COMPROMISED NETID

A compromised NetID can resemble a spear phishing attack, but it is quite different. Both spear phishing and compromised NetIDs look like they come from someone within the University, but spear phishing looks like it comes from someone you know, e.g., your boss, asking you to reply because they are not able to take a call and they need an urgent favor. If you click to reply, you will notice the reply-to address has suddenly become an external email address.

The compromised NetID actually comes from someone within the University, but that person has no idea they just emailed hundreds of people. Here are some clues to help you identify when you have received an email like this.

- The "sender" has a valid email from one of the UT campuses.
- If you were to reply, the message definitely goes to the UT employee's email address.
- The person who is shown as the sender likely works on a different campus than ours, but not always.
  - A recent example would be an email sent to many at the Institute and UTK. The address was from @utm.edu and that person had previous ties to the Institute.
- The real sender has sent mail from that person's compromised email attack using their contacts and/or using the UT Directory.
  - You may notice that the people getting the email when you did are listed in alphabetical order and usually with the same first letter of the last name as yours.
  - This grouping of people usually makes little sense and shows that the real sender is trying to catch anyone they can.
- The email's content is usually sparse and has no attachment, but there will be a link that you are directed to use.
- There is almost never a campus or institute logo in the signature, but if there is one, it will be a little off.
- There will be no logical reason for the person to send you this email.

As always, if you get an email as described above, please take extra caution to not click on any links. If you actually know the person, but the email still has clues from above, call the person and ask if they sent it. If the account has been compromised, they won't even realize emails had been sent from their account.

If you get one of these emails, please forward to abuse@utk.edu, as usual, to report the message. Be sure to send the Internet Headers, as well. OIT will investigate by using the headers and will disable the NetID account. This will cause the actual UT employee to call the HelpDesk to see why they can't access anything. The HelpDesk will then help reset that account.

References:
UTIA Glossary of Information Technology Terms
Spear Phishing Information
Reporting Phishing Attempts

For more information, contact Sandy Lindsey, CISO, at (865) 974-7292, or email sandy@tennessee.edu.