How to verify if an email originated from someone at MIT

Q: How to verify if an email originated from someone at MIT

Context

With cyber criminals becoming more clever with their methods of tricking us into divulging our personal information, it is important to know how to spot a trick when we see one. A frequent method of phishing mimics the kinds of messages that organizations might (or already do) send out to their constituents.

At MIT we have seen emails arrive in our inboxes that attempt to mimic a message that an IT organization might send out to its constituents, such as reporting an email account upgrade, or a change to some IT service. The “from” email appears to come from the System Administration team or Email Support team.

IS&T at MIT regularly sends out notices to the community. The best way to verify if an email originated from someone at MIT, is to look at the full header of the email. Once you obtain the full header content, see tips below on how to read the seemingly difficult to understand report.

Answer

An email originating from a legitimate MIT email account will come from an 18.9.x.x or 18.7.x.x IP address (example: 18.9.3.24). It will also originate from the Exchange email server (examples: W92EXHUB14.exchange.mit.edu or OC11EXHUB10.exchange.mit.edu).

This information will appear in the very LAST Received entry in the header. The header information is composed to show the path of the message starting from the bottom of the list and ending at the top.

Legitimate MIT email:

This is the header of a message that was sent from someone within the IS&T organization at MIT:
1. Scroll down to the last Received entry (see the first yellow highlighted section in the header above).
2. Verify that the Received entry information contains an 18. IP address plus was routed through the exchange.mit.edu server.
3. Scroll down to the Return-Path entry (see the second highlighted section in the header above).
4. Verify that the Return-Path leads back to a legitimate MIT email address. It is legitimate if you can find this address and person in the MIT directory.
5. Another indicator is the path the message took. Because it originated from within MIT and was received by someone within MIT, you see in the header that the email never left the network (always passing through a server on the mit.edu domain.

How to interpret this header:

1. Scroll down to the last Received entry (see the first yellow highlighted section in the header above).
2. Verify that the Received entry information contains an 18. IP address plus was routed through the exchange.mit.edu server.
3. Scroll down to the Return-Path entry (see the second highlighted section in the header above).
4. Verify that the Return-Path leads back to a legitimate MIT email address. It is legitimate if you can find this address and person in the MIT directory.
5. If the answer is yes to these verifications, then the email DID come from a valid MIT address and the message can be trusted.
6. Another indicator is the path the message took. Because it originated from within MIT and was received by someone within MIT, you see in the header that the email never left the network (always passing through a server on the mit.edu domain.
Fake MIT email (did not come from MIT):

Below is an example of a full email header from a source outside MIT, but trying to appear as if it came from our IT department:
What gives away that this is not an email originating from MIT:
1. See the first highlighted section above. The IP address is 10.147.66.21, and did not originate from the exchange.mit.edu server.
2. See the second highlighted section above. The Return-Path is to helen.calvert at everest.edu, clearly not an MIT email address.
3. The path the message took quickly passed through a Google mail server. A message coming from MIT would not pass through a Google mail server.
4. Conclusion: this email did NOT come from MIT.