🌱 Account Disable / Password Reset / Disconnect all User Sessions
- 🌱 Remove malicious emails
- 🌱 Block incoming & outgoing email to/from those domains that sent the emails until you have confirmed remediation.
- 🌱 Determine if any other portals/applications are impacted
- 🌱 Contact Trillium if you suspect malicious emails have been sent to us

**Always validate all emails using a trusted phone number prior to clicking a link or opening an attachment.**

**Thank you for your help!**

DO NOT REPLY to this email, as this is an unmonitored email address. If you have any questions please send an email to [IT.Support@TrilliumNC.org](mailto:IT.Support@TrilliumNC.org).

**URGENT NOTIFICATIONS FOR NETWORK PROVIDERS**

