Signs of a compromised MIT account

Q: Signs of a compromised MIT account

Answer

As cyber criminals become more clever at masking the origins of spam and phishing scams, one must be diligent in order to spot their tricks. Be aware that any email asking for personal information and claiming to be from MIT is a scam.

A frequent method of phishing is to mask the email account from which messages are sent. If the email "from" address does not match the name listed in the "from" field, the email may be a scam.

On occasion, cyber criminals will use email accounts they have illegally gained access to (a compromised MIT account, for example) for sending out phishing messages to other people within the account holder's organization.

Why? Because spam filters will not block these emails. When our receiving mail servers see that a message has originated from a mail server on our network, it believes that message to be legitimate and lets it through.

How can you know when an MIT email account has been compromised and is sending out spam?

The best method is to look at the message's full headers.

Below is the full email header of a message that was sent from a compromised MIT email account:

How to interpret this header:

1. First highlighted field: This is the return-path of the email message. This field is populated by the receiver's mail server, and is usually the address that will be used if mail bounces back to sender (receipt is denied by the recipient's mail server). In this case, the return-path shows an actual mit.edu email address and is a sign that it originated from an mit.edu account.
2. Second highlighted field: The from field can be spoofed, but in this case, because the spammer was pretending to be a person from MIT, they left the from field alone, showing the name and email address of an actual person at MIT.
3. Third highlighted field: This is the reply-to field of the email message. It is the email address that will be used if the recipient were to hit "reply." In this example, the reply would go to "grant_service2014 @mail.com."
4. Because the reply-to and return-path do not match, it can be deduced that this email message is a scam.
5. The path of the email shows which mail servers and networks the message passed through. To follow the path, read from the bottom of the header to the top. This example shows that the first receipt logged was a server on MIT's network (**exchange.mit.edu** and a **18.x.x.x** IP address). The message had to have come from an address within MIT. When using your mit.edu account to send mail, it doesn't matter if you are off campus or on campus; the email will always come through a server on the MIT network.

What should you do

See: What should I do if my email account gets hacked?