View this email in your browser

SANDBOX TECHNOLOGIES

Phishing Emails Targeting Intermedia Customers

We recently became aware of a malicious phishing scheme targeting users of the popular Intermedia.net email hosting service. If you are receiving this message, our records indicate that your organization uses this service.

While users should always be on the alert for fraudulent schemes of all types, we felt it worthwhile to provide an example of a phishing email targeting Intermedia customers.

EXAMPLE

From: Inter-Media <srvrdata-support-LogID-EEXS22554-mail@intermeda.net>
Sent: Thursday, February 3, 2022 9:30 AM
To: Your Name <YourName@CompanyName.com>
Subject: (2) New Service Messages For You
Importance: High

INTERMEDIA
The Business Cloud®

Hi (Your Name),

You have new important update notifications* for your intermedia e-mail that requires your immediate attention, you're required to follow the necessary steps using the button below.

Read This Messages

We are always working to give you an excellent and the best service across all our networks, Failure to comply to this may put you at risk of losing all your messages

Sincerely,

Intermedia Mail Team.

Privacy& Policy (Your Company Name) unsubscribe

Although the individual(s) behind this particular scheme took the time to include Intermedia's logo, a bit of scrutiny quickly reveals several key characteristics present in phishing schemes:

- The sender's domain contains a subtle misspelling. The malicious actors use the domain "intermeda.net" when the correct domain is "intermedia.net".

- The email is poorly written and rife with grammatical errors, e.g., "Read This Messages" instead of "Read These Messages", "Failure to comply to this" as opposed to "Failure to comply with this", etc.

- Similarly, punctuation is omitted where it should exist, and added where it should not.

- The sender(s) of phishing emails often attempt to create a sense of urgency. This is done to increase the likelihood of recipients quickly clicking on one or more of the links included without first scrutinizing the message. Examples of creating urgency include "requires your immediate attention", and (SIC) "Failure to comply to this may put you at risk of losing all your messages".

The email above is just one example of the countless fraudulent emails crafted and sent to unsuspecting targets on a daily basis. We recommend sharing this email with your fellow Intermedia users, as well as anyone who might benefit from this information. As always, think before you click and exercise caution whenever you receive anything that is unsolicited.

Warm Regards,

Aaron Arlotti
Manager, Remote Support Operations
Sandbox Technologies, Inc.